TD 92979EN

Troubleshooting Guide

WL3 and WL3 Plus WLAN Handset

29 January 2013 / Ver. A

About this document

This guide describes how to investigate and remedy Quality of Service problems experienced by handset users when accessing a WLAN and making calls using the Voice over IP Protocol (VoIP).

Cross-references in the document

Throughout this document you will find cross-references in the text which indicate further details that can be found in other sections of this document. The cross-references are colored blue and linked to the relevant place in the document. For example: see chapter 9. Document History on page 59. Positioning your cursor over the cross-reference text and clicking the left mouse button will take you to the relevant section.

To return to the original page after viewing a cross-referred page in Adobe Acrobat or Adobe Reader, click on the ''Previous View'' arrow (⬅ or ⬅).

Contents

1. Introduction

This guide describes procedures to validate and perform troubleshooting on a WLAN that supports a VoWiFi system. It identifies some of the more common problem areas associated with the operation of VoWiFi networks and suggests approaches to troubleshooting and the use of internal and external tools for investigating these problems. The guide contains detailed information about the behavior of the WLAN Handset under faulty or problematic conditions. This behavior may be different for different hardware and software versions of the handset.

1.1 Target Group

This guide is written for support engineers responsible for troubleshooting customer site Voice over Wireless Fidelity (VoWiFi) systems and the WLANs that support such systems. The guide may also be of considerable use to system administrators and network planners intending to design, implement, deploy and commission a new WLAN designed for VoWiFi access or upgrade an existing WLAN to support a new VoWiFi system. To this latter group, the importance of careful planning and provisioning through an exhaustive, rigorous and detailed site survey cannot be over emphasized. Many of the problems described in this guide arise because of poor provisioning and planning. In this respect, system administrators and network planners are recommended to read the document *System Planning, Ascom VoWiFi System for Siemens*.

1.2 Prerequisite

To gain the maximum benefit from this guide, readers should have experience in and knowledge of the following areas:

- Configuring a factory delivered handset and performing a handset software upgrade.
- How WLAN networks function up to the level of Certified Wireless Network Administrator (CWNA) certification or similar level.
- Sufficient knowledge in networking concepts and an understanding of the TCP/IP protocol suite.
- A basic understanding of Voice over Internet Protocol (VoIP) and the VoIP Session Initiation Protocol (SIP).
- Have read the configuration manual for the corresponding handset.
- Have read other documents related to the installation, for example WLAN specification and documents pertaining to the interoperability of the handset with the WLAN infrastructure.

1.3 Material Needed

To assist in troubleshooting, it is recommended that the support engineer is able to have at his or her disposal:

- The Portable Device Manager (PDM) application ‘‘WinPDM’’. The support engineer should be familiar with using the application for setting and modifying handset parameter values. Many error symptoms are related to a inappropriate configuration parameters values. Troubleshooting the PDM application itself is not covered in this guide.
- One or more handsets.
- A fixed phone, that is, a phone connected to the wired LAN.
- A tool that plays a continuous audio stream such as music, for example a radio or an MP3 player.

- An air trace tool or protocol analyzer such as Omnipeek or Wireshark for capturing traces on the LAN and WLAN. These require a WLAN adapter and network card respectively.
- A spectrum analyzer for detecting non 802.11 RF interference.

1.4 Software Version

This guide refers to a handset running software version 3.4.x or later.

1.5 Abbreviations and Glossary

The following acronyms and terms are used throughout this guide:

AP	Access Point.
B2BUA	Back-to-Back User Agent
BSS	Basic Service Set.
BSSID	Basic Service Set Identifier.
CAC	Call Admission Control
CCI	Co Channel Interference
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name Server.
DSCP	Differentiated Services Code Point. QoS on the Internet Layer. Used both for WLANs and LANs.
DTIM	Delivery Traffic Indication Message.
DTMF	Dual-Tone Multi-Frequency
EDCA	Enhanced Distributed Channel Access
ESS	Extended Service Set.
ESSID	Extended Service Set Identifier
IEEE	Institute of Electrical and Electronics Engineers
ITU-T	International Telecommunication Union-Telecommunication
MAC	Media Access Control.
PCAP	Packet Capture
PDL	Portable Device Logger. A troubleshooting tool.
PDM	Portable Device Manager.
PSTN	Public Switched Telephone Network
QoS	Quality of Service.
RFC	Request for Comments
RPCAP	Remote Packet Capture
RSSI	Received Signal Strength Indication.
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SNR	Signal-to-noise ratio
SSID	Service Set Identifier.

TAC	Technical Assistance Centre
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol (TFTP)
TIM	Traffic Indication Map
TSpec	Traffic Specification
TU	Time Unit
U-APSD	Unscheduled Automatic Power Save Delivery. Also referred to as WMM-PS.
UDP	User Datagram Protocol
UP 6	User Priority (value between 0-7). Wireless QoS at the MAC Layer.
URI	Uniform Resource Identifier
VoIP	Voice over IP.
VoWiFi	Voice over WiFi. Refers to a system running VoIP over WLAN.
WPA/WPA2	WiFi Protected Access 2.
WEP	Wired Equivalent Privacy.
WiFi	A Wireless Local Area Network based on the IEEE 802.11 standard.
WLAN	Wireless Local Area Network.
WMM	WiFi Multimedia.
WMM-PS	WMM Power Save. Also referred to as U-APSD.

1.6 Information Required by TAC

If an issue remains unresolved and a request needs to be opened with the Technical Assistance Centre (TAC) team, the following information should be forwarded:

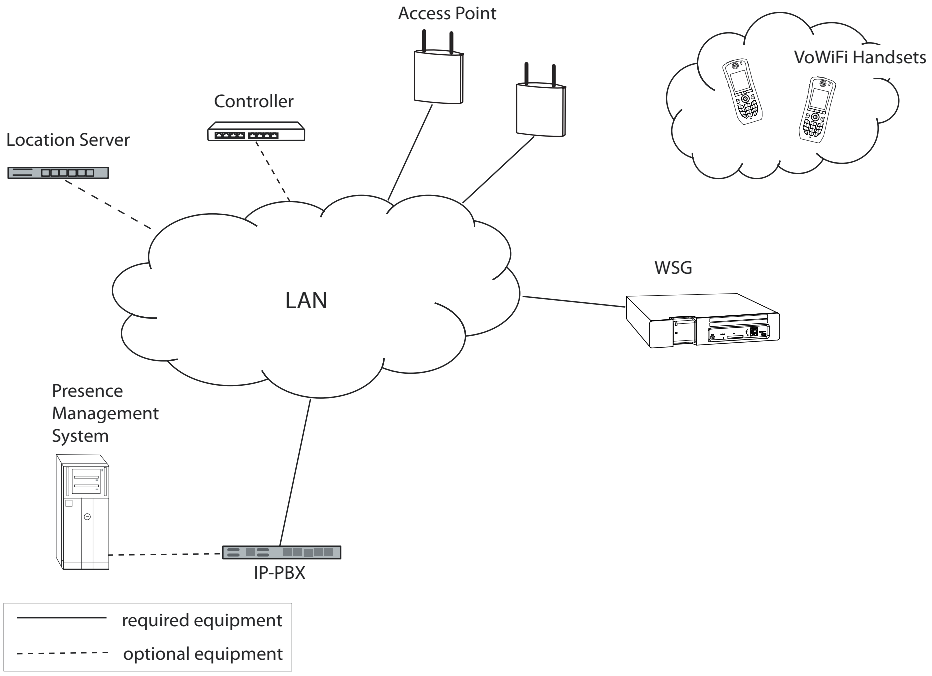
- A detailed description of the problem and what tests have been performed. Trace files should be attached and appended with descriptions of the tests and the MAC and IP addresses of the equipment used in the tests, for example, the handset, proxy and WLAN information.
- The values of parameters that have been configured, such as SSID, security setting and DTIM values.
- The frequency of the occurrence of the error and information about how to reproduce the error, if possible.
- The WLAN hardware and software versions of both the controller and APs.
- SIP proxy hardware and software.
- The handset software version.

2. WLAN Overview

A WLAN enables various devices, or WLAN clients, to communicate across RF channels through Access Points (APs). APs provide RF coverage throughout the site covered by the WLAN and this enables users, and their devices, to move around the site without being disconnected from the network. Each AP is identified by a hard-coded MAC address.

Initially, WLANs were designed to allow users to send and receive data from devices such as laptop computers but increasingly WLANs are being required to support different and more demanding types of traffic such as voice and multimedia. A VoWiFi system is illustrated in figure 1:

Figure 1. VoWiFi Overview



2.1 The Problem of Legacy WLANs

Legacy WLAN systems were designed for transmitting data packets; support for voice and other multimedia was never envisaged when these systems were designed, deployed and commissioned. So many traditional cell-based WLAN topologies proved unsuitable for handling channelization issues, AP-to-AP handoffs, and the unpredictably of system bandwidth that are introduced when VoWiFi is implemented. Voice is very susceptible to such issues being addressed satisfactorily. A WLAN that does not support VoWiFi but is being upgraded to do so therefore requires very careful planning, design, provisioning and hardware deployment to get the level of performance to adequately support voice. These problems are multiplied when different traffic types such as voice, video and data all contend for the same airspace. Adding voice to a WLAN may require radical changes of the APs placement and the amount of APs needed. If this is not considered feasible to undertake in a current installation VoWiFi may never perform as expected.

It follows that if a legacy WLAN is to support VoWiFi then an assessment of how suitable the WLAN is to support VoWiFi must be made. The number and deployment of additional devices involved in the WiFi solution must be carefully assessed. For example, the assessment should consider the adequacy of the current deployment in meeting cell boundary requirements because adequate cell overlap is a fundamental requirement for a voice system. The assessment should conclude with a readiness report documenting the suitability of the WLAN for both the wired and the wireless part of the network. The required parameter settings of the devices supporting the WiFi system should also be documented.

The following table lists some of the topics that should be included in an assessment document:

Topic	Comments
Are voice settings correctly set in the infrastructure, both LAN and WLAN devices?	Voice packet must have precedence over other types of traffic. The assessment must check for the ability to create an QoS solution across the entire network. Voice settings must be set according to vendor's recommendation and interoperability reports. **Note:** These reports provide important information for ensuring interoperability between handsets and vendor equipment. The reports are published as A*pplication Partner Program, Ascom Interoperability Report*s on the Ascom Partner web site.
Is the right software version installed on the devices?	Devices may need newer software or hotfixes to be able to support new devices. This is important when new features are added to current protocols. For example, when 802.11n is added to a WLAN.
Is there sufficient RF coverage?	Cell boundaries, cell overlap, and channel planning are extremely important for mobile devices which need to roam during usage. RF coverage must be checked using Site Survey tools.

2.2 WLAN Planning and Provisioning

To summarize, both a legacy WLAN that is to be upgraded to support VoWiFi and an entirely new WLAN purpose build to support VoWiFi and probably other kinds of media require:

- Comprehensive site surveys and detailed maps and floor plans of the areas where the WLAN is to provide coverage.
- Adequate provisioning of hardware, in other words, the deployment of sufficient APs in suitable locations to meet the coverage requirements of the WLAN
- Extensive and accurate documentation of the AP deployment using site maps and floor plans to illustrate the deployment
- A proper, well documented commissioning sequence including comprehensive testing
- A rigorous acceptance procedure before the commissioning is signed off as meeting the voice, and other, requirements, of the new or upgraded WLAN.

In addition, a legacy WLAN:

- Should have been documented properly to provide the basis and understanding implications of adding voice.
- May require a complete reassessment of its existing infrastructure before voice is added.

2.3 The Importance of Pre- and Post-Site Surveys

Modern site survey tools are valuable for pinpointing potential RF propagation problems, especially for large sites.

Modern site survey tools can do a lot more than just create the traditional heat maps that show the RF coverage areas from all access points. They can display co-channel interference areas, Signal-to-noise ratio (SNR levels), rogue access points and more.

Furthermore, most tools also include a pre-site survey WLAN CAD planning tool which a designer can use to do a simulation of RF coverage by using building drawings for a site. This computer based plan must be verified on place, once the APs have been installed and configured, by doing a live site survey at the site.

This pre-site survey is an aid to help the designer to plan for the placements of the APs in a new installation. The designer should make sure that the information gathered about the site is:

- Accurate and complete regarding the layout of the site
- The materials use in the construction of the building and their effects on RF propagation are fully appreciated
- The types of antennas to be used and deployed are provisioned for
- The power levels to use are fully understood.

Otherwise, the result of the survey will not accurately represent the anticipated RF propagation at the site. Performance problems will immediately manifest themselves once the WLAN is commissioned.

If a pre-site survey was performed in the traditional way, it should be followed up with a post-site survey after a network is deployed. This can be done by an installer requesting the site survey report and using the report to check that the installation is optimized for voice and that AP configurations are consistent and compliant with the vendors recommendations.

If the support engineer is subsequently required to visit a site to troubleshoot problems, he or she should initially verify that the content of the site survey still is accurate when it comes to AP placements, traffic load, and channel plans, etcetera. Special attention should be paid to areas where the layout of the building or concentration of VoWiFi clients may cause problems. The site survey features built into the handset described later in this guide are very useful in verifying the accuracy of the coverage predicted in the site survey and can, in some situations, quickly identify holes in the RF coverage.

2.4 WLAN Dynamics

Consideration must also be made that a WLAN is not a one-time installation. It changes constantly as people move around. The physical characteristics of the site may also change over time as furniture is moved, office partitions are redesigned and walls are build or removed. All of these factors can affect the propagation of RF signals.

2.5 Troubleshooting Implications and WLAN Design

It is beyond the scope of this guide to provide information about setting up a new WLAN to accommodate voice traffic or upgrading a legacy WLAN to do the same, except to emphasize the importance of those issues described in previous sections. In general, the role of the support engineer should be one of troubleshooting a system that once appeared to adequately meet the requirements of the enterprise (otherwise it wouldn’t have been signed off) but is now experiencing problems because of physical site changes, increasing personnel numbers, new applications and other factors that were never envisaged. Documentation that was completed during the setting up and deployments of the new site can therefore be a valuable reference in troubleshooting subsequent problems:

- Site maps and floor plans can indicate insufficient deployment and hence insufficient RF coverage
- Floor plans, as long as they are regularly updated to accurately represent the actual physical layout of the site, can indicate problems and disturbances to the RF environment that were not previously apparent.

3. The VoWiFi Handset as a Wireless Client

A handset is designed to be a part of a VoWiFi system that enables voice communication across RF channels. RF channels are provided by Access Points (APs) connected to a wired LAN. Before a handset can access the network, it must have been authenticated by the AP to verify that it is allowed to connect to the network. If the verification is successful, the handset forms an association with the AP and communications may begin.

A Basic Service Set (BSS) is an AP and the clients that are in communications range of that AP. A client, or handset, in the context of a WLAN becomes a member of the BSS when it becomes associated with the AP. In the usual implementation of a permanent, or infrastructure, WLAN, a BSS can only have one AP. The MAC address of the AP is used to uniquely identity the BSS and thereby provide the BSS identity (BSSID).

The BSSID of the AP that the handset is associated with can be read from the handset display as described in section 5.2.1 Show RSSI on page 31.

The name of a WLAN to which devices connect to is specified by a Service Set Identifier (SSID). All wireless devices connected to a WLAN must employ the same SSID to communicate with each other. The SSID is set on the AP and broadcast to all wireless devices in range. The SSID that a handset is connected to can be read from the handset display as described in section 5.2.1 Show RSSI on page 31.

3.1 VoWiFi Handset Protocol Layers

The handset uses protocols defined in a 4 layer TCP/IP protocol stack, which has similarities to some of the layers defined in the Open Systems Interconnection (OSI) 7 layer protocol model. A thorough understanding of the protocols at each level is essential to understanding how data is moved across a network. A support engineer with a good understanding of the media and the data structures and devices involved at each level of the protocol will have a systematic view of where problems may be occurring and a methodological approach to solving them. In addition, he or she will have a considerable armory of tools and utilities at hand for investigating sources of trouble.

The TCP/IP protocol stack is all about data communication across a WLAN and the use of protocols such as:

- Application layer for applications that interface with the transport layer, including PBX, WSG, Dynamic Host Name Configuration Protocol (DHCP) and Domain Name Server (DNS).
- Transmission Control Protocol (TCP). Transports User Datagram Protocol (UDP) and TCP packets. TCP ensures secure and correct delivery of TCP packets through retransmission of lost packets, congestion throttling and error free transmission.
- Internet Protocol (IP) assigns each networked device its logical IP address
- Link layer consisting od MAC and physical sub layers specified in 802.11 for defining the physical characteristics of the carrier medium and access protocols.

The role of the handset in moving data across the network between different physical and logical entities defined by the protocols is summarized below:

Layer		**Entity sending or receiving info**	**Function**
Application layer		Application data packets	There are mainly two services that are integrated in the handset: - VoIP using either the SIP or H.323 standard - WSG communication

Transport layer		TCP packets	The handset uses TCP/IP as the protocol to address packets to be delivered to other devices like a SIP PBX
Internet layer		IP packets	IP addressing - APs, controllers
Link layer	MAC sub layer	802.11 frames (Management, control and data frames)	The handset uses the IEEE 802.11 WLAN standard protocol suit to get access to the media and to send packets to the AP
	Physical sub layer	RF signals, digitized bit streams	

Link Layer - MAC and Physical Sub Layers

The physical sub layer and MAC sub layer, in the context of the TCP/IP model, replaces the data link and physical layers of the OSI model with a single link layer. This means that the link layer:

- Controls how data in the form of bit streams, is transmitted through the network on standard RF channels. The layer is about the interfaces between the RF channel and network devices such as the APs, controllers, if used, and handsets. The notion of the physical layer also defines the protocols that define the characteristics of the channels conveying data. The handset uses the standard RF channel on either the 2.4 GHZ band or the 5GHz band as defined by the 802.11a/b/g/n amendments.
- Manages the raw bit stream data received by the AP or controller from the handset radio, and packages the bits into 802.11 frames. 802.11 defines three kinds of frame for WLANS, one for management, one for control and one for data. The handset uses management and control frames for AP association and authentication.
- The MAC sub layer manages the physical MAC addressing scheme by encapsulating layer 2 PDUs in a MAC sub layer PDU. The MAC sub layer uses Address Resolution Protocol (ARP) to maintain logical IP to physical MAC address mapping of SIP servers in the call path.

Internet Level

The Internet level responds to UDP and TCP service requests from the transport layer and provides network to network routing.

Transport Layer

The transport layer provides the TCP/IP address used by network devices. TCP packets are routed using the IP addresses of WLAN network devices that may interwork with other networks such as the internet or Public Switched Telephone Network (PSTN). In the context of the VoWiFi system this is likely to be a VoIP gateway or IP-PBX

The transport layer also provides congestion throttling to maximize data throughput without overwhelming the resources of the network.

Application Level

The application layer includes the functions of OSI Application, Presentation Layer and Session Layer, which are often referred to as a user services. TCP/IP sockets and ports are used to describe the path over which applications communicate. Most application level protocols are associated with one or more port number.

The SIP protocol is an Application Layer protocol designed to be independent of the underlying Transport Layer.

3.1.1 Troubleshooting the Layers

Understanding the layers in the TCP/IP protocol stack and how they communicate with each other is important because it provides the support engineer with a consistent, structured and methodological approach to troubleshooting network issues. It enables the support engineer to adopt either a top down approach or a bottom up approach to troubleshooting and reconciling network issues.

With top-down troubleshooting, the support engineer starts with the layer 4, the application layer or user services level.

Bottom-up troubleshooting involves checking the device for physical problems such as no power, a bad cable or other physical problems. A positive response would confirm that network connectivity had been established, in which case it is safe to conclude that connectivity up to the Network layer was successful. The focus can now be turned to troubleshooting the upper four layers of the OSI.

3.2 Voice Transmission over a VoWiFi System

Voice over WiFi (VoWiFi) requires that digitized voice signals are sent over a WiFi network in the form of data packets as defined in layer 4 of the TCP/IP protocol stack. This basic requirement places a substantial overhead on a WLAN. If a WLAN is unable to support the VoWiFi requirement consistently, or only able to provide sporadic and irregular support, then noticeable and unacceptable levels of deterioration to the quality of the voice service occur.

For example, if voice data packets are unable to arrive at their destinations at regular time intervals, typically every 20 ms, distortions in the conversation are likely to occur. The VoWiFi system must also keep packet loss, delay, and jitter within required limits to avoid a loss or reduction in the voice service.

As a voice signal travels through the VoWiFi infrastructure of APs, Ethernet switches, routers, and gateways, packet loss, delay, and jitter can add up to reduce the signal quality, especially when the network gets congested with traffic.

3.3 Handset Startup Procedure

The handset is started in the following way:

1 The user presses the *On/off* button (*End key)*.

2 The handset loads the boot code, which then loads the latest installed firmware.

3 The handset loads licenses.

4 The handset actively scans for the configured SSID on all configured channels and chooses the best AP to associate with and authenticate to.

5 The handset is identified to the network by it’s IP address. If the handset Dynamic Host Configuration Protocol (DHCP) mode is ‘‘Enabled’’, the handset is dynamically assigned an IP address, otherwise the statically configured IP address is used.

6 The handset sends an ARP request for resolving the MAC addresses of the IP PBX and the WSG server.

7 The handset registers with the IP PBX and WSG server, and logs on to and synchronizes with these devices.

8 The handset displays the idle screen with signal strength indicator, the current time, battery status, date, user name, user number and license type. In this state, the handset is described as being in idle mode.

3.4 AP Scanning

When a handset is powered on or on the move, it needs to associate with an AP to be able to connect to the wired LAN. The scanning process checks the air for the available APs to associate with and, based on this information, the handset creates a linked list of candidate APs. The handset will then usually try and associate with the AP with the strongest RF signal.

3.4.1 Active Scanning

Active scanning occurs when a handset actively seeks to associate with an AP and ultimately connect to a network by transmitting 802.11 probe requests frames to APs on each of the channels the handset is configured to use. The probe request frames contain the SSID of the network that the handset wishes to connect to and all APs that are configured with the same SSID return a probe response to the handset. A handset with a null SSID, that is, it is not currently configured with a SSID, may also transmits probe requests. If an AP exists with no security settings at all, the handset may be able to associate with that AP.

If the handset receives probe responses from more than one AP, it can use a number of criteria to decide which AP too associate with. Although these criteria are vendor specific, a handset will usually select the AP with the strongest RF signal.

If no suitable AP is selected the ‘’No Network’’ message is displayed in the handset after about 5 seconds. For each subsequent 5 second intervals, the handset continues to perform actives probe for suitable APs using alternate broadcast and unicast probe requests. The process will not be interrupted until the handset either successfully associates with an AP or the battery runs out.

3.4.2 Passive Scanning

When a handset becomes associated with an AP but is not used to make a call, it will normally go into power save mode and start to perform passive, as opposed to active scanning. When the handset performs passive scanning it listens, on each channel it is configured to use and at specific intervals, for beacon frames transmitted by APs. When passively scanning for beacons, the handset transmits no frames itself.

Beacon frames are similar to the probe response frames transmitted by an APs when a handset is actively scanning, except that they contain additional information about traffic pending for the handset. For additional information about how passive scanning works when the handset is conserving power, see the section 3.5 Power Management on page 12.

3.4.3 Configured Channels and Scanning Intervals

When a handset is started from power off mode the procedure to find an AP to associate with depends on the parameter and protocol settings in the handset.

One of the default protocols that are used by the handset is 802.11d. This protocol transports regulatory domain information based on country information stored in the AP which is sent out in the beacon.

The handset needs to know this information before it can start to scan for APs so it can adapt to the country rules for channels to use, power level, etcetera. It therefore needs to use passive scanning to grab a beacon that contains that information. Thereafter the handset can start to use active probing, where it will send out a probe request packet with its configured SSID on each configured channel for the configured band. It will stay around 20ms on each channel waiting for replies.

The WLAN settings that are default are those for ''Network A'', which uses the 2.4 GHz band with the default channels 1.6 and 11.

Note: The handset will not change from 2.4 GHz channels to 5 GHz channels during the probing session, unless the handset has been configured to automatically switch between available networks. This capability is managed by setting the *Auto-switch network* parameter in the PDM as described in the *Configuration Manual, WL3 and WL3 Plus WLAN Handset, Handset Configuration* chapter.

The correct channel set up in a WLAN is quite important. The channels set up to be used by the handset on any of the 2.4 GHz or 5GHz has impact on the performance of the handset.

To be able to detect APs when in passive scanning mode the handset must listen to each channel slightly longer than the beacon interval, to be sure not to miss any beacon. The handset then has to switch the radio channel and starts to listen again on the new channel.

By default the channels used in any scanning process, including site survey, is for the 2.4 GHZ band *channel 1.6.11* and for the 5 GHz radio *all channels* for the domain.

Tip: For performance reasons when scanning, the amount of channels should be minimized and only include the channels that are used in the WLAN.

Active scanning of the 5 GHz UNII-2 and UNII-2e, the DFS-channels are not permitted in the 802.11 standard, so those channels will only be scanned in passive mode.

Note: The handset can use the DFS channels, but the Voice quality may be distorted. For additional information, see section 3.7 DFS Channel Probing on page 17.

3.5 Power Management

3.5.1 Overview

Power Save Battery conservation is supported through the use of the WMM standard Power Save mode (PS-mode) operation. The operation differs when the handset is idle or in call.

Idle

When the VoWiFi Handset is idle, it is in PS-mode and listens for broadcasts, multicasts and unicasts at a beacon interval, which is configurable at the AP.

Call

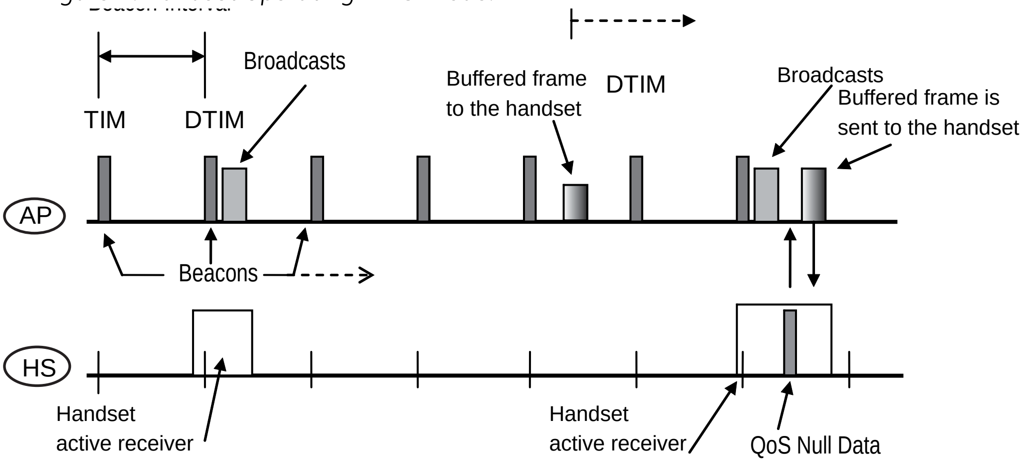
When in call, one of two different modes are used depending on how the handset has been configured and what functions are supported by the WLAN infrastructure:

- The handset parameter *Voice power save mode* is set to "none". The handset stays active during the call, only signaling PS-mode when scanning different channels in case of roaming. When the call is ended, it returns to idle (PS-mode).
- The handset parameter *Voice power save mode* is set to "U-APSD". In U-APSD the handset is in PS-mode also during the call. The U-APSD functionality is negotiated with the AP during association and provides the automatic release of buffered packets immediately after an uplink packet. U-APSD maximizes battery lifetime and performance. U-APSD must be supported by the WLAN infrastructure for a handset to be able to use it.

Beacons

A beacon is broadcast from an AP to all handsets in the BSS at a predefined beacon interval, which is normally 100 Time Units (TUs) of 1.024ms or 102.4ms. A handset wakes up at intervals determined by a Delivery Traffic Indication Message (DTIM) period, which is an elapsed time based on a number of beacons. Normally the DTIM set to 5 beacons, which means the handset wakes up every 512ms, that is, approximately twice a second. If, at that point, the beacon Traffic Indicator Map (TIM) announces it contains buffered data, the handset transmits a QoS Null data frame as a polling frame to the AP. The QoS Null frame releases the buffered frame and the AP proceeds to transmit the frame. The handset keeps it's receiver turned on until the frame is received. These concepts are illustrated in figure 2:

Figure 2. Handset Operating in PS-mode.



Battery Life

The implication for battery power consumption of a handset in PS-mode is that by decreasing the beacon interval or increasing the DTIM parameter, or both, the handset uses more power and shortens the battery time. However, the handset response time to any pending TIM will be faster.

Roaming Implications

When the handset hears a beacon and the signal level is below -70dBm, roaming is initiated and the scanning process starts. The handset will continue the scan process every 4 seconds as long as the RSSI value is less than -70dBm. For additional information about roaming periods and thresholds, see the section 3.6 Roaming on page 15.

3.5.2 U-APSD PS Mode Operation

The handset may be configured for U-APSD if the VoWiFi system manufactured by a product partner supports Unscheduled Automatic Power Save Delivery (U-APSD). The two power management modes are valid also in U-APSD mode and the AP buffers downlink frames only if the station is in PS-mode.

U-APSD is basically a polling scheme, like 802.11e PS management, but in U-APSD mode, QoS Null data frame acts as a polling frame and is called a "trigger frame".

An AP capable of supporting U-APSD indicates this capability through the QoS parameters found in the WLAN management system. If the supported U-APSD capability is only present in the type of WMM Power Save used, the capability is indicated in the QoS information field in the WMM parameter or information elements.

This information is present in Beacon, Probe Response, and (Re) Association Response management frames.

On association, the handset negotiates with the AP and trigger-enables all four Enhanced Distributed Channel Access (EDCA) categories. These are:

Category	**802.11e Priority**
Voice	6 or 7
Video	4 or 5
Best Effort	0 and 3
Background	1 to 2

For additional information about U-APSD and how to inspect and troubleshoot U-APSD setup, see section 7.2 U-APSD Troubleshooting on page 53.

U-APSD Flow Example

The example is based on a voice call with bi-directional flow and symmetric codec speech frames.

A call is established between two parties. In this the parties are assumed to be a VoWiFi handset and a fixed line phone that resides somewhere on the LAN.

1 In the AP, a voice packet from the fixed phone is received from the wired LAN. The packet is destined to the handset and the AP intends to transmit the packet on the RF interface immediately.

However, the destination, that is, the handset for the packet is in PS-mode and since the AP keeps track of all associated stations PS management mode, this is recognized and the packet is buffered in the AP.

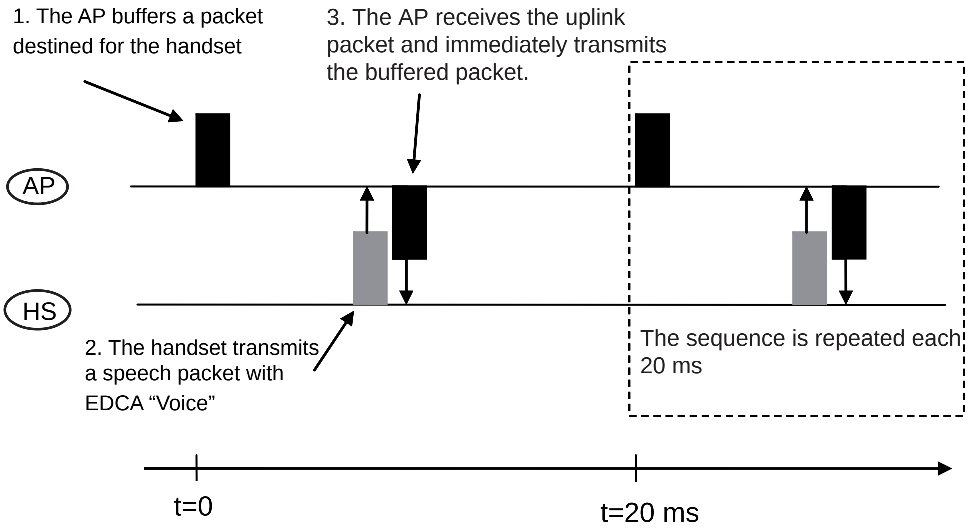
2 After a short while, the handset transmits a voice packet, as is done every 20 ms with default settings. This packet is transmitted within the EDCA Access Category ''Voice'', which means that it is highly prioritized.

3 The AP receives the packet from the handset, forwards the packet to the wired LAN and recognizes that the sending station has a buffered packet. The AP releases the packet and transmits the packet immediately to the VoWiFi handset that now is awaiting a packet.

The procedure when an AP transmits a buffered packet due to a trigger frame is called an ''Unscheduled Service Period''

4 The end of an unscheduled service period is when all of the buffered data has been released and there are no more frames to transmit. The event is indicated by the transmission of a QoS Null data frame.

Figure 3. Handset Operating in U-APSD PS Mode


1. The AP buffers a packet destined for the handset
3. The AP receives the uplink packet and immediately transmits the buffered packet.
AP
HS
2. The handset transmits a speech packet with EDCA “Voice”
The sequence is repeated each 20 ms
t=0
t=20 ms

An example of an U-APSD flow is described in detail in section 7.2.3 Packet Classification of U-APSD in the AP on page 54.

3.5.3 Recommended Values

A low DTIM value will cause the handset to wake up and check for incoming data more frequently. A normal value is a beacon Interval of 100 TUs and a DTIM of 5, which causes a wake up approximately 2 times per second.

Note: The DTIM value should normally be set to 5. Values lower than 5 reduce the handset sleep period and shorten the battery life.

For additional information, always check the *Application Partner Program, Ascom Interoperability Report*s for specific recommendations applicable to the particular vendor equipment.

3.5.4 Screen Saver

The handset LCD display also consumes a lot of power. Unnecessary use or browsing of the handset display can therefore consume battery power quickly. A *Screen saver* parameter setting exists in the handset configuration, which may be set to “black” in the PDM as an additional power saving measure.

3.6 Roaming

One of the most important design criteria for good functionality in a voice system is to deploy sufficient APs to create adequate RF coverage throughout a site. In addition, the coverage areas provided by the individual APs must be deployed in such a way as to allow a user to roam throughout the site without any deterioration in the quality of an ongoing call. The user must also remain connected to the network at all times even when the handset is in idle mode. Failure to adequately support roaming may result in audible clicks and other disturbances in a voice call.

Roaming can be described as disconnecting from the current AP as the user moves away from it and the signal attenuates. The user then connects to a new AP that offers an increasingly stronger signal as the handset is carried towards it. As a user moves away from an AP of decreasing received signal strength and towards one of increasing signal strength, it is predictable enough to be able to apply a roaming algorithm based on the measurement of received signal strength at fixed time intervals, for example, every 4 seconds. The algorithm then decides where and when a handset disconnects from one AP and connects to a different AP.

An additional factor that must be included in any roaming algorithm is to provision for sudden, large and often unpredictable reductions in received signal strength due to some dynamic event that is introduced into the physical environment, such as the closing of a heavily clad steel door or the handset user enters an elevator. These events can occur between the scans performed at the fixed time intervals and cause additional scans to be performed. The trigger for an additional scan is when a 6dBm or greater received signal strength reduction is detected since the last scan.

To ensure that unnecessary extra scans are not initiated between scheduled measurement periods, the reduction in received signal strengths is calculated accordingly:

reduction in dBm = 75% of scheduled AP RSSI measurement + 25% of beacon RSSI.

Note: Only beacons are used for RSSI calculations in the handset when the handset is not roaming. When roaming, probe responses are also used in the RSSI calculations.

For example, consider a doorway between an associated AP and a handset, with a metal door in the open position. if the door was momentarily closed and then opened, there might be a sudden 16bB reduction in received signal strength and a rapid loss in communication. However, this would be largely restored once the door was opened again and make an extra scan unnecessary and a waste of network resources. However, if the door was left closed, the loss in received signal strength would be sustained and probably worsen as the user moved away from the AP. An extra scan would therefore be justified.

Roaming is implemented differently depending on whether the handset is in idle mode or in a call. Different roaming algorithms apply to these modes.

3.6.1 Idle Mode

In idle mode, it is not so important to consider received signal strength and roaming as voice quality is not an issue. The following roaming algorithms are deemed sufficient for ensuring the handset is able to perform TIM discovery as the user moves between AP:

RSSI	**Scans**	**Roams**
> -70dBm	No scanning.	n/a
< -70dBm and > -73dBm	Every 4secs.	If a candidate AP offers an improvement of 6dBm or more
< -73dBm	Every 4secs.	If a candidate AP offers an improvement of 3dBm or more

Additional Scan in Idle Mode

An additional scan is triggered in idle mode when scanning is being performed and when a reduction of >= 6dBm is detected in a beacon being sent by the AP at the regular beacon interval.

3.6.2 Call Mode

In call mode, received signal strength is very important for ensuring voice quality, particularly if the user is moving around the site. The following roaming requirements are deemed sufficient for ensuring the handset is able to support adequate voice quality between APs:

RSSI	Scans	Roams
> -73dBm	Every 5secs.	If a candidate AP offers an improvement of 6dBm or more
< -73dBm	Every 5secs.	If a candidate AP offers an improvement of 3dBm or more

Additional Scan in Call Mode

An additional scan is triggered in call mode when a reduction of >= 6dBm is detected in a beacon being sent by the AP at the regular beacon interval.

3.6.3 System-Aided Roaming

When the handset operates in a WLAN where the system is responsible for roaming, use the PDM to set the handset to system aided roaming. From the menu Network, select the active network (A, B, C or D) and then select the parameter *Roaming methodology*. Set the value to ''System-aided roaming''. The handset will then only perform a scan when the RSSI drops below -70dBm both in call and in idle mode.

3.7 DFS Channel Probing

The 5 GHz band supports a minimum of 21 non-overlapping channels and potentially a few more depending on different regulatory domains. The following table, for example, shows the channels supported in the ETSI regulatory domain:

Band	Channel
UNII-1	36, 40, 44, 48
UNII-2	52, 56, 60, 64
UNII-2e	100, 104, 108, 112, 116, 132, 136, 140
UNII-3	149, 153, 157, 161
ISM	165

The radio channels in the UNII-2 and UNII-2e bands are DFS-channels, which may be used by civilian and military radar such as aviation and weather radar. Because radar always has a higher priority than a WLAN, additional procedures must be employed to prevent LAN devices from interfering with radar when the radar is using the DFS channels. This can increase latency and degrade the performance in a WLAN.

A client that does not support radar detection is not allowed to actively scan for APs in the DFS channels. The client is only allowed to perform passive scanning, which means that it can only listen 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 Dynamic Frequency Selection (DFS) channels in a voice enabled WLAN, but the voice quality can be distorted as the DFS channels must be treated differently in the scanning process.

The probing process above is repeated each time the handset needs to find roaming candidates, that means, when the signal quality on its current associated AP decreases.

Another reason that the use of DFS channels is not recommended in areas where radar may be operating, is the requirement of automatic switching of channels and the non-service time gap that occurs. Note that radar can be airborne, for example, used by aircraft for navigational purposes.

The regulations for using 5 GHz channels, generally known as DFS channels, in which radar operates, is that the handset uses a different approach while scanning.

The DFS regulations require that WiFi devices should check for radar that is currently operating before they initiate a session. This requires special software features and is normally only included in APs, which are the devices that are set to use a specific channel. If a radar signal is detected the AP should invoke a special procedure to automatically move to another channel. During this transfer to another channel, which takes a while, the transmission of packets in that cell is stopped and as a result the call can be lost.

Portable devices, like a handset, are not able to detect radar and thus are not allowed to initiate a conversation. Active probing on the DFS channels is therefore prohibited until is has been determined that no radar is present.

To detect an AP to roam to, the handset has to use passive scanning which means it has to listen to beacons on every configured channel.

The default beacon period in most APs is set 102.4ms. Using a short scanning interval of let's say 20ms on a channel the handset’s chances of hearing a beacon is about one in five. To improve the chances of the handset picking up a beacon the listening time on a channel can be extended or the beacon period made shorter.

For the DFS channels the passive listening time for the handset is set to 70ms, during which the handset may or may not hear a beacon. If the handset hears a beacon during this period or if the time period expires, it will immediately return to its currently working channel and exchange packets with the current AP that was buffered during the scanning process.

If the handset did hear a beacon it will do active probing on that channel and add the APs it hears to the roaming table. It will then go on with this process with the next channel it is set up to use. When it gets to the current channel it can immediately do a probe request to find any other APs on that channel to add to the roaming table.

Note: Since scanning for many channels takes a considerable time, it is important that the channels used in the scanning process are only those channels that have been setup for use in the WLAN system.

After finalizing the first round it will decide whether to roam or not, and which AP to use.

For optimal voice performance it is not recommended to use DFS channels. If they are used limit the number of channels to 8 otherwise roaming will be further degraded.

3.8 SIP

Session Initiation Protocol (SIP) is an application layer signaling protocol defined in the IETF standard RFC3261. It is used to setup, control and manage sessions between two or more endpoints in an IP based network. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences that use TCP, TLS/TCP or UDP for transport.

SIP is a fairly loose standard and the implementation is up to the manufacturer of the handset. Since each implementation may have some vendor specific code it is important that the handset is used together with a SIP-Proxy (IP-PBX) that is tested by the interoperability team. Only those solutions that have been tested are supported.

When troubleshooting VoIP in a handset a solid understanding of how a SIP session is established between two phones and where the voice packets are going will speed up the troubleshooting process.

3.8.1 SIP Components

SIP Proxy Servers

SIP servers receive requests from clients, process the requests and generate responses. A SIP server is usually a proxy server acting on behalf of the client by receiving and forwarding the requests to the recipient, receiving responses from the recipient and returning these to the client. Because the address of the recipient is not initially known when a request is initiated, a proxy server often contains a registrar server where location details of all the users registered with the network are contained.

SIP Clients

In general the notion of clients refers to the end users of applications running at the application layer of the TCP/IP protocol stack. The applications include softphone applications and voice and messaging applications for IP handsets.

SIP Registration Servers

One of the most important functions of SIP servers is to detect the location of users in the network and process requests from clients to register their current location. Users register their IP addresses with a server by sending a REGISTER message to the server informing them of their IP address. The server subsequently returns an acknowledgement in the form of a 200 OK message when the user IP address is registered.

The server is connected to a location database where an up-to-date mapping between the server, user and user IP address is maintained. The specific mapping is between the user Address of Record (AOR) and the user IP address, for example sip:user2@serverb.com -> 172.20.15.235. This mapping is refreshed on a periodical basis by REGISTER messages according to a negotiated expiry value between the client and server.

SIP Addressing

SIP uses email-style addresses to identify users, for example:

- Harry.Burger@millpond.se
- freddy@serverb.com
- 4112@serverb.com
- user2@serverb.com
- user1@servera.com

The SIP Uniform Resource Identifier (URI) defines the addressing scheme used to call parties via SIP and is written as:

```
sip:x@y[:Port]
```

For example:

```
sip:4112@serverb.com:5060
```

Parameters may also be added to addresses such as type or transport protocol. For example:

```
sip:user2@serverb.com;transport=tcp
```

SIP Ports

SIP provides the signaling part of a communication session. signaling information may be encrypted or non encrypted.

SIP clients send and receive non-encrypted signaling information in UDP or TCP packets to and from other SIP servers and SIP endpoints on the default port 5060.

Port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS).

Session Description Protocol

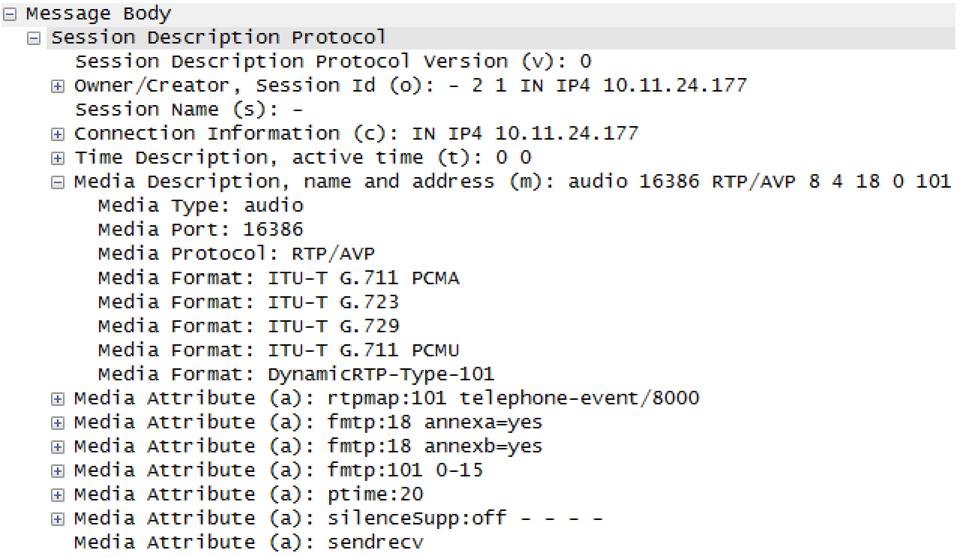
The Session Description Protocol (SDP) is used to initiate a media session and support the flow of RTP packets between SIP endpoints. An SDP message contains information about the SIP entity, such as an INVITE message, that created it. Such information describes the codecs that may be negotiated between the SIP endpoints, the transport protocol to be used, and the ports and IP addresses that RTP packets are to be sent to.

Codec negotiation is about selecting which codec to use on each leg of a call and SDP supports this negotiation. A handset that initiates a call announces to the called party handset the codec that it wishes to use for the media session. The called party confirms whether or not the desired codec is supported. In practice most SIP endpoints support multiple codecs, so the SDP codec negotiation process sifts through the choices and settles on a single codec to use.

To check the codecs supported by a handset, expand the message body associated with the SIP entity specifying the call invitation and then expand SDP and Media Description. The supported codecs are listed as Media Attributes followed by an ITU-T standard speech codec extension.

As SDP is a text-based protocol embedded into SIP Messages it is relatively easy to display and inspect the content of SDPs using a protocol analyzer such as WireShark. For example, the SDP part of a SIP INVITE request viewable from a WireShark trace is shown in figure 4:

Figure 4. SDP Part of SIP Invite



```
⊟ Message Body
  ⊟ Session Description Protocol
      Session Description Protocol Version (v): 0
    ⊞ Owner/Creator, Session Id (o): - 2 1 IN IP4 10.11.24.177
      Session Name (s): -
    ⊞ Connection Information (c): IN IP4 10.11.24.177
    ⊞ Time Description, active time (t): 0 0
    ⊟ Media Description, name and address (m): audio 16386 RTP/AVP 8 4 18 0 101
        Media Type: audio
        Media Port: 16386
        Media Protocol: RTP/AVP
        Media Format: ITU-T G.711 PCMA
        Media Format: ITU-T G.723
        Media Format: ITU-T G.729
        Media Format: ITU-T G.711 PCMU
        Media Format: DynamicRTP-Type-101
    ⊞ Media Attribute (a): rtpmap:101 telephone-event/8000
    ⊞ Media Attribute (a): fmtp:18 annexa=yes
    ⊞ Media Attribute (a): fmtp:18 annexb=yes
    ⊞ Media Attribute (a): fmtp:101 0-15
    ⊞ Media Attribute (a): ptime:20
    ⊞ Media Attribute (a): silenceSupp:off - - - -
      Media Attribute (a): sendrecv
```

The supported codecs and their respective properties are listed under the Media Description and Media Attribute followed by ITU-T standard speech codec extensions.

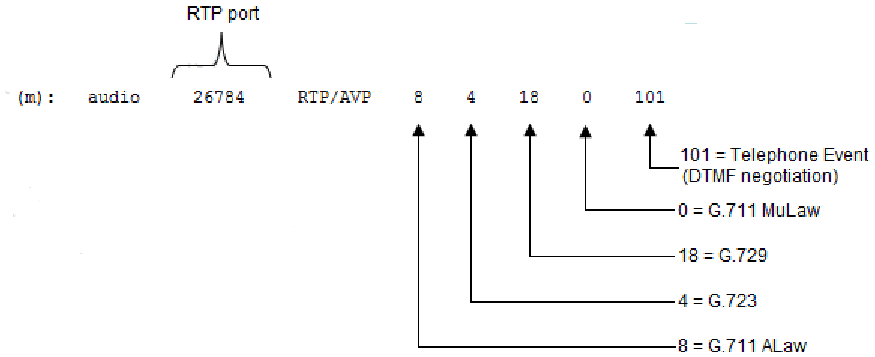
Media Description

The Media Description part of the SDP for audio contains:

- The RTP port number
- The RTP/AVP profile for the use of the RTP
- Payload types.

In figure 5 the media descriptor identifies four payload types that a particular handset supports. The first payload type "8" is the codec (G711 ALaw) preferred by this handset.

Figure 5. SDP Media Description:



In this example, the handset initiating the invite is indicating to the called party handset that the preferred codec for the media session is G.711 ALaw. If the called party handset does not support this codec, try G.723 as the next preference, G.729 the third preference and G.711MuLaw being the least preferred. In the unlikely event of the other handset not supporting any of the codecs suggested by the call initiator, a SIP unsupported media type message will be returned in response to the initial invitation to setup the call and the RTP media session will not be established.

Media Attribute

An example of an SDP media attribute is as follows:

```
Media attribute (a): fmtp:18 annexa=yes
```

It shows how the G.729 codec protocol is specified with it's payload type *annexa* set to "yes", that is, silence suppression. Silence suppression is thus set if the SIP endpoints negotiate this codec protocol for use in a connection.

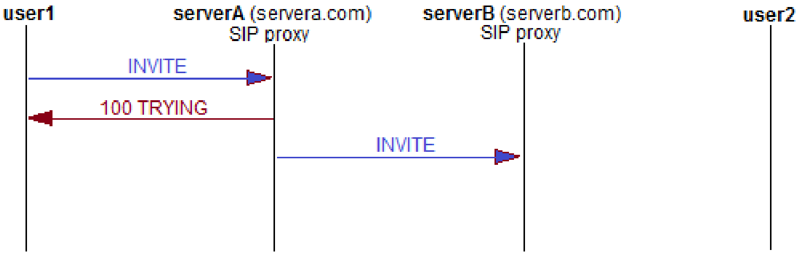
An understanding of how the properties of a connection are expressed through SDP media attributes can sometimes be of help in troubleshooting and resolving issues.

3.8.2 SIP Call Setup

An attempt to establish a SIP session begins when a calling party, say user1, makes an INVITE request to a called party, say user2. Because the call will be using IP, user1 ultimately needs to discover the IP address of user2. User1 thus forwards the INVITE request to its SIP proxy servera.com but ServerA realizes by the domain name part of the AOR (serverb.com) that user2 is not registered with its own domain servera.com. ServerA therefore needs to initiate a search for the proxy server in the network that is able to associate the AOR with an IP address.

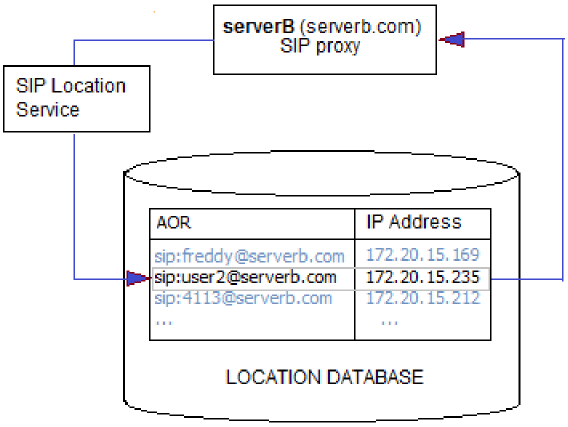
The first hop in this simplified example is to pass the INVITE request to serverB. ServerB realizes by the domain name in the AOR (serverb.com) that user2 is connected to it and it has no further need to forward the INVITE to any other servers in the network. Instead, it can now forward the INVITE to user2. The start of the process is shown in figure 6:

Figure 6. Call Invite



Before the INVITE message reaches the phone of user2, the SIP proxy serverB uses its registration server and location database to find the IP address of user2. ServerB performs a SIP service lookup on the database to find a match for the AOR that it has received from SIP proxy servera.com, as shown in figure 7:

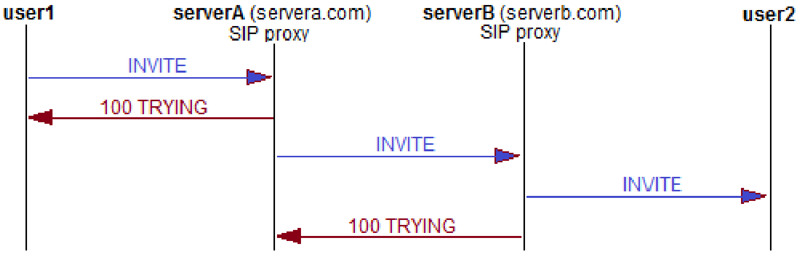
Figure 7. Far End Lookup



AOR	IP Address
sip:freddy@serverb.com	172.20.15.169
sip:user2@serverb.com	172.20.15.235
sip:4113@serverb.com	172.20.15.212
...	...

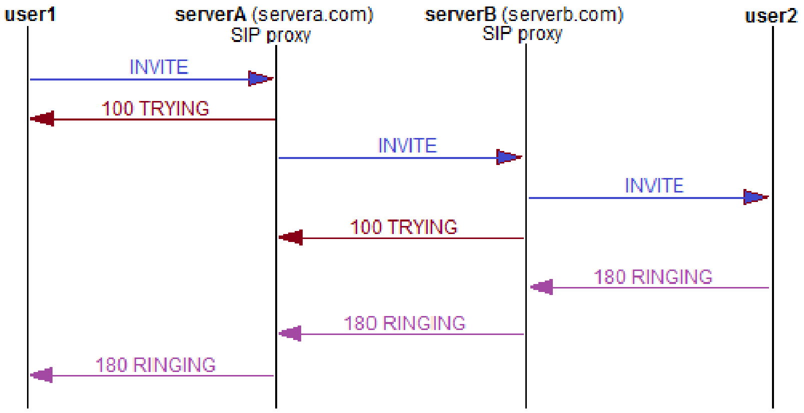
The result of the lookup is an IP address (172.20.15.235) that serverB can now bind the INVITE message to. Once the association is established, the INVITE message reaches user2, as shown below:

Figure 8. Number Binding



At this point serverB sends a 180 RINGING message back to user1's SIP server serverA and in turn serverA relays the message back to user1, as shown in figure 9:

Figure 9. Ringing

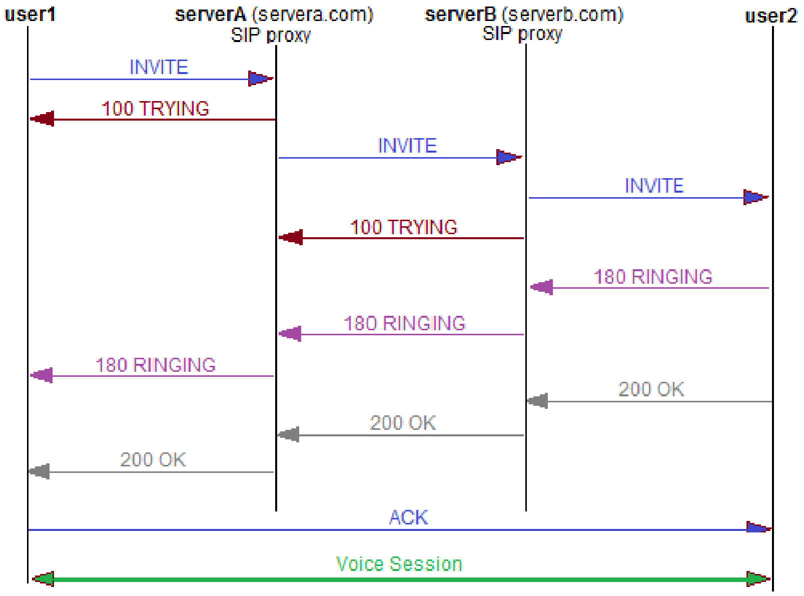


The user1 handset will now probably produce some kind of audible call pending tone that confirms user1 that the called party has been reached and their handset is ringing. If user2 answers, an 200 OK message is generated by serverB and forwarded to user1 via serverA. The call message flow as defined by the SIP standard is finally completed when the user1 handset sends the user2 handset an acknowledgement (ACK) as shown in figure 10.

After the ACK, SIP signaling is concluded and:

- A media session is established whereby a flow of RTP voice packets between the user1 and user2 handsets is established as shown in figure 10. The voice session continues until one of the parties terminates the call.
- A SIP dialog is established between user1 and user2. The SIP dialog is the critical component in the media session because it is associated with all requests and responses that are made and received during the session. The dialog is identified by a Call Identity, a tag value associated with the user-1, the initiator of the call, and a tag value associated with user-2, the recipient of the call and these values are used in all requests and responses.

Figure 10. Call Acknowledgement and Voice Session Establishment

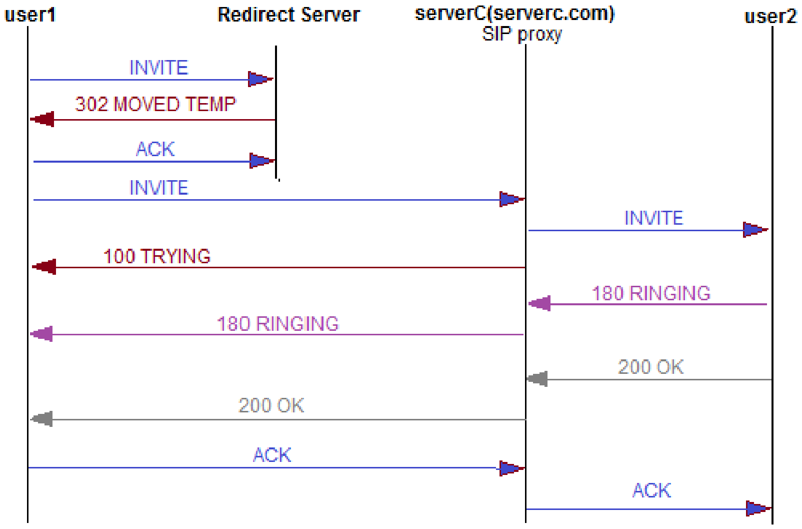


3.8.3 Redirect Servers

A redirect server generates 3xx responses to requests it receives, directing the client to retry the request using one or more alternative Uniform Resource Identifiers (URIs), which are presented in the 3xx response. 3xx is a SIP response class used to indicate that further action needs to be taken in order to complete a the request.

In the following example, user1 places a call to user2 using a redirect server because user2 has temporarily moved to serverc. User2's address has temporarily become sip:user2@serverc.com. The INVITE message is first sent to the redirect server, which returns a 302 MOVED TEMPORARILY response containing a contact header with user2's current SIP address. User1 then generates a new INVITE message and sends it to user2 via the proxy serverC:

Figure 11. Call Redirect

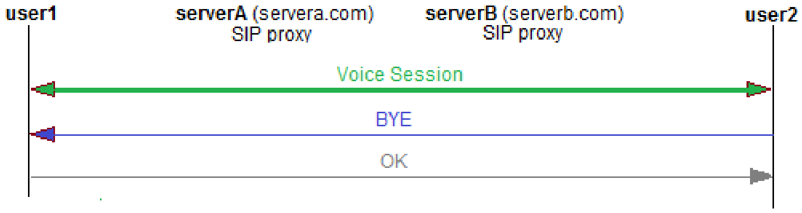


Note: A user attempting to call a recipient that has moved permanently to a new position will receive a 301 MOVED PERMANENT message after the initial INVITE.

3.8.4 Call Completion

When one of the parties terminates the call, a final exchange of SIP messages occurs. The party that initiates the termination sends a BYE message directly from one handset to the other party, and the other party handset returns an 200 OK and that is the completion of the call. For example:

Figure 12. Call Completion



Note: If the WLAN is using a controller based solution the SIP message flows in all of the above illustrations should include the controller because all WLAN traffic is bridged between wireless and wired network segments by the controller and not the APs. That means that traffic goes back and forth on the LAN cable to the controller. Depending on the configuration and functionality of the SIP proxy, the Real-time Transport Protocol (RTP) stream may be passing through the SIP proxy or may be routed directly between the VoWiFi Handsets when using a controller with thin APs.

3.8.5 Message Content

Requests and responses may contain a message header and message body that the support engineer can inspect using a protocol analyzer tool such as Wireshark. Traces of message headers and responses can provide valuable troubleshooting information.

An INVITE message, for example, would generate a message header with the following kind of content:

Field	**Description**
Via	Indicates the path taken by the request so far. The main purpose of the Via header is to ensure that responses take the same path as the requests so that responses can be routed back to the call initiator. A *Via* field value is added after the transport that will be used to reach the next hop has been selected. The entity that generates the header inserts its address in the *Via* field and all subsequent proxies that fall in the path also insert their own address as Via fields. A response that replies to a request keeps all the *Via* values in same order as they are received. Proxies that fall in the reply path then remove their own *Via* address and forward the response back. Hence, when the response reaches the call initiator it contains only the Via address of the call initiator. The call initiator strips off this Via value and finding that there are no more Via's left, processes the response. All requests must include a *Via* field. The protocol name and protocol version in the header must be SIP and 2.0, respectively. The field must also include a branch parameter. This parameter is used to identify the transaction created by the request. This parameter is used by both the client and the server
	Example 1: SIP/2.0/TCP servera.com:5060;branch=z9hG4bK74bf9 **Example 2:** (OK Response) Via: SIP/2.0/TCP servera.com;branch=z9hG4bK721; received=192.0.2.222 Via: SIP/2.0/TCP serverb.com;branch=z9hG4bK2d4;received=192.0.2.111 Via: SIP/2.0/TCP serverc.com;branch=z9hG4bK74b;received=192.0.2.101
From	The address of logical identity of the request initiator, possibly the user's address-of-record. The field contains a URI and optionally a display name. It is used by SIP elements to determine which processing rules to apply to a request. **Note: T**he field must contain a new tag parameter, chosen by the call initiator.
	Example: "Freddy" <sips:freddy@serverb.com>;tag=a48s
To	The address of the intended recipient of the request or the AOR of the user or resource that is the target of this request. **Note:** The field must contain a new tag parameter, chosen by the recipient. **Note:** The field always contains a tag once the dialog is established.
	Example: "Charlie"<sip:user2@serverb.com>;tag=6t3r
Call-ID	A unique identifier to group together a series of messages. It must be the same for all requests and responses sent by the calling and called parties within a dialog.
	Example: 123456@servera.com

Field	Description
Contact	Provides a single SIP URI that can be used to contact the sender of the INVITE for subsequent requests. The Contact header field must be present and contain exactly one SIP URI in an INVITE request that results in the establishment of a dialog. For these requests, the scope of the Contact is global. That is, the Contact header field value contains the URI at which the call initiator is expecting to receive requests, and this URI must be valid even if used in subsequent requests outside of any dialogs.
	Example: sip:bob@client.biloxi.example.com;transport=tcp

3.8.6 Troubleshooting Implications

A support engineer needs to be aware of the route the signaling and VoIP packets take through the network and which devices are involved.

If the problem with voice cannot be related to the correct settings of the SIP and VoIP parameters and the configuration of the IP-PBX used then a trace of the traffic flow may need to be done both on the wired LAN and the WLAN.

Tip: It can be very beneficial to use a fixed IP phone connected to the wired LAN as a terminal and thus quickly eliminate if there is a PBX problem or a WiFi problem. In this case there will also be just one AP and one VoWiFi Handset to troubleshoot.

4. Factors Affecting RF Propagation

There are many factors that can affect RF propagation and many of these factors concern the physical characteristics of the site such as its layout, design, floor plan and materials used in the site construction. Structural changes to the physical environment such as the moving of furniture and removing and setting up walls can cause permanent changes to the RF environment.

Many sites are also subject to dynamic elements than can adversely affect RF propagation. The RF propagation changes as people and objects move through coverages area. Even people leaving doors open, using cordless phones and Bluetooth devices and turning on all the microwave ovens at lunch time can all cause interference and increased noise, even though temporarily, in the RF environment.

RF signal propagation may also be affected by other APs and people roaming through the coverage area. Wireless APs and clients have therefore to constantly adapt to the changing RF environment, for example, by dropping the connection rate when an environment suddenly becomes noisier and restoring the connection rate when the environment quietens down.

When deploying dense WLAN networks, network administrators must therefore pay careful consideration to:

- The deployment of APs, particularly where there are many APs deployed in a relatively small area. Dense deployment of APs can cause RF interference with neighboring APs residing on the same or neighboring channels.
- RF interference and impedance from structural and temporary changes to the physical environment.

4.1 Jitter, Latency and Packet Loss

When the RF environment is compromised, the fundamental requirement of any system that transmits digitized voice signals over a WiFi network in the form of data packets may also be compromised. This is the requirement to preserve of the isochronous nature of the voice packet streams. Asynchronous pollution of the RF environment causes distortion to the voice quality and can occur when:

- The latency in voice packets exceeds certain limits, usually greater than 150ms in one direction or 300ms for both directions, between the receipt of each packet
- Delay variations from packet to packet, that is, jitter, that exceed 20ms
- Packet loss that starts to exceed 3%

Because voice signals have to travel across many network infrastructure components, packet loss, latency, and jitter can combine to reduce the signal quality especially when the network becomes congested with traffic. For additional information, always check the *Application Partner Program, Ascom Interoperability Report*s for specific recommendations applicable to the particular vendor equipment.

4.1.1 Signal Loss

RF loss is a decrease in the signal amplitude. There is always a clear and predictable loss as a radio signal propagates through the air, even if the airspace is completely unobstructed. The atmosphere causes the modulated signal to attenuate exponentially as the signal propagates farther away from the antenna. Signal loss can occur when metal, concrete, walls, or floors block transmission.

The physical site characteristics can considerably exacerbate signal loss because of obstructions in the airspace such as walls, doors and ceilings. The material used to manufacture and construct such obstructions can also affect the degree of signal loss. Therefore, the signal must have enough power to reach the desired distance at a signal level acceptable that the receiver needs.

4.2 Troubleshooting Methodology

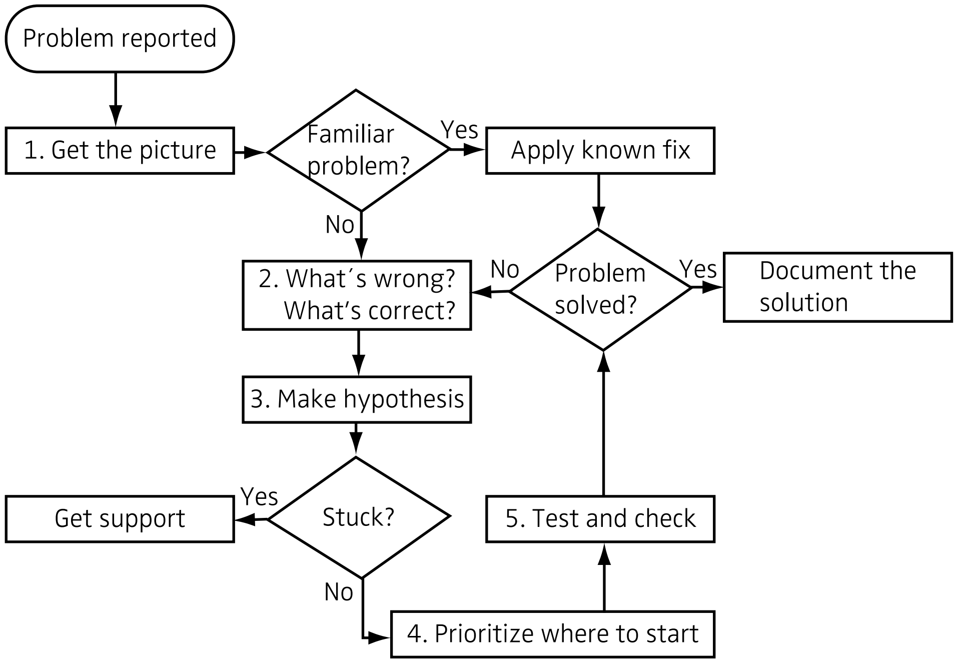
There are many troubleshooting models that can be used by a support engineer.

Many methods are based on a layered communication model with the root in the OSI or TCP/IP stack model and the models can be addressed as top-down or bottom-up approaches. Troubleshooting models also includes steps to take to try to define and isolate the problem area.

This guide does not describe troubleshooting theories in details, rather it will describe a suggested method that has successfully been used.

If the problem is in the LAN and WLAN infrastructure the support engineer has to learn the troubleshooting procedure that different vendors suggest in their operational guides. There is however usually a general approach that applies to most situations.

A very common method is a cycle model as illustrated below:



- Problem Reporting: Define the nature of the problems that users experience and the circumstances in which the problems arise. Problem types usually involve interruptions in the audio stream, disconnections, distortions such as echo and clicking noises, and delays. The user experiences that small discrete parts of the conversation are missing.
- Get the Picture: Try and elicit additional information from the user to try and picture the context and circumstances in which the problem occurs. For example, was the user stationary or roaming or in the proximity of other non 802.11 devices generating RF signals?
- Ascertain what is Working: In a complex installation like a VoWiFi system it is important to rule out the devices that are functional at an early stage of the troubleshooting process. Why a handset is not functioning when making a call depends on the correct function of several other devices.
- Form a Hypothesis: Make a list of possible causes. The fault is maybe on a device not primary a part of the solution, like a nonfunctional DHCP-server.
- Prioritize where to start. Eliminate causes that are quick to check first and do the more time-consuming later. Also eliminate causes that make less impact for the users first. Remember that whatever action you take may cause an interruption in the services. Make one change at a time and if problem is not solved unroll your new settings. Document what changes were done.
- Test and check: Make sure the appropriate tools are available for testing a proposed solution. If modifications to the LAN or WLAN are needed, liaise closely with those

responsible for managing and administering the network. Do not make unauthorized modifications.

Note: Do not change any security settings that will jeopardize the WLAN.

4.3 Isolate Problem Areas

An understanding of the above model can help in the troubleshooting process. A support engineer may use the model and ask questions and gather facts which relate to one of the protocol layers and thereby identify a single device, location or application that might be causing the problem.

In a top-down approach questions, like in the following example, can help the support engineer focus attention on a particular area. Start with testing the functionality of the applications and eliminate application configuration errors first:

Problem: A user cannot make a phone call.

Question	Layer tested	Result
Is more than one handset affected?	1-4	**Yes:** The problem may be on Level 2-4 but is probably caused by a malfunctioning PBX or WSG module. **No:** The problem is to be found in the single device.
Can a laptop reach the PBX or WSG through the WLAN by browsing or using ping?	1-3	**Yes:** This eliminates wrong configuration of the WLAN L2-L3. Combined with the question above it will remove L2 and L3 problems. **No:** Check WLAN settings in the system and handset.
Is both VoIP and WSG traffic affected or interrupted?	1-4	**Yes:** Check WLAN/LAN settings since something seems to block communication between the handset and PBX or WSG. **No:** This probably eliminates AP and LAN problems.
Is it possible to ping to the handset?	1-3	**Yes:** The problem is likely to be found in misconfigured parameters for VoIP or WSG in the handset or in the PBX or server platforms. **No:** Check WLAN/LAN settings since something seems to block communication between the handset and the PC.
Is it possible to ping from the handset?	1-3	**Yes:** The problem is likely to be found in misconfigured parameters for VoIP or WSG in the handset or in the PBX or server platforms. **No:** Check WLAN/LAN settings since something seems to block communication between the PC and the handset
Voice quality is unsatisfactory but calls still go through?	1-4	**Yes:** RF problem, QoS problem or misconfigured handsets. **No:** OK

Question	Layer tested	Result
Is the fault on more than one handset when used at a specific location?	1-3	**Yes:** The problem is in the AP and the network at that location or all handsets may be faulty. **No:** Check the specific handset configuration, for example, Differentiated Services Code Point (DSCP), channels used, power-save mode.

If using a bottom-up approach the same or similar questions as above can be used. In this approach the functionality of the radio is tested first (L1) and then continues upwards to check the access to the WLAN, then the LAN and last the services in that order.

When to use a top-down or bottom-up approach depends on which approach defines the problems fastest. To decide that, it is recommended to ask the following three questions:

- What information is available in the fault report?
- Has the problem been seen before?
- Are there well-known solutions to the problem?

The support engineer should be familiar with the handset startup-process as some issues may be due to initialization problems as the handset starts up. For additional information, see chapter 3.3 Handset Startup Procedure on page 10.

The support engineer should also be familiar with other typical questions used in troubleshooting. Examples of such questions are:

- Does the wired VoIP phone work?
- Has there been any redesign or equipment change in the installation?
- Has this problem been seen before?

5. The VoWiFi Handset as a Troubleshooting Tool

The handset provides the following kinds of built in troubleshooting tools that display information directly in the handset LCD:

- Information about the configuration of the handset. The *Device Info* menu is used by the support engineer to check handset configuration parameters.
- Information about the site that the handset operates in. The *Site survey tool* is used by the support engineer to check for possible RF problems caused by the layout of the site.
- The *Admin* menu for setting certain handset parameters and accessing logging tool menus for troubleshooting the RF environment

Handset commands are accessed using shortcuts. To use a shortcut, ensure that the handset main screen is displayed and then enter a shortcut in the format described below:

Shortcut	Information Provided
*#34#	Handset device information. See section 5.1 Handset Device Information on page 31.
*#76#	Turn on and turn off the Received Signal Strength Indicator (RSSI) display. See section 5.2.1 Show RSSI on page 31.
*#77#	Site survey tool. See section 5.2 Site Survey Tool on page 31.

5.1 Handset Device Information

The support engineer uses the handset information to check the values of parameters that define the configuration of the handset. Some of these entities are static, for example, the values of the software configuration parameters reflect the date, time and version of the last software upgrade. Other parameters however are dynamic, and vary under different circumstances. For example, the SSID and channel number parameters will change as the user roams through the network.

To display information about the configuration, select Menu > Settings > Device info or use the shortcut *#34#. Detailed device information about the configuration of the handset is described in Appendix B.1.

5.2 Site Survey Tool

The handset is the recommended tool for performing a site survey because of its radio performance. A laptop computer does not share the same characteristics as a handset and should not therefore be used to perform site surveys. To display site survey information in the handset, use the shortcut **#77#.

The site survey tool can be used to:

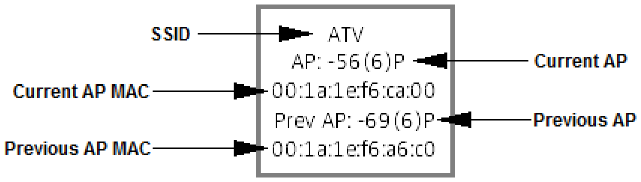
- Measure signal strength from all APs in the network
- Check for roaming candidates
- Detect areas with co-channel interference
- Detect rogue APs
- Check the channel plan, that is, check channel settings and APs coverage area.

5.2.1 Show RSSI

The *Show RSSI* menu item displays information in the handset LCD about the received signal strength, the current and previously associated APs and whether the handset is in power save or active mode during the association. To show RSSI information directly in the handset display without navigating through the *Site Survey tool* menu, use the shortcut **#76#.

The RSSI information is displayed directly in the handset display as shown in figure 13:

Figure 13. Handset SSID DIsplay



Note: In the example display above, the handset is in power save mode as indicated by the "P" following the RSSI and channel number of the associated and previously associated AP. A handset is in active mode is denoted by "A".

To turn off the RSSI display, reenter the shortcut **#76#*.

5.2.2 Creating Heatmaps

As a part of a troubleshooting procedure, it can be very useful to use the site survey tool to help create a graphical representation, or heatmap, of RF signal strengths surrounding an AP. The handset can be used to create a heatmap by sampling RF signal strengths in the vicinity of an AP and then superimposing these values on to a building plan where the exact location of the AP is shown. Several values can be selected for the handset *Beep range* and a heatmap of signal strengths can be drawn by repeated sampling. For additional information, see section 5.2.4 Range Beep on page 33.

5.2.3 Evaluate the Radio Environment

This section describes how to use the Site survey tool to evaluate the VoWiFi system RF environment.

Preparations in PDM or Device Management

1 When performing a site survey on the 2.4GHz band make sure that parameter *802.11b/g/n channels* are set to "All". The default is "1,6,11".

2 Set the *World mode regulatory domain setting* parameter to USA, ETSI or other listed countries.

Note: To scan channel 1-11, set the *World mode regulatory domain setting* parameter to "USA". If the scanning of channels 12-13 is also of interest, set the parameter to "ETSI".

3 Open the handset *Site survey tool* using the shortcut **#77#*.

4 Perform a site survey by selecting the following options from the site survey tool menu:

"Scan all channels": Returns a list of APs discovered for all available ESSIDs.

"Scan selected channel": Enter the required channel. This option returns a list of all the APs found on that channel regardless of ESSID.

Note: Be sure to walk slowly. Since the value is filtered sudden drops in field strength caused by the environment, for example walking through a door into a room, will be delayed. Thus it is important to walk slowly through the site to cover all weak spots.

Note: See also the section 5.2.2 Creating Heatmaps on page 32.

Note: It is important to remember to restore the handset to the channel and regulatory domain settings previously used if these were modified in steps 1 and 2 of this procedure.

5.2.4 Range Beep

A quick an easy way to check system coverage is to use the Range beep function. A beep is played in the handset whenever the handset measures a filtered field strength of below the configured value (default -70 dBm) from the currently associated AP.

To use the function, perform the following steps:

1 Open the handset *Site survey tool* using the shortcut *#77#.

2 From the *Site survey tool* menu, select the menu item *Range beep* and press the handset *Select* button

3 Enable the range beep function by selecting the *On* radio button. Press the handset *Back* button.

4 From the *Site survey tool* menu, select the menu item *Range beep level*.

5 In the *Level (-dBm)* field, enter the roaming threshold that the system is planned for. It is recommended to use -70dBm.

6 Walk through the site at a slow pace. If the RSSI for the handset drops below the value of the range beep level from the currently associated AP, the handset beeps.

Note: Occasional single beeps with a long interval in between is fairly normal as the handset moves through the edges of AP coverage areas. However, prolonged periods of repeated beeps point to coverages issues that need to be investigated.

Note: The roaming behavior is different between idle and call modes as described in the sections 3.6.1 Idle Mode on page 16 and 3.6.2 Call Mode on page 16 so the result of the coverage test will most likely differ when used in call and not. If the beep level is set to < -70dBm and the handset is in idle mode, the handset beeps at every roam because the roam level is set at -70bBm in idle mode.

Note: Because the measured field strength the value is filtered, sudden drops in field strength caused by the environment, for example walking through a door into a room, can be delayed. It is therefore important to walk through the site slowly to ensure that all weak spots are covered.

5.2.5 Coverage and Roaming Test

The purpose of the test is to verify that a handset is able to roam between different APs without losing connectivity or experiencing interruptions or distortions to the voice quality. The support engineer makes a call from a handset that can be physically moved around to another handset in a fixed location and then physically moves through an Extended Service Set (ESS).

1 Make a call from a handset that can be physically moved around to another handset in a fixed location.

2 Place a radio or other audio source playing music next to the handset at the fixed location.

Note: To be able to hear roaming delays, interruptions or distortions, a continuous audio source from a radio or MP3 player is recommended. A conversation between two people often consists of up to 50% of silent intervals and would not therefore be suitable for the test.

3 Walk around the site to find spots with weak coverage.

Note: Make sure that the walk takes place both directions to ensure that the handset has roaming options whenever the field strength drops low.

4 Make detailed notes of any areas where coverage is insufficient.

5.3 The Admin Menu

The *Admin menu* is a hidden menu for use by administrators and support engineers. To display the *Admin menu* enter Menu > Settings > 40022 from the handset main screen. The menus are used to:

- Provide an additional method for opening the *Device info* menu described in the section 5.1 Handset Device Information on page 31.
- Provide an additional method for opening the *Site survey tool* described in the section "Site Survey Tool" on page 31.
- Change certain parameters such as installing a handset, configuring the basic network settings, adding a license key or performing a factory reset. For additional information, see Appendix B.3.
- Configure some of the handsets WLAN, VoIP, WSG and Syslog parameters. These parameters are needed for accessing the built-in troubleshooting tools and configuring the handset so that trace and log information is available for external troubleshooting tools. For additional information, see Appendix B.3.

5.4 Handset Web Interface

The handset contains a small TCP/IP web server where system setup and troubleshooting information is maintained. This information can be accessed from a web browser in the following way:

1. From the handset, select Menu > Settings > Device info or use the shortcut **#34#*. The *Device info* menu is displayed.
2. Select the menu item *Network info* and note the value of the parameter *Phone IP*.
3. Open a web browser and enter the value of the *Phone IP* in the address bar. The handsets login panel is displayed together with information about the system under the *System* tab.
4. Locate and click the login link in the top right-hand corner of the panel. The *Windows Security* dialog is displayed. Enter the username "admin" and the password "changeme" and then click the *OK* button.
5. Click the *Troubleshoot* tab. The *Troubleshoot* pane is opened with the *Log*, *Statistics* and *Tools* tabs displayed.

5.4.1 Logs Tab

The Logs tab provides the following information from the links displayed to the left or the panel:

- *Info*: General information about the Log tab function
- *Syslog*: Real-time information about the actions taken by the handset, like setting up a call, WLAN changes and power level.
- *Errorlog*: The error log stored in the handset in case of a restart. Click the *Download* button to download the error log to your PC.

Note: The syslog and error log may contain information requested by support when responding to trouble reports.

5.4.2 Statistics Tab

The *Statistics* tab displays information about voice calls and WLAN connectivity:

Voice Call Statistics

Voice statistics can only be recorded for an active call. The statistics are collected from the RTP module and from the jitter buffer and concern the receipt and transmission of data frames containing RTP voice packets. The following statistics can be investigated by the support engineer for any values that might be indicating poor voice quality:

Rx Voice Packet Loss	The number of lost RTP frames relative to total number of transmitted and received frames.
Rx Voice Packets	The number of voice packets received during the call.
Tx Voice Packets	The total number of voice packets sent during the call.
Rx Min Pkt Interarrival time	The minimum time recorded during the call, in ms, between the receipt of one RTP frame and the receipt of the following frame.
Rx Max Pkt Interarrival time	The maximum time recorded during the call, in ms, between the receipt of one RTP frame and the receipt of the following frame.
Rx RTP Avg Jitter	The mean value of the RTP jitter over time. The value given is provided from samples with a default sampling rate of 8 kHz.

Performing a Voice Test

The following example illustrate how to use the handset web interface to check various statistics that might give an indication as to why voice problems are being experienced:

1 Start the handset web interface as described in steps 1 to 5 in the section ''Handset Web Interface'' on page 34.

2 Select the *Statistics* tab, *Voice* option. The *Voice Statistics* pane is displayed with the message ''No channel open'' displayed.

3 Connect a call from one handset to another. One of the handsets must be the handset with the IP address used to open the handset browser.

4 Complete the call but do not hang up.

5 From the *Voice Statistics* pane click the *Refresh* button and make a note of the voice statistics. The call may now be hung up.

6 Inspect the values of the statistics displayed in respect of the test being conducted. The following table illustrates some tests and conclusions that could be drawn from the values returned:

Test	**Description**
Jitter	Verify that the *Rx RTP Avg Jitter* statistic is reasonable, that is, less than ~100 samples per second, depending on codec used. The default codec is G711. This codec can be sampled 8000 times per second, which equals 0.125 ms for one sample. **Note:** During normal operation the ''Max Jitter'' may be quite high (~300 ms) even though there is no problem with the voice traffic.
Voice Packet Loss	Inspect the *Rx Voice Packet Loss* statistic. A loss of up to 5% for a WLAN is probably not noticeable if the packet loss is distributed evenly throughout the call.

WLAN Connectivity Statistics

WLAN statistics are cumulative from boot or from the last time the statistics were reset. The statistics return the following information about the number of transmitted and received RTP packets:.

RX packets	The number of RTP packets received.
RX bytes	The total number of bytes in the received RTP packets
RX dropped	The number of received RTP packets dropped.
TX packets	The number of RTP packets sent.
TX bytes	The total number of bytes in the sent RTP packets
TX dropped	The number of sent RTP packets dropped.

Performing a WLAN Test

The following example illustrate how to use the handset web interface to check various statistics that might give an indication as to why WLAN problems are being experienced:

1 Start the handset web interface as described in steps 1 to 5 in the section 5.4 Handset Web Interface on page 34.

2 Select the *Statistics* tab, *WLAN* option. The *WLAN Connectivity Statistics* pane is displayed.

Note: The statistics display cumulative totals. To reset the values to zeros, click the *Reset* button.

3 Connect a call from one handset to another. One of the handsets must be the handset with the IP address used to open the handset browser.

4 Complete the call but do not hang up.

5 From the *Voice Statistics* pane click the *Refresh* button and make a note of the WLAN statistics. You may now hang up.

6 Inspect the values of the statistics displayed in respect of the test you are performing. The following table illustrates some tests and conclusions that you could make from the values returned:

Test	**Description**
Voice Packet Loss	Verify that the *Rx Voice Packet Loss* statistic is reasonable, that is, less than ~5% for a LAN.

5.4.3 Tools Tab

The Tools tab provides the *Ping* and *Traceroute* utilities

Ping

Ping is used to test whether or not a host on an IP network can be reached and to measure the round-trip time for messages sent from the originating host to a destination such as an IP PBX, WSG server, router or a handset.

To run Ping, select *Ping* from the *Tools* pane and enter the IP address of the destination. The results of the ping is statistical summary of the response packet received and the round-trip time taken for the packet in the message to be sent and received. For example:

```
Reply from ::ffff:10.30.32.166: bytes=32 time=28ms TTL=127
```

The destination IP is pinged ten times.

The following output indicates that the device has not been reached:

```
Request timed out
```

The following output indicates that the device is taking an unusually long time to be reached:

```
Reply from ::ffff:10.30.32.166: bytes=32 time=2738ms TTL=127
```

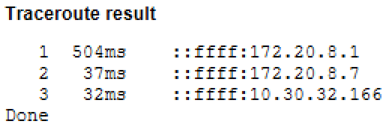
Note: The Time to Live (TTL) can be used to determine approximately how many router hops the packet has gone through. If the TTL field varies in successive pings, it could indicate that the successive reply packets are going via different routes, which is not desirable.

Traceroute

The traceroute utility is a network diagnostic tool for displaying the route and measuring transit delays of packets between two devices across an IP network. One device is usually a handset making a call and the other device is the device to be reached, such as a handset or a PBX or WSG server.

To run traceroute, select *Traceroute* from the *Tools* pane and enter the IP address of the device to be reached from the calling device. The result of the traceroute looks like this

Figure 14. Traceroute Result



Traceroute result

```
   1  504ms    ::ffff:172.20.8.1
   2   37ms    ::ffff:172.20.8.7
   3   32ms    ::ffff:10.30.32.166
Done
```

5.4.4 Quality of Service (QoS) Test

It is important to perform a QoS test on all possible call scenarios such as calls between handsets on the same APs or controller, on different APs or controller, between handsets and fixed phones, and internal to external phones. QoS tests can be performed using handset web interface in the following way:

1. Login to the web interface and open the *Troubleshoot* pane as described in the section 5.4 Handset Web Interface on page 34.
2. Make a call from the handset.
3. On the left of the Troubleshooting panel, locate and select *Syslog*. A dump of the syslog is displayed.
4. Locate the row in the log with an entry of Voice Rx. Check that the handset has received voice data in the voice queue (UP 6) by verifying that the Syslog entry is as follows:

   ```
   Voice Rx IP DSCP: 0x2e UP: 6
   ```
5. Locate the row in the log with an entry of Voice Tx. Check that the handset has sent voice data in the voice queue (UP 6) by verifying that the Syslog entry is as follows:

   ```
   Voice Tx IP DSCP: 0x2e UP: 6
   ```

   Note: The DSCP channel value is set in handset parameter *IP DSCP for voice* and should be set to match the LAN/WLAN configuration. The handset parameter is displayed from the PDM Edit parameters > Network > Active network.

   Note: The UP value displayed in Syslog is from the first voice package at call startup. To ensure that all voice data is sent in the voice queue perform an air trace such as that described in Appendix A.

   Note: The handset always sends voice data in the voice queue (UP 6) unless CAC/ TSpec settings in the WLAN system prevent it from doing so. Traffic Specification (TSpec) lets a 802.11 client signal its traffic requirements to an AP.

6. Troubleshooting Scenarios

This section illustrates, through examples, how a support engineer might approach SIP call problems by analysing the setup and flow of a call between two parties. The section focuses upon how traces and logs of SIP signaling and RTP voice packet flows can be analyzed, the kinds of information these sources provide, and how this information can be used by the support engineer to identify problems. The section therefore suggests an approach to troubleshooting issues rather than providing a single definitive method for resolving issues.

6.1 SIP

The following troubleshooting scenarios are described:

- Attended Transfer problem and one-way audio: user1 places a call to user2, and user2 transfers the call to user3. However, either user3 cannot hear user1 or user1 cannot hear user3. In this scenario, user1 is the call transferee, user2 the call transferor and user3 the call target.
- Name Presentation problem: user1 places a call to user2, but when user2 accepts the call, user2's number is not displayed on the handset of user1.

Depending on the configuration and functionality of the SIP proxy the RTP stream may be passing through the SIP proxy or may be routed directly between the handsets.

A support engineer needs to be aware of the route the signaling and VoIP packets take through the network and which devices are involved.

If the problem with voice cannot be related to the correct settings of the SIP and VoIP parameters and the configuration of the IP-PBX used then a recording of the traffic flow may need to be made on both the wired LAN and the WLAN.

Tip: It can be very beneficial to use a Fixed IP phone connected to the wired LAN as a terminal and thus quickly eliminate if there is a PBX problem or a WiFi problem. In this case there will also be just one AP and one handset to troubleshoot.

6.1.1 Attended Transfer Example

A call transfer happens when user2 transfers a call from user1 to another user, say user3. The sequence of the transfer is as follows:

1 user1 (number, for example: 4111) dials user2's number 4112 and presses the handset *Call* button.

2 user2 accepts the call by pressing the handset *Accept* button and begins a conversation with user1. user1's number 4111 is displayed in user2's handset.

3 During the conversation the parties agree that user1 should be talking to user3 instead. user2 agrees to transfer the call to user3.

4 user2 presses the handset *More* button and selects the menu item *Tranf. to new*

5 user2 enters 4113, the number of user3, in the *Transfer to* input field, then clicks the *OK* button. A *Transferred* message is displayed in user2's handset.

6 user3's phone rings with 4111, the number of user1, displayed in the handset.

7 user3 selects *Accept* and begins the conversation with user1. user3's number 4113 is displayed in user1's handset.

8 The conversation between user1 and user2 is dropped and user2's handset reverts to displaying the idle screen.

9 user1 and user3 continue the conversation until one of the parties hangs up.

The following sections describe the exchange of SIP requests and responses required to support the transfer scenario described above. The scenario from a signaling perspective occurs in three broad steps:

- RTP sessions are established between the users but are then put on hold pending the transfer
- The signaling of the actual transfer takes place; existing RTP sessions are terminated between the transferee (user1) and transferor (user2) and transferor and transfer target (user3). A new RTP session is established between user1 and user3.
- One of the parties terminates the call, and a final exchange of SIP messages takes place to signal the completion of the call.

Parties on Hold with Transferor

The flow of SIP messages in the setup between user1 and user 2 analogous to any conventional SIP call between two parties such as that depicted in Appendix 10. The initial INVITE message creates a header that would contain the following kind of sample data:l

INVITE user1 -> user2

From: user1 <sip: user1@servera.com>;tag=u1

To: user2 <sip: user2@serverb.com>

Call ID: u1-to-u2-cid

However, after the establishment of an RTP session between the parties, user2 initiates a transfer of the call from the handset to user 3. This requires user2 to start the transfer by putting user 1 on hold in the following way:

1 user2 sends user1 an INVITE to hold the current RTP exchange. The message header contain the following sample data:

INVITE (hold) user2 -> user1

From: user2 <sip: user2@servera.com>;tag=u2

To: user1 <sip: user1@servera.com>;tag=u1

Call ID: u1-to-u2-cid

2 user1 responds with a 200 OK

3 user2 acknowledges with ACK

4 user1 indicates that it now neither wishes to send nor receive media from user2 by marking the RTP stream as inactive through the SDP session attribute "a=inactive".

5 The RTP exchange stops and user1 is now on hold

user2 announces the transfer to user3 with a dialog of messages that is again identical to a conventional SIP call, up to the establishment of an RTP exchange. The initial INVITE message creates a header with the following sample data:

INVITE user2 -> user3

From: user2 <sip: user2@servera.com>;tag=**u2-2**

To: user3 <sip: user3@somewhereelse.com>

Call ID: u2-to-u3

Of significance is the new user 2 tag, u2-2, associated with the invite. A new user2 tag is required to differentiate between the tag used with user1 and the tag used with user3.

The dialog with user3 must also indicate that there is a pending transfer and this is also achieved through an INVITE to hold message from user2 to user3. user2 puts user3 on hold with the following dialog:

1 user2 sends user3 an INVITE to hold the current RTP exchange between user2 and user3:

INVITE (hold) user2 -> user3

From: user2 <sip: user2@servera.com>;tag=u2-2

To:	user3 <sip: user3@somewhereelse.com>; tag=u3
Call ID:	u2-to-u3

2 user3 responds with a 200 OK

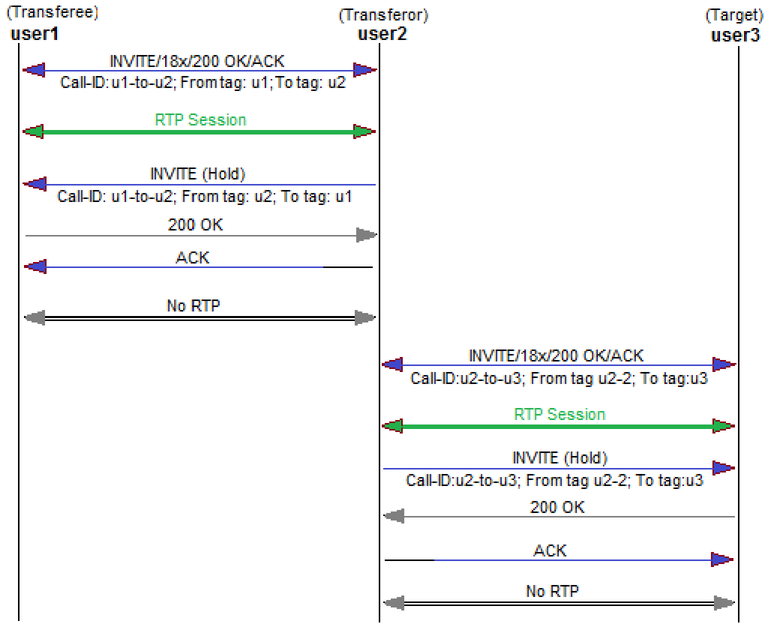
3 user2 acknowledges with ACK

4 user2 indicates that it now neither wishes to send nor receive media from user3 by marking the RTP stream as inactive through the SDP session attribute "a=inactive".

5 The RTP exchange stops and user3 is now on hold

The situation as it currently stands is summarized in figure 15:

Figure 15. SIP Attended Transfer


(Transferee)
user1
(Transferor)
user2
(Target)
user3
INVITE/18x/200 OK/ACK
Call-ID: u1-to-u2; From tag: u1; To tag: u2
RTP Session
INVITE (Hold)
Call-ID: u1-to-u2; From tag: u2; To tag: u1
200 OK
ACK
No RTP
INVITE/18x/200 OK/ACK
Call-ID:u2-to-u3; From tag u2-2; To tag:u3
RTP Session
INVITE (Hold)
Call-ID:u2-to-u3; From tag u2-2; To tag:u3
200 OK
ACK
No RTP

In step 3 above, the 200 OK from user3 is also of significance as the OK message header now holds the call id and the From and To SIP URIs are now tagged with values so that all subsequent messages can now be associated with the previous INVITE message.

Transferee to Target Transfer

The next step is for user2 to refer user1 to user3 so that an RTP exchange can ultimately take place between user1 and user3.

When the transferor user2 gets an indication that the target is ringing, it sends the transferee a Refer request (RFC 3515) with a Replaces header in the Refer-to header. The Refer-to header instructs the transferee user1 to issue a triggered SIP INVITE request to the target user3, to transfer Call-ID u2-to-u3 from user2 to user1. The REFER message includes the following information for achieving the referral, for example:

REFER user2 -> user1

From:	user2 <sip: user2@servera.com>;tag=u2-2
To:	user1 <sips:user1@servera.com>;tag u1
Call ID:	u1-to-u2
Refer-to	<sips:user3@somewhereelse.com?Replaces=u2-to-u3; to tag=u3; from tag=u2-2; Require=replaces>
Referred-by	<sip: user2@serverb.com>

user2 puts user1 on hold then calls user3 to announce the transfer, then places user3 on hold. user2 transfers user1 to user3, which replaces the session between user2 and user3. user3 then disconnects the session with user2. user1 reports success of transfer to user2 with an ACCEPTED message and user2 now disconnects with user1. In this example, the Replaces header [RFC3891] is copied into the Refer-To URI by user2. Note that the Refer-To URI is the Contact URI returned by user3 in the 200 OK response. This ensures that only the correct instance of user3 is reached.

The way is now clear for user1 to setup a signaling relationship with the final recipient user3 and replace the RTP session between user2 and user3. The Replaces header indicates that the initial call leg identified by the Call-ID u2-to-u3 is to be shut down and replaced by the incoming INVITE request:

INVITE user1 -> user3

From:	user1 <sips:user1@servera.com>;tag=u1-2
To:	user3 <sips:user3@somewhereelse.com>
Call ID:	u1-to-u3
Replaces:	u2-to-u3;to-tag=u3; from-tag=u2-2
Supported:	replaces

During the signaling setup, user1 keeps user2 informed about the progress of the setup through one or more NOTIFY requests.

The first NOTIFY request from user1 receives a provisional 180 response from user2 to confirm that it’s INVITE to setup the call to user3 is proceeding and that the subscription between user1 and user2 is active. During the user1 to user3 setup, user1 must wait, for up to 60 seconds, until the setup is complete. The NOTIFY includes the following field indicating this subscription state:

NOTIFY user1 (Transferee) -> user3(Target)

Subscription-State active; expires=60

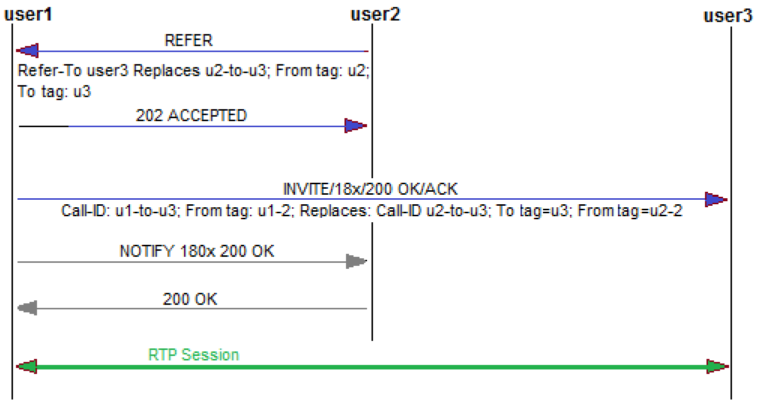
On expiry of 60 seconds, a further NOTIFY can be issued. This NOTIFY receives a 200 OK response from user2 confirming user2’s release from both user1 and user3. The NOTIFY includes the following kind of information to reflect this state:

NOTIFY user1 (Transferee) -> user2(Transferor)

Subscription-State terminated; reason: =noresource

The RTP session between user1 and user3 is now established:

Figure 16. Transferee to Target Transfer


user1
user2
user3
REFER
Refer-To user3 Replaces u2-to-u3; From tag: u2;
To tag: u3
202 ACCEPTED
INVITE/18x/200 OK/ACK
Call-ID: u1-to-u3; From tag: u1-2; Replaces: Call-ID u2-to-u3; To tag=u3; From tag=u2-2
NOTIFY 180x 200 OK
200 OK
RTP Session

6.1.2 PBX Basic Call Analysis

A more common architecture than the RFC example described in section 6.1.1 Attended Transfer Example on page 38 above is a network architecture that relays calls between two or more parties via an IP-PBX, which may also be called a Back-to-Back User Agent (B2BUA). It is this kind of scenario where a detailed knowledge of a call flow is required because a PBX performs functions that a proxy does not perform, such as hiding the identity of the initiator of the call from the destination, enabling header modification and SDP manipulation of codecs, media IP and Port, and so on.

A B2BUA acts as an endpoint to the calling party and then creates a new call to the called party. The B2BUA therefore is an intermediate point in the call between remote endpoints. The PBX contains functions to manage and control the call between the remote endpoints.

Other SIP functions, for example when calls are transferred to an additional party using REFER, involve additional PBX functionality.

A call established through a PBX requires that a signaling connection initially be established by the calling party to the PBX and then for the PBX to establish a connection to the called party. From a SIP perspective, there are two different calls established with two different Call-IDs.

The following is a real-life example of a basic SIP call setup via a PBX where:

- The calling party has the extension of 9910.
- The called party has the extension 9920.
- A SIP server has the IP address of 10.11.24.244. The server functions as a registrar and defines the locations of users registered with it, for example 9910@10.11.24.244 and 9920@10.11.24.244.
- The first call has the Call-ID of **4af6 and the second call a Call-ID of **02fd.

To facilitate the analysis of the call flow, the handset needs to be setup to support Remote Packet Capture (RPCAP) logging and a trace is taken using Wireshark. For additional information, see Appendix D.2.

Note that for the sake of clarity in the following example, only the last four characters of the call ids are used.The asterisks denote the excluded part of the respective Call-IDs.

After these calls have been setup, RTP streams are transmitted from Party 9910 to Party 9920 and vice versa via the PBX.

The first call setup is established with an INVITE from the calling party to the called party, and the creation of the call ID **4af6 between the calling party and the PBX:

INVITE sip:9920@10.11.24.244

From:	"9910"<sip:9910@10.11.24.244>;epid=00013e124af6;
	tag=2363920757

To:	<sip:9920@10.11.24.244;user=phone>
Call ID:	ab5e5a3de909d311b77400013e124af6@10.11.24.177
P-Preferred-Identity:	"9910" <sip:9910@10.11.24.244;user=phone>
Referred-by	<sip: user2@serverb.com>

The P-Preferred-Identity header field is used from a user agent to the PBX to carry the identity the user sending the SIP message wishes to be used for the P-Asserted-Header field value that the PBX will insert. Using this method the PBX can indicate what identity should be presented to the called party and what identity should be used for authenticating the call. This feature is also useful when the PBX redirects an incoming call to a PSTN number, for example a cell phone, to preserve the original Caller ID.

In the next message, the PBX issues a Proxy-Authenticate header consisting of a challenge that indicates the authentication scheme and parameters applicable to the proxy:

SIP/2.0 407 Proxy Authentication Required

From:	<sip:9910@10.11.24.244>;epid=00013e124af6;
	tag=2363920757

To:	<sip:9920@10.11.24.244;user=phone>;tag=3629151890
Call ID:	ab5e5a3de909d311b77400013e124af6@10.11.24.177
Proxy-Authenticate:	Digest realm="10.11.24.244",nonce="2af9fe71e909d311", qop="auth",algorith

The INVITE is acknowledged as follows:

ACK sip:9920@10.11.24.244

From:	"9910" <sip:9910@10.11.24.244>;epid=00013e124af6;
	tag=2363920757

To:	<sip:9920@10.11.24.244;user=phone; tag=3629151890>
Call ID:	ab5e5a3de909d311b77400013e124af6@10.11.24.177
Contact:	<sip:9910@10.11.24.177:5060;transport=UDP>

The calling party 9910 now responds to the challenge contained in the 407 response for required authentication by resending the initial INVITE request; however, this time the INVITE request includes user 9910’s authorization credentials contained in a Proxy-Authorization header:

INVITE sip:9920@10.11.24.244 (with proxy authentication)

Proxy-Authorization:	Digest username="9910", realm="10.11.24.244",
	nonce="2af9fe71e909d311",
	response="245f23415f11432b3434341c022"

From:	"9910" <sip:9910@10.11.24.244>;epid=00013e124af6;
	tag=2363920757

To:	<sip:9920@10.11.24.244;user=phone>
Call ID:	ab5e5a3de909d311b77400013e124af6@10.11.24.177
Contact:	<sip:9910@10.11.24.177:5060;transport=UDP>
P-Preferred-Identity:	"9910" <sip:9910@10.11.24.244;user=phone>

The PBX now attempts to establish a connection with the called party. The PBX updates the name information field with a P-Asserted-Identity of ‘’Charlie’’ to assert the identity of the originator:

INVITE sip:9920@10.11.24.246:2051

From:	"Charlie" <sip:9910@10.11.24.244;user=phone>; tag=3629151892
To:	<sip:9920@10.11.24.244;user=phone>
Call ID:	88f277aee909d311942f0090331e02fd@10.11.24.244
Contact:	<sip:9910@10.11.24.244:5060;user=phone;transport=TCP>
P-Asserted-Identity:	"Charlie" <sip:9910@10.11.24.244;user=phone>

The calling party now responds to the PBX with the name ‘’Charlie’’ that has been assigned to it in a 180 RINGING response to the INVITE:

180 Ringing

From:	"Charlie" <sip:9910@10.11.24.244;user=phone>; tag=3629151892
To:	<sip:9920@10.11.24.244;user=phone>;tag=4184284236
Call ID:	88f277aee909d311942f0090331e02fd@10.11.24.244
Contact:	<sip:9920@10.11.24.246:2051;transport=TCP>
P-Preferred-Identity:	<sip:9920@10.11.24.244;user=phone>

The PBX updates the 180 RINGING with the name "Freddy" in the P-Preferred-Identity, thus asserting ‘‘Freddy’’ as the name of the called party. The 180 RINGING is sent back to the originator of the call so that ‘‘Freddy’’ is presented to the originator before the call is actually answered:

180 Ringing

From:	"9910" <sip:9910@10.11.24.244>;epid=00013e124af6; tag=2363920757
To:	"Freddy" <sip:9920@10.11.24.244;user=phone>; tag=3629151891
Call ID:	ab5e5a3de909d311b77400013e124af6@10.11.24.177
Contact:	<sip:9920@10.11.24.244:5060;user=phone;transport=UDP>
P-Preferred-Identity:	"Freddy" <sip:9920@10.11.24.244;user=phone>

The final ACKS and 200 OK result in the RTP media session being established.

6.1.3 Identifying Problems

A problem that can occur is that one party cannot hear the other party. In this example scenario, an analysis of the trace reveals that despite the problem, signaling has been completed successfully. In this situation the support engineer should:

- Take a Wireshark trace and expand the message headers to check for errors in the SDP negotiation, such as codecs or ports. To do this, the handset needs to be setup to support RPCAP logging as described in Appendix D.2.
- Take a trace from the handset that is unable to hear the other party and establish whether or not RTPs packets are being sent to the handset.
- Determine where RTPs are being sent, for example, are they being sent to the correct port or the correct IP address.

Check SDP Negotiations

There are a number of different SDP negotiations between endpoints that can be considered and investigated in response to problems such as one way audio. The negotiations that should be focused on and investigated through a trace from the wired LAN are:

- Port negotiation. Check that the correct port numbers are used for the RTP session.
- IP address negotiation: Check whether or not the other party has updated its SDP with its IP address.
- Payload negotiation: Whether the correct codec has been configured.
- DTMF negotiation. DTMF may be generated inband or through SIP info.
- Packet interval negotiation: check whether the RTP packet interval between the endpoints is too great. For example, one way audio may be the result of the receiving end supporting a minimum packet interval of 30 ms while the sending end negotiates that packets are sent every 20 ms.

Send the trace to support for further analysis.

Make sure that the attributes of the SDP signaling on either side are correct and that the RTP stream is bidirectional.

Check that one of the parties is not still on hold.

Refer to RFC 3665 for additional information. This describes the best common practice for SIP calls.

Voice Activity Detection

Voice Activity Detection (VAD) detects if the speaker is silent. To save bandwidth, the transmitting device refrains from transmitting RTP packets for the duration of the silent period. However, total silence can also lead to problems such as a perception by the parties that the call has been dropped, sudden jarring changes in noise levels as the conversation is resumed, and a general choppiness to the overall conversation.

To ameliorate these effects, a synthetic background or so called comfort noise may be used to fill the silent periods and make them sound more natural.

When troubleshooting one way or no audio problems, check if one of the parties is using VAD and comfort noise. If, for example, the other end is not being heard, then turn off VAD at that end to see if that resolves the issue.

6.1.4 Name Presentation Problems

Names are presented in a header in SIP messages, for example "Charlie" <sip:Charlie@10.11.24.244>.

Name updates are an issue with transfers or call diversions. The kinds of problems that arise when names are missing from SIP headers are:

- The intended recipient of a call has moved temporarily or permanently but cannot be reached by the calling party
- The called party details are not displayed in the calling party’s handset.

There are three methods of naming used by handsets that are used in the following order of priority:

1 P-Preferred-Identity/P-Asserted-Identity: A call from a handset uses P-Preferred-Identity and then the PBX changes it to P-Asserted-Identity. It might also add a name to the P-Asserted-Identity. For example, the user may also suggest a name in the form "NAME"<SIP URI>.

2 Remote party ID (Cisco compatible naming).

3 From field. A SIP header From field is used, that is, the "NNNN" part of the from field where the field contains " NNNN" <SIP URI>.

Of importance to the support engineer is the content of these headers when they reach the calling or called parties. The header information is sent in the 18x provisional messages and 200 OK messages.

6.2 WLAN Troubleshooting Scenarios

This section illustrates, through examples, the kinds of performance issues that may arise when operating a handset in a WLAN. Because the characteristics of sites using VoWiFi and the issues experienced by users are likely to be very different, it would be difficult to provide a single definitive method for resolving issues. Instead, the information in this section suggests an approach to investigating and solving common WLAN issues.

6.2.1 Voice Problems while Roaming

User experience voice problems, both poor voice quality or audio gaps while moving through the site.

Software

Check that the WLAN and handset have compatible software versions and are configured properly:

1 Using the shortcut *#34# open the handset *Device Information* menu and select *Software*. Note the value of the *SW version* parameter.

2 Obtain the *Application Partner Program, Ascom Interoperability Report*s for vendor equipment from the Ascom Partner web site.

Analyze Result

3 Check that the WLAN and handset have compatible software versions and are configured according to interoperability report. Are incorrect configurations or software version incompatibilities found?

Yes: Perform a system upgrade or open the PDM to reconfigure parameters,

No: Go to the section Coverage.

Coverage

Check the RF coverage with the built in Site Survey tool:

4 Using the shortcut *#76# activate the RSSI screen

5 In idle mode, slowly walk around the site, noting the RSSI at frequent intervals.

6 Repeat the procedure in step2 in call mode.

Analyze Result

7 The signal strength should not fall much below -70dBm. Does the signal strength fall below -80dBm?

Yes: There are coverage gaps that may explain the problem the customer is experiencing.

No: Go to the section Roaming.

Roaming

Check if audio problems are present while moving through the site in call mode:

8 Make a call to another party and move through the site while holding a conversation with the other party.

9 During a call, with the RSSI screen activated, monitor the RSSI value and see if the audio problem is experienced during the handset roam.

Analyze Results

10 Are audio problems experienced?

Yes: Go to step 14.

No: Investigate possible problems caused by incorrect QoS settings, RF access problems and internal interference described in steps 11 to 13.

QoS

11 Control QoS in the handset Syslog and confirm that both Rx and Tx have UP 6, if not QoS needs to be corrected in the LAN/WLAN. For additional information, see section Figure 14. Traceroute Result on page 37.

RF Access

12 Is CAC or TSpec implemented?

No: Go to step 13.

Yes: Go to step 17.

13 Investigate whether load balancing or Call Admission Control (CAC) can be Implemented to ensure that voice traffic has access to the RF. Use a protocol analyzer to analyze RF traffic. Inspect the WLAN controller log for any errors or system overloads.

14 In case RX is not set in UP6 (Voice AC), make sure that both handset and system is configured to utilize CAC. Before a client can send traffic of a certain priority type, it must have requested to do so via the TSpec mechanism. For example when a handset wants to use the voice AC it must first make a request for use of that AC via the action frame type ADDTS. If the voice AC is controlled by TSpec, the system must grant the handset access to the requested AC before it could be used. In case no TSpec request is sent, all downlink traffic will be directed to BE. For additional information, see section Figure 14. Traceroute Result on page 37.

15 Perform an air trace to determine whether the ADDTS action frames are exchanged successfully and that the system grants the handset access to the voice AC (Status code: Admission accepted). For additional information, see Appendix A.

16 Does the handset display the message ''Network busy'' when attempting to establish a call?

Yes: There is no access to the medium, that is, the system is declining the clients request to use the voice AC. Go to step 17.

No: Go to the section External Interference.

17 Check system utilization

If the system utilization is reaching the limit set for when a new call is allowed to be established, then CAC/TSpec are functioning as they should by limiting the number of calls accepted and thereby preventing the network from becoming congested

If the system utilization is low and the ''Network busy'' message is still displayed, this indicates that the thresholds for CAC/TSpec are incorrectly set.

External Interference

18 External interference may occur when VoWiFi devices are forced to share the RF spectrum with other devices. Such devices often create interference for wireless LAN users. Perform a site survey with a spectrum analyzer to identify sources of interference.

Check RTP Traffic

19 Perform an air trace of a roam to determine whether or not RTP data is both sent and received by the handset. If RTP data isn't received by the handset investigate that the LAN switch is routing the RTP to the AP correctly. For additional information, see Appendix A.

Security

If Extensible Authentication Protocol (EAP) security is used, check if the full EAP exchange is performed during the roam with an air trace or log of the Radius server. Normally the key-caching function in the WLAN system and handset prevent a full EAP exchange during roam.

7. VoWiFi Handset Problem Solving Scenarios

7.1 Handset Errors

This section describes fault messages in the handset display and also other faults that can be rectified using the handset troubleshooting tools.

7.1.1 Startup Problems

Fault	Probable cause	Action
The display stays dark or handset does not boot.	Low battery level or faulty handset.	Charge the battery. If the handset does not work after charging, replace the handset.
The handset hangs during the boot process.	A failed upgrade of the software.	Use the rescue operation and try to recapture the handset with the old software, see Recapture the Earlier Software on page 48.
No main menu is displayed. Device info shortcut is available on the right softkey.	The handset is factory reset and has no access to any WLAN or has the wrong WLAN parameters set.	Store the required WLAN parameters in the handset using the PDM. Alternatively, use the *Admin menu* described in the section 5.3 The Admin Menu on page 34.
Remotely updated	The handset restarts after a parameter upgrade.	

Recapture the Earlier Software

To boot the old firmware perform the following procedure:

1 Press and hold the keys 7 and 8 and press the On/Off key at the same time.

The handset displays the message "Using the backup application" and a bar-graph.

2 The handset loads the earlier software and keeps it until it is restarted.

Tip: Use this function when comparing functionality between software versions.

7.1.2 Errors Displayed on the Handset

A "No Network" message indicates a Layer 1 or layer2 fault. If there is no access to the WLAN, there is no AP to associate with, which may be caused by the handset being out of range or by incorrectly configured WLAN network parameters.

The signal strength bar graph indicates that no signal is being received and the handset starts to beep once per minute. A vibrator may also be configured to indicate that no signal is being received by accessing the parameter Device > General > No system warning. If the parameter is set to "Sound repeatedly", the vibrator is turned on and the handset vibrates for up to 30 minutes.

Tip: To turn off the beep, press the mute button on the left side of the handset.

Examples of incorrect WLAN parameter settings include:

- Incorrect network profile selected
- Missing or incorrect SSID
- Incorrect security parameters
- Incorrect radio settings.

Check Incorrect Network Profile

1 From the PDM, *Edit parameters* dialog, select Network > General and inspect the value of the *Active network* parameter.

2 Check that the correct system (A, B, C or D) setting is selected. (The handset may be configured for four different sets of WiFi parameters). This can be checked from the *Connections* menu and the *Device Manager,* Network > General menu. If the parameter *Auto-switch network* is "Enabled", make sure that the Network is included in the auto-switch network. To confirm this, check that the Network's parameter *Include in auto-switch network* is set to "Yes". Note that this parameter is only visible when *Auto-switched network* is enabled.

Check Missing or Incorrect SSID

1 From the handset, select the PDM menu Network > Network or from the handset display select Admin menu, Network setup > SSID.

Note: The SSID is case sensitive.

2 Inspect the value of the SSID in the handset display.

Check Security Parameters

1 From the PDM, Edit parameters dialog, select *Network*.

2 From the list of Network A, B, C and D select the active network.

3 From the handset, select the PDM menu Network > Network or from the handset display select *Admin menu*, Network setup > Security mode.

Note: Security settings, that is, authentication and encryption must match the settings in the WLAN infrastructure.

4 Check for 802.11d multi-regulatory domain settings.

The handset has a parameter specifying whether or not 802.11d should be used. This is normally provided by the infrastructure according to the 802.11d amendment. If this is not the case, the domain code must be set in the handset using the PDM.

Check Radio Settings

1 From the PDM, Edit parameters dialog, select *Network* and from the list of Network A, B, C and D select the active network. Alternatively, from the handset display, select *Admin menu* then Network setup > 802.11 protocol.

2 Inspect the value of the *802.11* parameter and make sure the correct protocol value is configured.

3 Inspect the value of the *802.11<protocol> channels* parameter and check what channels are used.

Note: The handset uses by default the channels 1, 6 and 11 for the 2.4 GHz band. If the infrastructure is configured to use any other channel, change it to use only 1, 6 and 11 as this is the recommended setting. If the WLAN is using another channel scheme like 1, 7, 13 (not recommended because chances are higher for other-channel interference) the channels must be set in the handset using the PDM.

Check that for the 5 GHz band, that the channels that are selected, are the same as the network channels. The default value is "All". A good choice is to use one of the preset UNII band selections. It is also possible to manually enter the channel numbers, to exactly meet the setup of the Voice WLAN.

Note: The handset can use the DFS channels in a Voice enabled WLAN, but the Voice quality can be distorted as the DFS channels must be treated differently in the scanning process. See section 3.7 DFS Channel Probing on page 17.

7.1.3 No Access

A "No access" message indicates a Layer 3 fault. The handset has successfully associated with an AP but it cannot connect to either the IP-PBX or the WSG system. This may be because the application services are not running or the services are running but the handset is unable to connect to the services due to faulty IP address configuration.

Tip: A support engineer will often need to check for problems on the wired side of the installation as well as the wireless side and should be equipped with adequate tools for troubleshooting wired LANs.

1 Check IP address. From the handset Device info > Network info menu described in Appendix B and inspect the value of the *Phone IP* parameter to see if the handset has an IP address.

- If using static IP addresses: Check that the settings are correct and that there is no IP conflict with another device. Pay special attention to the value of "Default gateway" if the IP PBX is on another subnet or VLAN.

- If using DHCP-server delivered IP addresses: Check that there is connection to the DHCP server.

2 DHCP problems may also be the case if the there is no access to the DCHP server in a LAN that is segmented using subnets or VLANs.

To test DHCP problem perform one or more of the following steps:

- Try to set the IP-address parameters manually. If access is restored it clearly indicates a DHCP problem.

Tip: To exclude TCP/IP stack problems in the handset, ping the handset from a laptop and also browse to the handset's web interface.

- Use a laptop with a wireless card to see if the laptop receives an IP address.

- Use a wired connection to the same switched network/VLAN as the AP (or controller) is connected to, to test if it receives an IP address over DHCP.

- It is also possible to take help of a network administrator and try to ping to or from an AP or other device to the DHCP server. If this is successful the DHCP problem is in the wireless part of the site.

Tip: If a wireless sniffer is available, configure it for the correct encryption key and try to decode packets both from and to the handset.

If the handset initiates the DHCP handshake function, the problem is that the AP isn't forwarding DHCP offers or the wrong address is sent out. Check for the possibility that the WLAN internal DHCP server does not work.

A common cause is that the VLAN/SSID/USER CLASS mapping is wrong and that the DHCP server cannot be reached from the wireless side.

3 If the handset has an IP-address the problem is either in the Services setup, or the IP-PBX and WSG services are not reachable.

Major causes can be:

- Wrong IP address parameter settings for VoIP and WSG.
- Login credentials to the services are wrong.
- The handset is not registered in the services.
- Services are on another (sub) network and routing to that LAN is not functioning.

Test the access for VoIP and WSG (for Messaging and Alarm functions) individually as follows:

Test for Voice Access

1 Try to ping the PBX from a handset or a laptop.

2 Was the ping successfully echoed?

No: Check the PBX settings in the LAN as the problem is access to the PBX.

Yes: If ping is successful from another client to the PBX, check the Voice settings (for example PBX address) in the handset. This can be done from the PDM application or the handset.

3 From the handset *Device info* menu or the PDM, check the following:

- The IP address of the handset is on the same subnet as the IP-PBX or there is a route to the IP-PBX in the network. Note that the value of the default gateway must point to a route that can forward the package.
- That the IP-address of the IP-PBX is correct set in the handset.
- That the supported VoIP protocol is selected.
- That the handset has an Endpoint number or Endpoint ID that is registered in the IP-PBX and if passwords are used for access to the IP-PBX, that it is correct.

4 Check that the APs maps VoIP packets to the Voice VLAN if such are used. To do this, access to the AP setup is needed, otherwise a ‘‘wired and wireless sniffing session’’ must be carried out.

Test for WSG **Access**

A test for WSG access is, for example, to login to the Central Device Manager and see if it is successful. Check that the hardware the WSG service is installed on is running, by performing the following steps:

1 Ping the WSG hardware from the handset or a laptop.

2 Was the ping successfully echoed?

No: check the IP settings of the WSG module.

Yes: check if other handsets are listed as online in the Central Device Manager.

3 Check the WSG settings in the handset. The handset must have a User ID set.

Tip: Some of the WSG login parameters can be read from the *Admin menu* in the handset but it is best to use the Device Manager in the PDMand WSG.

4 Check the following parameters using the Device Manager in the PDM :

- The IP address to the Messaging gateway.
- If the correct password has been used at login.

7.1.4 Messaging or Voice Only

Messaging Only

A ‘‘Messaging only’’ message indicates that the handset is configured to use both Voice and Messaging, but has lost contact with the PBX.

1 Perform the same checks for Voice problems described in section Test for Voice Access on page 51. Test for Voice access and then go to step 2.

2 Try to send a message. The idle connection check interval to the WSG is much longer than to the gateway.

Note: Sometimes when all network connections are lost the handset will show "Messaging only" for quite some time because it discovers it has lost connection to the gateway much faster than it discovers loss of connection to the WSG.

Voice Only

A "Voice only" message indicates that the handset is configured to use both a PBX and an WSG Messaging gateway , but has lost contact with the Messaging gateway.

1 Perform the checks described in the section Test for WSG Access on page 51.

Note: When a handset is placed in the programming cradle that is connected to a PC running PDM will it display "Voice only" and not receive SMSs.

2 If the Messaging function is not used in the system, verify that the IP-address to WSG is set to the default value of "0.0.0.0".

7.1.5 No Channel

A "No channel available" message indicates one or more of the following situations:

- The handset did not receive the expected answer from the PBX during call setup.
- The user attempts to make a call when the handset is displaying "Messaging only".

7.1.6 Battery Power is Low

If the battery level drops significantly faster than expected, two major causes are that the battery is old and discharges rapidly or the handset is using its radio too often when not making calls. Even when not making a call the handset needs to use its radio to perform background tasks such listening for incoming calls, for performing scans at cell boundaries and for collecting information for location services.

If the handset is unable to leave active status when performing background tasks, the battery drains fast. The same problem arises if U-APSD has not been setup correctly and the power save mode is not working correctly.

To investigate battery problems, perform the following checks:

1 Use a different battery to check if the problem reoccurs on one or more phones. <If the problem reoccurs, check that the correct chargers are being used.

2 Check the production date of the battery and replace with a new one if necessary. The battery has a minimum 80% capacity left after 400 charging cycles at 20±5°C.

3 Check *Beacon interval* and *DTIM* periods in the AP using the handset Device info > WLAN info menu described in Appendix B.1. These values should be set to the recommended value for the infrastructure according to Interoperability documentation. For additional information, see Figure 3. Handset Operating in U-APSD PS Mode on page 15.

Note: The settings are done in the WLAN infrastructure and not in the handset. Incorrect settings will reduce battery time on all handsets in the cell.

4 If the system is setup to use U-APSD for voice calls, check the voice power save mode parameter in the PDM. Pay special attention to the QoS settings and ensure that these are set correctly.

5 Use a protocol analyzer on both the wired and wireless side, and check the amount of broadcast traffic that is transmitted over the WLAN.

Broadcasts created in the LAN normally are conveyed over the WLAN as broadcast or multiple unicast packets. A WLAN administrator may block this translation. Note that broadcasts are sent at the lowest mandatory speed, and if changed to unicast, may create copies for each client.

One example of a protocol that uses broadcasts is the ARP protocol. Blocking ARPs to handsets can normally be set in the AP, that will act as an ARP proxy on behalf of the handset, and send the ARP reply instead.

7.1.7 Connected Call but No Sound or One-way Sound

Check for an IP address conflict by performing the following steps

1 For each handset, obtain the IP address using the handset Device info > Network info menu described in Appendix B.1

2 Write down the IP-address of each handset.

3 Turn off the handsets.

4 Ping each handset IP address noted in step 2.

5 Did the ping return a result for one or both of the pinged IP addresses?

Yes: The problem is an IP-address conflict.

No: Go to step 6.

6 Enable logging in the handset *Admin menu* as described in Appendix D.2.1. Check that ARP requests from the handset are answered by the system and that RTP data is bi-directional.

7.2 U-APSD Troubleshooting

This section describes how to verify that U-APSD is set-up and configured correctly. U-APSD is normally present and does not need to be specially enabled. However, some WLAN infrastructures may need to tune the parameters associated with U-APSD. For additional information, refer to the infrastructure configuration notes for the equipment manufactured by a particular product partner.

The screenshots used in this section are captured from the OmniPeek protocol analyzer.

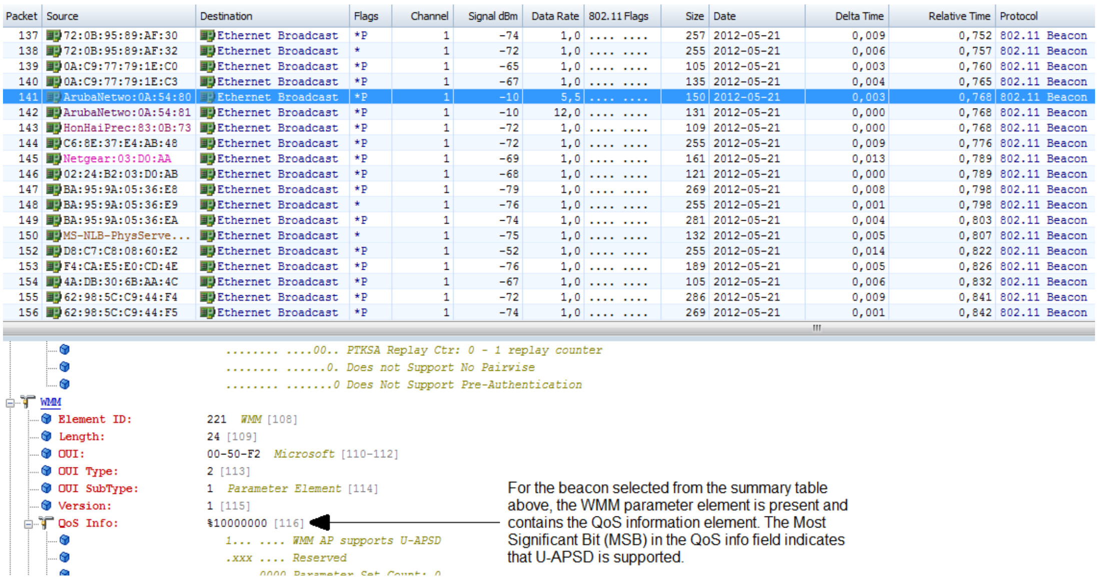
Various APs are used in the following examples since all APs supporting this functionality use the same information element codings.

7.2.1 Determining if the AP Supports U-APSD

A handset will not be able to use U-APSD if the AP does not support U-APSD. U-APSD support is indicated in the QoS information element.

To locate the QoS element, select the 802.11 Beacon from the *Protocol* column shown in the Capture > Packets summary table in figure 17. Detail information for the selected beacon is displayed in the text area under the summary table. The WMM tag of interest is present in beacons and probe responses and is shown in the WMM parameter element. In the example in figure 17, the WMM parameter indicates that U-ASPD is supported:

Figure 17. Capture Packets Trace



Packet	Source	Destination	Flags	Channel	Signal dBm	Data Rate	802.11 Flags	Size	Date	Delta Time	Relative Time	Protocol
137	72:0B:95:89:AF:30	Ethernet Broadcast	*P	1	-74	1,0	....	257	2012-05-21	0,009	0,752	802.11 Beacon
138	72:0B:95:89:AF:32	Ethernet Broadcast	*	1	-72	1,0	....	255	2012-05-21	0,006	0,757	802.11 Beacon
139	0A:C9:77:79:1E:C0	Ethernet Broadcast	*P	1	-65	1,0	....	105	2012-05-21	0,003	0,760	802.11 Beacon
140	0A:C9:77:79:1E:C3	Ethernet Broadcast	*P	1	-67	1,0	....	135	2012-05-21	0,004	0,765	802.11 Beacon
141	ArubaNetwo:0A:54:80	Ethernet Broadcast	*P	1	-10	5,5	....	150	2012-05-21	0,003	0,768	802.11 Beacon
142	ArubaNetwo:0A:54:81	Ethernet Broadcast	*P	1	-10	12,0	....	131	2012-05-21	0,000	0,768	802.11 Beacon
143	HonHaiPrec:83:0B:73	Ethernet Broadcast	*P	1	-72	1,0	....	109	2012-05-21	0,000	0,768	802.11 Beacon
144	C6:8E:37:E4:AB:48	Ethernet Broadcast	*P	1	-72	1,0	....	255	2012-05-21	0,009	0,776	802.11 Beacon
145	Netgear:03:D0:AA	Ethernet Broadcast	*P	1	-69	1,0	....	161	2012-05-21	0,013	0,789	802.11 Beacon
146	02:24:B2:03:D0:AB	Ethernet Broadcast	*P	1	-68	1,0	....	121	2012-05-21	0,000	0,789	802.11 Beacon
147	BA:95:9A:05:36:E8	Ethernet Broadcast	*P	1	-79	1,0	....	269	2012-05-21	0,008	0,798	802.11 Beacon
148	BA:95:9A:05:36:E9	Ethernet Broadcast	*	1	-76	1,0	....	255	2012-05-21	0,001	0,798	802.11 Beacon
149	BA:95:9A:05:36:EA	Ethernet Broadcast	*P	1	-74	1,0	....	281	2012-05-21	0,004	0,803	802.11 Beacon
150	MS-NLB-PhysServe...	Ethernet Broadcast	*	1	-75	1,0	....	132	2012-05-21	0,005	0,807	802.11 Beacon
152	D8:C7:C8:08:60:E2	Ethernet Broadcast	*P	1	-52	1,0	....	255	2012-05-21	0,014	0,822	802.11 Beacon
153	F4:CA:E5:E0:CD:4E	Ethernet Broadcast	*P	1	-76	1,0	....	189	2012-05-21	0,005	0,826	802.11 Beacon
154	4A:DB:30:6B:AA:4C	Ethernet Broadcast	*P	1	-67	1,0	....	105	2012-05-21	0,006	0,832	802.11 Beacon
155	62:98:5C:C9:44:F4	Ethernet Broadcast	*P	1	-72	1,0	....	286	2012-05-21	0,009	0,841	802.11 Beacon
156	62:98:5C:C9:44:F5	Ethernet Broadcast	*P	1	-74	1,0	....	269	2012-05-21	0,001	0,842	802.11 Beacon

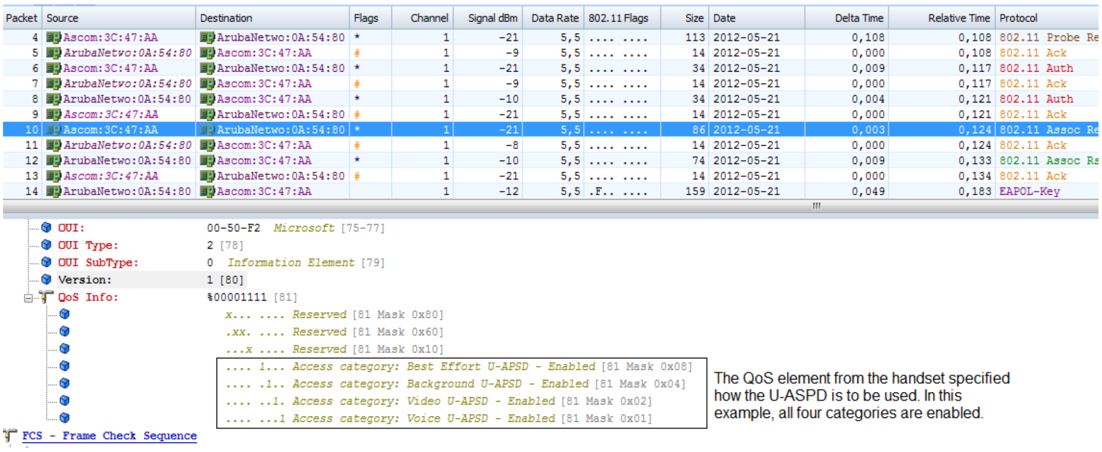
```
                        ........ ....00.. PTKSA Replay Ctr: 0 - 1 replay counter
                        ........ ......0. Does not Support No Pairwise
                        ........ .......0 Does Not Support Pre-Authentication
WMM
    Element ID:         221  WMM [108]
    Length:             24 [109]
    OUI:                00-50-F2  Microsoft [110-112]
    OUI Type:           2 [113]
    OUI SubType:        1  Parameter Element [114]
    Version:            1 [115]
    QoS Info:           %10000000 [116]
                          1... .... WMM AP supports U-APSD
                          .xxx .... Reserved
                               0000 Parameter Set Count: 0
```

For the beacon selected from the summary table above, the WMM parameter element is present and contains the QoS information element. The Most Significant Bit (MSB) in the QoS info field indicates that U-APSD is supported.

7.2.2 Determining if Handset Signals its use of U-APSD

The handset advertises its use of U-APSD and negotiates the use of U-APSD during the association process. An association process when U-APSD is enabled is illustrated in figure 18:

Figure 18. U-APSD Category Assignment



Packet	Source	Destination	Flags	Channel	Signal dBm	Data Rate	802.11 Flags	Size	Date	Delta Time	Relative Time	Protocol
4	Ascom:3C:47:AA	ArubaNetwo:0A:54:80	*	1	-21	5,5	....	113	2012-05-21	0,108	0,108	802.11 Probe Re
5	ArubaNetwo:0A:54:80	Ascom:3C:47:AA	#	1	-9	5,5	....	14	2012-05-21	0,000	0,108	802.11 Ack
6	Ascom:3C:47:AA	ArubaNetwo:0A:54:80	*	1	-21	5,5	....	34	2012-05-21	0,009	0,117	802.11 Auth
7	ArubaNetwo:0A:54:80	Ascom:3C:47:AA	#	1	-9	5,5	....	14	2012-05-21	0,000	0,117	802.11 Ack
8	ArubaNetwo:0A:54:80	Ascom:3C:47:AA	*	1	-10	5,5	....	34	2012-05-21	0,004	0,121	802.11 Auth
9	Ascom:3C:47:AA	ArubaNetwo:0A:54:80	#	1	-21	5,5	....	14	2012-05-21	0,000	0,121	802.11 Ack
10	Ascom:3C:47:AA	ArubaNetwo:0A:54:80	*	1	-21	5,5	....	86	2012-05-21	0,003	0,124	802.11 Assoc Re
11	ArubaNetwo:0A:54:80	Ascom:3C:47:AA	#	1	-8	5,5	....	14	2012-05-21	0,000	0,124	802.11 Ack
12	ArubaNetwo:0A:54:80	Ascom:3C:47:AA	*	1	-10	5,5	....	74	2012-05-21	0,009	0,133	802.11 Assoc Rs
13	Ascom:3C:47:AA	ArubaNetwo:0A:54:80	#	1	-21	5,5	....	14	2012-05-21	0,000	0,134	802.11 Ack
14	ArubaNetwo:0A:54:80	Ascom:3C:47:AA		1	-12	5,5	.F..	159	2012-05-21	0,049	0,183	EAPOL-Key

```
    OUI:                00-50-F2  Microsoft [75-77]
    OUI Type:           2 [78]
    OUI SubType:        0  Information Element [79]
    Version:            1 [80]
    QoS Info:           %00001111 [81]
                          x... .... Reserved [81 Mask 0x80]
                          .xx. .... Reserved [81 Mask 0x60]
                          ...x .... Reserved [81 Mask 0x10]
                          .... 1... Access category: Best Effort U-APSD - Enabled [81 Mask 0x08]
                          .... .1.. Access category: Background U-APSD - Enabled [81 Mask 0x04]
                          .... ..1. Access category: Video U-APSD - Enabled [81 Mask 0x02]
                          .... ...1 Access category: Voice U-APSD - Enabled [81 Mask 0x01]
FCS - Frame Check Sequence
```

The QoS element from the handset specified how the U-ASPD is to be used. In this example, all four categories are enabled.

7.2.3 Packet Classification of U-APSD in the AP

Section 3.5.2 U-APSD PS Mode Operation on page 13 describes the procedure where an AP starts an unscheduled service period and delivers buffered frames when it receives a trigger frame from the handset. A voice packet acts as the trigger.

This section describes how the an unscheduled service period may be interpreted in an OmniPeek trace. In figure 19 an uplink trigger frame triggers buffered data and the correct QoS settings are verified. These settings are UP 6 for both the voice queue and signaling data.

In figure 19, the numbered points illustrate the following:

1 The five packets that have been buffered by the AP for delivery to the handset.

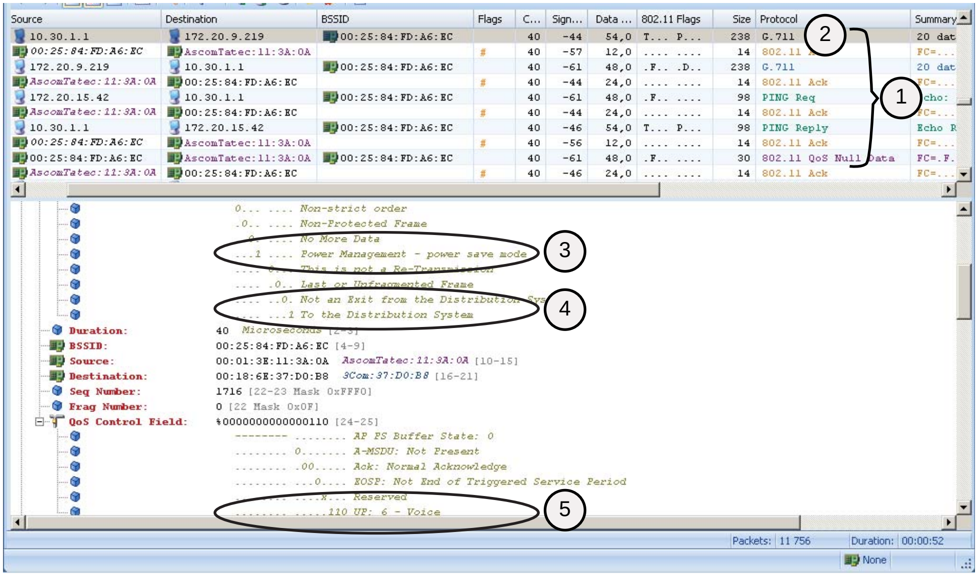
2 The voice packet that acts as the trigger frame from the handset.

3 Confirmation that the handset is in PS mode.

4 Indicates that the packet is in the uplink direction.

5 Verification that the packet is transmitted in the category for voice, that is, UP 6.

Figure 19. Handset Uplink Voice Packet



Source	Destination	BSSID	Flags	C...	Sign...	Data ...	802.11 Flags	Size	Protocol	Summary
10.30.1.1	172.20.9.219	00:25:84:FD:A6:EC		40	-44	54,0	T... P...	238	G.711	20 dat
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-57	12,0	....	14	802.11 A	FC=...
172.20.9.219	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F.. .D..	238	G.711	20 dat
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
172.20.15.42	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F..	98	PING Req	cho:
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
10.30.1.1	172.20.15.42	00:25:84:FD:A6:EC		40	-46	54,0	T... P...	98	PING Reply	Echo R
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-56	12,0	....	14	802.11 Ack	FC=...
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		40	-61	48,0	.F..	30	802.11 QoS Null Data	FC=.F.
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-46	24,0	....	14	802.11 Ack	FC=...

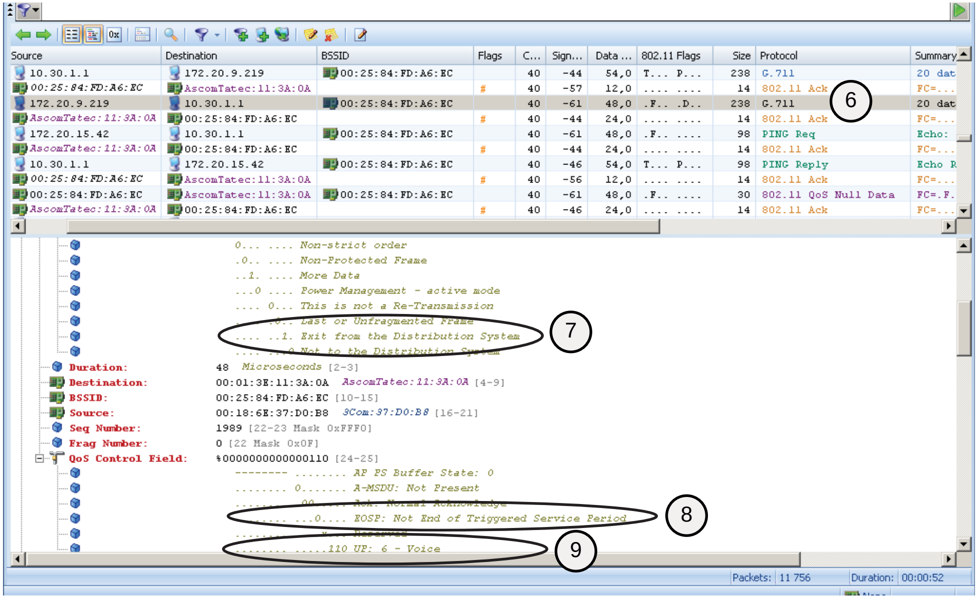
```
                    0... .... Non-strict order
                    .0.. .... Non-Protected Frame
                    ..0. .... No More Data
                    ...1 .... Power Management - power save mode
                    .... 0... This is not a Re-Transmission
                    .... .0.. Last or Unfragmented Frame
                    .... ..0. Not an Exit from the Distribution Sys
                    .... ...1 To the Distribution System
Duration:           40  Microseconds [2-3]
BSSID:              00:25:84:FD:A6:EC [4-9]
Source:             00:01:3E:11:3A:0A  AscomTatec:11:3A:0A [10-15]
Destination:        00:18:6E:37:D0:B8  3Com:37:D0:B8 [16-21]
Seq Number:         1716 [22-23 Mask 0xFFF0]
Frag Number:        0 [22 Mask 0x0F]
QoS Control Field:  %0000000000000110 [24-25]
                    -------- ........ AP PS Buffer State: 0
                    ........ 0....... A-MSDU: Not Present
                    ........ .00..... Ack: Normal Acknowledge
                    ........ ...0.... EOSP: Not End of Triggered Service Period
                    ........ ....x... Reserved
                    ........ .....110 UP: 6 - Voice
```

Packets: 11 756 Duration: 00:00:52

None

The transmissions by the AP in response to the trigger are shown in figure 20:

Figure 20. AP Downlink



Source	Destination	BSSID	Flags	C...	Sign...	Data ...	802.11 Flags	Size	Protocol	Summary
10.30.1.1	172.20.9.219	00:25:84:FD:A6:EC		40	-44	54,0	T... P...	238	G.711	20 dat
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-57	12,0	....	14	802.11 Ack	FC=...
172.20.9.219	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F.. .D..	238	G.711	20 dat
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
172.20.15.42	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F..	98	PING Req	Echo:
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
10.30.1.1	172.20.15.42	00:25:84:FD:A6:EC		40	-46	54,0	T... P...	98	PING Reply	Echo R
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-56	12,0	....	14	802.11 Ack	FC=...
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		40	-61	48,0	.F..	30	802.11 QoS Null Data	FC=.F.
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-46	24,0	....	14	802.11 Ack	FC=...

```
                    0... .... Non-strict order
                    .0.. .... Non-Protected Frame
                    ..1. .... More Data
                    ...0 .... Power Management - active mode
                    .... 0... This is not a Re-Transmission
                    .... .0.. Last or Unfragmented Frame
                    .... ..1. Exit from the Distribution System
                    .... ...0 Not to the Distribution System
Duration:           48  Microseconds [2-3]
Destination:        00:01:3E:11:3A:0A  AscomTatec:11:3A:0A [4-9]
BSSID:              00:25:84:FD:A6:EC [10-15]
Source:             00:18:6E:37:D0:B8  3Com:37:D0:B8 [16-21]
Seq Number:         1989 [22-23 Mask 0xFFF0]
Frag Number:        0 [22 Mask 0x0F]
QoS Control Field:  %0000000000000110 [24-25]
                    -------- ........ AP PS Buffer State: 0
                    ........ 0....... A-MSDU: Not Present
                    ........ .00..... Ack: Normal Acknowledge
                    ........ ...0.... EOSP: Not End of Triggered Service Period
                    ........ ....x... Reserved
                    ........ .....110 UP: 6 - Voice
```

Packets: 11 756 Duration: 00:00:52

6 The second packet is a downlink packet that the AP transmits immediately in response to the trigger frame.

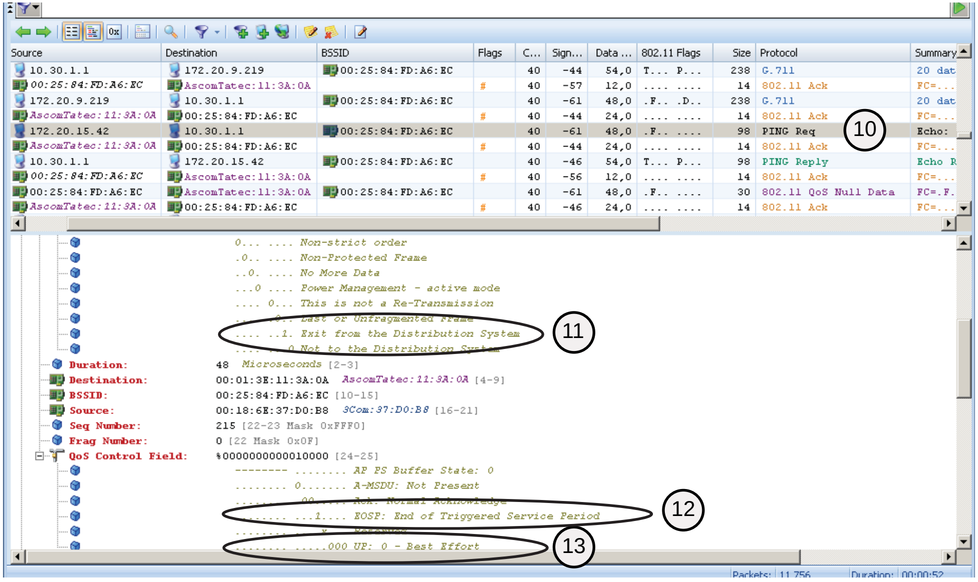
7 Confirmation that the packet is a download packet

8 Informs the handset that more packets are buffered and will be transferred immediately following this packet

9 Verification that the packet is transmitted by the AP in the correct category, UP 6 - Voice.

The third packet in the sequence is a PING request as shown in figure 21. Even though the packet is not a voice packet, it is transmitted during the unscheduled service period.

Figure 21. Non-Voice Packet Transmission



Source	Destination	BSSID	Flags	C...	Sign...	Data ...	802.11 Flags	Size	Protocol	Summary
10.30.1.1	172.20.9.219	00:25:84:FD:A6:EC		40	-44	54,0	T... P...	238	G.711	20 dat
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-57	12,0	....	14	802.11 Ack	FC=...
172.20.9.219	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F.. .D..	238	G.711	20 dat
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
172.20.15.42	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F..	98	PING Req	Echo:
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
10.30.1.1	172.20.15.42	00:25:84:FD:A6:EC		40	-46	54,0	T... P...	98	PING Reply	Echo R
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-56	12,0	....	14	802.11 Ack	FC=...
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		40	-61	48,0	.F..	30	802.11 QoS Null Data	FC=.F.
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-46	24,0	....	14	802.11 Ack	FC=...

```
                         0... .... Non-strict order
                         .0.. .... Non-Protected Frame
                         ..0. .... No More Data
                         ...0 .... Power Management - active mode
                         .... 0... This is not a Re-Transmission
                         .... .0.. Last or Unfragmented Frame
                         .... ..1. Exit from the Distribution System
                         .... ...0 Not to the Distribution System
Duration:               48  Microseconds [2-3]
Destination:            00:01:3E:11:3A:0A  AscomTatec:11:3A:0A [4-9]
BSSID:                  00:25:84:FD:A6:EC [10-15]
Source:                 00:18:6E:37:D0:B8  3Com:37:D0:B8 [16-21]
Seq Number:             215 [22-23 Mask 0xFFF0]
Frag Number:            0 [22 Mask 0x0F]
QoS Control Field:      %0000000000010000 [24-25]
                         -------- ........ AP PS Buffer State: 0
                         ........ 0....... A-MSDU: Not Present
                         ........ .00..... Ack: Normal Acknowledge
                         ........ ...1.... EOSP: End of Triggered Service Period
                         ........ ....x... Reserved
                         ........ .....000 UP: 0 - Best Effort
```

Packets: 11 756   Duration: 00:00:52

The following information is shown in figure 22:

10 The PING packet that is downloaded from the AP to the handset

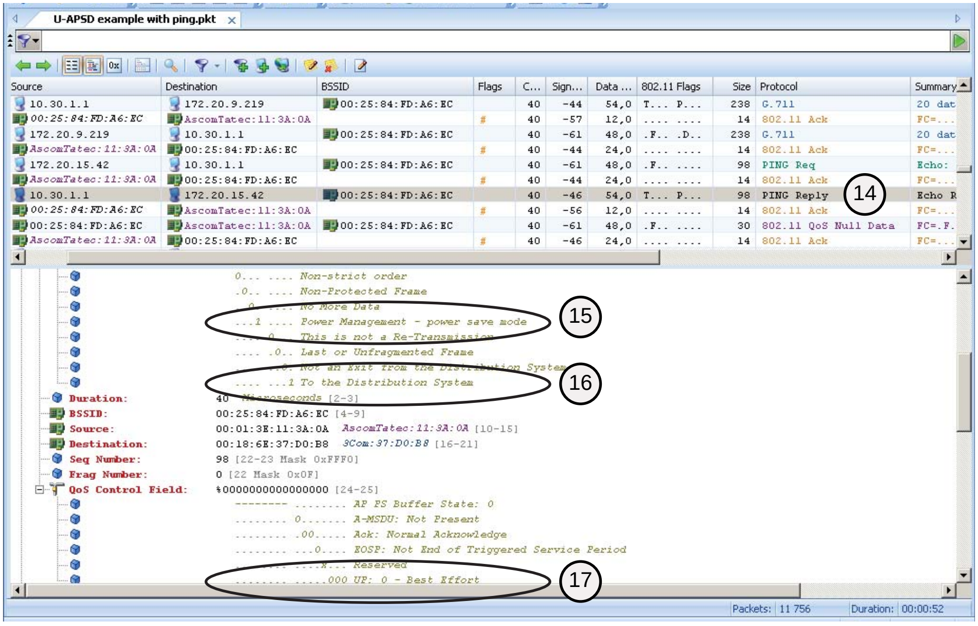
11 Confirmation that the packet is a download packet

12 Informs the handset that no more packets are buffered. This packet marks the end of the unscheduled service period.

13 Verification that the packet is transmitted by the AP in the correct category, UP 0 - Best Effort.

The fourth packet is the response to the previous PING request and is shown in figure 22. Because the last unscheduled service period ended with the last received packet, this packet starts a new unscheduled service period.

Figure 22. Ping Response Packet



Source	Destination	BSSID	Flags	C...	Sign...	Data ...	802.11 Flags	Size	Protocol	Summary
10.30.1.1	172.20.9.219	00:25:84:FD:A6:EC		40	-44	54,0	T... P...	238	G.711	20 dat
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-57	12,0	....	14	802.11 Ack	FC=...
172.20.9.219	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F.. .D..	238	G.711	20 dat
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
172.20.15.42	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F..	98	PING Req	Echo:
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
10.30.1.1	172.20.15.42	00:25:84:FD:A6:EC		40	-46	54,0	T... P...	98	PING Reply	Echo R
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-56	12,0	....	14	802.11 Ack	FC=...
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		40	-61	48,0	.F..	30	802.11 QoS Null Data	FC=.F.
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-46	24,0	....	14	802.11 Ack	FC=...

```
                         0... .... Non-strict order
                         .0.. .... Non-Protected Frame
                         ..0. .... No More Data
                         ...1 .... Power Management - power save mode
                         .... 0... This is not a Re-Transmission
                         .... .0.. Last or Unfragmented Frame
                         .... ..0. Not an Exit from the Distribution System
                         .... ...1 To the Distribution System
Duration:               40  Microseconds [2-3]
BSSID:                  00:25:84:FD:A6:EC [4-9]
Source:                 00:01:3E:11:3A:0A  AscomTatec:11:3A:0A [10-15]
Destination:            00:18:6E:37:D0:B8  3Com:37:D0:B8 [16-21]
Seq Number:             98 [22-23 Mask 0xFFF0]
Frag Number:            0 [22 Mask 0x0F]
QoS Control Field:      %0000000000000000 [24-25]
                         -------- ........ AP PS Buffer State: 0
                         ........ 0....... A-MSDU: Not Present
                         ........ .00..... Ack: Normal Acknowledge
                         ........ ...0.... EOSP: Not End of Triggered Service Period
                         ........ ....x... Reserved
                         ........ .....000 UP: 0 - Best Effort
```

Packets: 11 756   Duration: 00:00:52

The following information is shown in figure 22:

14 The packet containing the response to the Ping.

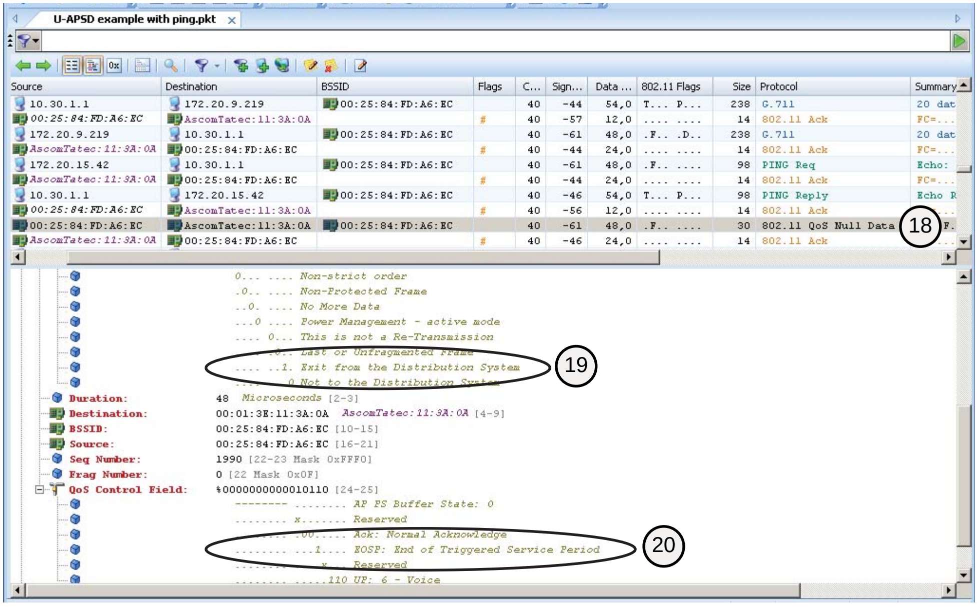
15 Confirmation that the handset remains in PS mode

16 Confirmation that the packet is an uplink packet

17 Verification that the packet is queued in the correct category, UP 0 - Best Effort.

The fifth and final packet illustrated in figure 23 is a QoS Null data frame that indicates that there are no buffered packets of any access category currently in the AP. The following information is shown in figure 23:

Figure 23. QoS Null Data Frame



U-APSD example with ping.pkt

Source	Destination	BSSID	Flags	C...	Sign...	Data ...	802.11 Flags	Size	Protocol	Summary
10.30.1.1	172.20.9.219	00:25:84:FD:A6:EC		40	-44	54,0	T... P...	238	G.711	20 dat
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-57	12,0	....	14	802.11 Ack	FC=...
172.20.9.219	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F.. .D..	238	G.711	20 dat
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
172.20.15.42	10.30.1.1	00:25:84:FD:A6:EC		40	-61	48,0	.F..	98	PING Req	Echo:
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-44	24,0	....	14	802.11 Ack	FC=...
10.30.1.1	172.20.15.42	00:25:84:FD:A6:EC		40	-46	54,0	T... P...	98	PING Reply	Echo R
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A		#	40	-56	12,0	....	14	802.11 Ack	...
00:25:84:FD:A6:EC	AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		40	-61	48,0	.F..	30	802.11 QoS Null Data	F.
AscomTatec:11:3A:0A	00:25:84:FD:A6:EC		#	40	-46	24,0	....	14	802.11 Ack	...

```
        0... .... Non-strict order
        .0.. .... Non-Protected Frame
        ..0. .... No More Data
        ...0 .... Power Management - active mode
        .... 0... This is not a Re-Transmission
        .... .0.. Last or Unfragmented Frame
        .... ..1. Exit from the Distribution System
        .... ...0 Not to the Distribution System
Duration:          48  Microseconds [2-3]
Destination:       00:01:3E:11:3A:0A  AscomTatec:11:3A:0A [4-9]
BSSID:             00:25:84:FD:A6:EC [10-15]
Source:            00:25:84:FD:A6:EC [16-21]
Seq Number:        1990 [22-23 Mask 0xFFF0]
Frag Number:       0 [22 Mask 0x0F]
QoS Control Field: %0000000000010110 [24-25]
        -------- ........ AP PS Buffer State: 0
        ........ x....... Reserved
        ........ .00..... Ack: Normal Acknowledge
        ........ ...1.... EOSP: End of Triggered Service Period
        ........ ....x... Reserved
        ........ .....110 UP: 6 - Voice
```

18 The QoS Null data frame

19 Confirmation that the packet is a download packet

20 Informs the handset that no more packets are buffered. This packet marks the end of the unscheduled service period.

When the handset receives a packet that marks the end of the unscheduled service period, it shuts down the radio receiver and enters idle mode until the next uplink voice packet is transmitted 20 ms later.

8. Related Documents

Configuration Manual, WL3 and WL3 Plus WLAN Handset	TD 92930EN
System Planning, Ascom VoWiFi System for Siemens	TD 92945EN

9. Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
A	29 January 2013	First version.

Appendix A: Making Air Traces of 802.11 Traffic

Ascom recommends Omnipeek from Wildpackets as the airtrace tool for capturing data on a designated channel. The tool can employ several WLAN adapters simultaneously in promiscuous or monitor mode to capture the data.

Note: If other air trace tools than Omnipeek are used, the traces must be saved in Packet Capture (PCAP) format. This is a TAC requirement.

Prerequisite

- The support engineer should have already investigated and ruled out relatively easy to identify causes such as incorrectly configured parameters and incompatible software versions.
- Layer 1 problems, that is, RF problems, should also have been investigated and eliminated as a cause of a problem through a site survey and by doing a site survey and spectrum analysis. Problems like co-channel interference, under or over coverage, rogue WLAN transmitters and analog interference sources should also have been addressed.

Requirements

To perform an air trace, the support engineer should be equipped with the following:

- A portable PC
- The Omnipeek Airtrace tool. This is used to take wireless sniffer traces of:
  - The AP that is transmitting
  - The handset that is transmitting
  - Other air traffic
- 3 WLAN adapters for the g-radio band (dual band is recommended) and 4WLAN adapters for the a-radio band

  Note: If there is only one specific problem that is easy to reproduce, one WLAN adapter is sufficient.

Prerequisites

It is important to note the following before starting a trace:

- Captured traces might not be 100% true. The trace consists of data heard by the adapters, which may miss data transmitted by handset or AP. It is therefore recommended to take several captures to ensure that a complete data flow is logged.
- If more than one handset is used for the trace and the handsets are placed too close together, RF disturbances between the handsets may occur.

To optimise the trace, ensure that:

- The distance between handset and adapter should be no less than 50cm and no more than 100cm
- A clear line-of-sight exists between the handset and the adapter
- The adapter is placed between AP and handset

Note: If the handset is already experiencing WLAN communication problems, it is not recommended to enable RPCAP tracing in the Admin menu because this will generate additional WLAN traffic.

Appendix B: Handset Parameters

B.1 Device Information

The following read-only information about the configuration of a handset can be displayed from the Settings > Device info menu or by using the shortcut **#34#*.

Software

The handset is configured with the following hardware characteristics

Parameter	**Remark**
SW version:	The handsets current software version, it's release date and time.
Release date:	The date when the software was released.
Release time:	The time of the day when the software was released.
WLAN version:	The version of the WLAN driver, WLAN chipset firmware.

Hardware

The handset is configured with the following hardware characteristics:

Parameter	**Remark**
S/N:	Serial number. Use when ordering licenses and for handset inventory in the Device Manager. **Tip:** It is also possibly to scan the number from the label behind the battery.
Unit ID:	For information purpose only.
MAC:	The sub layer 1 MAC address used in frames sent and received. Same address is used independent of the frequency band selected. **Tip:** The first six octets are useful in creating filters in air-log files to remove other WLAN packets.
HW type:	For information purpose only.
HW rev:	For information purpose only.
Production date:	For information purposes only. Identifies the year and week the handset was produced.

License

Combined list of installed handset version licenses and feature licenses.

Note: The actual license key is hidden; only the license type is visible in the handset.

WLAN info

Shows a combination of information retrieved from the associated AP's beacon and stored information in the handset.

Parameter	Remark
SSID (channel):	The configured ESSID for the selected network profile and the associated APs radio channel. The channel number whether the handset is running in the 2.4 GHz or 5 GHz band. **Note:** This value must be set for the intended WLAN. Check the spelling if there is no access to the network as this value is case sensitive. **Tip:** The SSID value can be configured from the Admin menu. For additional information, see the section SSID on page 64.
Security mode:	The current authentication and encryption selected in the association.
Beacon period:	The beacon period value set in the associated AP.
DTIM:	Shows the current DTIM period used by the AP. Possibility to, via the handset, check that the value should be the same as the deployment settings used by the APs and the recommended settings in the interoperability documents.
QoS:	The current Quality of Service (QoS) used.
Privacy:	If on, it shows if any kind of encryption is used.
Tx power:	The current transmit power.

Network Info

The current IP address (and related information to it) received from the DHCP server, if used, or if set manually.

Note: There is no indication if the IP addresses were set by a server or manually.

Parameter	Remark
Phone IP:	The current handset IP address.
Subnet mask:	The current subnet mask.
Default gateway:	The current default gateway IP address.
Primary DNS:	The current DNS IP address.
Syslog server IP:	The current Syslog server IP address used to transfer the Syslog messages from the handset to a remote location.
Firmware TFTP IP:	The current firmware Trivial File Transfer Protocol (TFTP) IP address. Alternative way to upgrade the handset firmware using the boot process.

User ID

The login ID used to login to the is normally the same as the phone number. The Endpoint number is also synchronized with this value.

B.2 Site Survey Tool

To display the Site Survey Tool in the handset, use the shortcut *#77#. The Site Survey Tool displays the following site information:

Show RSSI

Parameter	Remark
SSID:	The identity of the currently associated SSID
Current AP:	The handset displays the following information about the AP it is currently associated with: - The strength of the RF signal it is receiving from the AP, expressed in dBm - The channel the associated AP is using - The power save mode where "P" denotes Power Save mode and "A" denotes Active mode.
Current AP MAC:	The MAC address of the AP, that is, its BSSID.
Previous AP:	If the user has been roaming while the RSSI screen is active, the handset displays the following information about the previous AP that the handset was associated with: - The strength of the RF signal, expressed in dBm, that is was receiving as the user left that AP's coverage area. - The channel that the previous AP used - The power save mode where "P" denotes Power Save mode and "A" denotes Active mode.
Previous MAC address:	The radio MAC address of the previous AP, that is, its BSSID.

Note: The Show RSSI display can be displayed without the rest of the Site Survey Tool parameters by using the shortcut *#76#. For additional information, see section 5.2.1 Show RSSI on page 31.

Scan All Channels

Scans the channels defined in the handset to detect the access points, by default for 2.4 GHz: Channel 1,6,11 and for 5 GHz: All channels.

Note: Regulatory domain may further limit which channels that are used by the handset.

Scan Selected Channel

Scans selected channel in the handset to detect the AP on any channel. (The handset does not need to be configured for the channel.)

Range Beep

A beep that is played whenever the handset measures a filtered field strength of below the configured value (default -70 dBm) from the currently associated AP.

Note: Since the value is filtered, sudden drops in field strength caused by the environment, for example walking through a door into a room, can be delayed. It is therefore important to walk through the site slowly to ensure that all weak spots are covered.

Range Beep Level

Configures the RSSI threshold value.

Location Survey

Possibility to use Site survey mode for Ekahau that will cause location scanning to be performed at shorter intervals: 1s.

B.3 Admin Menu Information

Device Info

See section 5.1 Handset Device Information on page 31.

Site Survey Tool

See section 5.2 Site Survey Tool on page 31.

Network Setup

Note: The Network Setup function should only be used to check settings and modify parameter values while troubleshooting problems. It should not be used as the main method for setting up and configuring handsets. The PDM is provided for this purpose.

Option	**Remark**
Network name	Allows a user friendly name for the current Network profile used in the handset. The network name is not the SSID but it can be set to correspond to it.
IP addresses	The default IP address set by DHCP. However, a static IP address may be entered manually. If using a static IP address, the following parameters can be set: - Phone IP - Subnet mask - Default gateway - Primary DNS IP-address - TFTP server IP address
SSID	Specifies the SSID setup in the WLAN. **Note:** Entering a SSID with a complex combination of alphanumeric characters may not easy from the keypad. The PDM provides an alternative means of entering the SSID by selecting Network > <network id> > SSID. **Tip:** The SSID is also shown in Device info> WLAN info, as long as the handset is associated with an AP.
802.11 protocol	Configures the radio settings (802.11 b/g, 802.11 b/g/n, 802.11a or 802.11a/n.
Security mode	Configures the various encryption and authentication schemes: - Open (Default setting in handset with no security) - WEP (64 or 128 bits) - WPA-PSK/WPA2-PSK (If both are supported by the AP the handset selects the stronger WPA2.)

Unite

IP address	If using any Unite based services like Messaging or Alarm functions, the IP address of the centralized management module is set here.
Password	Used to protect the login to the Unite system. **Note:** Password must match the password set in the Unite system. The default value is an empty string.

VoIP

Endpoint ID	Many PBXs allow a handset to register with an Endpoint ID, for example, a user name instead of the number. If used, this value must match the value set in the PBX. For example this can be used for SIP registration. **Note:** To use the Endpoint ID for registration, use the PDM and access the parameter *VoIP > SIP > Registration identity* and change the value of the parameter from the default "Endpoint number" to "Endpoint ID". **Note:** If both Endpoint ID and Endpoint number are configured, some PBXs require that both numbers must match.
Protocol	H.323 or SIP may be selected. Click the handset *Edit* button to access the parameters associated with the respective protocol and then check with a systems or PBX administrator for the required values. For H.323 the following values are required: - Gatekeeper IP address or Gatekeeper ID - Gatekeeper password For SIP the following values are required: - SIP proxy IP address or SIP proxy ID - SIP proxy password

Syslog

Syslog mode	Turns Syslog forwarding on or off.
Syslog server IP	Defines where to forward the Syslog information from the handset.

Logging

Logging mode	The handset can be configured to one of the following logging modes: - Trace: Used together with the Portable Device Logger (PDL) troubleshooting tool. **Note:** This mode must only be used if requested by TAC. - RPCAP: Used with Wireshark or similar tools when WLAN access to the handset is functional. - PCAP over USB: Used with the PDL (version 1.6.0 or later) troubleshooting tool when WLAN access to the handset is not working. **Note:** May sometimes produce a corrupt PCAP file that cannot be fully opened in WireShark.
Extended logging	A handset configured to one of the above logging modes may also be configured to include one or more of the following types of traffic: - Phone: Internal signal debugging traces - SIP: Logs including SIP traffic - H.323: Logs including H.323 traffic. - Network Traffic: Logs all WLAN traffic application frames, for example SIP, H.323, ARP, DHCP, RTP etcetera.

For additional information about the handset PCAP log function when setting up Wireshark traces, see AppendixAppendix D.2.

Troubleshooting

Used for extended authentication of WLAN. When the function is enabled, one of the following dialogs is displayed in response to the particular problem:

Dialog	Description
"WLAN authentication failed"	Authentication to RADIUS server failed, possibly due to wrong user or password.
"WLAN authentication timed out"	Authentication to RADIUS server timed out. Possibly due to incorrectly configured RADIUS server or connection to the RADIUS server (wrong IP address). Also shown if authentication fails in any step, for example, supplicant times out during key negotiation for WPA(2)-PSK (Pre Shared Key).

Enter License Key

License keys can be obtained from the handset supplier. Use this manual entry feature if access to any Device Manager is missing.

Factory Reset

Erases all settings back to the default values except for the License key setting.

Appendix C: Digital Certificates

TLS is a security mechanism based on cryptography (see 4.1.3 Cryptography) and is used for encrypting communications between users and TLS-based Websites. The encryption prevents eavesdropping and tampering with any transmitted data.

TLS operates on the OSI Model Level 5 and uses PKI (see Appendix C.1).

C.1 Public Key Infrastructure

Public Key Infrastructure (PKI) is a component of Public Key Cryptography (PKC) that uses:

- Public Key Certificates, see Appendix C.1.1.
- Certificate Authorities, see Appendix C.1.2.

C.1.1 Public Key Certificates (Digital Certificates)

Public Key Certificates are used for key exchange and authentication. They are simply electronic documents (files) that incorporate a digital signature to bind together a public key with an identity (information such as the name or a person or organization, their address, and so forth).

The signature may be signed by a trusted entity called a Certificate Authority or Certification Authority (CA), see Appendix C.1.2.

The most common use of public key certificates is for TLS certificates (https websites).

C.1.2 Certificate Authorities

A CA is a trusted entity which issues public key certificates. The certificates contain a public key and the identity of the owner. The CA asserts that the public key belongs to the owner, so that users and relying parties can trust the information in the certificate.

A Certificate Signing Request (CSR) or Certification Request is a message that is generated and sent to a CA to apply for a TLS certificate. Before the CSR is created a key pair is generated, the private key kept secret. The CSR will contain the corresponding public key and information identifying the applicant (such as distinguished name). The private key is not part of the CSR but is used to digitally sign the entire request. Other credentials may accompany the CSR.

If the request is successful, the CA will send back an identity certificate that has been digitally signed with the CA’s private key.

A CSR is valid for the server where the certificate will be installed.

C.2 Cryptography

Cryptography is the encoding of messages to render them unreadable by anyone other than their intended recipient(s). Modern cryptography uses complex algorithms implemented on modern computer systems.

Cryptography tasks can be divided into the two general categories Encryption and Authentication.

C.2.1 Encryption

Encryption is the scrambling of information so that the original message cannot be determined by unauthorized recipients by applying an encryption algorithm to the message plaintext producing ciphertext (apparently random bits). A decryption algorithm, if given the correct key, converts the ciphertext back into plaintext. Public key algorithms use paired keys, one for encryption and another for decryption.

C.2.2 Authentication

Authentication is the verification of a message’s sender. This requires the message to be protected so it cannot be altered, usually by generating a digital signature formed by a hash of the message. Only the correct key can generate a valid signature.

Appendix D: External Troubleshooting Tools

A support engineer of LAN and WLAN installations should be equipped with a software toolbox containing additional troubleshooting tools commonly used in the trade. The toolbox should preferably contain tools for both the Wired and Wireless LAN.

Tools are available from many sources like:

- WLAN and LAN infrastructure vendors.

  If you work often with a specific WLAN vendor it can be beneficial to learn the tools that are produced by that vendor. Some tools may be free while others are costly.
- Niche commercial software publishers.

  Commercial software products are often highly priced but a license will give you support, and there are often training programs available to attend.
- Free or low cost tools that can be downloaded from the Internet.

Note: The tools that may be used are, in general, a matter of the support engineer's personal preference. However when the support of the Ascom TAC team has been requested in resolving an issue, they may request information, in the form of a trace or dump, from a specific tool.

The tools can be divided in groups as follows:

- VoIP tools

  -Software IP-PBX and Software clients

  - Performance measurement tools
- WLAN tools

  - RF tools such as spectrum analyzers, heat mapper tools and site survey tools
- Protocol Tools

  Wireless supported Protocol Analyzer (Sniffer)
- Report Tools.

D.1 Protocol Analyzer Tools

Capturing the traffic data with a wireless or wired protocol analyzer can be very useful when troubleshooting a system. Specifically when using WLAN, capturing traffic in the spot where the problems arise may provide valuable information about the traffic that is not transferred over to the wired network, for example, retransmissions, rates, etcetera. Since the wired side is almost always a switched network capturing traffic is not trivial since access to the switches is needed to create a spanned port to get the data mirrored out to the sniffer. On the other hand, capturing the WLAN which is a broadcasted medium is very convenient. The only equipment needed is a laptop, for physical mobility, and a wireless network card that the sniffer software supports.

General Practices

- Always try to capture as much data as possible. If filtering options exists try to filter the result after the capture is saved. Applying a filter to the capture itself may exclude interesting packets and ultimately render the capture useless.
- When capturing wireless bear in mind that the capture device has the same limitations as other wireless devices, that is, it will miss packets, be subjected to disturbances and can be out of range. To ensure the best possible wireless capture try to place the capture device in between the monitored devices, that is, between the handset and the AP. Do not place the capture device too close to another wireless device and keep at least 0.5 m between the capture device and monitored devices. If placed too close, traffic may be overheard on the wrong channels, for example packets on channel 6 will appear on channel 11, or not heard at all due to saturated receivers.

- A result without knowing what happened during the capture is of little use. Try to make note of what the capture is designed to capture and what devices are involved, what devices are present and what was expected to happen but did not.
- Try not to influence the monitored system. For example, if capturing wired traffic with Wireshark or OmniPeek, consider disabling name resolution because each IP/name lookup will generate traffic from your PC to the DNS server.
- If data on one channel is to be recorded the WLAN adapter can only be set to listen to one channel. If roaming is going to be monitored, two or more channels need to be monitored, in which case one adapter per channel is required.

D.2 Setting up the Handset for Wireshark Traces

Wireshark is a packet capture and trace tool that is particularly useful for analysing network traffic and statistics captured from various protocols. With Wireshark, the support engineer can capture and analyze traffic from a live network. Wireshark captures network traffic in PCAP format, which requires the handset to be set to RPCAP logging mode.

To setup the handset for a Wireshark trace, perform the following steps:

D.2.1 Enable Logging

1 With the handset in idle mode, enter **Menu > Settings > 40022**. The *Admin menu* is displayed.

2 Select **Logging**. The *Logging* menu is displayed.

3 Is the first menu item **Logging mode RPCAP**?

Yes: The handset is already setup for RPCAP logging. Go to step 7.

No: Go to step 4.

4 Select **Logging mode <xxx>** where **xxx** is one of the available alternative logging modes. The *Logging mode xxx* menu is displayed.

5 Deselect the radio button associated with the alternative logging mode and select the *RPCAP* radio button.

6 Return to the *Logging* menu by pressing the handset *Back* button.

7 Select **Extended logging**. The *Extended logging* options are displayed.

8 Tick the *SIP* checkbox. Ensure that the other checkboxes are not ticked.The handset is now configured to provide Wireshark with the required traffic logs for the analysis.

D.2.2 Run Wireshark

To run a Wireshark session, you require the IP address of the handset. perform the following steps:

1 With your handset still in Administrative mode, return to the *Admin menu*.

2 Select **Device info**. The *Device info* menu is displayed.

3 Select **Network info**. The *Network info* menu is displayed.

4 Make a note of the value of the **Phone IP** address.

D.2.3 Analyze Call

To analyze a call from the handset using Wireshark, perform the following steps:

1 Start Wireshark from the Wireshark icon on your desktop, taskbar or Start Programs menu. The *Wireshark Network Analyzer* window is displayed.

2 Click **Capture Options**. The *Wireshark: Capture Options* window is opened.

3 Click the **Add Remote Interfaces** button. The *Wireshark: Remote Interfaces* dialog is opened.

4 In the *Host:* field, enter the IP address of the handset that you noted down in step 4 of the previous procedure followed by /trace. For example: `172.20.15.139/trace`.

5 Click the *OK* button. The *Wireshark: Capture Options*, *Capture* pane is updated with the details of the trace you have specified for the handset.

6 Tick the Capture checkbox next to the new trace and click the *Start* button. The *Capturing from Network adapter 'TRACE' on remote node <ip address>* pane is displayed, where IP address is the address of the handset from step 4. Wireshark is now ready to trace a call from the handset.

7 Initiate a call from the handset. Try to reproduce exactly the conditions as described in the issue or ticket that describes the problems that the user or users have reported.

8 On the termination of the call, halt the Wireshark trace by clicking the *Stop the live capture* icon from the toolbar.

9 Packets captured in a Wireshark trace are displayed in the *Network Adapter TRACE on remote node >handset IP address>* pane.

Note: The setup described in the above example may vary depending on the Wireshark function being used.

For additional information about Wireshark, see http://www.wireshark.org.

Appendix E: Ports

This appendix lists the TCP and UDP ports the handset listens on for incoming and outgoing traffic. The information applies to firewalls, network devices, traffic shaping and third-party product settings.

E.1 Signaling

E.1.1 SIP

The following port numbers are configurable through the PDM:

Application	Direction	Local Port Number
UDP	outgoing	UDP: 5060
	incoming	UDP: 5060
TCP	outgoing	TCP: any free port
	incoming	TCP: 5060
TLS	outgoing	TCP: any free port
	incoming	TCP: 5061

E.1.2 H.323

Application	Local Port Number
Gateway interfaces	UDP: 1718 UDP: 1719 TCP: 1720
Gateway interfaces, additional ports	TCP: 2048-2100

E.2 Voice Traffic

For a voice connection, one RTP and one RTCP port are used. A call therefore uses two free UDP ports selected from the RTP port range. The RTP port range is, by default, from 16384 to 32767. The port range is then used for H.323 and SIP calls.

E.3 Other Services with Fixed Local Ports

Application	Local Port Number
DNS UDP	53 OUT
DHCP UDP	68 OUT
TFTP UDP, Software Updates	69 OUT
Web (HTTP) TCP traffic	80 IN
Netwise **Note:** The application listens on port 80 by default. However this may be modified using Netwise. The ports that are eventually used are decided by the Netwise server.	80 IN
Network Time Protocol (NTP) UDP synchronization	123 OUT
Simple Network Management Protocol (SNMP) UDP	161 IN
Unite traffic TCP	33000 IN/OUT
Ekahau UDP (Configurable in PDM)	8552 IN
RPCAP TCP	2002 IN

Index