Product description

Aastra 340w and Aastra 342w VoWLAN telephones

Voice over Wireless LAN communication for the Workplace.

Content

1 Introduction to Aastra 340w and Aastra 342w

Aastra 340w and **342w** are suitable for all users who need a corporate communication tool that offers mobility, quality as well as access to business applications.

They improve the productivity and responsiveness of mobile professionals on site in a wide range of sectors, and meet the needs of targeted vertical markets, such as:

- **The healthcare sector** - hospitals and clinics use wireless phones to rationalize communications in order to quickly meet the needs of patients. This results in more patient satisfaction and better general healthcare quality. Since it also makes the healthcare personnel more efficient, it enables hospitals to cope with the shortage of qualified healthcare professionals while improving nurses' loyalty. Some specialized applications such as bar-code-based medicine management equally reinforce the safety of patients by reducing medical errors.
- **Retail business** – Shop managers and staff are mobile and visible. They spend more time with customers in order to better respond to their enquiries concerning stocks, products and promotions They react faster in case of incident in the premises, such as if a drink is poured or in the event theft.
- **Manufacturing industry** – The wireless handsets eliminate delays related to loudspeaker announcements, improve the effectiveness of operations and enable the personnel to quickly react to problems and emergencies, thus reducing downtime and production delays. The PTT (Push-to-Talk) technology replaces walkie-talkie systems thanks to enhanced functionalities.
- **Tourism and hotel sectors** – Wireless systems at workstations offer an economical alternative to portable phones, which enables companies to offer more services to customers while remaining much more efficient.
- **Offices** – Employees such as project managers, administrative assistants and IT professionals use wireless phones to limit "phone tags" and increase the productivity of staff members always attending meetings or absent from office.

Based on open standards, Aastra 34xw improves the distribution of mobile corporate applications thanks to the powerful thin-client technologies and browser available to professionals inside a user-friendly and easy-to-manage interface. Moreover, Aastra 34xw supports the widest range of interfaces with some telephone standards, wireless LANs and corporate infrastructure, to ensure maximum interoperability with low acquisition cost.

The strong points of this product range are:

- Integrated bar code reader (on A342d only)

- Integrated WebKit browser and XML API, available for web application deployment
- Integration with the communication server via the SIP standard
- Reliability and quality of the terminal which can be used in demanding industrial environments (standard IP-64)
- Noise-cancellation function allowing the use of A34xw in noisy environments
- Compatibility with 802.11n (data transmission via a wireless link) in addition to other standards
- Management of the alarm system for isolated workers: emergency call button, triggering of alarms following disorganized movements, absence of movement (immobility), or loss of verticality
- HD-voice-compatible answering station

2 Characteristics of Aastra 340w/342w

Presentation of A340x/A342w telephones:

The main difference between these two terminals can be seen at the back of these terminals:

2.1 Advantages and functions:

Ease of use

- A **clear display** thanks to a wide (2.2”), color (240x320) and backlit screen
- **Easy navigation** thanks to large keys, 4 programmable (or interactive) keys, a navigation keypad and intuitive graphic interface
- A very **portable** terminal: light (159g to 176g), belt clip (optional)
- A **resistant** terminal thanks to:
  - its compatibility with **IP-64** (protection against dust and splash) and **MIL-STD 810F** (covers a wide range of tests which measure the reliability of a device in difficult or even hostile conditions of use),
  - a **reinforced cover** and plastic molding
- **Unifying communications** with:
  - voice calls,
  - text messages from centralized management, or patient calls via an Aastra communication gateway
  - bar code reader (A342w)
- A **hands free** terminal: wired headset and Bluetooth compatible, answering station with loudspeaker
- **High quality communications**: HD voice, perfect noise cancellation function, usable in noisy environments, full duplex loudspeaker
- **Customizable** ringtones (10), beeps (10), vibration options, speed dialing, automatic replies, profiles

Managing work flows

- **Push to Talk** via a preconfigured key: loudspeaker call with a number of predefined terminals
- **Terminal sharing** thanks to customizable user profiles
- **DATI alarm management**: emergency call button for manual alarm, (disorderly) movement alarm, immobility alarm, loss of verticality alarm

Technical data (IT)

- A **professional safety level**:
  - WLAN - compatible with WEP, Personal and Enterprise WPAWPA2, 802.1X (EAP-FAST, PEAP-MSCHAPv2), Fast AP hand-off (Opportunistic Key Caching (OKC) and Cisco Centralized Key Management (CCKM),
  - Network - compatible with SRTP (Secure Real-Time Protocol), TLS (Transport Layer Security), 128 bit AES (Advanced Encryption Standard – and HTTPS (secure transfer protocol)
- **Easy integration** thanks to the following protocols:
  - SIP
  - Wi-Fi Standard QoS
  - IEEE 802.11 a, b, g and n
  - XML API
- **Simplified management**:
  - Configuration via a PC or via air interface (OTA)
  - Syslog
  - Site survey: conducting tests simulating the use of the Wi-Fi network in a targeted environment - Wi-Fi planning, site survey and troubleshooting)
  - Real time location system: RTLS

- Event log
- Hardware diagnosis
- Roaming

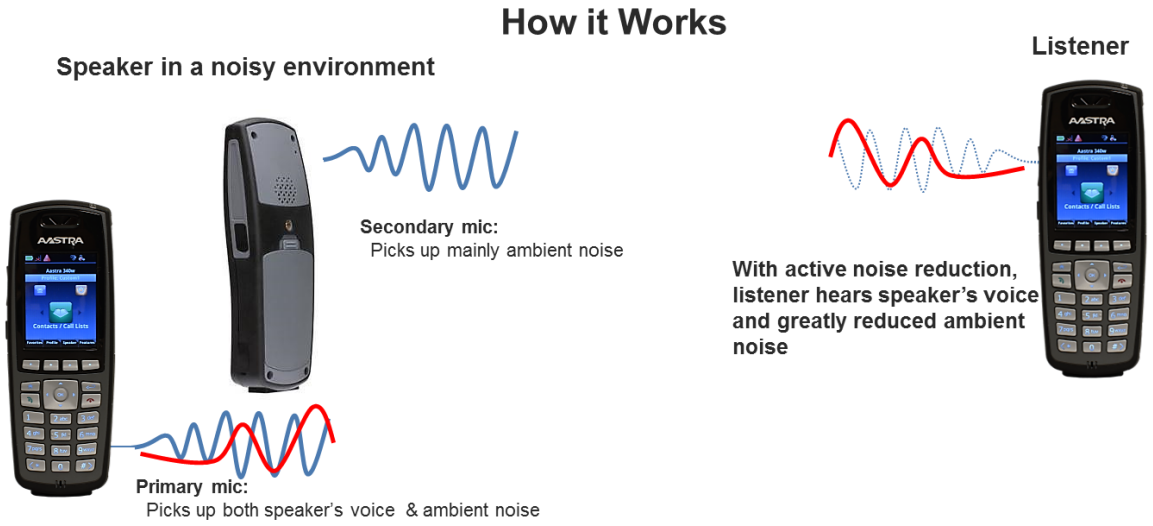
To complete this offer, a range of accessories is available. For all the details, see the section "Accessories".

2.2 Robustness and high quality

Terminals A340w and A342w have been designed for use in demanding or even difficult business environments with high-quality hardware and technologies, which offer a very high level of robustness:

2.3 Active noise reduction

Background noise is significantly reduced thanks to active noise reduction. Therefore, the terminal can be used in noisy environments.



2.4 Accessories

Accessories:

In addition to the terminal, the offer comprises the following additional items:

For a list of available accessories, please see the Ordering Information document.

Batteries:

Two battery types are available, each one with the following characteristics:

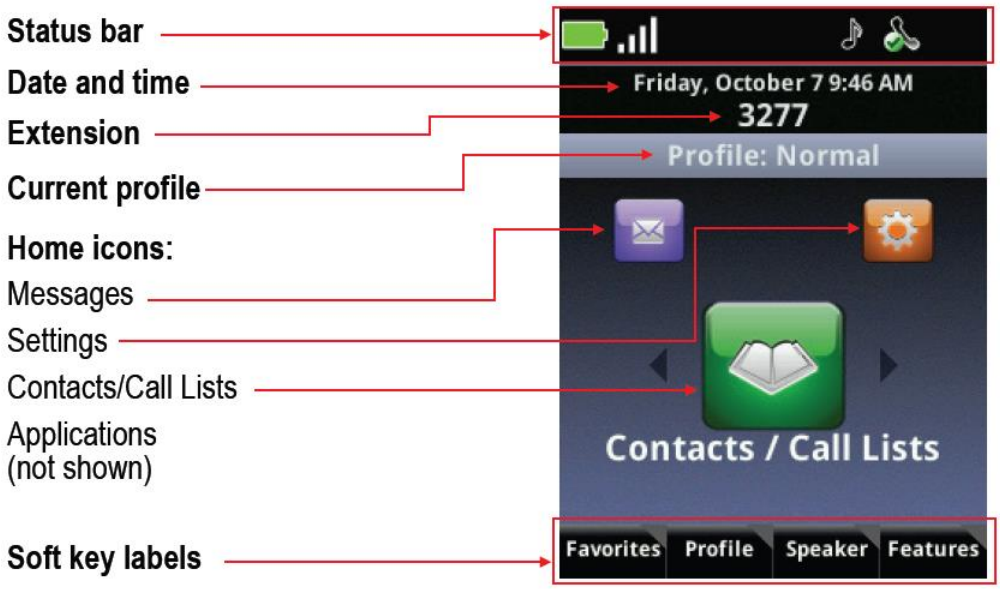
	Autonomy in conversation mode	Autonomy in standby mode	Charging time (with rack charger)
Standard battery	8 hours	80 hours	3.5 hours
Long-lasting battery	12 hours	120 hours	5 hours

2.5 Description and use

2.5.1 Ergonomic

Aastra A340w/342w offers the user a convenient and intuitive design.

In standby mode, the user has access to a range of information like on the welcome screen below:



Icons on the welcome screen:

- **Contacts/Call lists**: this icon gives access to the contact directory.
- **Messages**: this icon gives access to voicemail and instant messaging.
- **Settings**: this icon gives access to the configuration menu of the phone's numerous functions.
- **Applications**: this menu depends on the terminal configuration: it gives access to customizable applications (bar code reader on A342w, etc.).

Call status icons:

Status and Call Icons

Status Icon	*Indication*	*Call Icon*	*Indication*
	Battery full		Incoming call ringing
	Signal strength with location services		Outgoing call
	Mute		Call active
	Do not disturb		Call on hold
	Missed call with number indicator		Conference call
	Voicemail with number indicator		Conference leg/ with HD audio
	Bluetooth available		PTT/Page receive
	Bluetooth connected		PTT/Page transmit
	Profile: Normal		PTT/Page idle
	Profile: Silent		Dialer–Outgoing call
	Profile: Custom		Dialer–Incoming call
	Profile: Meeting		Dialer–Missed Call
	All phone lines are available		Call list–Outgoing
With green dot means active call With red dot means call on hold			Call list–Incoming
	Phone lines are unavailable		Call list–Missed
Personal Alarm Icons			
	Alarm state		
	Monitoring state		
	Suspend state		

Pop-up menu:

The interactive keys at the bottom of the screen are used to select some functions.

The grey triangle in the upper right corner of the interactive keys (

) indicates that some additional options are available via a popup menu.

To select an option from a popup menu, just use the ▲ and ▼ navigation keys then press **OK** or press the option number directly on the keypad.

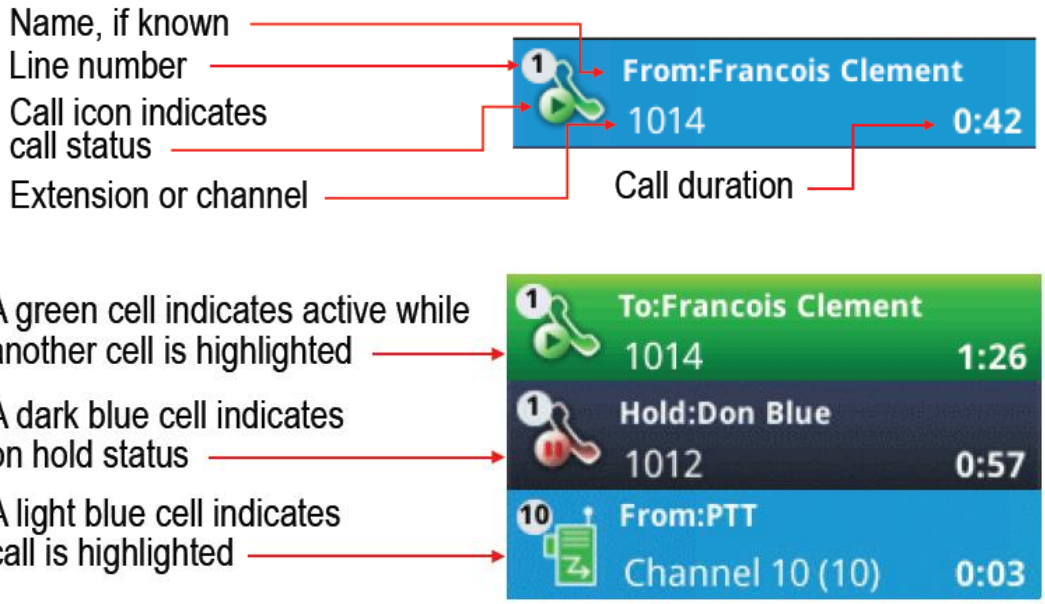
The greyed out options are not available.

2.5.2 Call management

The terminal can handle up to 8 call sessions at the same time (phone calls, distributions), any time and with any handset.

Each call session is visible thanks to a color code on the Session Management screen.

The cells are displayed with a call icon indicating the call status, a line number indicator, the correspondent's name and number/channel and call duration, as shown in the example below:



When a cell is highlighted, the programmable keys are displayed so this call can be assigned while the other cells remain unchanged.

The ▲ and ▼ navigation keys are used to highlight a call, while the OK key is used to select the highlighted item.

2.6 Application integration

Aastra 340w and 342w terminals have a web browser and a complete development toolkit allowing a strong integration into business applications.

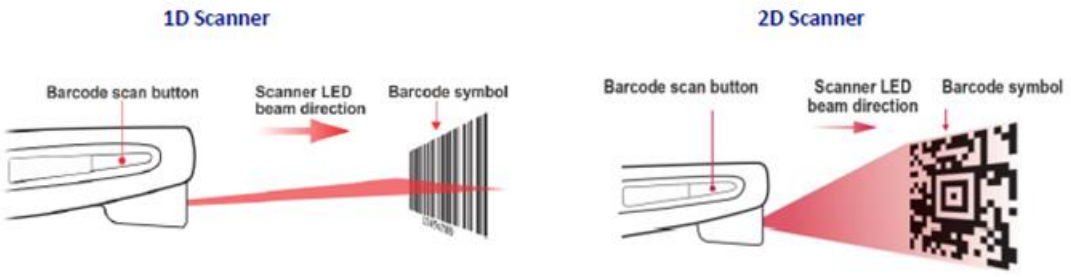
API and toolkit can be downloaded from A2P2 Infochannel portal https://infochannel.aastra.com/ICA2P2/qnprod.nsf/.

2.6.1 Web browser

It is possible from the terminal to browse through some business applications, or to access a web service.

2.6.2 Bar code scanner and its applications

This application is used to combine in the same tool the bar code reader and the user's terminal. Out of the proposed terminal range, only A342w has a bar code reader. It is a scanner with one or two dimensions.



The bar code reader can be used with 2 types of applications which can be installed on the terminal. A browser can be opened to enter information with the bar code in the right application.

It is possible to send the code bar to a PC application using the QBC (Quick Barcode Connector) software. Several users can transmit on the QBC application; this application may be centralized or distributed by user.

2.6.3 DATI integration

Terminals A34xw meet the expectations of isolated workers. In fact, it is possible to activate a DATI alert using 4 criteria; each one is configurable. If an alert activation condition is met, the terminal alerts the user, and if the user does not stop the pre-alarm, it is set off.

The 4 alarm criteria are:

- **Manual alarm**: the user presses the emergency call button located on the left side of the terminal, twice in less than 2 seconds. A call is made to the preset number.
- **Movement alarm**: the terminal detects some disorderly movements during a certain minimum period (5 seconds).
- **Loss of verticality alarm**: the terminal detects its loss of verticality, during a certain (configurable) period in seconds.
- **Immobility alarm**: the terminal remains immobile for a certain (configurable) period in seconds, potentially indicating that the user is no longer moving about.

These criteria can only be centrally configured via the provisioning server and configuration files.

The users have on their screen the activation status and not the DATI function, and the activated function.

The user may suspend the activated function for a certain time, as shown on the screenshot below:

The alarms are activated according to their set threshold, and first alert the user who can then deactivate the alarm: in this case, the alarm is not sent to the security department.

The user may choose to cancel the local alarm before sending it to the emergency service. If he fails to do so, the emergency alarm is set off, and a call is made to a preset number.

The user can directly stop the ringer and vibration but to acknowledge the alarm, he must go to the alarm acknowledgement menu.

The DATI function is inactive when the terminal is connected to its power supply charger or answering station.

Location

The entire range of terminals A34xw supports integration with an RTLS location system, Ekahau. The terminal regularly sends location information to the Ekahau server. To optimize the battery an administrator may set the timeout to a 1 minute interval, for instance. In case of an event, the system may be set to send out location information more frequently, for example every 10 seconds. This enables the Ekahau location software to provide an up-to-date position. The Ekahau system can then send this information to notification systems.

Other location solutions such as those from the company Aeroscout can indicate the location of terminals A34xw.

2.7 Technical features

Aastra terminals 340w and 342w have the following characteristics:

	Aastra 340w	Aastra 342w
Physical specifications		
Terminal dimensions (LxDxH) in mm	147x53x25	146x54x34
Weight (with standard battery)	145g	162g
Mains power unit charger	X	X
Hearing aid compatibility		X
G711, G729a, G722	X	X
Headset socket	X	X
Bluetooth version 2.1 HSP version 1.2 support class 1 with a range of close to 10m	X	X
Screen		
Screen size (number of lines / characters)	2.2 inches 240*320 in resolution	2.2 inches 240*320 in resolution
Screen colors	65000 colors	65000 colors
Back-lit keypad	X	X
Contrast adjustment	X	X
Audio quality		
Audio quality standard TIA 810B, TIA 920	X	X
Full duplex audio according to IEEE 1329	X	X
Working conditions		
Working temperature	0 to 40°C	0 to 40°C
Storage temperature	-30 to 60°C	-30 to 60°C
Reliability: MIL STD 810F, Method 516.5 Procedure VI	X	X
IP 64 in accordance with IEC 60529	X	X
Hardened cover	X	X
Magnesium LCD assembly	X	X
Keys (with or without associated LEDs) & LED		
4 context-sensitive keys	X	X
Dedicated Push to Talk key	X	X
5-direction navigation & control	X	X
Menu & return navigation key	X	X
Volume control (high/low)	X	X
Start and stop key	X	X
Bar code reader		X

	Aastra 340w	Aastra 342w
Message LED	X	X
LED outside coverage area	X	X
Call signaling LCD	X	X
Peripherals		
USB interface for wall-mounted power supply and configuration	X	X
2.5 mm TRS socket for wired headset	X	X
Bluetooth	X	X
Features		
Customizable screen background	X	X
Ringer setting (10 ring tones)	X	X
Notification setting (10 alerts)	X	X
Buzzer and buzzer-based notification options	X	X
Internal speed dial number	X	X
Internal contact directory: 1000 entries	X	X
(Incoming, outgoing and unanswered) call logs - 20 each	X	X
Emergency call button	X	X
Answering without picking up the handset	X	X
Quality of Service		
Multimedia WMM Wi-Fi	X	X
WMM Power Save WMM Admission Control	X	X
IEEE 802.1p/Q tagging (VLAN)/DSCP tagging	X	X
Applications		
Ekahau Real Time Location Services	X	X
Calendar - Exchange Server integration Display of day - month, agenda popup	X	X
Instant messaging: terminal to terminal or client to terminal via Microsoft OCS or Lync	X	X
Webkit browser for application integration	X	X

2.8 Telephony features

Users have access to SIP communication services.

The main telephony functions are:*

- Up to six (6) telephone line appearances
- Call Hold/Resume function
- Last Call Return
- Music on Hold, Consultation Hold
- Call Waiting, Call forward, call Transfer
- Overlap dialing
- Bridged Line Appearance (BLA)
- Three-Way Conferencing (local)
- Find-Me call forking
- Automatic Answer
- Call Park & Retrieve
- Group Call Pickup
- Multiple Calls per Line
- Do Not Disturb
- Caller and Calling line information
- Call Reject

*Summary only – actual feature support will vary among call platforms. Please refer to call platform documentation for list of supported features.

3 WLAN infrastructure and integration of Aastra 340w/342w

The following requirements apply to WLAN access points:

- Wireless network management standard **IEEE 802.11a, b g or n**
- Support of **WPA2 encryption** (Wi-Fi Protected Access) (recommended)
- For WPA, compatibility with **Pre-Shared Key (PSK) authentication**
- The access points must take into account the WMM Wi-Fi Multimedia standard.
- The access points must support and have activated **WME** (Wireless Media Extensions), also known as **WMM** (Wi-Fi Multimedia) or **802.11e**. Otherwise, terminals A340w & A342w will not be able to connect to the access points. The operator boxes do not necessarily support these standards, just like RFP 43w, today.
- A study of voice over Wi-Fi deployment is necessary to ensure a level of radio service, especially for handover.

3.1 IEEE 802.11 WLAN standards

The IEEE 802.11 (ISO/CEI 8802-11) standard is an international standard covering the characteristics of the local wireless network (WLAN).

The table below shows the various revisions of standard 802.11 and what they mean:

Standard	Surname	Description
802.11a	Wi-Fi 5	Standard 802.11a (known as *Wi-Fi 5*) ensures that a high flow rate can be achieved (within a radius of 10 meters: 54Mbit/s theoretical, 30Mbit/s actual). It specifies 52 channels of radio sub-carriers on the 5GHz frequencies (U-NII band = Unlicensed – National Information Infrastructure), eight non-stacked combinations can be used for the main channel.
802.11b	Wi-Fi	Standard 802.11b offers a theoretical flow of 11Mbit/s (6 Mbit/s actual) with a broadcast range that can reach 300 meters in a clear environment. The range of frequencies used is the 2.4 GHz band (ISM band = Industrial Scientific Medical) which has, in France, 13 available radio channels of which a maximum of 3 are non-stacked.
802.11e	Quality of Service	The purpose of Standard 802.11e is to provide quality of service possibilities in the *data link* layer. Thus, the aim of the standard is to define the needs of the various packages in terms of appropriate band and transmission time in order to provide, in particular, better transmission of voice and video.
802.11f	Roaming	Standard 802.11f is a recommendation for improved inter-compatibility between access points from different vendors. It offers the *Inter-Access point roaming protocol* which allows a roaming user to change his access point in a transparent way when he changes location, no matter the access point markers that exist in the network infrastructure. This is known as *roaming*.
802.11g		Standard 802.11g provides a high flow rate (54 Mbit/s theoretical, 26Mbit/s actual) on the 2.4 GHz bandwidth. Standard 802.11g is backwards compatible with standard 802.11b, which means that 802.11g equipment will work with 802.11b. This capacity means that new equipment can offer 802.11g while still being compatible with the existing networks which often still work in 802.11b. It is possible to use a maximum of 3 non-stacked channels.

Standard	Surname	Description
802.11i		The purpose of standard *802.11i* is to enhance transmission security (key management and distribution, encryption and authentication). This standard is based on the AES (*Advanced Encryption Standard*) and offers encrypted communications for transmissions using 802.11a, 802.11b and 802.11g technologies.
802.11n	WWiSE (World-Wide Spectrum Efficiency) or TGn Sync	The theoretical flow achieved is 540 Mbit/s (actual flow 100 Mbit/s in a range of 90 meters) thanks to MIMO (Multiple Input Multiple Output) and OFDM (Orthogonal Frequency Division Multiplexing) technologies. Standard *802.11n* will use the 2.4 and 5 GHz frequencies simultaneously. It can combine up to 8 non-stacked channels.

Wi-Fi terminals A340w and A342w support the following Access Point configurations:

Standard	Frequency	Flow
802.11a	5.15 - 5.25 GHz 5.25 - 5.35 GHz 5.47- 5.725 GHz 5,725 - 5,825 GHz	6, 9,12, 18, 24, 36, 48, 54 Mbps
802.11b	2.4 - 2.4835 GHz	1, 2, 5.5, 11 Mbps
802.11g	2.4 - 2.4835 GHz	6.9, 12, 18, 24, 36, 48, 54 Mbps
802.11n	2.4 & 5Ghz	21.7, 43.3, 65, 72.2 Mbps

3.2 Access Points and Aastra A340/A342w interoperability tests

Aastra 340w/342w have been tested and validated with following Wi-Fi solutions:

VIEW Partner	AP Models	WLAN Controller Models	QoS	Security	Software Version
Alcatel-Lucent	12x	OmniAccess 43xx, 4504, 4604, 4704, 6000	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	6.3.1.2
Aruba	12x	6xx, 3xxx, 6000, 7200	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	6.1.3.4
Avaya(Nortel)	8100 Series	8180	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	2.0.0.084
Avaya (Juniper)	233x	WSS 2350,2360, 2361, 2380, 2382; MX2800	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	7.6.3.1
Brocade	AP 7131N, 7131, 650 (650 must have controller)	RFS 4000, 6000, 7000 or standalone	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	5.2.3.0
Cisco	60x, 70x, AP801, AP802, 104x, 113x, 114x, 124x, 125x, 126x, 155x, 160x, 260x, 350x, 360x	2500, 5500, 7500, 8500, WLC SW for SRE, WiSM2 , Virtual Controller	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	7.4.110.0 7.5.102.0
	60x, AP801, AP802, 104x, 113x, 114x, 124x, 125x, 126x, 155x, 260x, 350x, 360x	2500, 5500, WiSM2, WLC SW for SRE	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	7.3.101.0 7.2.110.0
	60x, AP801, AP802, 104x, 1121, 113x, 114x, 122x, 123x, 124x, 125x, 126x, 13xx, 155x, 350x	2100, 2500, 4400, 5500, 7500, 3750G, WLC SW for SRE, WiSM, WiSM2	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	7.0.220.0
	AP801, 113x, 114x, 1121, 122x, 123x, 124x, 125x, 13xx	2100, 4400, 5500, 3750G, WiSM, WLC Module	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	6.0.202.0
	104x, 114x, 126, 160x, 260x, 350x, 360x	autonomous	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	15.2.4-JA1
Dell	W-AP68, 92/93, 104/105, 124/125, 134/135	W-620, 650,651, 3200, 3400, 3600, 6000/6000M3	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	6.1.3.4
Enterasys	3605,3610,3620,3630, 3640	C 20, 25, 4110, 5110, 5210; V2110	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	8.11.06.0002
Extreme Networks	AP 4532, 4600 (4600 must have controller), 4710, 4750, 4760	WM 3400, 3411, 3600, 3700 or standalone	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	5.2.3.0
Juniper (Trapeze)	WLA372, 422, 432, 522, 522E, 532, 532E	WLC2, 8, 200, 216, 800, 880, 2800	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	7.6.3.1
Meru Networks	AP3xx	MC1000, 1500, 3000, 4100, 5000	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	4.0SR5-5
Motorola	AP 6532, 7131N, 7161, 650 (650 must have controller)	RFS 4010, 4011, 6010, 7010; NX 9000, 9500	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	5.2.3.0
Ruckus	ZF 7363, 7982	ZD 1100, 3000, 5000	Wi-Fi Standard	WPA/WPA2 PSK WPA2 Enterprise	9.5.0.99.124

Note: this list is subject to change and evolution. Please contact your Aastra representative in case of any question.

3.3 Quality of Service (QoS)

3.3.1 Supported protocols

Quality of Service (QoS) is a generic requirement in the IT network sector and, therefore, also applies to WLAN networks.

The encoding laws supported are:

- Codec G.711 - 10, 20 or 30ms (Recommendation: 30ms, in order to save the telephone battery).
- G.729A - 10 to 80ms (per 10ms). Recommendation: 30ms, in order to save the telephone battery
- G0.722

The telephones use the following ports:

- RTP 2222 & RTCP 2223.

The quality of service on a WLAN network is characterized by specific protocols described in the IEEE 802.11e protocol. The 802.11e protocol includes the 3 specifications - Wi-Fi multimedia (WMM), WMM Power Save, and WMM Call Admission Control. By default, terminal A34xw is set to WMM.

The Access Points must be compatible with all these specifications. If not the terminals will not be able to connect to them. For instance, these terminals may not be able to connect to provider boxes such as Livebox which does not support these characteristics or other standard Access Points.

Moreover, the DECT RFP / Wi-Fi RFP 43 does not support these protocols in its current version. Therefore, terminals A340w/A342w cannot connect to them.

The 1st WMM specification allows some priorities to be managed, and the recommended prioritization categories are:

Table 4 - WMM Access Categories

WMM Access Category	Priority level	802.1d tags	Client wait time + random backoff window (slots)	SIP traffic type
Voice (AC_VO)	highest	7, 6	2 + 0 to 3	Voice
Video (AC_VI)		5, 4	2 + 0 to 7	Call control
Best Effort (AC_BE)		0, 3	3 + 0 to 15	Other (PTT, OAI, RTLS)
Background (AC_BK)	lowest	2, 1	7 + 0 to 15	Not used

A340w/A342w can be configured in terms of prioritization marking: DSCP/ToS fields for signal (SIP) and voice (RTP) traffic. These classifications allow the Access Point to prioritize traffic

The terminal's default DSCP values are:

- Voice: 46
- Signaling: 44
- Others (Push To Talk, OAI and RTLS): 0

To benefit from this QoS, it is important that the WLAN infrastructure processes these fields and prioritizes the packets. The WLAN infrastructure must map this Diffserv classification in the "ToIP" VLAN of the client's IP LAN in order to offer an end-to-end quality of service.

WWM Call Admission:

This specification allows each Access Point to accept or reject the flow associated with a request. However, in the Wi-Fi environment, there are too many negotiation requests which considerably reduces the bandwidth. Therefore, we recommend for voice over Wi-Fi, not to activate this service on the Access Points. So, it is necessary to monitor the traffic in order to then modify the radio engineering and possibly add some Access Points and provide more bandwidth.

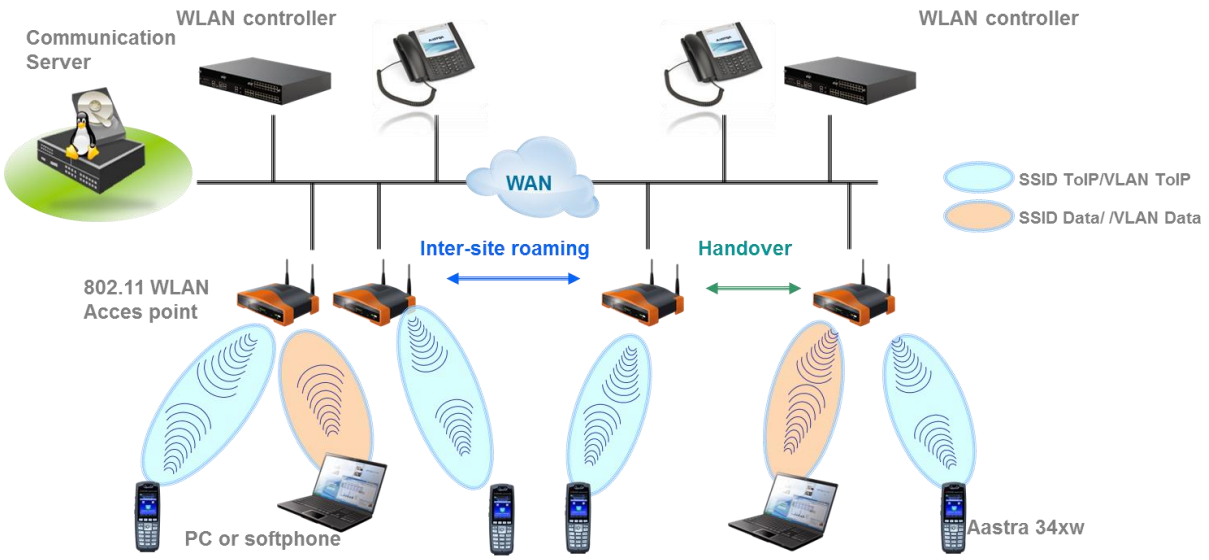
Roaming or "Fast Roaming":

The process whereby a terminal changes from one base station to another (roaming) is managed by the WLAN system controller and is very often (in fact always) a proprietary protocol. Which means that certain WLAN systems manage it better than others. Generally, WLAN solution designers call this "Fast Roaming". The Aastra 34xw handset does not require any particular protocol for roaming, but deployment must be carried out to make a sufficient coverage recovery so the negotiation can take place in a sufficiently transparent manner.

When roaming, in order to make/receive a call without interference, the transfer time from one base-station to the next must be less than 30ms. Beyond that, the user may notice a switchover.

We recommend that a specific ToIP SSID be used in order to separate the ToIP flows from the data flows on the Access Point and limit broadcasts.

Roaming or « Fast Roaming » :



3.3.2 Battery, 802.11e, WMM

The Aastra 34xw battery is a lithium-ion polymer battery. Its capacity is 1250mAh with a voltage of 3.7 V.

Maximum transmission power is 100mW.

The storage batteries' energy consumption rate depends on the properties of the Access Points (AP) used, namely through protocol activation. It is possible to deactivate some parameters in order to save the terminal batteries.

The terminal and WLAN infrastructure must respect the WMM Power Save protocols. In fact, if the terminal is set to Power Save mode and not its infrastructure, its autonomy will still be more reduced than if the Power Save mode had not been activated because there will be no response to Power Save requests.

Aastra 34xw supports various modes:

- The most powerful power saving algorithm is WMM/U-APSD mode (Unscheduled Automatic Power Save Delivery) defined in 802.11e. If this mode is selected in the terminal's WLAN profile whereas it is not supported by the AP, the result will be worse; the AP and terminal must have the same configuration.
- The other battery power saving mode is mode 802.11 PS-Poll. This mechanism was initially defined in standard 802.11. Its major inconvenience is that it delays a major part of the packets. This delay corresponds to the low-power beacon interval, and voice quality is affected by this. Nevertheless, this mode may be useful when no other power-saving mode is supported by the access point but a long conversation time is required.

These two modes are used when a communication is made. In standby mode, it is possible to use the DTIM function (Delivery-Traffic-Indicator-MAP) in order to enhance standby autonomy.

If these characteristics are not supported, the storage battery life may be reduced by half. The handset's power saving settings are available in the WLAN profile information.

Note that if the quality of the link is bad (because the handset is far from the AP), the autonomy in conversation and standby modes is drastically reduced. It is also reduced if the speaker or tone volume is high, if the key and screen backlight function is often used or if the vibrator/buzzer is activated.

3.4 WLAN network coverage

The range of the WLAN handset is lower than that of the fixed WLAN peripherals of a PC used solely for data transfer. In fact, data traffic tolerates more packet losses than voice communications. It is therefore necessary to ensure that voice communication starts with a signal intensity of - 70dBm on the AP.

The range may be limited by walls or reinforced concrete, microwave ovens, obstacles, floor heaters, etc. In fact, the Wi-Fi technology shares frequencies with other devices like microwave ovens or radars (alarms). Moreover, the companies' urban landscape may also be subject to interferences from adjacent peripheral devices belonging to individuals or other companies, since Wi-Fi is now widely used (internet box, etc.).

Particular attention should be paid to the coverage study. The design of a WLAN network supporting voice and data is not the same as the design of a network supporting data only.

The WLAN design is equally different between a voice over Wi-Fi network and a data over Wi-Fi network, due to the use of this different application:

- **Voice**: coverage of the entire site (corridors, coffee machines, etc.)
- **Data**: specific coverage areas (conference rooms, temporary offices, etc.).
- **Overlap** between the Wi-Fi base stations in order to provide a handover service between the Access Points (necessary but not sufficient condition). In fact, it is important for the terminal to detect the second base station, to authenticate to it and switch over during communication from one Access Point to another. Therefore, it is necessary to have enough coverage recovery between the Access Points to offer this service. A 15 to 20% radio recovery between Access Points is generally sufficient for a user walking under a radio coverage. If this user is running or driving a vehicle, this overlap must be increased to allow handover between the Access Points. The negotiation process of Wi-Fi terminal A34xw between 2 Access Points takes less than one second. However, it is necessary for a person walking to have 2 to 3 seconds overlap time so the negotiation can take place. The switching choice is made when the signal of the nearby base station is 10dB more than the base station to which the user is connected.

The Access Points must be configured to authorize low data transmission rates. This has the advantage of maximizing the radio range of the Access Points. If not, the Access Points must be multiplied if only high transmission rates are authorized. It is necessary to configure the Access Points with the lowest data transmission rate; the other transmission rates must be set to "supported".

For example:

- If an 802.11b/g Access Point with 1Mbps, 2Mbps, 5.5Mbps and 11Mbps is set to "Mandatory" for all the terminals, the handset requires -75dBm in all the areas.
- If an 802.11b/g Access Point with 1Mbps is set to "Mandatory", and the other flow rates to "Supported" for the other terminals ("or Authorized"), the handset requires -75dBm in all the areas.
- If an 802.11a Access Point has 6Mbps, 12Mbps and 24Mbps on "Mandatory" for the terminals, and the other terminal flow rates on "Supported", the handset requires -58dBm 60dBm in all the areas.

Moreover, in environments with high electromagnetic disturbances (staircases, lifts) the 5Hz range is sufficient, and it is then pertinent to set the Access Points to 2.4Ghz.

The recommended signal characteristics are given in the table below: The maximum range of each Access Point is determined by using this data.

Table 1 – 2.4GHz

	2.4GHz 802.11b/802.11g (CCK)				2.4GHz 802.11g (OFDM)							
Rate (Mb/s)	1	2	5.5	11	6	9	12	18	24	36	48	54
Best Practices (dBm)	-75	-70	-69	-65	-67	-66	-64	-62	-60	-56	-52	-47

Table 2 – 5GHz

	5GHz 802.11a (OFDM)								5GHz 802.11n (OFDM)							
Rate (Mb/s)	6	9	12	18	24	36	48	54	6.5	13	19.5	26	39	52	58.5	65
Best Practices (dBm)	-67	-65	-63	-61	-58	-54	-52	-50	-67	-65	-63	-61	-58	-54	-52	-50

Table 3 – 5GHz

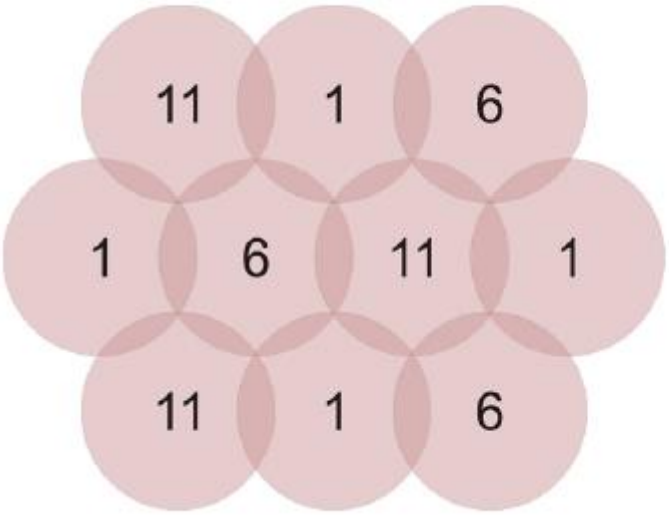
	5GHz 802.11a (OFDM)							
Rate (Mb/s)	6	9	12	18	24	36	48	54
Best Practices (dBm)	-60	-59	-58	-56	-53	-49	-47	-45

This need must be taken into account and then results in a strong extension of the Wi-Fi network to support voice.

Selecting channels

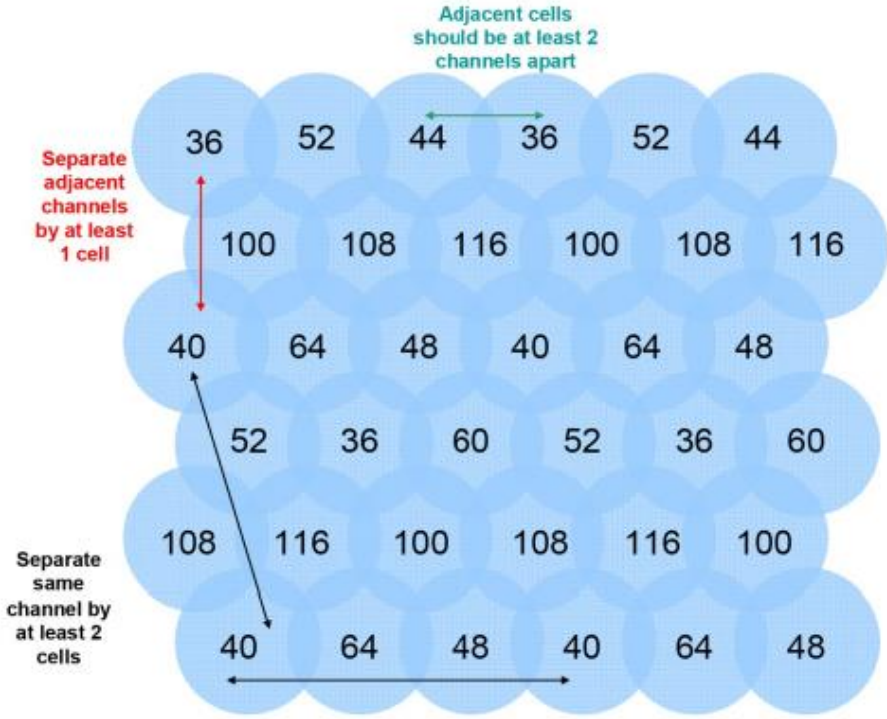
While deploying and configuring Access Points, it is important that the channels do not overlap between adjacent Access Points as described in the diagram below.

Figure 3 - 802.11b/g Non-interfering Channels with Overlapping Cell Coverage



In 802.11a the number of channels is higher; it is then possible to perform this type of configurations:

Figure 5 - 802.11a Non-interfering Channels with Overlapping Cell Coverage



For more information, see the voWLAN solution deployment guide.

3.5 Access Point traffic

The bandwidth is directly linked to the codec used, the payload of each packet (20, 30 ms…) and IP network headers. However, the bandwidth required in 802.11a/b/g is higher and is not a linear function.

Example: a G711 – 64kbit/s call uses 4.5% of the bandwidth of an Access Point at 11Mbit/s and approx. 12% at 2 Mbit/s. In this example, 4 simultaneous calls on this Access Point consumes approx. 18% of the bandwidth of the Access Point at 11Mbit/s or approx. 48% at 2Mbit/s or approx. 90% at 1Mbit/s.

The maximum number of simultaneous calls per Access Point is determined by dividing the recommended bandwidth by the percentage of the bandwidth used by each individual call.

Note that 25 to 35 % of the Access Point bandwidth must be reserved to channel negotiations and reconnection attempts. So only 65 to 75% of the theoretical bandwidth is available.

For example, if all the calls on the same Access Point are theoretically using 5.4 % of the bandwidth at 11Mbit/s, the number of potential simultaneous calls at this flow rate would be 12 (65% of available bandwidth / 5.4 % per call).

Moreover, there are other parameters specific to each Access Point or to each configuration, which makes the number of simultaneous calls per Access Point very difficult to evaluate before deployment on site.

3.6 Security on a WLAN and Aastra 34xw

In order to use a WLAN some precautions need to be taken with regards to the problem of security, both for the Access Points and for the WLAN terminal.

It is necessary to take the following into account:

- Authentication on the network
- Authentication on the communication server application.

In terms of network authentication, the terminal range supports different methods which offer a level of security but also has some more or less strong impacts on the telephony application:

- WPA, personal WPA 2 (PSK)
- WPA2 Enterprise (PEAPv0 with MSCHAPv2 and EAP-FAST)
- PEAPv0/MSCHAPv2
- EAP-FAST
- OKC

Note about WPA 2 Enterprise

Depending on the Radius server configuration and the access and negotiation delay on this Radius server, it is possible to significantly process calls during handover from one Access Point to another, especially if the Radius server is centralized and only accessible via A WAN. We recommend using Access Points with Fast Handoff mechanisms (authentication cache on the Wi-Fi network). We support two Fast Handoff mechanisms: OCK and CCKM. We recommend that the authentication server be located on the user's site.

Mac address and authentication based filtering

One of the authentication methods may be based on Mac address analysis by the Access Point. This method requires a too heavy CPU load for the Access Points to be compatible with a voice service and, in particular, a handover function. **This configuration should not be programmed with terminals A34xw.**

Filtering by Virtual LAN

We recommend using distinct VLANs between data and voice and mapping the SSIDs with the VLANs to filter the different uses. It is necessary to configure a voice SSID.

Firewalls and traffic filtering

It is possible to filter flows through a firewall. However, the configuration must not affect the voice quality in terms of delays and delay variations.

The list of SIP terminal A34xw flows is as follows:

Port Number	Protocol	Outgoing	Incoming	UDP or TCP
21	FTP	Provisioning, Logs		TCP
22	SSH	Admin	Admin	TCP
23	Telnet	Admin		TCP
53	DNS			UDP
67	DHCP	Server		UDP
68	DHCP	Client		UDP
69	TFTP	Provisioning, Logs		UDP
80	HTTP	Provisioning, Logs, Pull Web Interface, Poll		TCP
123	NTP	Time Server		UDP
389	LDAP			
443	HTTPS	Provisioning, Logs		TCP
514	Syslog	Logs		
636	LDAP			
2222	RTP	Media Packets	Media Packets	
2223	RTCP	Media Packets Statistics	Media Packets Statistics	
5060	SIP	SIP Signaling	SIP Signaling	
5061	SIP over TLS	Secure Signaling	Secure Signaling	
7778	OCS			

These flows are used according to site configuration.

3.7 Managing Aastra 34xw

It is possible to manage this terminal from a central point, for provisioning purpose.

This terminal has the following management characteristics:

Self-provisioning

- DHCP services
- Protocol: FTP (by default)/ TFTP / http / https
- Automatic provisioning on start-up
    - Association, by default, with SSID
    - Automatic routing to the DHCP server address bootp option 66
- File format
    - .cfg (Generic Configuration File)
- Configuration
    - Network / Wi-Fi / Security / SIP Proxy, account / system settings (language, time, location) / standard call / DATI / Bar codes / Bluetooth / Softkeys
- Updating the latest firmware

The following DHCP options are possible for a terminal A340/2w.

DHCP Option	Value Expected	Purpose
1	IP Address (i.e. 255.255.255.0)	Subnet Mask
3	IP Address (i.e. 192.168.1.1)	Default Gateway
6	IP Address (i.e. 192.168.1.10)	DNS Server IP Address
7	IP Address (i.e. 192.168.1.20)	Syslog Server
15	String (i.e. mycompany.com)	DNS Domain Name
42	IP Address (i.e. 192.168.1.30)	SNTP Server Address (Network Time Protocol)
66	IP Address (i.e. 192.168.1.40)	Boot Server (Provisioning Server)
151	IP Address (i.e. 192.168.1.45)	SIP Server Address
152	IP Address (i.e. 192.168.1.60)	OAI Gateway

Updating the firmware manually

- Updating the firmware via the telephone menu, from the local server.
- Protocol: TFTP/http/https.

Administration

- The administrator menu is protected with the administrator password.

SNTP synchronization

Diagnosis

- Network/ WLAN / RTP / Ping test / Hardware diagnosis, etc.

The user configures the download server IP address on the terminal and selects the protocol: http, https, TFTP:

3.8 Troubleshooting tool

The user has a troubleshooting tool, integrated into the terminal. It can make some pings on the network, and run some diagnosis on the radio quality and on the signals received. He also has some statistics on sent, received, and failed packets. It can also send SYSLOG commands. Please refer to configuration manual for more information.

3.9 Deploying external WLAN tools

In order to use VoWLAN solutions it is necessary to ensure and check that the security and WLAN network compliance rules are respected. Most importantly, interference problems must be detected:

- WLAN interference is due to several WLAN networks using similar channels.
- Non-WLAN systems can generate interference because they use the same radio frequencies (alarms, micro-waves, fire systems, etc.)

It is necessary to carry out a Voice over Wi-Fi deployment radio study before deploying any terminal.

4 Communication Server support

4.1 Aastra Communication Servers

Aastra 340w/342w are supported with the following Aastra communication servers:

- MX-ONE from R5.0 (SP4)
- Aastra 5000 from R5.4 (SP2)

Please refer to call manager documentation for more information on features and prerequisites.

4.2 Third Party Call Managers

Aastra 340w/342w are SIP standards based VoWLAN telephones that complies with many SIP enabled call managers.

Please refer to call manager documentation for more information on features and prerequisites.