



Avaya, Aruba and Nokia Mobility Solution

IP Telephony

Contact Centers

Mobility

Services

APP NOTE

Abstract

This application note describes the Avaya, Aruba and Nokia mobility solution. This document is not a user guide or sales brochure. It is a 'how-to/tips' application note for the Avaya, Aruba and Nokia Wi-Fi solution targeting engineers and administrators.



TABLE OF CONTENTS

1. Terminology and Acronyms.....	4
2. Dual Mode Solution Overview	5
General Solution Architecture.....	5
3. Avaya one-X Mobile Edition Dual-Mode Application	6
Avaya Communication Manager and SIP Enablement Services.....	6
Nokia E-Series Devices.....	7
4. Equipment and Software Validated	8
5. WiFi System Description	9
6. WiFi System Architecture	9
ArubaOS Software	9
Aruba Mobility Controllers	10
Aruba Access Points	11
Centralized Network Management.....	11
7. ARUBA Access Point Controllers	11
8. Access Points.....	12
9. VoIP Performance Metric	12
10. Dual-Mode Test Configuration	13
11. WiFi System Settings for VoIP Dual-Mode	14
General WiFi Settings.....	14
1. SSID	14
2. Data Rates (Default setting).....	14
3. DTIM (power save settings).....	14
4. RTS threshold (Default Settings).....	14
5. Antenna Diversity	14
6. Band Preference.....	15
7. RF Management / Channel and power settings (ARM).....	15
8. Call Admission Control.....	15
9. Miscellaneous.....	16
Extended Battery	16
Proxy-arp.....	16
Local probe response	16
12. WiFi Security Settings	17
Open.....	17
WEP	17
WPA-TKIP-PSK	17
WPA2-AES-PSK.....	18
WPA2 PEAP 802.11i	18

13. Security Firewall Settings and QoS	19
14. WiFi Multi-Media (WMM) Basic Support	20
QoS (802.11e) Parameters to Optimize Voice.....	20
15. Avaya one-X Mobile Edition Settings	20
16. VoIP Settings	21
Nokia phone Administration	21
Create and configure your WLAN Access Point Profile	21
17. Create and configure SIP Profile	36
18. Setting different dual-mode network modes:	38
19. Dual-Mode Assisted Handover	38
20. References	40

1. Terminology and Acronyms

Term	Meaning
AST	Advanced SIP Telephony
Avaya CM	Avaya Communication Manager
Avaya SES	Avaya SIP enablement services
EC500	Avaya EC500 (Extension to Cellular) – An offer that lets cell phones under control of a public wireless carrier function as if they were extensions on an Avaya CM .
FMC	Fixed Mobile Convergence
FNE	A Feature Name Extension is a phone extension you can dial that allows you to access an Avaya CM feature from your cell phone.
FNU	Feature Name URI
OPS	Off-PBX station
PBFMC	PuBlicFMC, RTU needed for CM 4.0 Dual-Mode (maps to user's cell phone)
PVFMC	PriVateFMC, RTU needed for CM 4.0 Dual-Mode (maps to user's cell phone)
PBX	Private Branch Exchange – A generic name for a premise based switch supporting telephony features owned by an enterprise. The Avaya CM is a type of PBX.
SES	Avaya SIP Enablement Services
SIP	Session Initiation Protocol

2. Dual Mode Solution Overview

This application note describes the Avaya, Aruba and Nokia mobility solution. This document is not a user guide or sales brochure. It is a 'how-to/tips' application note for the Avaya, [Aruba and Nokia](#) WiFi solution targeting engineers and administrators.

The Dual Mode solution has been verified by the Avaya engineers. This application note describes the configuration steps and the software version information that was tested for the solution in the Avaya labs.

➤ General Solution Architecture

- Avaya one-X Mobile for S60 3rd Edition Dual Mode
 - Client/Phone/Device Software is responsible for all the handoff decisions
 - NO EXTRA H/W required
 - Re-use existing Avaya servers (CM and SES)
 - Reuse EC500 FNEs and SIP AST FNUs
 - Provides Enterprise Telephony Features such as Transfer, Conference, Call Park, Call Pickup, etc.
 - *Bottom-line:* Get Dual-mode features without adding additional servers
- Provides simple user access to Avaya Communication Manager mobile telephony services and features
- Designed to simplify user experience and access to Extension to Cellular features
- Bind graphical menu with Feature Name Extensions (FNE's)
- One Business Number
- Simplified access to "Top 20" PBX features – a business softphone on a mobile phone
- Full business call control: hold, conference, transfer, assistant support, extension dialing
- It is your office phone!
- One number access – incoming office phone calls extended to mobile phone
- One voice mail to check
- Outgoing calls use corporate network
- Centralized management & reporting
- Easily switch between personal and business use of mobile phone
- Support for 11 Languages

3. Avaya one-X Mobile Edition Dual-Mode Application

Avaya one-X mobile Dual Mode refers to a device that is capable of using two networks: GSM and Wi-Fi/SIP (WLAN 802.11b/g) one-X mobile Dual Mode = GSM + Wi-Fi/SIP

➤ Avaya Communication Manager and SIP Enablement Services

Following are the software requirements for the Avaya Communication Manager and Avaya SES:

Avaya CM Requirements

- CM SW Release 3.1.2 Load 632.1 and higher (CM 4.0).
- RTUs/Licensing
 - CM 3.1.2: Needs EC500 and OPS
 - CM 4.0: Needs PBFMC and PVFMC (PuBlicFMC / PriVateFMC)
 - SIP Trunking licenses required
- Need to administer “no-hld-cnfr” button on all stations for conferencing to work.
- Need to have respective feature buttons such as “call-park”, “call-pkup”, if being used.

Avaya SES Requirements

- SES 3.1 Release or greater.
- Licensing
 - Client licenses required
 - Home or Home/Edge licenses required

➤ **Nokia E-Series Devices**

Nokia Device Requirements

- Only E60, E61, and E70 are supported for dual-mode.
- Device must have at least the following FW:
 - On the main Nokia screen, enter following sequence as a phone number:
*#0000#
 - You should see the FW version here; needs to be at least 2.0618.06.05
 - If the device has an older FW, Nokia allows users to flash the FW using a Software Update Tool from Nokia's website
 - There are known issues with certain Nokia E-Series models and upgrading the firmware to the minimum version 2.0618.06.05. This has to do with the region code of the E-Series set. Some users are not able to upgrade their phones (No Software Upgrade Available).
Note: more detail is available at
<http://discussions.europe.nokia.com/discussions/board/message?board.id=swupdate&message.id=451>

For support and help, contact your local Nokia support center.

4. Equipment and Software Validated

The following equipments and software were used in the configuration shown in Table 1.

Table 1: Equipment and the Software versions used

Equipment	Software
Avaya SIP-Enablement Services (SES)	SES 3.1.1 SES03.1.1-03.1.114.0
Avaya CM	Communication Manager 3.1.2 R13x.01.2.631.1
Nokia E-61	2.0618.06.05
Aruba Controller: Aruba 800	2.5.4.0(build 12461)
Aruba Access Point: Aruba-AP 61	

Note: Refer to user guide and administration guide for other supported devices and configurations. User guide and administration guide will be available for download from Avaya Support Site.

- Go to <http://www.avaya.com/>
- Click on 'Support' link
- Click on 'Find Documentation and Downloads by Product Name' or click on 'Downloads'
- Click on 'one-X Mobile Edition'
- Click on 'Documents'
- Select Release 4.0

5. WiFi System Description

The solution is designed to interoperate with the Avaya Communication Manager, Avaya SES, and Nokia handsets at the edge. Avaya's Communication Manager integrates telephony call processing, call control, messaging, contact center and a widely accepted application programming interface into a highly scalable architecture designed to support both circuit-based and IP-based telephony within a distributed Enterprise communications network.

Note: Section 4 through 8 and 10 through 13 were provided by Aruba.

6. WiFi System Architecture

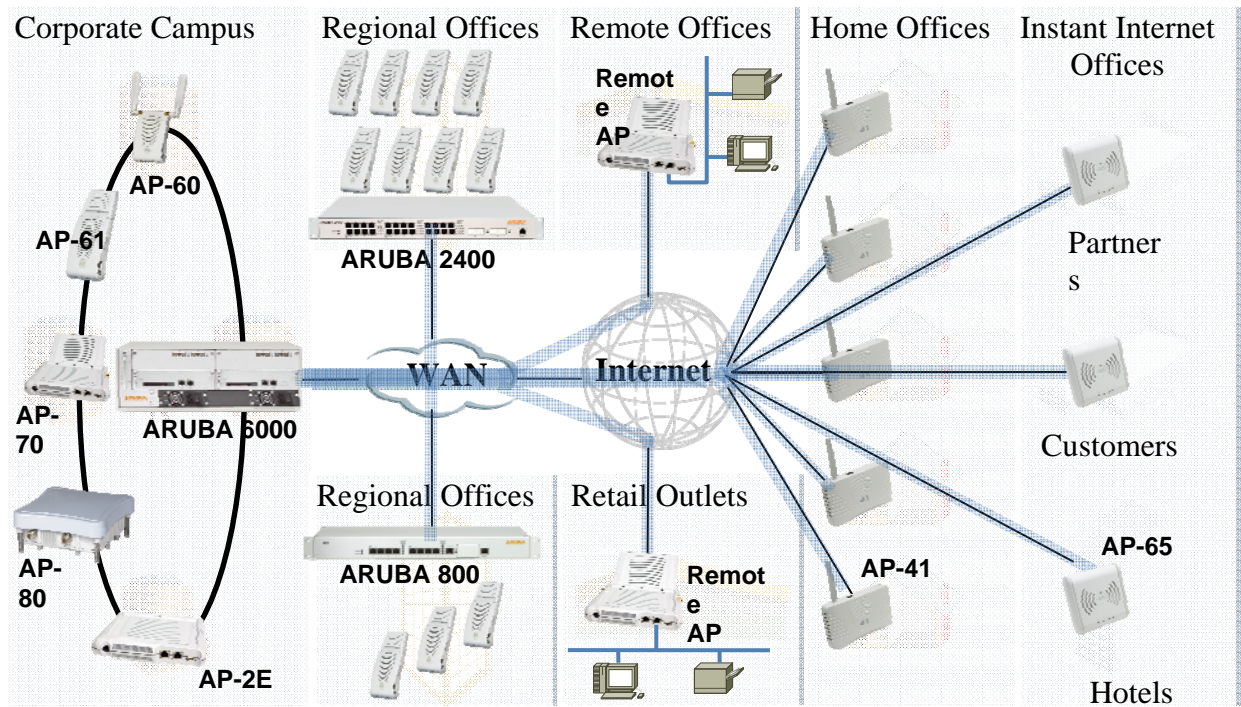
Aruba's Mobile Edge allows users and devices to connect over the air and across any network, to securely gain access to Enterprise resources. It is a new layer in the network that logically sits on top of existing, fixed networks and fulfills the requirements of security, mobility and convergence without requiring major upgrades to the existing network. The Mobile Edge is architected to work securely over existing IP network facilities, and extends across both private Enterprise networks as well as the public Internet. Aruba's Mobile Edge System consists of four components:

ArubaOS Software

Providing unified services to power the Mobile Edge, ArubaOS is a comprehensive suite of system software for Aruba Mobility Controllers and Access Points. ArubaOS uniquely integrates services of security, mobility, application-awareness, management and RF-tuning together to deliver the most secure and reliable anywhere, anytime access for Enterprise users.

Aruba Mobility Controllers

Enabling secure mobile services requires a combination of network elements and RF intelligence. Aruba offers the only mobile security system with an integrated ICSA-certified stateful firewall and hardware-based encryption. All Aruba Mobility Controllers combine powerful packet processing with 10/100/1000 Mbps Ethernet switching, stateful LAN-speed firewall, VPN termination, wireless intrusion protection, AAA, client integrity, captive portal and advanced RF management within a single network device. All Aruba Mobility Controllers integrate non-disruptively into any existing L2/L3 wired network with no logical or physical re-configuration of the underlying transport infrastructure required.



Aruba Access Points

When Aruba dependent Access Points (APs), are connected to an IP network, they automatically discover the Aruba Mobility Controller, configure themselves and begin operating: the Mobility Controller is responsible for downloading software images, configuring and coordinating all dependent APs. APs continuously scan the RF environment, supplying information to optimize radio coverage and provide wireless intrusion prevention without having to deploy a separate sensor network. Aruba's dependent AP architecture coupled with radio planning optimization and workspace deployment options – out of the ceiling – greatly reduces WLAN deployment costs. IT staff can place APs supporting power over Ethernet (PoE), in employee cubicles leveraging existing Ethernet cabling.

Aruba offers a range of APs with single- and dual-radio capability: all are capable of operation in the 2.4 GHz (802.11b/g) and 5 GHz (802.11a) bands. Indoor and outdoor options are provided, including integrated wireless bridges.

Centralized Network Management

Comprehensive network planning, configuration and monitoring are all achieved with either a single Mobility Controller or a dedicated Mobility Management System (MMS). In both cases, the management interface is presented to clients as an intuitive graphical user interface (GUI). To extend management capabilities further, either system can be used with existing NMS systems and best of breed management tools.

7. ARUBA Access Point Controllers

The bulk of the intelligence of the Aruba Mobility System resides in the controllers. Aruba supports a number of controller models which differ only in their capacities (number of APs and number of users supported). All the controllers support the same functionality. Various software licenses need to be enabled on the controller to enable its various functionalities. The controller will still operate as a basic WLAN switch without any of these licenses but it is recommended to enable the security and QoS license to secure the WiFi network and to ensure QoS. Ensure that at a minimum the *Firewall Policy Module* is enabled on the controllers in use. The firewall Module License enables session awareness, prioritized traffic processing and packet tagging on the controller.

- Release 2.5.4.0 and below support on the air QoS in the downstream direction and wired QoS. However these images do not support WMM. Ensure that a 3.0 and above release of the software is used if WMM is being used in the environment.
- The Nokia phones have been tested for interoperability with the 2.5.4 images.
NOTE: Enabling WMM on the controllers in 3.X.X does not require additional licenses
Source: Aruba

8. Access Points

The Aruba Solution supports 802.11a and 802.11b/g mixed environments. When using dual radio APs (AP70, AP65), 802.11a and 802.11b/g modes can be enabled simultaneously. The Nokia handsets are 802.11b/g handsets. The recommended setting would therefore be to enable the 802.11b and 802.11g rates. This setting ensures that the b and g clients share the 2.4 GHz band without hidden node issues.

Note: Recommended setting is to ensure that both b and g rates are enabled on the Access Points.

- To interoperate with the Nokia handsets ensure that the single mode APs are configured to operate in the 802.11b/g modes and the dual radio APs have their b/g radios enabled and set to AP mode.

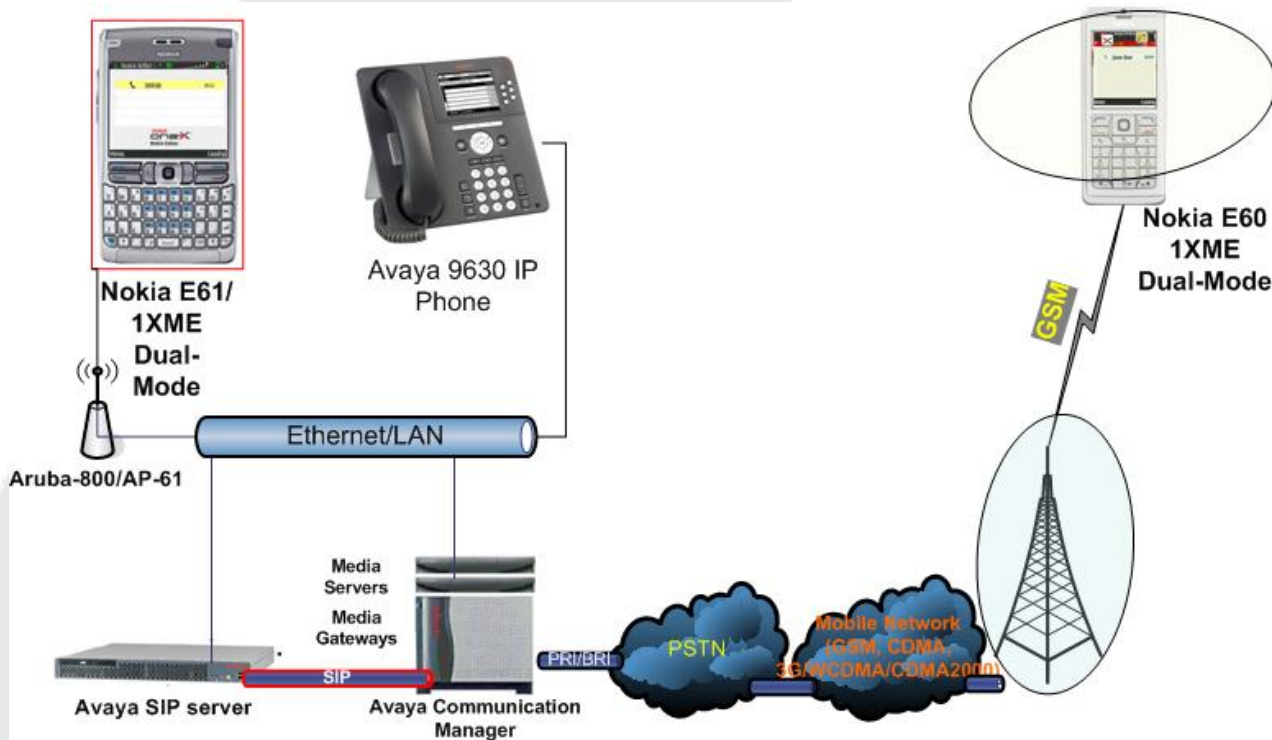
9. VoIP Performance Metric

Aruba has implemented a number of features enhancing QoS and dramatically improving client density, with independent test results showing maximum figures of 22 calls using 802.11b and 75 calls with 802.11g or 802.11a. These features allow a 2-radio Access Point to support up to 150 active voice calls under ideal conditions.

In actual deployments, not all clients will connect at the highest rate, and the network manager may choose to leave some bandwidth available for data applications. This can be achieved using the Aruba Call Admission Control feature. The CAC limit can be set in the range 10-15 for 802.11b and 25-40 for 802.11g. This ensures that the remainder of the bandwidth is used for the data devices. This data was obtained by using real G.711 phones and quality measurement tools to measure the call quality when the devices are in call. Assumption has made Since Nokia also supports SIP G.711, the call scaling numbers should be the same for scalability.

Avaya has not yet verified above voip performance statistics.
Source: Aruba

Dual-Mode Test Configuration



10. WiFi System Settings for VoIP Dual-Mode

The following section describes the settings as recommended by Aruba. For details on configuring the various parameters, refer to the Aruba user guides.

➤ General WiFi Settings

All the WiFi settings, unless otherwise specified, are made at the AP configuration level on the Aruba system.

1. SSID

The Aruba system supports all SSID formats as per the standards.

2. Data Rates (Default setting)

Recommended Setting

Basic Rates 1, 2

Transmit Rates 1,2,5,11,6,9,12,18,24,36,48,54

3. DTIM (power save settings)

The power save mode helps the WiFi devices conserve battery life. On the controller, set the DTIM value to recommended setting from Nokia (Comment: In the absence of a recommended setting for the handset use the DTIM value to 3).

Optionally, the extended battery feature of the Aruba System can be used to extend the battery life. For this to work, set DTIM to 100 and enable the extended battery life feature (see 9 Miscellaneous -> Extended Battery Life)

Recommended Setting

DTIM = 3 (if no recommendations from voice vendor)

DTIM = 100 when testing extended battery life feature.

4. RTS threshold (Default Settings)

Recommended Setting

Leave as default (2333)

5. Antenna Diversity

Recommended Setting

Leave as default

When changing this value please contact the Aruba team for additional information.

6. Band Preference

When using with the Nokia handsets

- Set the band to 802.11b/g for the dual mode single radio APs (AP61 / AP60 / AP41). Enable the radios.
- set the 802.11b/g radio to enable and in ap-mode for the dual mode APs (AP65 / AP70)

Recommended Setting

Set the band to 802.11 b/g and ensure that both b and g data rates are supported by the infrastructure.

7. RF Management / Channel and power settings (ARM)

The Aruba recommended setting for Channel and Power settings is to allow Aruba's Adaptive Radio Management to choose the right power and channel values. Enable ARM at the AP level for all the APs (can be enabled at the global level under location 0.0.0).

Recommended Settings

Enable ARM assignment and set value to single band

Enable ARM scanning

Enable VoIP aware Scan

8. Call Admission Control

Advanced Call Admissions Control is a feature unique to Aruba that prevents any single AP from becoming overly congested with voice calls. While most WLAN implementations solve congestion problems by relying on well-behaved clients that understand AP load advertised in beacons, or proprietary methods that only work with one vendor's clients, Aruba has a simple, accurate solution. Since Voice Flow Classification gives the firewall knowledge of which clients have active voice calls, ArubaOS allows direct control of the upper limit of calls per AP. Once that threshold is reached, other idle voice devices in that cell are load-balanced to adjacent cells, avoiding disruption of calls in progress.

The 802.11e standard includes TSpec signaling, which will be used by future voice clients to accomplish bandwidth reservation and assured CAC. Aruba supports the TSpec signaling protocol as an additional input to the Advanced CAC feature, but as it may be some years before it is widely

implemented on clients, Advanced CAC functionality will be required for the foreseeable future.

Recommended Settings

Enable VoIP Call Admission Control (default is disable)

Enable VoIP Active Load Balancing (default is disable)

Enable VoIP CAC Drop SIP Invite (default is disable)

Enable VoIP CAC Disconnect Extra Call (default is disable)

Set VoIP SIP Call Capacity to 10-15 for 802.11b and 25-40 for 802.11g

Set VoIP Call Handoff Reservation 20 (in % of the Call Capacity for roaming clients, set to default)

Set VoIP High-capacity Threshold 20 (in % of the Call Capacity for sticky clients, set to default)

9. Miscellaneous

- Extended Battery

This feature helps improve the battery life for the handsets. With this feature enabled, handsets can sleep for very long durations (100 – 200 DTIM periods)

Recommended Settings

Set Battery-Boost to enable (CLI support only, AP location sub command)

- Proxy-arp

Proxy-arp allows the controller to respond on behalf of the WiFi clients limiting the multicast traffic in the air. This allows the clients to sleep longer extending the battery life.

Recommended Settings

firewall voip-proxy-arp enable (CLI support only, command available under the config mode)

- Local probe response

Enable local probe response feature on the controller for the voice or converged data SSID if and only if load balancing is disabled.

11. WiFi Security Settings

Aruba strongly recommends using unique SSIDs for secure and insecure profiles. For example- the same SSID can be configured to support 802.1x and 802.11i but not open and shared keys. Aruba does not recommend using a single SSID with both open and static key encryption settings.

- Open

Supported on the Aruba System but not recommended. Highly insecure.

- WEP

Supported. Static WEP keys are not recommended as they are also highly insecure. (Wireless data can be captured and decrypted)
Dynamic WEP or 802.1x is supported.

- WPA-TKIP-PSK

WPA-PSK is higher level of encryption than WEP and is recommended if the device cannot support 802.1x or 802.11i. This mechanism is also recommended if the Voice device does not support good roaming times for 802.1x or 802.11i.

When configuring the SSID via the WebUI, select Mixed TKIP/AES-CCM (if TKIP is used), and the PSK TKIP/AES-CCM option.
Configure the PSK Passphrase key.

WLAN > Network > Edit SSID « Back

Edit SSID		Forward Mode	Encryption Type
SSID	aruba-ap	<input type="radio"/> Bridge <input checked="" type="radio"/> Tunnel	<input type="radio"/> NULL <input type="radio"/> WEP <input type="radio"/> TKIP <input type="radio"/> AES-CCM <input checked="" type="radio"/> Mixed TKIP/AES-CCM Mixed TKIP/AES-CCM <input checked="" type="radio"/> PSK TKIP/AES-CCM <input type="radio"/> WPA/2 TKIP/AES-CCM <input type="checkbox"/> Enable Pre-authentication
Radio Type	802.11 a/b/g		
Hide SSID	<input type="checkbox"/>		
SSID Default VLAN	0 <-- None		
Ignore Broadcast Probe Request	<input type="checkbox"/>		
DTIM Period	1		
PSK AES Key/Passphrase			
Retype PSK AES Key/Passphrase			
Format		Hex	

- **WPA2-AES-PSK**

Recommended. In case pre-shared keys have to be used or in the absence of an authentication server, this is the most recommended static-key option. When configuring the SSID via the WebUI, select the AES-CCM option and then select the PSK AES-CCM option.

- **WPA2 PEAP 802.11i**

Highly recommended. This method required the use of an Authentication server. In the absence of an auth server in the network please revert back to WPA/WA2 pre shared keys.

To configure 802.1x or 802.11i
WiFi settings

Set the encryption to AES-CCM (if AES is used) and Mixed TKIP/AES-CCM if TKIP is used. Set the mixed AES-CCM setting to WPA/2 TKIP/AES-CCM. Apply the changes.

Authentication

Enable 802.1x, Configure the radius server and the role derivation policies. Refer to the Aruba guide for information on configuring 802.1x and 802.11i.

When using 802.1x and 802.11i please disable Opportunistic Key Caching on the Aruba infrastructure if the client does not support it.

Also ensure that the Enable Termination radio button is unchecked if the EAP offload feature on the Aruba system is not used.

Avaya has not yet verified above 802.1x configuration.

Avaya uses Microsoft IAS server as its standard RADIUS solution.

Recommended Setting: 1st choice: WPA2-AES-PSK , 2nd choice: WPA-TKIP-PSK

Note: When using 802.11i and 802.1x, in extreme cases the client may experience a small space when on call as the client roams from one AP to another. This is because the client authentication needs to occur every time the client moves across the APs and during the re-key interval. The re-key interval on the Aruba platform is configurable and should be set to large values for voice clients

12. Security Firewall Settings and QoS

On the Aruba system users are identified by Roles. The roles are derived based on user authentication and define the access rights of the users. A group of users with similar access rights can be assigned the same role provided that their authentication mechanisms and security enforced on these users are the same.

Ensure that the user role assigned to the handsets supports sip communication to and from the network. Ensure that the ACL “any any svc-sip-udp any permit queue high” and “svc-sip-tcp permit queue high” are part of the access rights of the user-role. The E-series set support both SIP/UDP and SIP/TCP and configurable on the set.

To enable QoS ensure that the CoS and TS bits are set on the controller for the traffic streams.

Alternatively, the pre-voice ACL can be edited to include the ToS and CoS bits and added to the handset user’s access rights.

Security > User Roles > Edit Role(pre-voice) > Edit Policy(sip-acl)

Location: 0.0.0

Rules

Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	BlackList	TOS	802.1p Priority	Action
any	any	svc-sip-udp	permit			low		No	46	6	Delete
Add											
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Black List	TOS	802.1p	
any	any	Service	permit	<input type="checkbox"/>	<input type="checkbox"/>	Low		<input type="checkbox"/>	46	6	
		svc-sip-tcp (tcp 5060)	permit	<input type="checkbox"/>	<input type="checkbox"/>	High		<input type="checkbox"/>			
New											
Add											

Avaya has not yet verified above configuration.

13. WiFi Multi-Media (WMM) Basic Support

➤ QoS (802.11e) Parameters to Optimize Voice

Aruba supports the default QoS settings as per the WMM standard. To enable WMM in a 3.0 and above image, check the WMM enable radio button under the RF profile for the WiFi settings.

Section 4 through 8 and 10 through 13 were provided by Aruba to configure the WLAN for the Dual Mode Nokia handsets.

14. Avaya one-X Mobile Edition Settings

Following sections describe the configuration of an Avaya one-X mobile edition and phone settings.

- Detailed information and configuration steps are in the installation & configuration guide and can be found at <http://support.avaya.com/japple/css/japple?PAGE=ProductArea&temp.productId=251422&temp.bucketID=160257>
- Tasks
 1. Complete CM and SES administration
 2. Configure WLAN Access Point Profile on the device
 3. DO NOT CONFIGURE SIP PROFILE USING S60/Nokia Settings
 4. Check WLAN connectivity to see if you can establish connection
 5. Install one-X Mobile Edition Software
 6. Install one-X Mobile Edition configuration file with SIP profile settings
 7. Complete the on-device configuration of the SIP profile (manually need to map AP with SIP profile)

15. VoIP Settings

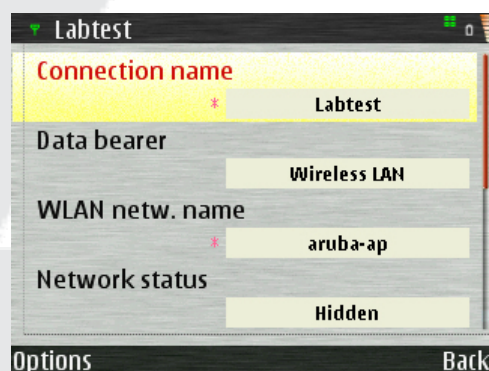
➤ Nokia phone Administration

Following is the set of instructions [that will help you to administer the Wireless LAN profile and SIP profile settings](#), which is necessary for this dual-mode experience.

It is highly recommend to configure the WLAN Access Point settings first prior to installing/configuring the Avaya one-X mobile Edition client.

➤ Create and configure your WLAN Access Point Profile

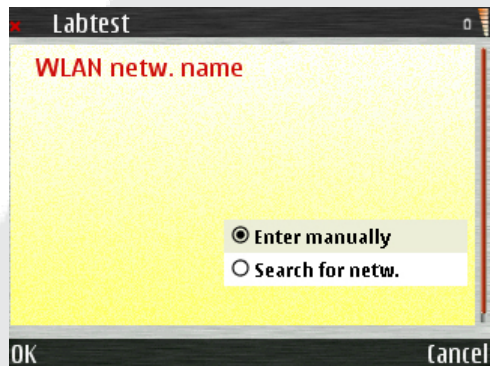
1. Press **Menu** button on the phone
2. Navigate to **Tools->Settings->Connection->Access Points**
3. Select **Options->New access point->Use default settings**
4. Enter a unique **Connection Name**



5. Select **Wireless LAN** for Data bearer

6. Enter your unique 'WLAN netw. Name'

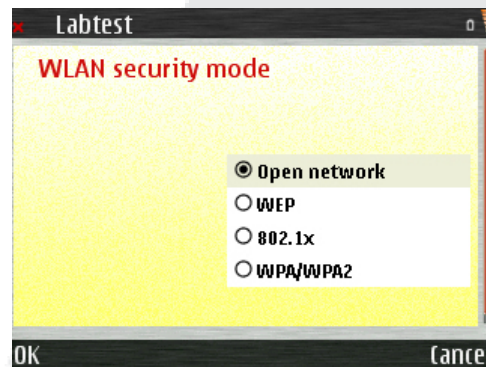
Recommendation: Search for netw. (If SSID is not hidden)

**7. Set your Network status to Public or Hidden**

Select Hidden if the network you are connecting to is hidden, or public if it is not hidden.

8. Set your WLAN netw. Mode to Infrastructure

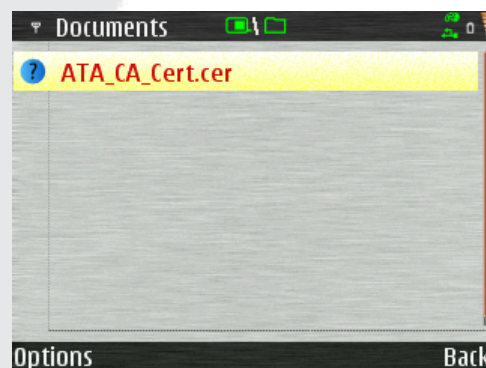
9. Set your WLAN security mode based on your security infrastructure



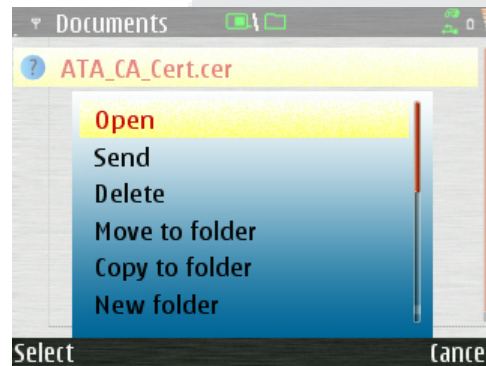
- **Following Section will provide necessary steps to configure WPA2 using 802.1x authentication.**

Similar steps will also be used for the E60 and E70.

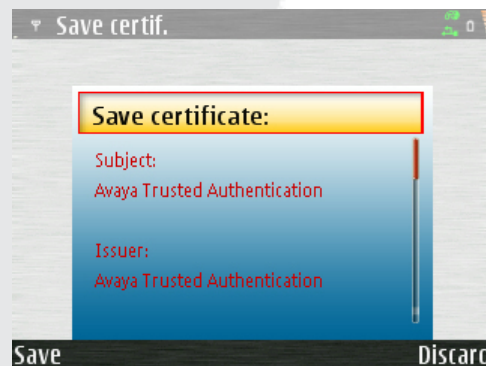
- First step is to download the trusted root certificate (e.g. ATA_CA_Cert.cer).
- Using the Nokia Phone Browser move that file over to the E61.
- Open the file using the File Mgr. Application (Located under Office/Documents from the Main Menu)



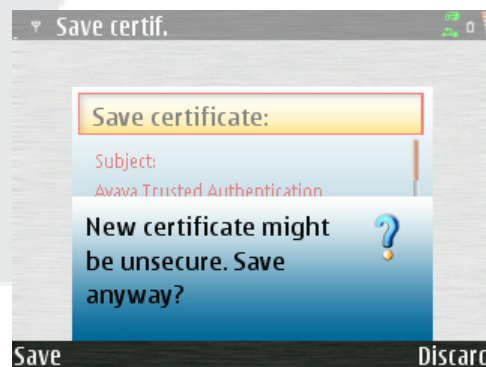
- When you open the file it will give you an option to save, select OK.



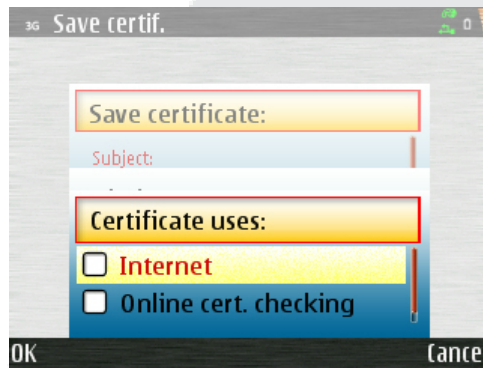
- Make sure the subject and Issuer source is from Trusted Authentication (e.g. Avaya Trusted Authentication).



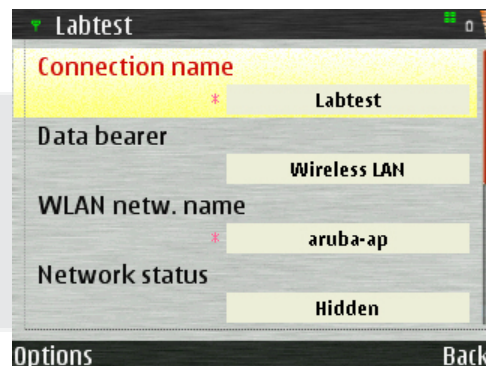
- Select "Save"



- Choose appropriate certificate uses



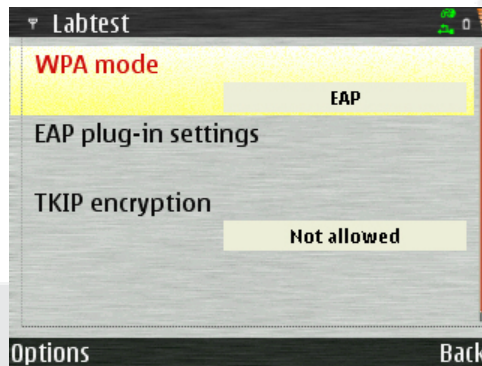
- Following section describes the steps how to configure access point with WPA2/802.1x mode on the E-61.
 - Push the Menu Button
 - Select Tools
 - Select Settings
 - Select Connection
 - Select Access Points
 - Push the Options Button
 - Select “New Access Point”
 - Select “Use default settings”
 - In “Connection” Name Put something meaningful (i.e. Labtest)
 - In “Data Bearer” Choose Wireless LAN
 - In “WLAN netw. Name” put the ssid (e.g. employee@avaya)



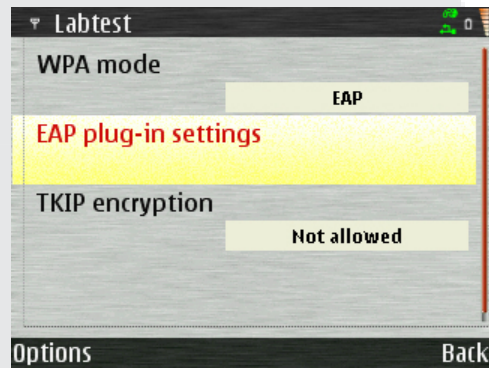
- In “Network status” choose Hidden
Select Hidden if the network you are connecting to is hidden, or public if it is not hidden
- In “WLAN netw. Mode” choose Infrastructure
- In “WLAN security mode” choose WPA/WPA2



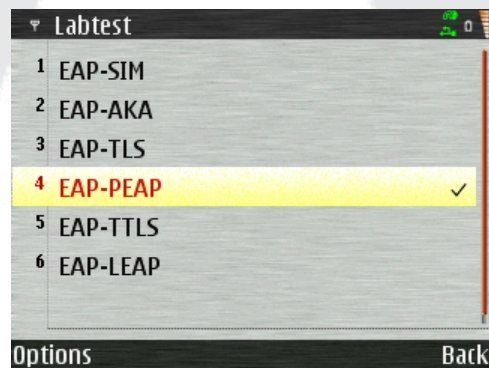
- In “Homepage” put a valid home page if you want to.
- Select “WLAN security sett.”
 - In “WPA mode” choose EAP
 - In “TKIP encryption” choose Not allowed.



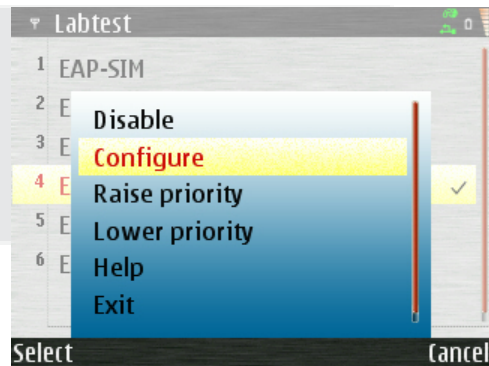
- Choose “EAP plug-in settings”



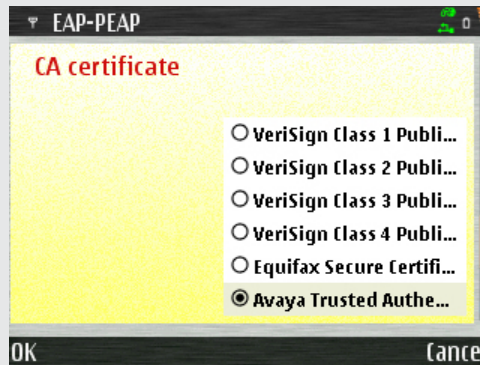
- Disable everything except EAP-PEAP
- Highlight EAP-PEAP



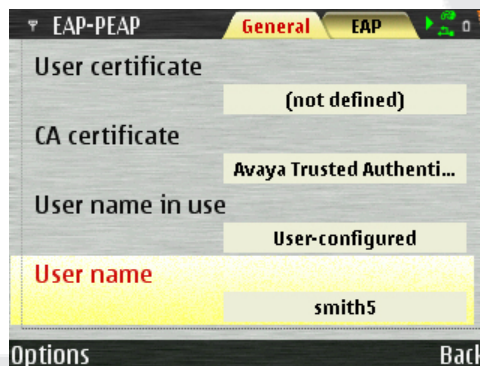
- Push Options
- Select configure



- Leave “User certificate” at (not defined)
- In “CA certificate” scroll to and select the “appropriate Authentication” certificate (e.g. Avaya Trusted Authentication).



- In “User name in use” choose User-defined
- In “User name” put in the valid ID (just the ID nothing else, i.e. smith5)



- In “Realm in use” choose User-configure
- In “Realm” leave this field blank

EAP-PEAP General EAP

User name in use: User-configured

User name: smith5

Realm in use: User-configured

Realm

Options Back

- In Allow “PEAPv0” leave it yes
- In Allow “PEAPv1” leave it yes
- In Allow “PEAPv2” leave it no

EAP-PEAP General EAP

Realm

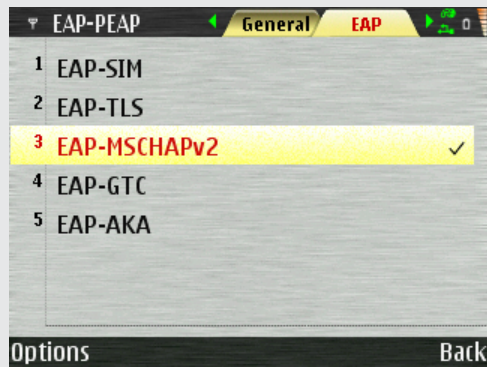
Allow PEAPv0: Yes

Allow PEAPv1: Yes

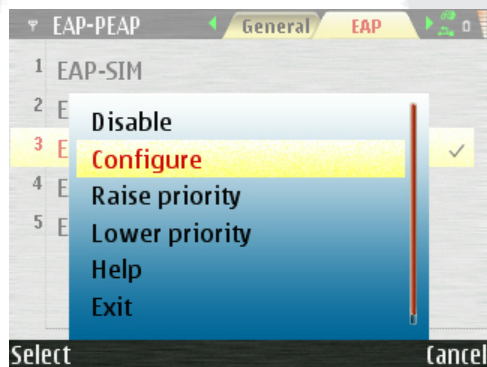
Allow PEAPv2: No

Options Back

- Scroll to the left for the EAP Tab
- Disable everything except “EAP-MSCHAPv2”
- Highlight “EAP-MSCHAPv2”



- Push Options
- Scroll to Configure and select it



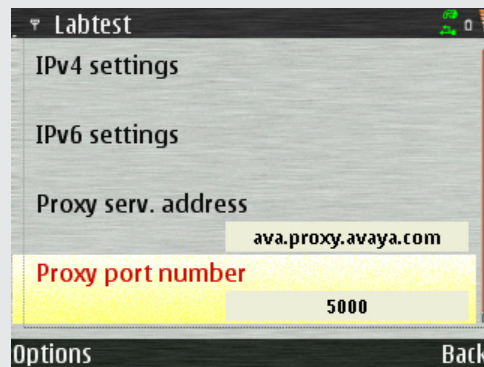
- In “User name” put in the **valid ID** (just the ID nothing else, i.e. smith5)
- In “Prompt password” Choose **No**
- In “Password” put in the **valid password**

The screenshot shows the 'MsChapV2' authentication window. It has three input fields: 'User name' with the text 'smith5', 'Prompt password' with the text 'No', and 'Password' with masked characters '*****'. The 'Prompt password' field is highlighted in yellow. At the bottom, there are two buttons: 'Options' and 'Back'.

- **Select Back**
 - **Select Back**
 - **Select Back**
 - **Select Back**
- **Select Options**
 - **Scroll to and select Advanced Settings**

The screenshot shows the 'Labtest' network settings window. It has several sections: 'Network status' with a dropdown set to 'Hidden', 'WLAN netw. mode', and 'WLAN'. A context menu is open over the 'WLAN' section, showing options: 'Change', 'Advanced settings' (highlighted in yellow), 'Help', and 'Exit'. At the bottom, there are two buttons: 'Select' and 'Cancel'.

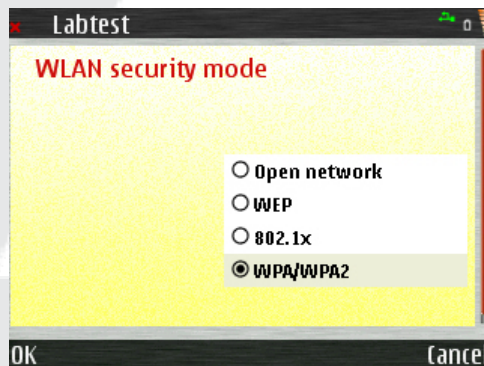
- In “Proxy serv. Address” put in a valid proxy server (i.e. `ava.proxy.avaya.com`)
- In “Proxy port number” (i.e. 5000)
- Select Back



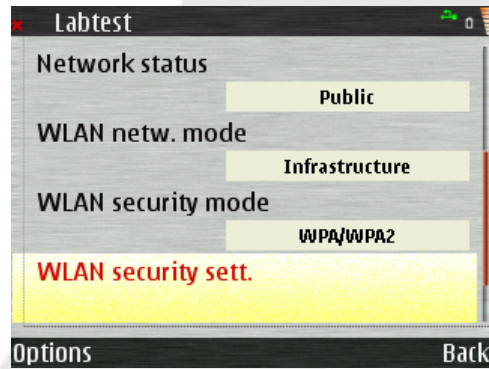
- Select Back

➤ Following is an example of configuring **WPA/WPA2 PSK** security option

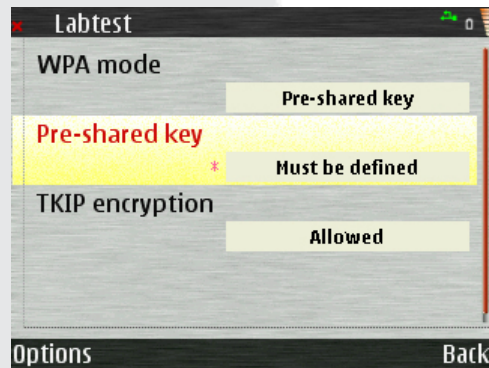
- In “WLAN security mode” choose WPA/WPA2



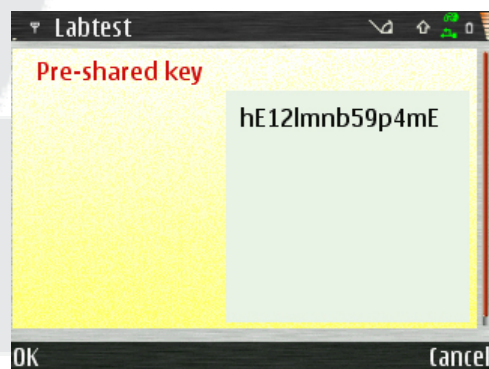
- Now enter your **WLAN security sett.**



- Set WPA mode to “Pre-shared key”

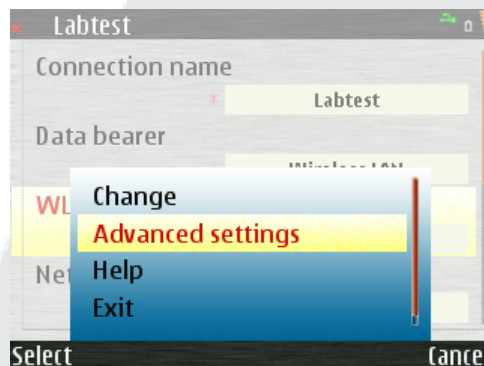


- Set your Pre-shared key

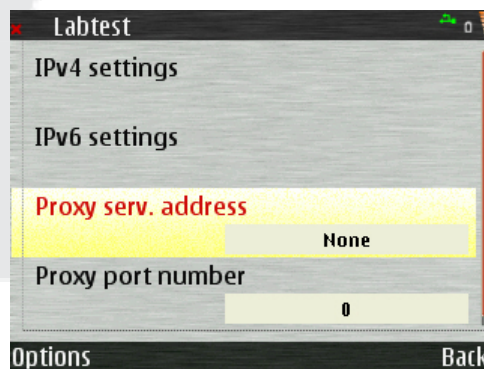


- Leave TKIP encryption as “Allowed”

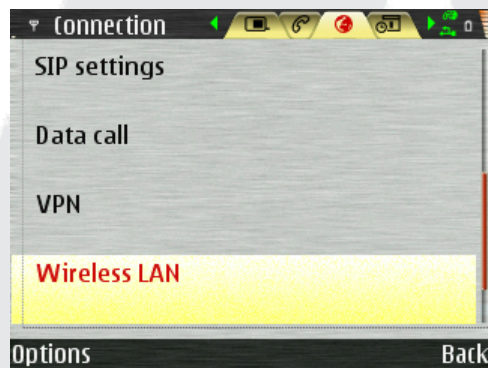
10. Enter HTTP proxy settings by selecting the left softkey, **Options->Advanced Settings** menu



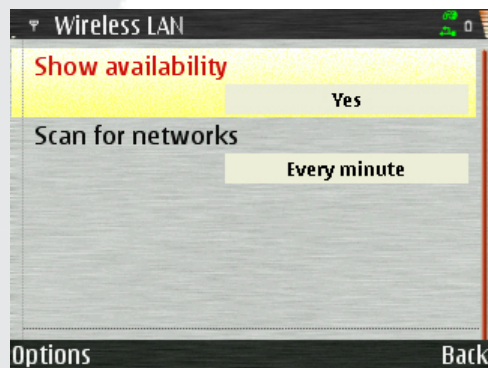
11. Here define your HTTP proxy settings (only needed for browsing web on E-series devices, if one is required)
12. If you would like to enter a static IP address and/or HTTP proxy settings, then select the left softkey, **Options->Advanced Settings** menu
13. Here you can define a static IP address (if you do not have a DHCP server) and also define your HTTP proxy settings (only needed for browsing web on E-series devices, if one is required).



14. Select **'Back'** to save and close the profile
15. Select **'Back'** again
16. Select **'Back'** again
17. Navigate to **'Wireless LAN settings'**



18. Change **'Show availability'** setting to **"Yes"**
19. Change **'Scan for networks'** to either **"Every minute"** or **"Every 5 minutes"** or less. This helps when moving back in to the WLAN coverage.



16. Create and configure SIP Profile

Do not create the SIP profile using Nokia Settings. Avaya one-X mobile client is not aware of any SIP profiles created via Nokia Settings. Please create SIP profiles using the Avaya one-X mobile client only

NOTE: If you have already included SIP Profile Settings in the “settings.1xme” file and have installed the configuration file using this guide, then you may skip this step.

1. Launch the Avaya one-X Mobile Edition application
2. Press Menu->Settings->Options->Wi-Fi (tab)->Menu->Create New Profile
3. Enter a unique name for the profile (For Example: My SIP Proxy)
4. Open the Options menu and select *Edit*

Profile name:	<i>A Unique profile</i>
Service profile:	IETF
Default access point:	<i>your Wi-Fi access point</i>
Public user name:	sip: <i>SIP user@domain or IP address (currently only numeric user name is supported; for example 12345@avaya.com)</i>
Use compression:	No
Registration:	Always on (This setting is highly recommended to set as Always on, or else your SIP profile will not be automatically registered)
Use security:	No

Proxy server:

Proxy server address:	<i>IP address of your SES server</i>
Realm:	<i>domain (or realm of your SES server)</i>
User name:	<i>SIP user</i>
Password:	<i>Password</i>
Allow loose routing:	Yes
Transport type:	UDP
Port:	5060

Registrar server:

Registrar serv.addr.:	<i>IP address of your SES server</i>
Realm:	<i>domain (or realm of your SES server)</i>
User name:	<i>SIP user</i>
Password:	<i>Password</i>
Transport type:	UDP
Port:	5060

The following step is quite necessary as well, if you do not create a profile in “**Internet tel. Settings**”, you may get associated to the Access Point, but it will not register your device with a SIP server.

Navigate to *Tools->Settings->Connection->Internet tel. settings:* and create a *New profile* in the Options menu with the following settings:

Name:	Default (or whatever you want to call it...)
SIP profiles:	<i>previously defined profile</i>

[NOTE: The SIP profile that you set here needs to be the one that was created using Avaya one-X mobile Edition and make sure that it is also the default profile in Avaya one-X mobile Wi-Fi settings.]

The following step is necessary so that you are notified of all the incoming SIP calls effectively.

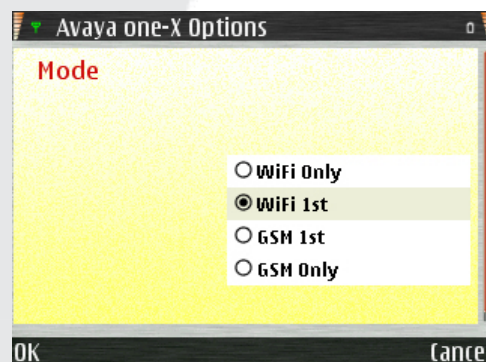
To switch between normal GSM calls or VOIP calls, navigate to ***Tools->Settings->Call->Default call type.***

- Select **Activated** for 'Internet call waiting'
- Select **On** for 'Internet call alert'
- Select **Internet** for 'Default call type'.

17. Setting different dual-mode network modes:

You can set different modes in the Avaya one-X mobile Edition client so that it manages handover scenarios and network appropriately.

1. Launch Avaya one-X Mobile Edition application
2. Press Menu->Settings->Options->General (tab)
3. Scroll to get to the 'Mode' setting



18. Dual-Mode Assisted Handover

This product allows you to switch between GSM and Wi-Fi modes. That is, when you are in Wi-Fi/SIP coverage, you can make and receive incoming and outgoing calls using WLAN bearer instead of using your cellular (GSM) minutes. Moreover, if you are leaving the Wi-Fi coverage, you can handoff the active call to the GSM (cellular) **bearer**. The software will present a user with a handover notification dialog box similar to one below with an audio beep tone:



So it's up to the user to decide to handover the call from Wi-Fi to GSM or GSM to Wi-Fi.

NOTE: You may also initiate the handover from by pressing the **Menu->Handover to GSM (or Wi-Fi)** option.

20. References

1. SIP Enablement Services (SES), R3.1 Implementation Guide, 16-300140
Issue 3.0, February 2006
<http://support.avaya.com/japple/css/japple?temp.documentID=285404&temp.productID=160073&temp.releaseID=283912&temp.bucketID=160257&PAGE=Document>
2. Communication Manager: Administration and System Programming
<https://support.avaya.com/japple/css/japple?temp.documentID=232041&temp.productID=136527&temp.releaseID=282185&temp.bucketID=159898&PAGE=Document>
3. Avaya Extension to Cellular User's Guide
<https://support.avaya.com/japple/css/japple?temp.documentID=282562&temp.productID=136527&temp.releaseID=282185&temp.bucketID=160257&PAGE=Document>
4. Feature Description and Implementation for Avaya Communication Manager
<http://support.avaya.com/japple/css/japple?temp.documentID=282739&temp.productID=107622&temp.releaseID=287624&temp.bucketID=159898&PAGE=Document>
5. Aruba references and white papers
<http://arubanetworks.com/solutions/mobility/>
6. Nokia E-series Phone Support
<http://europe.nokia.com/A4143002>

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.