Nokia Eseries Deployment Guide version 1.1

IPCBU Technical Marketing

Disclaimer

Nokia Deployment Guide
Table of Contents

1.1. Voice over Wireless LAN 4
1.2. Nokia Eseries Dual-mode Phones 4
1.2.1. Connecting to Cisco Communications Manager and Communications Manager Express 5
1.2.2. Endpoints 6
1.2.3. Using Signaling Protocols 6
1.2.4. Version 1.1 7
1.2.5. Installing Intellisync Call Connect for Cisco 8
1.2.6. Configuring the Nokia Eseries for Communications Manager and Communications Manager Express 10
1.2.7. Supported Communications Manager and Communications Manager Express Versions 15
1.2.8. Adding Nokia S60 Device Type to CUCM 15
1.2.9. Nokia Eseries TFTP Interaction 18
1.2.10. Dialing International Destinations 18
1.3. RF Basics and Site Survey 19
1.3.1. Different Deployment Types of Overlapping WLAN 20
1.3.2. Recommended Environment for the Nokia Eseries 22
1.4. Nokia RF Tools 23
1.4.1. Using Connection Manager 23
1.4.2. Supported Security Mechanisms 25
1.5. Roaming 26
1.5.1. Layer 2 Roaming 26
1.5.2. Roaming between WLAN and GSM 27
1.5.3. Registration Behavior 27
1.6. Quality of Service 28
1.6.1. Quality of Service for Voice Traffic 28
1.7. Understanding Differences Between Nokia Eseries and Cisco Wireless IP Phones 30
1.8. Upgrading To Version 1.1 Using BAT 32
1.8.1. Migrating Steps for CUCM Version 6.0 ..... **Error! Bookmark not defined.**
1.8.2. Migration Steps for CUCM Version 5.x 42
1.8.3. Migrating Steps for CUCM Version 4.x 52
1.9. Further Reading 66
1.10. Appendix: A 67
1.11. Appendix: B 69
1.12. Appendix: C. 71
1.13. Appendix: D. 72
1.14. Appendix F: Configuring the Nokia E-Series for EAP-PEAP 74
1.14.1. Converting the CA certificate 74
1.14.2. Installing the certificate on the Nokia E-Series 74
Turning on the IR port of the Nokia 74
Transferring files to the Nokia 74
Installing the certificate 75
1.14.3. Configuring the Access-Point 75
Access-Point Configuration 75

1.14.4. Configuring for EAP-PEAP....75
Configuring the EAP-PEAP settings....76
Configuring EAP-MSCHAPv2....76
Configuring the EAP Cipher....76

1.1. Voice over Wireless LAN

In recent years there have been two key technologies that have driven major productivity increases in the enterprise: Wireless LANs (WLANs) and IP Telephony. There is little doubt that Wireless LAN's offer businesses tremendous benefits which have led to the explosive growth in enterprise wireless access. These networks offer anytime and anywhere access to key network resources that can lead to substantial productivity gains. The increasing availability of wireless voice clients and the recent announcements on dual-mode (wireless and cellular) smart phones coupled with the increased productivity realized by enabling a mobile workforce is moving enterprise WLANs from a convenience to a critical element of the enterprise network infrastructure. Similarly, the IP Telephony revolution begun by Cisco Systems has changed the world of communications. The Cisco Unified Communications platform allows businesses to communicate in ways never before imagined and has created a momentous shift in the telephony market away from traditional PBX systems to flexible IP based architectures.

The convergence of these two key technologies is an inevitability that is beginning to gain momentum. Its deployment has been primarily into several vertical markets such as healthcare and manufacturing, where the productivity increases have been easiest to achieve and nature of the work environment requires mobility. There have been technology hurdles that had to be overcome to adopt WLANs to the needs of voice related services.

Voice traffic has a very different nature than data traffic and requires special handling to meet its rigorous needs. Unlike data traffic, voice traffic has a low bandwidth requirement, but needs to be delivered in a timely fashion and is much less resilient to packet loss. Voice clients also have a tendency to roam frequently and into areas that may not have been given coverage in a data only environment. These clients will require that coverage between these areas is seamless and that handoffs between access points that is fast so that voice gaps are not heard. Underlying all of these requirements is the need to provide all of this over a highly secure network. Cisco has addressed all of these areas by incorporating the latest advances in Quality of Service (QoS), seamless fast roaming across Layer 2 and Layer 3 IP boundaries, centralized management, and support for a broad range of security types into it's Unified Wireless Network.

A full discussion of all of these areas is out of the scope of this document, but it is ***highly*** recommended that a full reading of Mobility and IP Telephony Solutions Reference Network Design (SRND) documents is done prior to installation. These documents do cover all of the design and implementation aspects of both wireless and IP Telephony networks.

To access Cisco's SRND documents see the link below:
http://www.cisco.com/go/srnd

1.2. Nokia Eseries Dual-mode Phones

The Nokia Eseries are referred to as "dual-mode" because they can operate in both cellular and Wireless LAN mode. As of this writing, Nokia has designed their ESeries phone to operate with both radios on simultaneously. This allows users to choose their preferred method of calling as the default, but they always have the option to choose either cellular or VoIP at the time of dialing. All 802.11b and 802.11g speeds are supported, which allows for use in most currently deployed wireless networks.

A substantial number of advanced features are supported on the Nokia Eseries. For more info on the Nokia Eseries features see their site at:
http://www.nokiaforbusiness.com/emea/Eseries/

1.2.1. Connecting to Cisco Communications Manager and Communications Manager Express

Cisco Unified Communications Manager is the core call processing software for the Cisco IP Telephony solution. It builds call processing capabilities on top of the Cisco IP network infrastructure. Cisco Unified Communications Manager extends enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice over IP (VoIP) gateways, and multimedia applications.

You can deploy the call processing capabilities of Cisco Communications Manager according to one of the following models, depending on the size, geographical distribution, and functional requirements of your enterprise:

- Single-site call processing model

In the single-site model, each site or campus has its own Cisco Communications Manager or cluster of Cisco Communications Managers to perform call processing functions. No voice traffic travels over the IP WAN; instead, external calls or calls to remote sites use the public switched telephone network (PSTN).

- Multi-site WAN model with centralized call processing

In the multi-site WAN model with centralized call processing, the Cisco Communications Manager cluster resides at the main (or central) campus, and communication with remote branch offices normally takes place over the IP WAN. If either the central site or the IP WAN is down, the remote sites can continue to have service through a feature called Survivable Remote Site Telephony (SRST), which runs on Cisco IOS gateways.

The remote sites can also place calls over the PSTN if the IP WAN is temporarily oversubscribed, and you can interconnect a number of central sites through intercluster trunks.

Note: The Nokia Eseries does NOT support SRST as of this writing.

- Multi-site WAN model with distributed call processing

In the multi-site WAN model with distributed call processing, each site has its own Cisco Communications Manager cluster for call processing. Communication between sites normally takes place over the IP WAN, with the PSTN serving as a backup voice path. With this model, you can interconnect any number of sites across the IP WAN.

- Clustering over the IP WAN

You may deploy a single Cisco Communications Manager cluster across multiple sites that are connected by an IP WAN with QoS features enabled. To provide call processing redundancy, you can deploy backup servers either locally at each site or at a remote site across the WAN. Clustering over the WAN is well suited as a disaster recovery plan for business continuance sites or as a single solution for small or medium sites.

- Branch Office / SMB

Utilizing Cisco Communications Manager Express companies can deploy an IP telephony solution in one of Cisco Integrated Service Routers (ISR). Communications Manager Express can be configured to work with Communications Manager as part of a larger deployment, or deployed independently in the remote office.

1.2.2. Endpoints

A communication endpoint is a user instrument such as a desk phone or even a software phone application that runs on a PC. In the IP environment, each phone has an Ethernet connection. In addition to various models of desktop Cisco IP Phones, IP Telephony endpoints include the following devices:

- Software-based IP phones

Cisco IP SoftPhone and IP Communicator are desktop applications that turn your computer into a full-featured IP phone with the added advantages of call tracking, desktop collaboration, and one-click dialing from online directories. Cisco software-based IP phones offer users the great benefit of having a portable office IP phone to use anywhere an Internet connection is available.

- Video telephony endpoints

Video telephony capability is now fully integrated with Cisco Communications Manager Release 4.0 and later. In addition, Cisco VT Advantage introduces a Windows-based application and USB camera that can be installed on a Microsoft Windows 2000 or Windows XP personal computer. When the PC is physically connected to the PC port on a Cisco IP Phone 7940, 7960, or 7970, users can make video calls from their IP phones simply by dialing the extension number of another video device on the network. Several new third-party video devices are also compatible with the Cisco IP Video Telephony solution.

- Wireless IP phones

Using wireless phones to connect to Communications Manager is becoming a mainstream communication medium. The Cisco 7920 and 7921 Unified Wireless IP Phones extend the Cisco family of IP phones from 10/100 Ethernet to 802.11 wireless LAN (WLAN) and represents a single-mode Wi-Fi phone. A single-mode phone is only used on the 802.11 wireless networks. The Nokia Eseries also utilizes the wireless network, but is considered a dual-mode device. A dual-mode phone has the capability to run on both a mobile operator's network and the enterprise wireless network. Dual-mode phones can offer additional value to customers due to their flexible usage, increased productivity, and potential for ROI.

1.2.3. Using Signaling Protocols

Devices such as phones and gateways must use a protocol to communicate with Communications Manager. There are several such protocols such as H.323, MGCP, SIP, and Cisco's SCCP (Skinny), that all can provide the capability to setup calls and support supplementary services. The Nokia Eseries supports both SIP and SCCP, but the supported method to connect to Communications Manager at this time is to use Nokia Intellisync Call Connect for Cisco client which uses SCCP. This client is installed on the handset.

Skinny Client Control Protocol (SCCP) is a Cisco protocol which has been used by Cisco as an endpoint signaling protocol for many years. It provides a stable and feature rich environment for end users. The following call features are supported on the Nokia Eseries:

- Hold
- Transfer
- Conference
- Do-Not-Disturb (local to device, does not utilize CUCM)
- DTMF
- Voice Mail
- MWI
- Calling Line Presentation

- Calling Line Restriction
- Call Forwarding
- Call Pick Up
- Group Pick Up
- Call Park

The Nokia Eseries will register to Cisco Unified Communications Manager via two methods:

- As a Nokia S60 device type
- As a Cisco 7970 device type (CUCM Express Only) with version 1.1 (7960 with version 1.0)

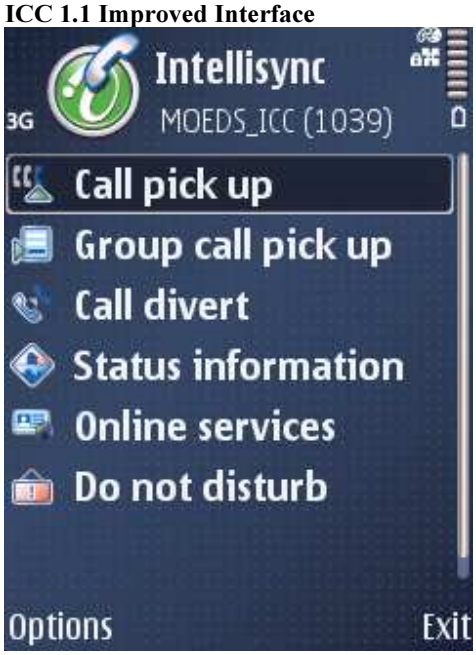
Which one depends on if you have installed the Nokia S60 device type. When registration is attempted, the Nokia will first attempt to register as device type 7970, and then an S60. The software to install the Nokia device type should be available through your Nokia dealer and is required for support as of version 1.1.

It is recommended that you install the Nokia device type if possible to prevent potential registration issues.

1.2.4. Intellisync Call Connect for Cisco Version 1.1

The release of Intellisync Call Connect for Cisco (ICC) version 1.1 brings many new features and functionality.

ICC 1.1 Improved Interface



Caller ID over WLAN – ICC client picks up the caller ID from incoming call and shows CUCM caller ID info instead of number.

Updated Client Interface – ICC has been updated with a new look and feel, and also added the features Call Divert, Online Services, and Do Not Disturb.

Online Services – allows users to easily access any web based service with a predefined URL.

Switch to Cellular – capability to manually transfer from an active WLAN call to a pre-defined cellular number. Available only on the S60v3.1 platforms such as the E51.

License Management – activated when user first accesses the Intellisync Call Connect client and allows for either a full license or a 60 day trial license.

To obtain the installation files, please, log in to Nokia support site at https://support.nokia.com and browse to page "Support / Software / Nokia ES Products / Mobility Solutions / Mobility Solutions / Mobile Voice Solutions / Nokia Intellisync Call Connect for Cisco". Direct link to Nokia ICC for Cisco v1.1 article is: https://infocenter.knowledge.nokia.com/InfoCenter/index?page=content&id=1610720

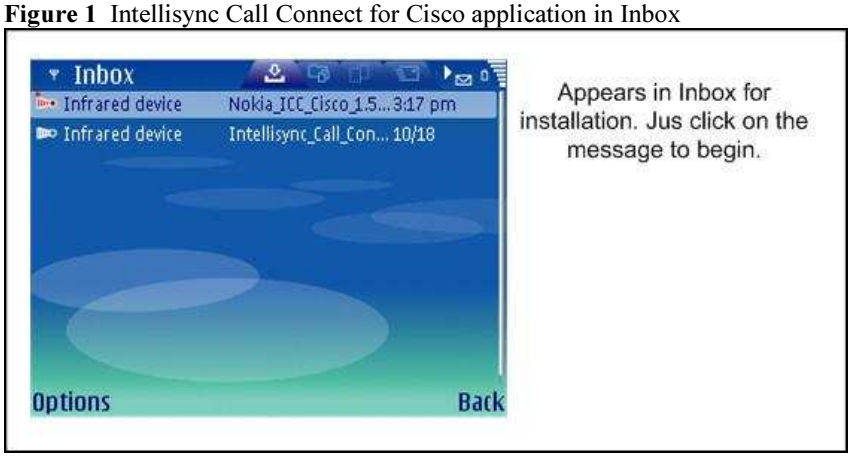
To find more information about updating the firmware of the Nokia ESeries see the link below, or browse to the page "Get support and software / Download software" at http://www.nokia.com: http://europe.nokia.com/link?cid=PLAIN_TEXT_14905

1.2.5. Installing Intellisync Call Connect for Cisco

By default the Nokia Eseries do not come with the Intellisync Call Connect for Cisco (the SCCP application) installed. The client must be purchased from Cisco via the Solutions+ Program. It can be installed via several methods such as using Nokia's Intellisync Device Manager (OMA DM Edition providing over the air installation/configuration) Nokia Configuration Tool, PC-Suite or sending the file to the phone over USB cable, infrared or Bluetooth. Once the application shows in the phones Inbox it can be clicked on and the installation will begin. Below we have stepped through installing the application via Infrared from a laptop.

Enable the Infrared port on the phone and align this with your laptop infrared port. Once you have picked the file you wish to send and the transmission completes, it will show in your Inbox as **Figure 1** shows:

Figure 1 Intellisync Call Connect for Cisco application in Inbox



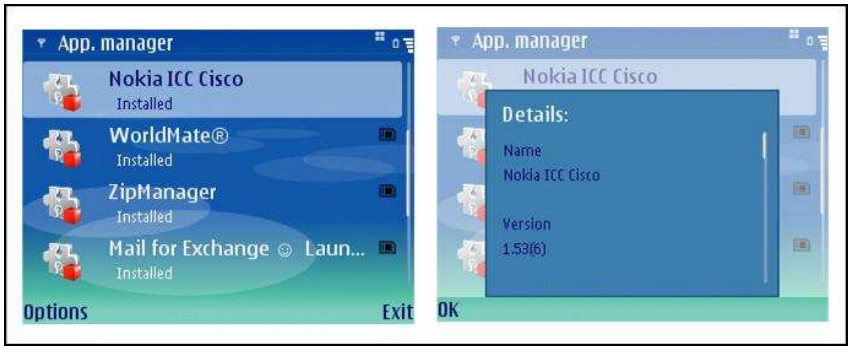
Once you select this message you will be prompted to install. You will want to verify that the version you are installing is the correct one.

Note: If you are upgrading from ICC 1.0 to ICC 1.1 be aware that you MUST uninstall version 1.0 prior to 1.1 install, and after 1.1 install the device must be reset. To remove version 1.0 browse to Menu > Installations, highlight the Intellisync icon, and choose Options > Remove. Your old ICC 1.0 settings will migrate to version ICC 1.1.

Figure 2 Installing Intellisync Call Connect for Cisco application

After the installation is complete you can view installed applications under the Application Manager. By clicking on the installed application you will see further details about it. **Figure 3** shows how we can verify our currently installed version of the Intellisync Call Connect for Cisco applications. If you are installing version ICC version 1.1 be sure to reset the phone after the install.

Figure 3 Viewing Install Applications
Menu button > Tools > Application Manager



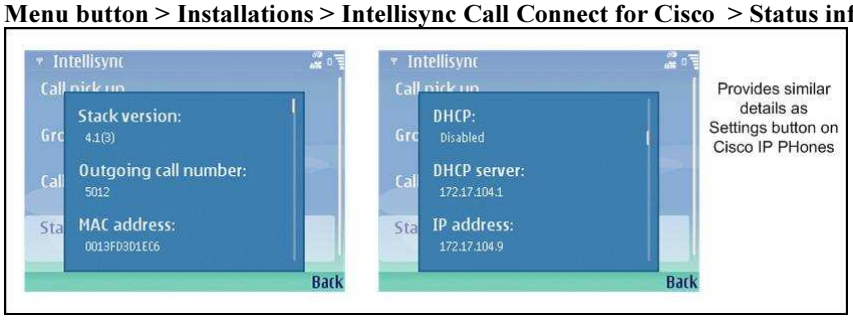
As of ICC version 1.1 there is a new licensing architecture. With the purchase of ICC 1.1 a license code should be provided, or the 60 day trial license can be used. Licensing is validated at Nokia via an Internet connection from the phone. Please see the ICC 1.1 release notes for additional information on licensing.

To begin the license process you will need to access the SCCP UI. Once the SCCP UI is accessed you will be prompted to license the code. This can be done from **Menu > Installations > Intellisync**

Note: If you are in a lab setting and need to configure multiple units, a single SIM card with data services can be used for all devices one at a time.

To view the settings of the Intellisync Call Connect for Cisco application you should browse to it from **Menu button > Installations > Intellisync > Status information**. This view is very similar to other Cisco Unified IP Phones Settings button display. Here we can find our assigned Communications Manager directory number, MAC address, IP Address and Cisco Communications Manager settings such as TFTP and Communications Manager list. **Figure 4** shows some of these.

Figure 4 Viewing the Settings of Nokia Eseries
Menu button > Installations > Intellisync Call Connect for Cisco > Status information



Note: The MAC address can be found 3 ways: **1**) From the Menu button > Installations > Intellisync Call Connect for Cisco > Status information page **2**) Type in the following key sequence at the idle screen: *#62209526# **3**) On some models it is printed behind the battery.

1.2.6. Configuring the Nokia Eseries for Communications Manager and Communications Manager Express

Before beginning the configuration manually, verify that Intellisync Call Connect for Cisco application has already been installed (see above). There are several steps needed to properly configure the Nokia Eseries for use on the wireless LAN, and then for registration to Cisco Communications Manager. All of the configurations are done under Settings, which can be reached from **Menu button > Tools > Settings > Connection**. Nokia encourages users to have an active SIM card inserted into the phone and to not use Offline mode.
The available settings under Connection are:

- Access points
- Access point groups
- Packet data
- Internet telephony settings
- SIP settings
- SCCP settings
- Data call
- VPN
- Wireless LAN
- Configurations

To configure the phone to work with Cisco Communications Manager we will be performing the following configuration tasks (in the order listed):

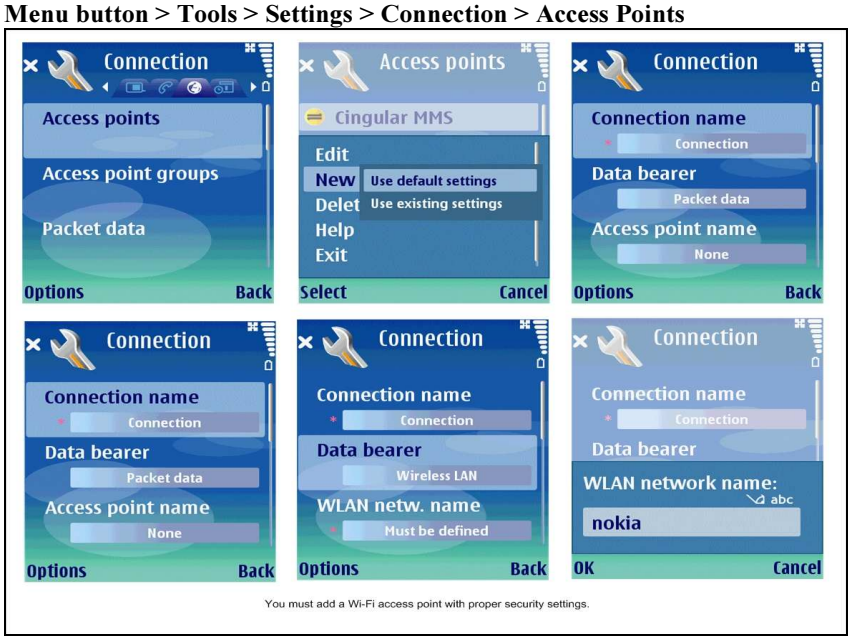
- Define Access Point
- Configuring the SCCP profile
- Configure an Internet telephony setting

Note: The Nokia Eseries does support SIP natively; however, at the time of this writing it has not been tested by Cisco's 3rd party certification program and is unsupported.

Note: Icons on the Nokia can be moved to make configuration easier. The steps given here assume the default locations at the time of writing. You may find it easier during daily use to move your Settings, Internet Telephony, Intellisync Call Connect for Cisco , Connection Manager, and Application Manager icon's under one folder.

If you have not already added an access point (to connect to the wireless network) to the Nokia this should be done first. Here we add an access point using the default settings.

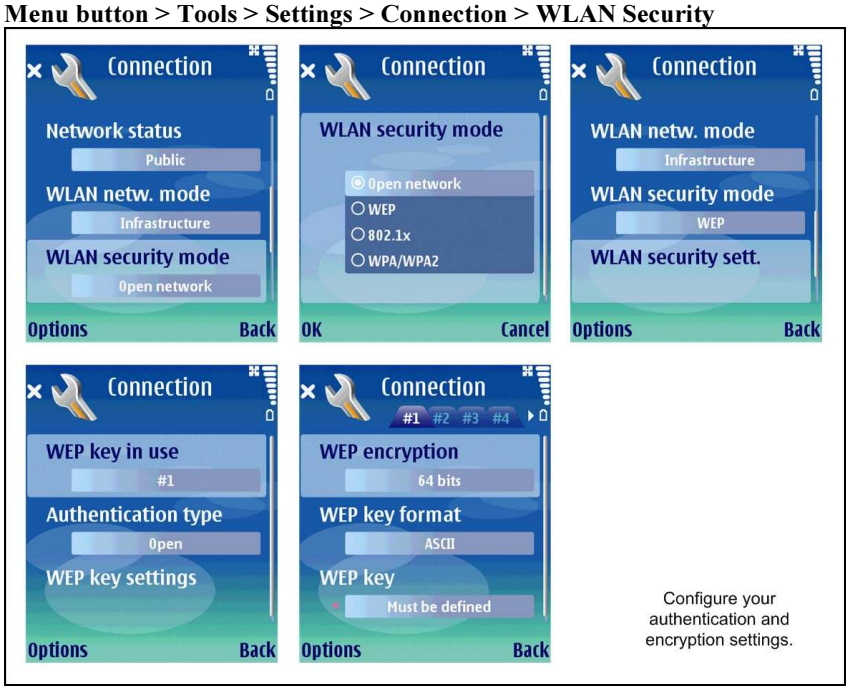
Figure 5 Configuring the Access Point
Menu button > Tools > Settings > Connection > Access Points



Notice that we changed the Data Bearer setting to Wireless LAN and changed the WLAN Network Name setting to be the SSID of our WLAN.

Next in **Figure 6** the security settings for the Access Point need to be configured. In our example below we step through a simple WEP configuration, but the Nokia Eseries is capable of several forms of authentication and encryption. See the appendix for EAP-PEAP configuration steps.

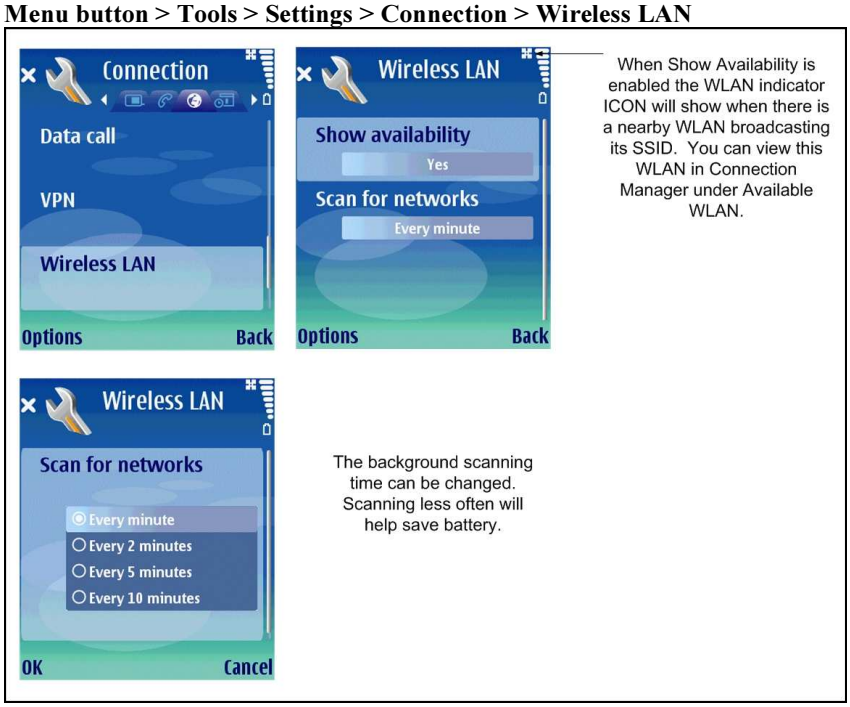
Figure 6 Setting WLAN Security
Menu button > Tools > Settings > Connection > WLAN Security



When the Nokia Eseries is not associated to an access point it will occasionally scan to see if there are WLANs available. To adjust the delay between scan times you will need to adjust the **Scan for networks** setting number **Wireless LAN**. This setting can decrease the connection time to Communications Manager once a user has roamed into an area where it was previously unregistered. **Figure 7** shows the steps.

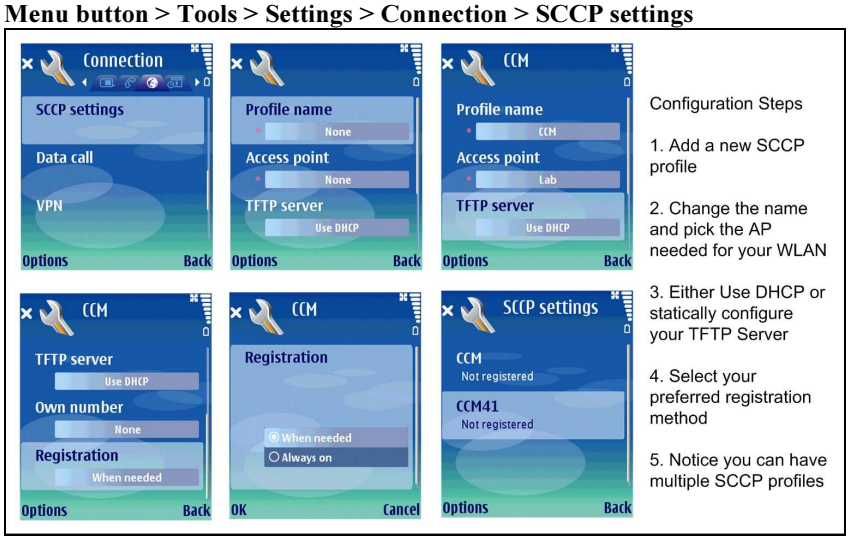
Note: If the phone is associated to an access-point and uses the Always on setting, and due to TX failure, beacon loss, or RSSI looses its association to the access point it will aggressively attempt to re-register.

Figure 7 Setting Wireless LAN
Menu button > Tools > Settings > Connection > Wireless LAN



The next required step is to configure the SCCP settings. Here is where you combine the access point previously configured to an SCCP profile. The TFTP server can be configured to use DHCP via Option 150 or set statically. The Registration setting can either be **When needed** or **Always on**. When the Registration setting is **When needed** the user can manually force a registration attempt, but the phone will not attempt one on its own. This registration attempt is made from the Internet telephone application (shown in later steps). The recommended setting for daily use is **Always on**. With this setting the Eseries will attempt to register to Cisco Communications Manager when the AP configured for SCCP is in range. This will allow users to roam in and out of the building without having to manually reregister their phones. When the Always On setting is configured background WLAN scanning is activated automatically. The **When needed** setting can be useful when troubleshooting. See **Figure 8** for an overview.

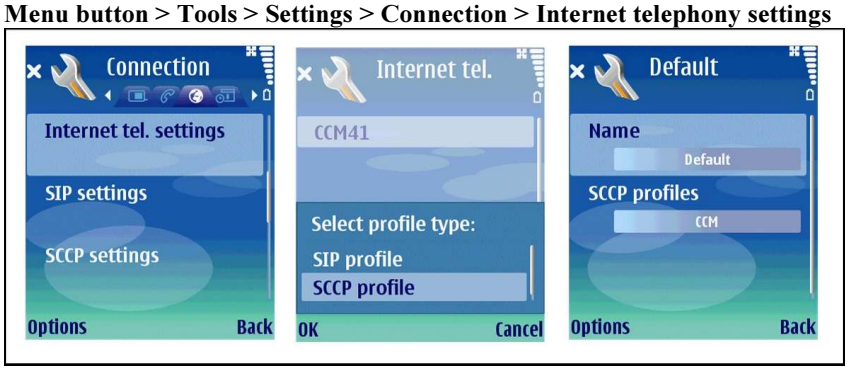
Figure 8 Configuring the SCCP Settings
Menu button > Tools > Settings > Connection > SCCP settings



Now that your SCCP settings are added all that is left is to add an Internet telephony profile. Assuming that your Nokia Eseries (MAC address) was added to Communications Manager previously or auto-registration is enabled on Cisco Communications Manager, your phone should be able to register after this step. If you are using Communications Manager Express and have auto register (which is default) and auto assign enabled, the phone should automatically register. The preferred method would be to set up the desired ephone # containing, mac-address , single or dual DN, type 7970. The Nokia E series will emulate a subset of the Cisco 7970 capabilities.

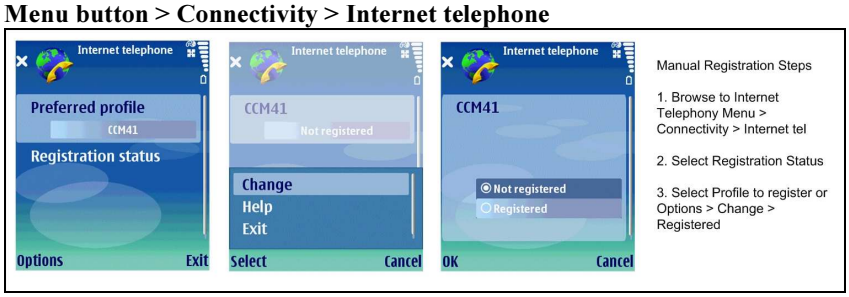
Note: If you are using ICC version 1.0 the Nokia will register as a 7960, not 7970. Installing the Nokia .cop file and registering as an S60 device is still the recommended path.

Figure 9 Configuring Internet Telephony Settings
Menu button > Tools > Settings > Connection > Internet telephony settings



If you choose to set your registration to **When needed** there is an additional step to getting the phone to register. To register you must go to the Internet Telephony application and force a registration attempt. When the phone is set to register manually it will not register again on its own if it is roamed out of WLAN coverage. This setting is primarily useful for testing.

Figure 10 Manually Registering to Communications Manager
Menu button > Connectivity > Internet telephone



Note: Nokia recommends that the Offline profile not be used. A SIM card is needed to avoid the Offline profile.

Note: Nokia recommends the Always On setting for the SCCP setting.

1.2.7. Supported Communications Manager and Communications Manager Express Versions

The Nokia phones are supported in Communications Manager and Communications Manager Express as separate device types. The device types have been created such that unnecessary features are not presented for these phones. Your Communications Manager may need to be upgraded to the latest version to support the Nokia phone. The following versions of Communications Manager are supported:

- 4.1(3)
- 4.2(3)
- 5.x
- 6.x (ICC version 1.1)

The following versions of Communications Manager Express are supported:

- 4.0
- 4.0(1) – 12.4(4)XC1
- 4.0(2) – 12.4(11)T
- 4.0(3) – 12.4(4)XC4
- 4.1 and later
- UC500

Communications Manager Express Eseries SCCP limitations:

- As was eluded to in step eight the Nokia Eseries emulate a limited subset 7970's capabilities. It is recommended that only 1 dual line DN be attached to button 1 and know other DN's or button be attached to the Eseries phone. Call-forwarding options are available, i.e. forward to voicemail.

- While on SCCP Wi-Fi calls, incoming GSM calls will not alert, either visually or audibly. If voicemail has been configured for the GSM number the call will go into cellular voicemail.

- While on a GSM call, incoming SCCP Wi-Fi calls alert normally.
- The MWI (Message Waiting Indicator) light may not re-indicate the presence of messages if the phone is power cycled while currently illuminated.

- G729r8 and G711ulaw only are supported.

1.2.8. Adding Nokia S60 Device Type to CUCM

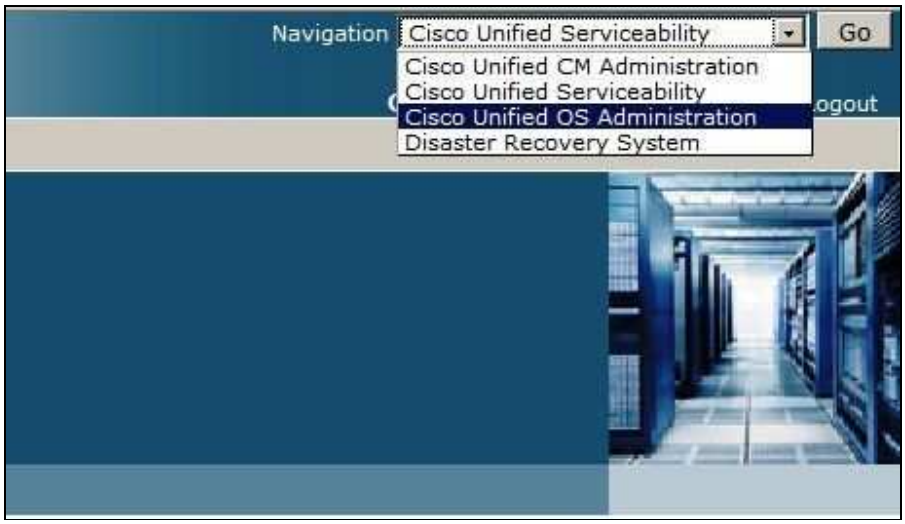
Adding the Nokia S60 device type to CUCM is the supported method for configuring Nokia devices to register and perform correctly. To get the device type added to CUCM an installation file must be run. This is either and installation file for the Windows 4.x version, or a .cop file for 5.x and 6.x versions of CUCM.

To obtain the installation files please
https://infocenter.knowledge.nokia.com/InfoCenter/index?page=content&id=1610720

Installing CUCM .cop Files

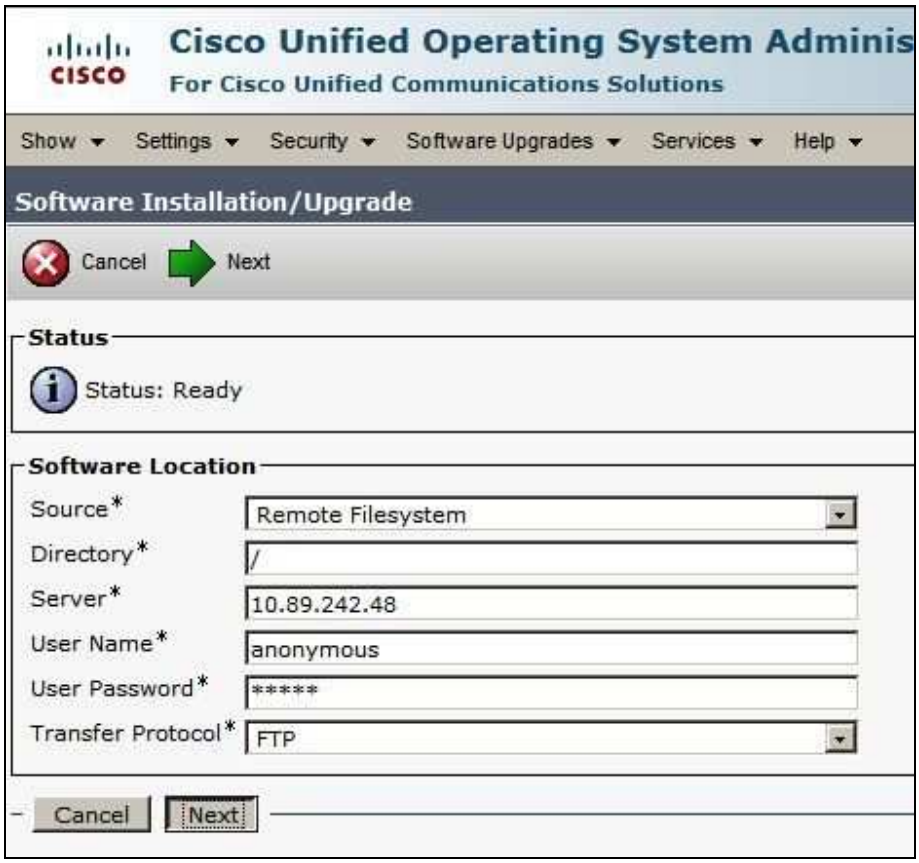
Installing the .cop file for 5.x and 6.x are basically the same. You'll need an SFTP/FTP server that is reachable by CUCM, and the user credentials to access it. Adding install files is as simple as dropping the .cop file into a directory on the file server and pointing CUCM to it. The steps for installing are below.

First you will need to get to the OS Administration pages which can be accessed from the Navigation drop down.

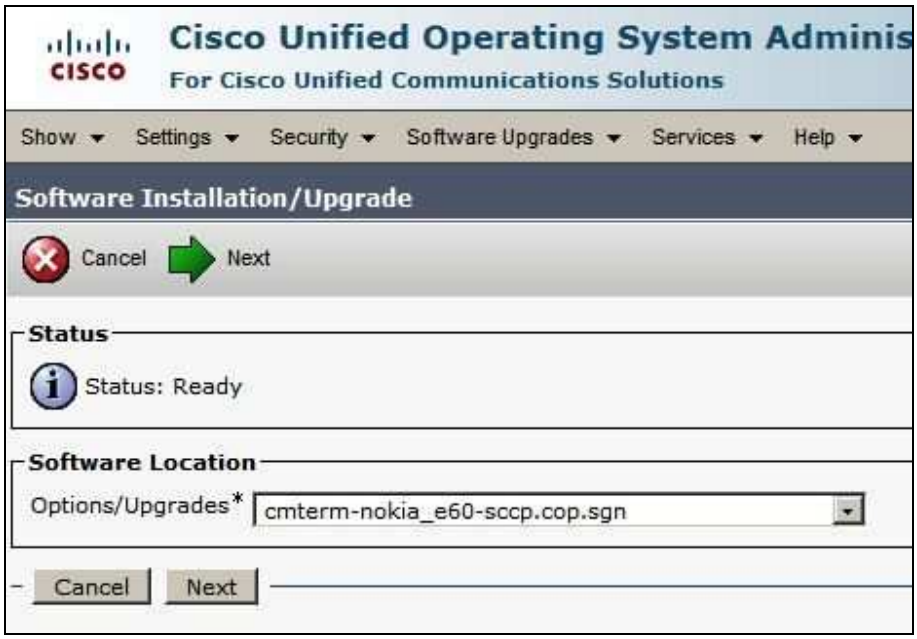


Once there browse to Software **Upgrades > Install Upgrade.**

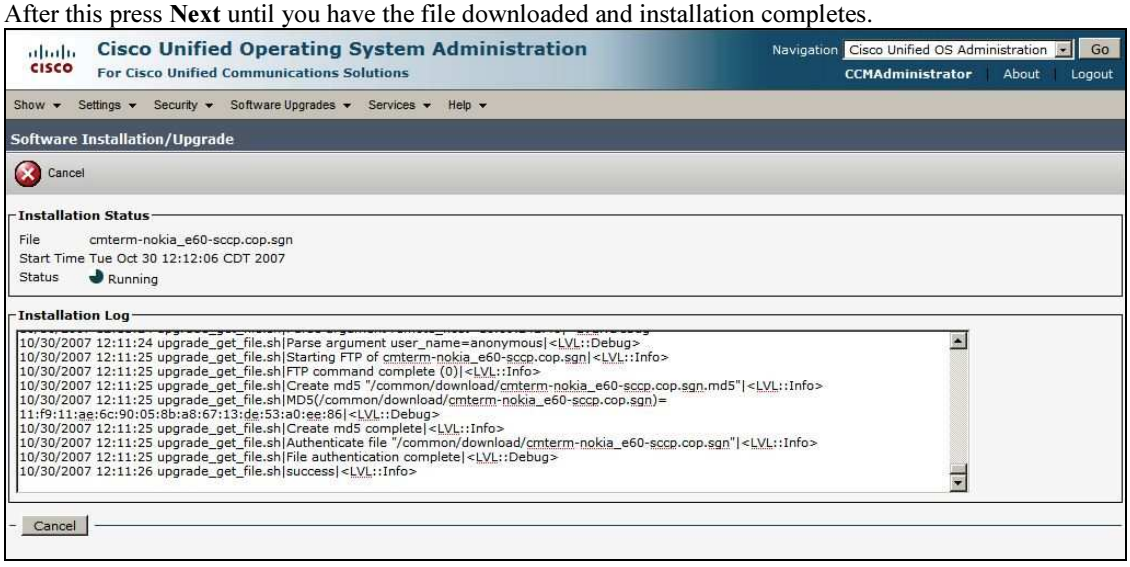
This will bring up the software installation page where the FTP information can be added. Add in the correct server info and click **Next**.



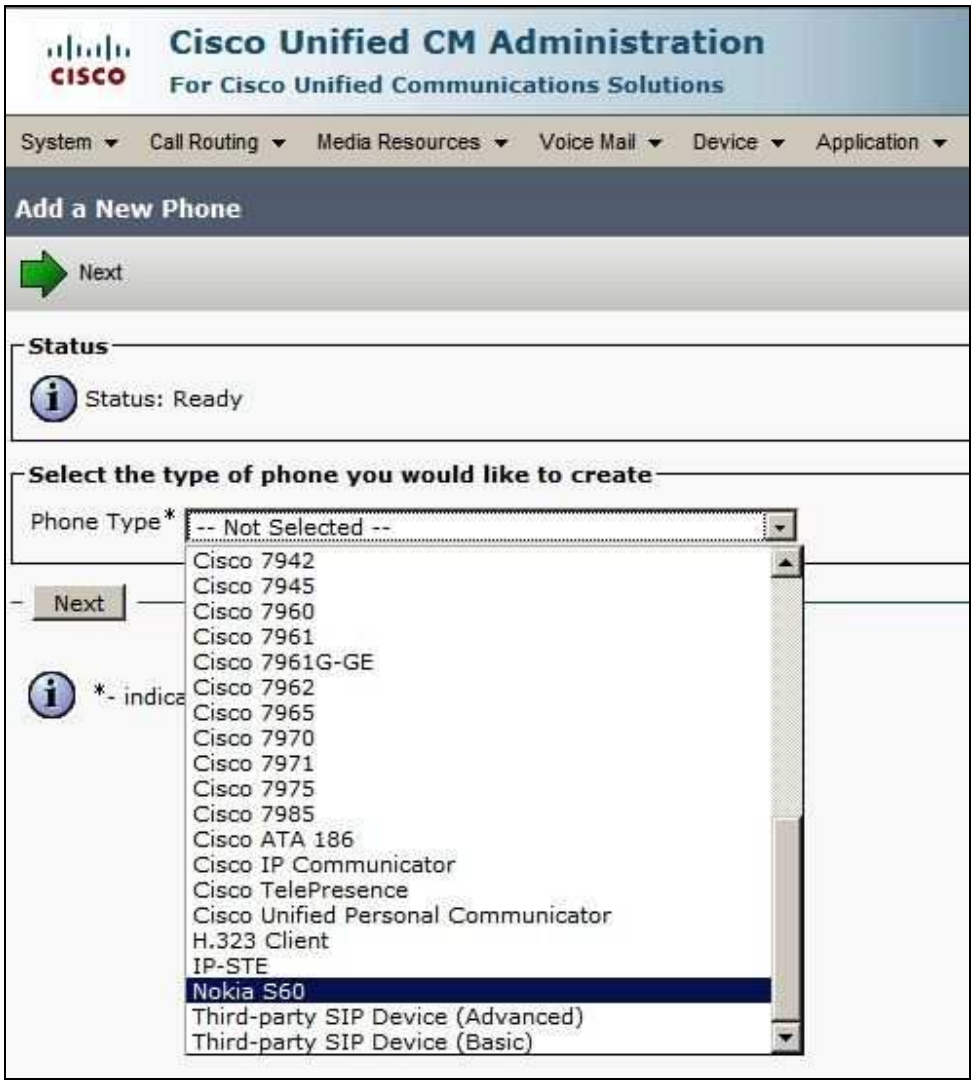
Once you have accessed the FTP server you should get a list of available files to install. Select the Nokia .cop file and press **Next**.



After this press **Next** until you have the file downloaded and installation completes.



To verify that the data was installed into the database simply browse back to CUCM administration, run through the steps to add a new phone, and verify that the S60 is an available device.



1.2.9. Nokia Eseries TFTP Interaction

Cisco's TFTP server is not used for downloading firmware, as is the case with Cisco IP Phones. Instead the Nokia Eseries only use relevant configuration options in the configuration file. To update the firmware of your Nokia Eseries you will need to contact your local Nokia representative for flashing or use the online tools. To find more information about updating the firmware of the Nokia ESeries see the link below, or browse to the page "Get support and software / Download software" at http://www.nokia.com:
http://europe.nokia.com/link?cid=PLAIN_TEXT_14905

1.2.10. Dialing International Destinations

When a user dials an international destination from a mobile device, the generally accepted practice is to insert a plus "+" sign at the beginning. In current versions of Communications Manager the "+" sign is not recognized as a digit that can be dialed. To address this issue, Nokia converts the "+" to two zeros "00", which can be added to a route pattern in Communications Manager for international dialing. This can be updated to other patterns using Nokia Intellisync Device Manager.

1.3. RF Basics and Site Survey

The Nokia Eseries devices are 802.11b and 802.11g compliant. This section covers the basic RF information necessary to properly deploy the Nokia Eseries phones in a Cisco Unified WLAN network.

Note: The Nokia ESeries support 802.15 Bluetooth (BT) and 802.11b/g. Because both radios share the same antenna and frequency band, a BT earpiece should not be used with these phones when they in 802.11 b/g mode. Significant degradation of voice quality can result.

A chart of the BT and 802.11b/g frequencies is shown in appendix A. A BT headset connected to the phone during a call causes a poor call quality that may degrade to the point of a dropped call. The BT transmission of will also negatively affect the quality of other nearby calls that are using 802.11b/g. Calls as far away as 75 feet from BT maybe affected. A laptop user that has BT enabled on the laptop for communication to a BT mouse will also experience lower quality VoWLAN calls. Charts of jitter created on a call with a BT enabled versus a call without a BT enabled are shown in appendix B.

All sites using 802.11b/g phones should be frequency scanned and surveyed for interference to determine where performance challenges will be due to interference.

Nokia phones at this time do not support call limiting per RF channel. They do not support pre-emptive or assisted roaming logic. Because channel capacity and advanced L2 roaming is not processed by the phones RF channels may become over subscribed and call quality can degrade.

The Nokia Eseries conform to the data rate settings of the access point. If the access point is configured for a maximum data rate of 24Mbps the client does not transmit at above that rate. If the maximum is set for example 12Mbps and the phone is within a distance of the access point that supports 24Mbps it use the 24Mbps data rate. Such behavior is not uncommon in WiFi devices with 11g data rates. If there are no 11g data rates enable on the access point, then the phone will only do 11b rates. This is important when designing cells for capacity instead of coverage.

The Nokia phone was tested with the new Cisco AP1240 with diversity enabled and using the AIR-ANT4941 antennas. The Nokia clients at 36Mbps had a signal of -68 and at a noise level of -96 had a 1% packet error rate (PER) at the distance of 70 feet in an open office of typical cubes. The coverage cell edge at the 36Mbps is -68. At distances greater than 70 feet or a noise level greater than -96 the PER went higher that 1%. This is provided as an observation and is not a design recommendation. The Nokia phones have internal WiFi antennas. The user may inadvertently place their hand over antenna which reduce receive signal strength and transmit signal strength by 4dBm. There are charts in appendix C. A common rule of thumb is a 9dB loss in an indoor environment will reduce by half the coverage of a 2.4GHz radio. It is recommended that the coverage be designed with this condition in mind.

Key WLAN design notes for Nokia E61 phones:

- If the WLAN had been carefully design to the 7920 design guide of a cell edge of -67dBm for 11Mbps then the Nokia phone should be able to work in that coverage cell, with the AP1240 and AP1230 at a 802.11g data rate of 12Mbps. The AP1230 and AP1240 support 802.11g rates with a maximum transmit power of 50mW(17dBm). The receive sensitivity of the radios is also better than previous 802.11g rates. The combination of increased transmit power and receiver sensitivity give these two access point a coverage area at the 802.11g rate of 12Mbps that is equal to the previous access point coverage of 802.11b rate of 11Mbps.

- All indoor installations need diversity antenna support on the access point. Signal strength alone will not provide good signal quality. Indoors the 2.4GHz signal of the radios will bounce off some objects and be absorbed at various levels by other objects. Diversity support significantly improves throughput by reducing retries, which particularly important to an application like voice. Without diversity antenna support on the phones it becomes more important to have diversity enabled on the access points. The antenna appendix lists recommended antennas.
- The antenna placement should be selective. Antennas should not be mounted near metal objects. Putting transmission and reception of signals near metal increases multipath problems. See the antenna appendix for recommended antenna installation.
- Same channel separation is an important design consideration. Channel utilization affects the numbers of calls on the channel and channel utilization. Channel separation also reduces the noise floor. The channel is the collision domain.
- The CLI and GUI of the autonomous and LWAPP access points should be used to verify the signal level and data rate of the phones as seen by the access points. The coverage of the phone during survey and coverage checks should be done with active calls.
- When there needs to be a high density of calls in a given floor space. The best way to reduce cell size is to reduce transmit power of all radios. That is both access point and phones. While faster data rates have smaller cells, most clients will use the data rate they want to use and not the data rates set on the access point. Therefore it is better to plan cell size by power settings. The recommended means for managing the transmit power of the phone and other clients is "Client Power Local" on the autonomous access points. The LWAPP access points default to that method. This means the access points tell the clients to use the transmit power as the access point.

For a detailed discussion on Voice over WLAN design please see the Mobility Design Guide at:
http://www.cisco.com/en/US/netsol/ns656/networking_solutions_program_home.html

1.3.1. Different Deployment Types of Overlapping WLAN

How much overlapping WLAN coverage you set in your wireless network depends on the usage. Wireless networks can be deployed for Location-Based Services, Voice, or Data-Only networks. The difference is in the pattern that the APs are laid out in and the amount of RF overlap in the coverage area. If the deployment has voice and data, then follow the voice deployment guidelines. If the deployment has Voice, data and Location Based Services, follow the voice recommendations and fill in the coverage area with monitor mode APs.

Data-Only Deployments

Data only deployments will not require a large amount of overlap (above 10% overlap). If you have lower data rates enabled, 802.11 clients will respond to a lower signal from a nearby AP, should one fail, by stepping down their data rate and taking a longer time to transmit or roaming to a new AP. While the smaller overlap minimize co-channel interference, data clients will drop packets as they shift data rate or roam to a new AP. This will slow data throughput on the wireless network.
The required overlap will be determined by the WLAN data rate requirement discussed in the subsection below. Minimal overlap is required for data-only networks which allow all data rates. For data-only networks, the rule of thumb for separation of APs is typically 120-130 feet. But, when making your estimation for AP separation, remember to factor in objects that affect RF coverage such as wall densities, machinery, elevators, or even wide open space with steel cages, as your results may vary depending on the RF environment. Radio Resource Management (RRM) has been developed for this type of deployment and is very useful for controlling the RF coverage.

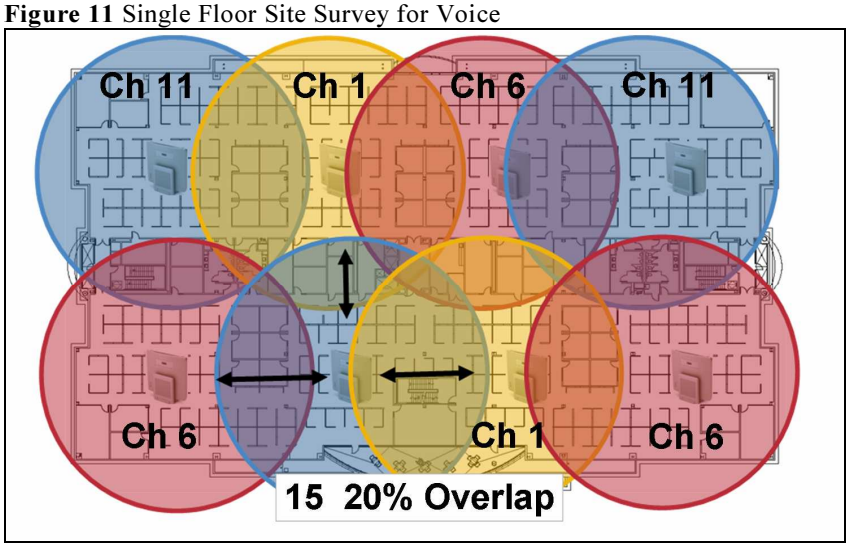
Voice Deployments

Figure 11 shows the voice network pattern and overlap. The APs are grouped closer together and have more overlap than a data-only installation because voice clients need to roam to a better AP before dropping packets. Although only one AP is required to handle its defined area of the coverage area for a voice deployment, it is recommended that you have 2 AP's on non-overlapping channels. For the Nokia Wi-FI voice deployment, it is recommended that you have a Received Signal Strength Indication (RSSI) above -67dBm at all time in your installation. This is to ensure that the VOIP phone has good reception as well as providing coverage and enhances roaming ability for the phone.

Pre and post site surveys are often helpful in designing AP coverage. When VoIP applications are involved, the rule of thumb is 100' separation typically. When making your estimation for separation, remember to factor in objects that affect RF coverage such as wall densities, machinery, elevators, or even wide open space with steel cages, as your results may vary depending on the RF environment.

Please see the Voice section of the Cisco Enterprise Mobility Design Guide for further reading on deploying Voice of WLAN.

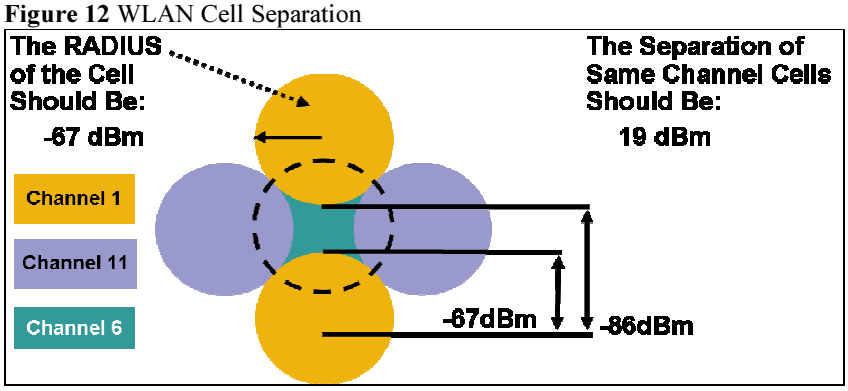
Figure 11 Single Floor Site Survey for Voice



Note: This is the cell perspective from the access point. Each phone has its own cell. Looking at channel 6 in the lower right corner, it can be seen that phone associated to that access point could have channel overlap with the channel 6 access point in the middle. It is recommended that you have a Received Signal Strength Indication (RSSI) above -67dBm at all time in your installation, at 12Mb.

The same channels need to be transmit power adjusted so that they separated by 19dBm. This reduces the size of the collision domain and will reduce a noise floor effect that the like channels will have on each other.

Figure 12 WLAN Cell Separation



1.3.2. Recommended Environment for the Nokia Eseries

The Nokia Eseries uses RSSI (Received Signal Strength Indication), TX failure, and beacon loss as its primary tools for making roaming and association decisions. In order to have a successful wireless voice deployment it is highly recommended that you conduct a site survey specifically for voice due to the uniqueness of voice deployments. When deploying an environment for the Nokia Eseries observe the following guidelines:

- Cisco recommends that you have no more than approximately 15 – 25 devices per AP.
- Maintain a minimum speed of 12Mb. Enabling lower speeds will result in lower call capacity.
- Deploy a minimum of two AP's on no-overlapping channels, with an RSSI that is greater than **-67 dBm** for speeds of 12Mb.
- Separate overlapping channel sets by approximately 19 dBm.
- Strive to maintain the highest possible speed throughout your coverage area.
- Overlap coverage areas by a minimum of 20% to ensure smooth roaming.
- With optimal settings and minimal data throughput 7 call legs per AP at 12 Mb can be achieved. Higher rates have not yet been verified. A call leg is a single phone on a call. A call between two phones associated to the same AP counts as two active call legs.
- Ensure your packet error rate and beacon loss is 1% or less.

Note: If enabled on the AP, Dynamic Transmit Power Control (DTPC) allows the AP to broadcast transmit power, and clients can automatically configure themselves to that power while associated with that AP. The Cisco IOS command for enabling DTPC is **power client** and was first introduced in Cisco IOS version 12.2(4)JA.

Clients operating on 802.11b can operate on AP's that support 802.11g as well, assuming that the 802.11b speeds are enabled. However, mixing these slower clients can significantly reduce the throughput for the faster 802.11g users, and can reduce the number of calls per AP. For a discussion on mixing 802.11b and 802.11g clients see:
http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml

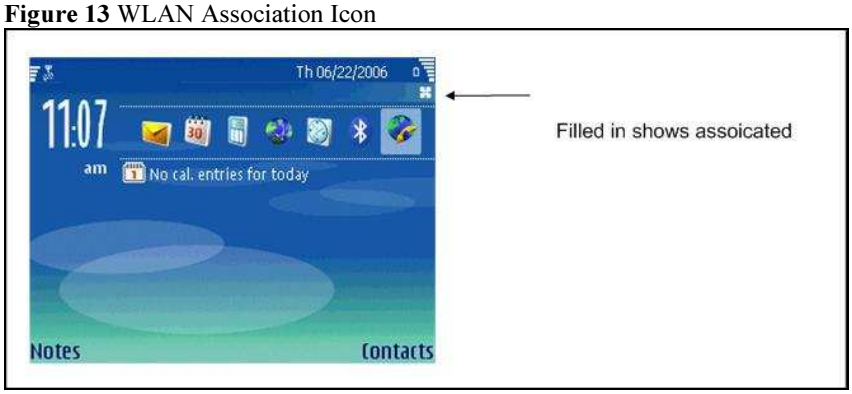
1.4. Nokia RF Tools

There are several tools on the Nokia Eseries for evaluating the availability and security of the wireless environment. When the Nokia Eseries is in the presence of a wireless network that is not hidden (broadcasting its SSID) there will be an indication on the screen. If the phone has not yet associate to the WLAN, the indicator boxes will not be filled in. When this icon is shown the users immediately knows that there is an access point in the area and it is advertising its SSID.

For deployment of the Nokia Eseries it is recommended that you enable broadcasting of the SSID. This has been found to significantly improve phone performance on the WLAN.

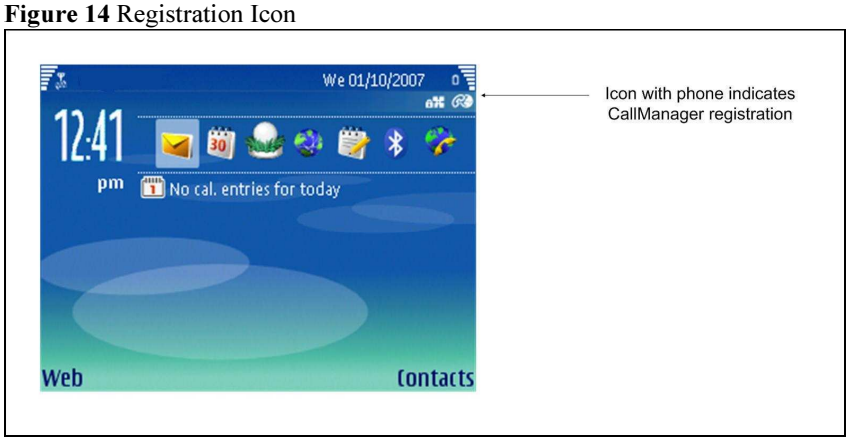
When the phone associates to an access point the icon boxes change to a filled in state as show in **Figure 13**.

Figure 13 WLAN Association Icon



After associating with the access point and registering to Communications Manager, a new icon will be shown below in Figure 14.

Figure 14 Registration Icon

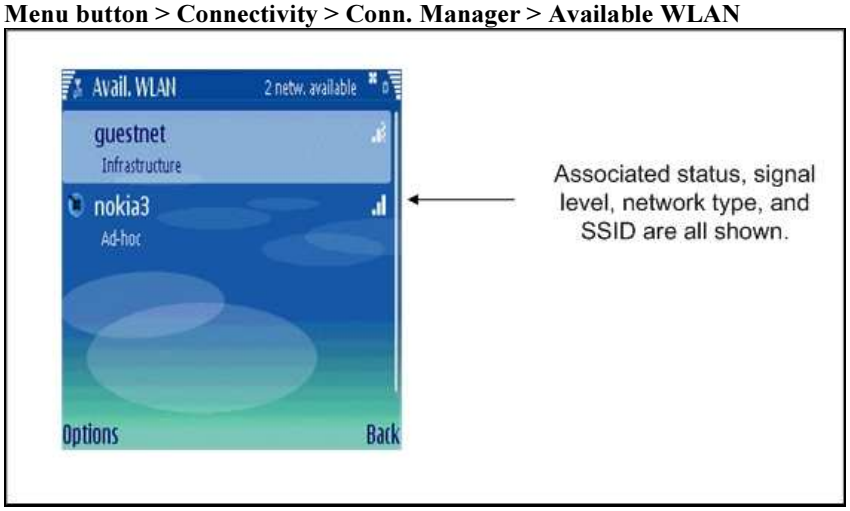


1.4.1. Using Connection Manager

The Connection Manager is comprised of two important applications, the Active Data Connections and the Available WLAN application. These tools give users a detailed view of wireless environment.

Available WLAN
By selecting the Available WLAN utility you can quickly determine all of the networks that the phone is able to sense via SSIDs that are being broadcast, the approximate signal level, whether the AP is open or secured, and if your phone is currently associated to that AP. In **Figure 15** we can see that there are currently two WLANs in the area, that the signal is low on the guestnet and higher on nokia3. When a network is secured it will show as having a lock icon on it and that we are associated to that network currently. Notice that we are currently associated to the nokia3 network, which is indicated by the associated icon in a circle next to that wireless network.

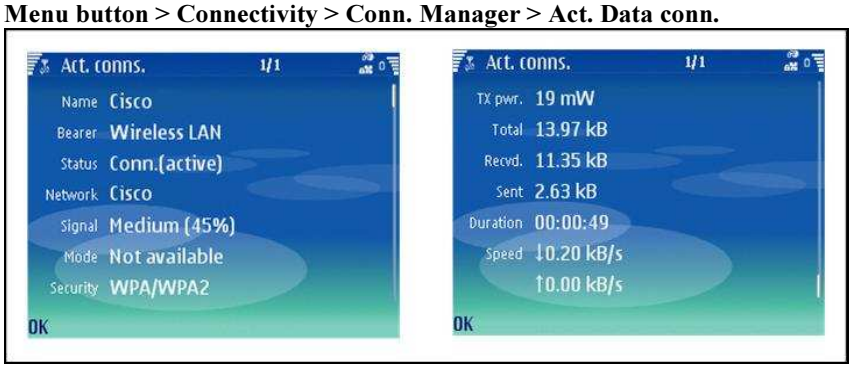
Figure 15 Nokia Available WLAN
Menu button > Connectivity > Conn. Manager > Available WLAN



If we now highlight and open an SSID we can see more details about this network including the SSID name, the security type, speed, how many AP's are available with this SSID, and also the signal strength. See the section labeled Evaluating Signal Strength for more details on how this can assist users.

Active Connections
The Active Connections tool presents a very detailed view of our current wireless connection. The key points of this tool are the Status and TX Power. The status of an active connection will show the received signal strength in a percentage generically as Strong, Medium, or Weak. When this document references a recommended signal strength percentage, it is referring to it as shown in this tool. The TX Power indication is useful for ensuring that the AP and phone have synchronized their transmit power levels.

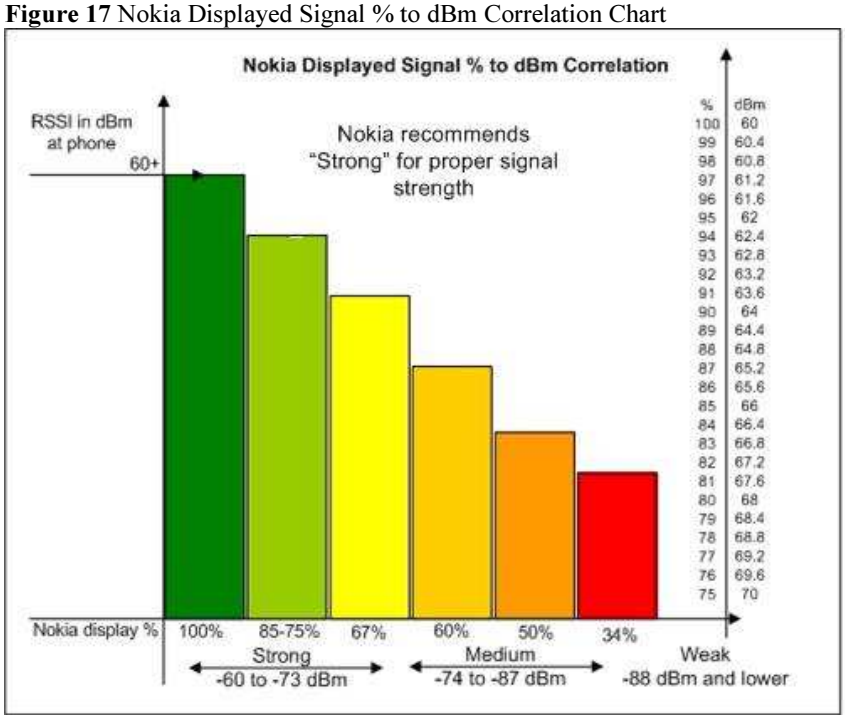
Figure 16 Nokia Active Data Connections
Menu button > Connectivity > Conn. Manager > Act. Data conn.



Evaluating Signal Strength
The Nokia Eseries does not display its WLAN signal strength indication in dBm. Below in Figure 18 is an approximation of shown percentage to dBm. Use this to assist in determining if the phone is receiving adequate signal. It should be noted that there can be significant difference in signal level when simply viewing the phone and when it is placed to the ear with a hand covering the phone.

It is recommended to keep the phone in the Strong area of coverage. Strong indicates signal strength of 67 – 100%. If you are operating at a rate of 48 – 54Mb then the recommended signal strength is 75% and higher. This level of signal will help the phone to give good voice quality and roam more smoothly.

Figure 17 Nokia Displayed Signal % to dBm Correlation Chart



1.4.2. Supported Security Mechanisms

The Nokia Eseries supports the following key management types:

- WEP 64bit
- WEP 128bit
- 802.1X with dynamic WEP
- WPA-PSK
- WPA2-PSK
- WPA-Enterprise
- WPA2-Enterprise
- CCKM

The following EAP types are supported as well:

- EAP-TLS
- EAP-PEAP
- EAP-LEAP
- EAP-TTLS
- EAP-SIM
- EAP-AKA

- EAP-MSCHAPv2
- EAP-GTC
- MSCHAPv2

Note: Currently Nokia does not support EAP-FAST.

The following encryption methods are supported:

- WEP 64bit
- WEP 128bit
- TKIP
- AES

Note: To facilitate faster roaming Cisco recommends that CCKM (Cisco Centralized Key Management be utilized.

1.5. Roaming

An integral concept for wireless networks is device roaming. It is important to understand what roaming is, how and when it occurs, what types of roaming there are, and how the types differ. One of the obvious benefits of WLAN IP Phones compared to wired IP Phones is the ability of the user to move from place to place while having a conversation. But unlike cellular phone services, where coverage areas are usually nationwide or international, WLAN IP Phones have smaller coverage areas. In addition, administrators of WLAN IP Phone networks need to understand and consider their IP addressing schemes before deploying WLAN IP Phones. They need to consider how WLAN IP Phone coverage overlays with the Layer 2 and Layer 3 addressing within the IP network. A Layer 2 network is defined as a single IP subnet and broadcast domain, while a Layer 3 network is defined as the combination of multiple IP subnets and broadcast domains.

1.5.1. Layer 2 Roaming

In voice systems, roaming usually refers to physical movement and the locations from which a call can originate. For 802.11 data networks, roaming also refers to physical movement, but it is often associated with data connectivity while physically moving.

This type of roaming does not include moving from the 802.11 environment to the cellular network. The Nokia Eseries does not support roaming from Wi-Fi to cellular. At this time both the GSM and 802.11 radios are active at the same time.

Nokia uses TX failure, beacon loss, and RSSI (received signal strength) to determine whether or not to roam. An association will be made to the AP with the highest RSSI. When the phone is associated to a WLAN network it does not perform periodic background scanning by default. If the RSSI drops below -80dB (40% - 50% in Connection Manager) a scan of all channels will begin. Because of this threshold, if you have moved within range of an access point with better signal strength, but you are still currently above -80dB the phone will not initiate roaming.

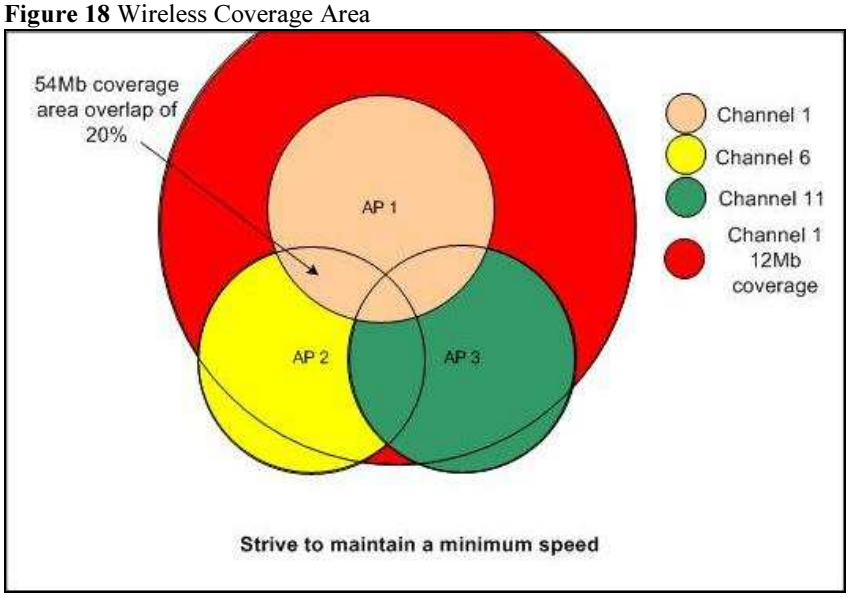
It is recommended that you strive to maintain a consistent minimum speed throughout your coverage areas. Mixing speeds can cause phones to stay associated to those AP's even though they are in range of better.

Figure 18 illustrates this problem. AP1 has been configured for all OFDM rates of 12Mb and higher. AP's 2 and 3 are configured for 54mb. All AP's have the same transmit power level. Notice that because 12Mb requires less frequency it has a much larger coverage area than 54Mb does. This causes the phone to stay associated to AP1 even though AP2 is in closer proximity and has a higher signal and available speed.

To facilitate smooth roaming it is recommended that Cisco Centralized Key Management (CCKM) be implemented in the WLAN. Using CCKM requires 802.1x authentication with EAP-LEAP, PEAP, EAP-TLS, or EAP-TTLS. The use of CCKM can significantly speed up roaming between access points by reducing the need for clients to reauthenticate against the authentication server when a roam is initiated due to an RSSI threshold being exceeded. For an overview of CCKM see the link below:
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_brochure.html

Design your VoWLAN network to the minimum speed that is configured. For example, if you access points are configured for 24Mb and higher, you should design your coverage overlap and estimate calls per AP based on this minimum value. If the phones are in a coverage area allowing them to transmit at 54Mb it will increase the potential number of calls per AP, but unless the entire network is fixed at this speed it is impossible to accurately estimate the call capacity of a mixed environment.

Figure 18 Wireless Coverage Area



1.5.2. Roaming between WLAN and GSM

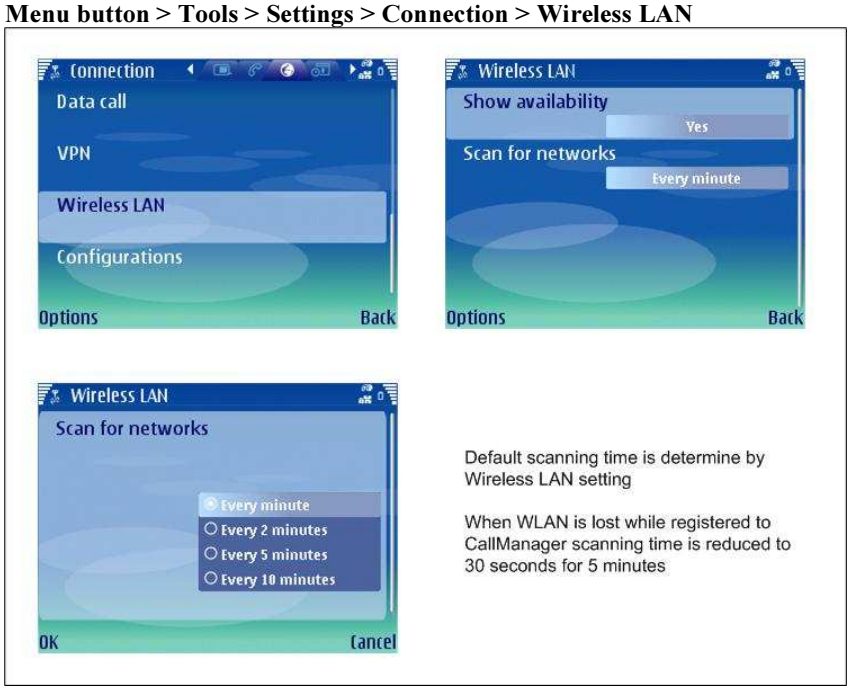
Currently there is no capability for roaming between the GSM network and the wireless LAN. If you are on an active WLAN call, and roam out of coverage area your call will be disconnected.

1.5.3. Registration Behavior

The WLAN scanning time is determined by the Wireless LAN setting from **Menu button > Tools > Settings > Connection > Wireless LAN**. This setting determines how often the Nokia phones will scan for WLANs if it is currently not associated to an access point, and the default for the setting is 5 minutes. If a Nokia ESeries is registered to Communications Manager and the WLAN connection is dropped, the SCCP client application will change the background scanning time to 30 seconds for the next 5 minutes. This allows the phone to quickly find a new access point and reregister to Communications Manager. If an

access point is not found during this 5 minute window the phone will revert back to the default configuration, which can be adjusted. The options are 1, 2, 5, and 10 minutes.

Figure 19 Background Scanning Time
Menu button > Tools > Settings > Connection > Wireless LAN



1.6. Quality of Service

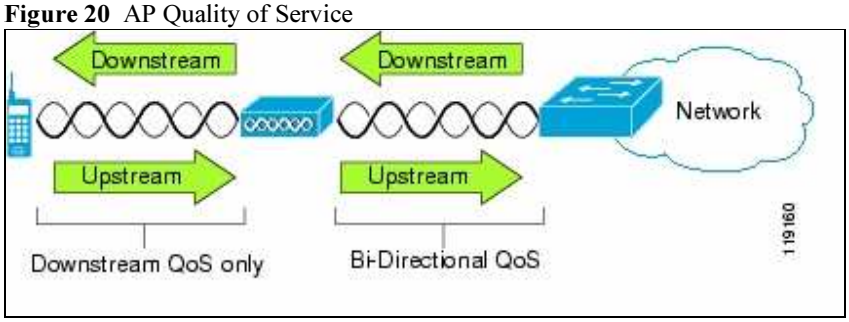
Voice traffic on the Wireless LAN, like data traffic, is susceptible to delay, jitter, and packet loss. These issues do not impact the data end user, but have serious implications for a voice call. To ensure that voice traffic receives timely and reliable treatment with low delay and low jitter, you must use Quality of Service (QoS), and use separate virtual LANs (VLANs) for voice and data. By isolating the voice traffic onto a separate VLAN, you can use QoS to provide priority treatment for voice packets when traveling across the network. You need the following VLANs on the network switches and the access points that support voice connections on the WLAN.

• Voice VLAN—Voice traffic to and from the wireless IP phone
• Data VLAN—Data traffic to and from the wireless PC
• Native VLAN—Data traffic to and from wireless devices

1.6.1. Quality of Service for Voice Traffic

Unlike wired networks with dedicated bandwidth, WLAN networks have to consider traffic direction when implementing QoS. Traffic is considered as either upstream or downstream from the point of view of the AP, as shown in Figure 20.

Figure 20 AP Quality of Service



The data VLAN should not be VLAN 1which is typically the default native VLAN for all network devices.

Assign separate SSIDs to the voice and to the data VLANs. You can also configure a separate management VLAN in the WLAN, but do not associate an SSID with the management VLAN.

By separating the phones onto a voice VLAN and marking voice packets with higher CoS, you can ensure that voice traffic gets priority treatment over data traffic. You can management traffic resulting in lower delay and fewer lost packets.

Beginning with Cisco IOS Release 12.2(11)JA, Cisco Aironet APs support EDCF-type QoS, with up to eight queues for downstream (toward the 802.11b clients) QoS. These queues can be allocated in any of the following ways:

- Based on ToS or DSCP settings of the packets
- Based on Layer 2 or Layer 3 access lists
- Based on VLAN
- Based on dynamic registration of devices such as the Cisco 7920 Wireless IP Phone

Voice (RTP) and signaling (SCCP) traffic should be placed into the highest priority queue, and all data traffic should be placed into a best-effort queue. While 802.11b EDCF does not guarantee that voice traffic will be protected from data traffic, using this queuing model should provide the best statistical results for voice QoS.

Note: The Nokia Eseries phones mark the SCCP signaling packets with a DSCP value of 24 and RTP packets with DSCP 46.

To improve the reliability of voice transmissions in a non-deterministic environment the Nokia Eseries is Wi-Fi Multimedia (WMM) capable. WMM enables differentiated services for voice, video, best effort data and other traffic. However, in order for these differentiated services to provide sufficient Quality of Service for voice packets, only a certain amount of voice bandwidth can be serviced or admitted on a channel at any one time. If the network can handle "N" voice calls with reserved bandwidth, when the amount of voice traffic is increased beyond this limit, i.e. to the "N+1" call, the quality of all calls will suffer.

Note: The Nokia Eseries is CCX version 3 compliant and supports Wi-Fi Multimedia (WMM).

Implementing Quality of Service in the connected Ethernet switch is highly recommended to maintain good voice quality. To configure the QoS correctly on the AP see the section above labeled Interacting with the Cisco Access Point.

Individual configurations will vary; however, examples are given below of potential switch QoS commands to implement.

```
mls qos
mls qos map cos-dscp 0 8 16 24 34 46 48 56
mls qos map ip-prec-dscp 0 8 16 24 34 46 48 56

interface FastEthernet0/10
 switchport access vlan 11
 switchport mode access
 switchport voice vlan 111
 no ip address
 mls qos trust dscp
 wrr-queue cos-map 1 1
 wrr-queue cos-map 2
 wrr-queue cos-map 3 2 3 4 6 7
 wrr-queue cos-map 4 5
 priority-queue out
 spanning-tree portfast
```

Note: If you are using a Cisco Catalyst 4000 Series Switch as the main router in the network, ensure that it contains, at a minimum, either a Supervisor Engine 2+ (SUP2+) or Supervisor Engine 3 (SUP3) module. The SUP1 or SUP2 module can cause roaming delays, as can the Cisco Catalyst 2948G, 2980G, 2980G-A, 4912, and 2948G-GE-TX switches.

Note: Implementing proper QoS on the access point and Ethernet switch is highly recommended.

The SCCP signaling messages are marked with DSCP 24 and RTP packets are marked with DSCP 46 which match the DSCP markings of wired phones.

1.7. Understanding Differences Between Nokia Eseries and Cisco Wireless IP Phones

The Nokia Eseries and Cisco Wireless IP Phones have many similar capabilities; however, there are many key differences that need to be considered.

The Cisco 7920 and 7921 wireless IP phones are designed to behave very similar to Cisco's desk phones, such as the 7960 and 7970. This means that the access services such as directory and XML services in the same manner. Even though the Nokia Eseries devices do register as an SCCP endpoint, they behave in the same fashion as other GSM devices, and are optimized for cellular and data usage rather than just VoWLAN as the 7920 and 7921 are. Table 4 lists key feature differences.

Table 4 Nokia Eseries and Cisco Wireless IP Phone Features

Feature	Nokia Eseries	Cisco Wireless IP Phones	Notes
Directory	E51 Only	Uses XML directory lookup	
XML	Not Available	Available	XML can be used on Cisco phones for application and directory integration
IPCC Express support	Not Supported	Supported	Nokia Eseries is not intended for call center usage.
TFTP firmware download	Not Supported	Supported	Firmware must be obtained from Nokia, not Communications Manager
TFTP configuration	Supported	Supported	
GSM / GPRS capability	Supported	Not Supported	Cisco wireless IP phones are considered 'singlemode' and do not support cellular services
SRST fallback	Not Supported	Supported	
SCCP signaling	Supported	Supported	
SIP signaling	Available, but Not Supported on Communications Manager	Not Available	
Encryption	WEP, TKIP, AES	WEP, TKIP, AES	WPA2 available on Cisco 7921 only
Authentication	EAP-TLS, EAP-PEAP, EAP-LEAP, EAP-TTLS, EAP-SIM, EAP-AKA, EAP-MSCHAPv2, EAP-GTC	WPA, EAP-FAST	
QoS	WMM	WMM, CDP	
Call Admission Control	Not Supported	TSPEC, QBSS	
802.11b/g	Supported	Supported	802.11g on 7921 only
802.11a	Not Supported	Supported	7921 only
Roaming	Signal strength and packet loss	Signal strength, packet loss, and QoS	The Nokia Eseries will not roam unless the signal strength or packet loss exceed preconfigured thresholds
Power save	U-APSD (E51, via Device Manager Server for other modesl), PS-POLL	U-APSD, PS-POLL	

1.8. Upgrading To Version 1.1 Using BAT

Users who have already deployed on Intellisync Call Connect for Cisco 1.0 (ICC 1.0) may need to eventually upgrade to version ICC 1.1. In version 1.0 registration of Nokia ESeries as a 7960 device type could be used due to a lack of S60 device type in CUCME. However, in version 1.1 this has been disallowed in CUMC for several reasons:

- Device type has changed to a 7970 in CUCME
- Incorrect configuration of 7960 in CUCM could result in registration failure
- Licensing issues

If you have already configured your Nokia dual-modes as 7960's in CUCM and upgrade the SCCP application to version 1.1 your phones will fail to register correctly to CUCM due to a device type mis-match. Once version 1.1 is installed the Nokia Eseries will attempt to register as a 7970 or S60 device type, not a 7960, and auto-registration will fail due to the MAC address already being present in the database.

Note: Upgrading the Nokia dual-mode to ICC version 1.1 BEFORE migrating them to the S60 device type will cause registration failures for those devices. ICC version 1.1 changes device registration type from 7960 or S60 to 7970 or S60. The supported CUCM method is as a Nokia S60 device type.

As of version 6.0, CUCM does not support a method of migrating devices from one device type to a different device type. To do this requires that the current device profile be deleted and a new device added with the same MAC address. Automating this process can be done via BAT, though there are some caveats:

- User associations are not migrated
- MobilityManager configurations are not automatically migrated
- Due to DLU differences between 7960's and S60's, it is possible to exhaust the DLU pool

If you have a small number of devices it may be easy to update them one at a time, by deleting and re-adding them. However, for larger numbers of phones we have tried to provide a more automated method.

The upgrade from ICC 1.0 to ICC 1.1 is unlike that of typical devices registered to CUCM due to the firmware not being controlled by the TFTP process. Instead, users are free to upgrade their Nokia's to version 1.1 regardless of what has been done on CUCM. For this reason administrators may want to proactively migrate their devices to the S60 device type (which does NOT require version 1.1) to prevent potential phone outages.

What we have provided below is a step-by-step example of how to migrate Nokia's from 7960 to S60 devices. This assumes that the correct installation of the Nokia S60 device type has been added to CUCM.

To obtain the installation files, please, log in to Nokia support site at https://support.nokia.com and browse to page "Support / Software / Nokia ES Products / Mobility Solutions / Mobility Solutions / Mobile Voice Solutions / Nokia Intellisync Call Connect for Cisco". Direct link to Nokia ICC for Cisco v1.1 article is:

https://infocenter.knowledge.nokia.com/InfoCenter/index?page=content&id=1610720

Note: The steps outlined below for device type migration using BAT are done primarily to provide a template for doing so in your own installation. Device configurations are necessarily simplified to convey the idea, but it should be understood that actual deployments may require modifying the steps below to accommodate specific configurations.

The first step in the process of migrating device types is to **turn off auto-registration for CUCM**. Once the phones are removed from CUCM via BAT they will attempt to register again as 79XX devices.

1.8.1. Migration steps for CUCM Version 6.x

In our example below we have several Nokia devices registered as 7960's which will be migrated to Nokia S60 devices. The overall process requires the following steps:

- Create the S60 phone template
- Create the Nokia phone file
- Export the current device data
- Modify the exported data for insertion
- Delete the current devices
- Import the new device data
- Validate the devices can now register

1.8.1.1. Creating an S60 Phone Template

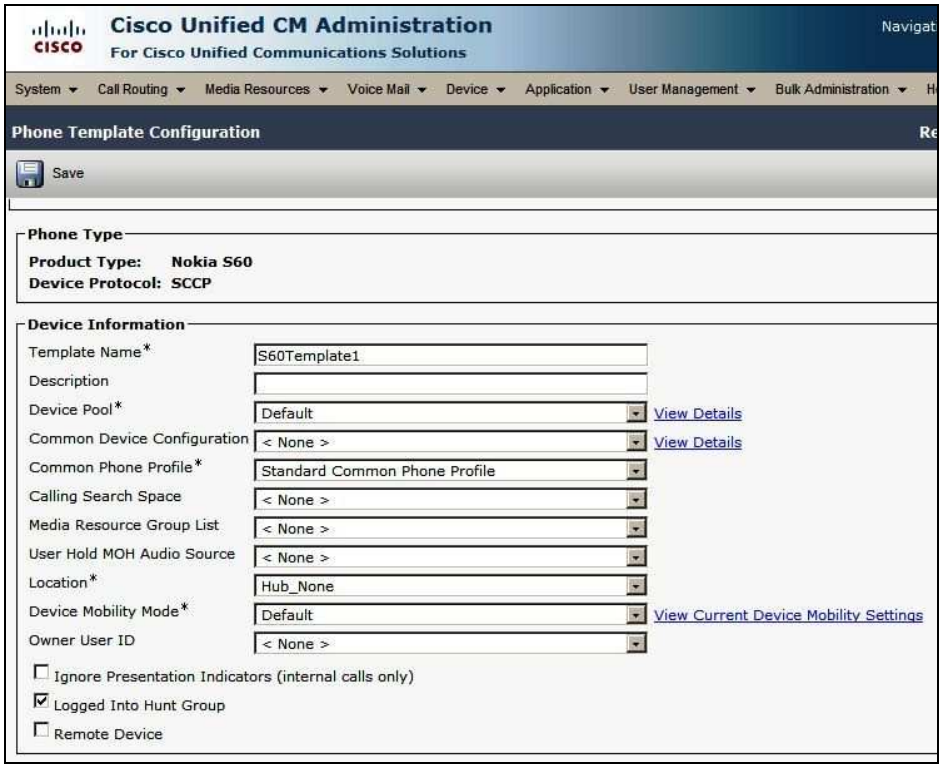
The S60 phone template is created for re-inserting the Nokia's into the database. There should be an S60 template that will be used. In our example we will only be creating one template, but the system is flexible enough to allow for multiple templates to be created. If you do not see the S60 device listed you may not have run the device installer for the S60.

First navigate to the Bulk Administration drop down in CUCM and find the Phone Template heading as in seen below.

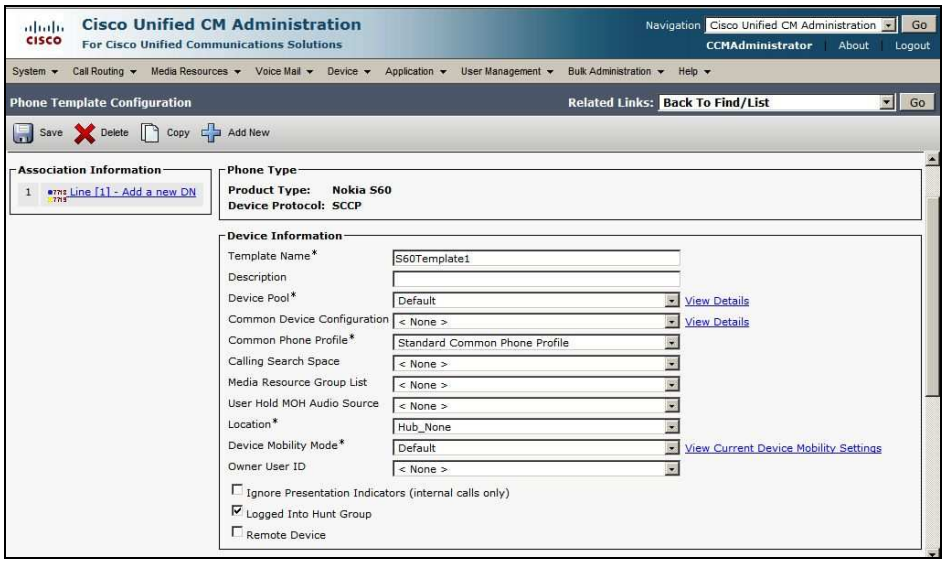
BAT > Phone Template > Phones > Phone Template

Now we are going to create an S60 phone template for the phones we want to insert. The actual configurations shown in the following steps are meant to be used as a guide, and are therefore simplified. In actual customer configurations it is expected that more configuration may be necessary.

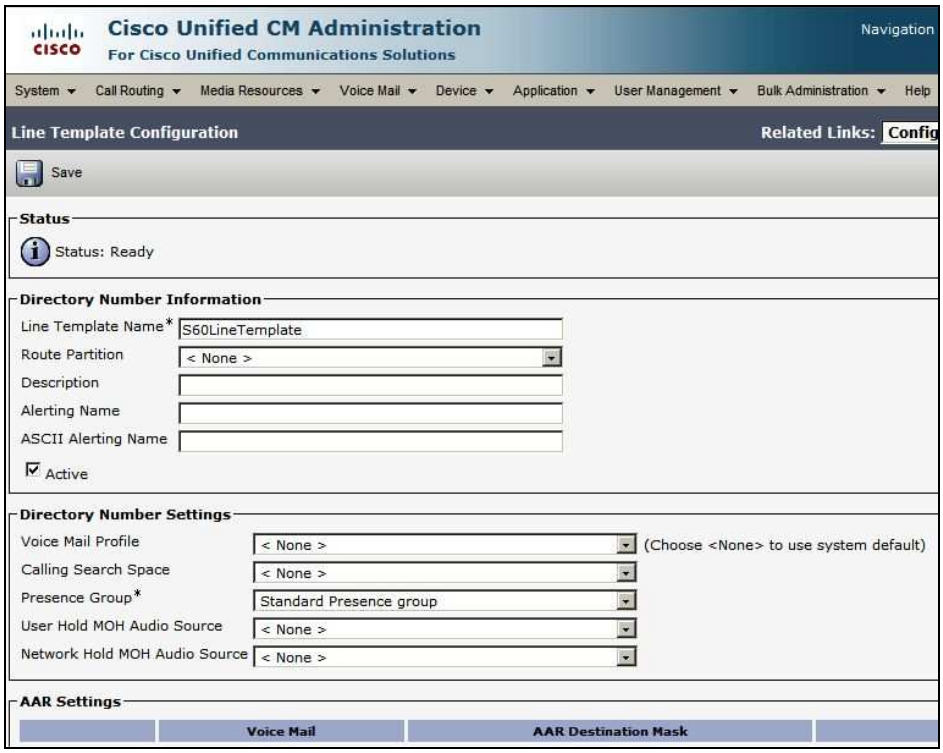
Here we fill in fields as needed for the Nokia's that will be inserted with this template.



Once the fields have been filled in appropriately click the Save button. This will save the template and also allow the Line information to be added. If the Line configuration is not completed the insert will not be done correctly.



In the section below we show the template configuration for the Line. Click Save when you have finished configuring the line.



This completes the Phone Template configuration.

1.8.1.2. Phone File Configuration

A Phone File is used for exporting information about devices. In this case we are attempting to migrate as much of the current information from the currently registered devices as possible. BAT comes with a Default and Standard phone file template, but we are going to create one from scratch.

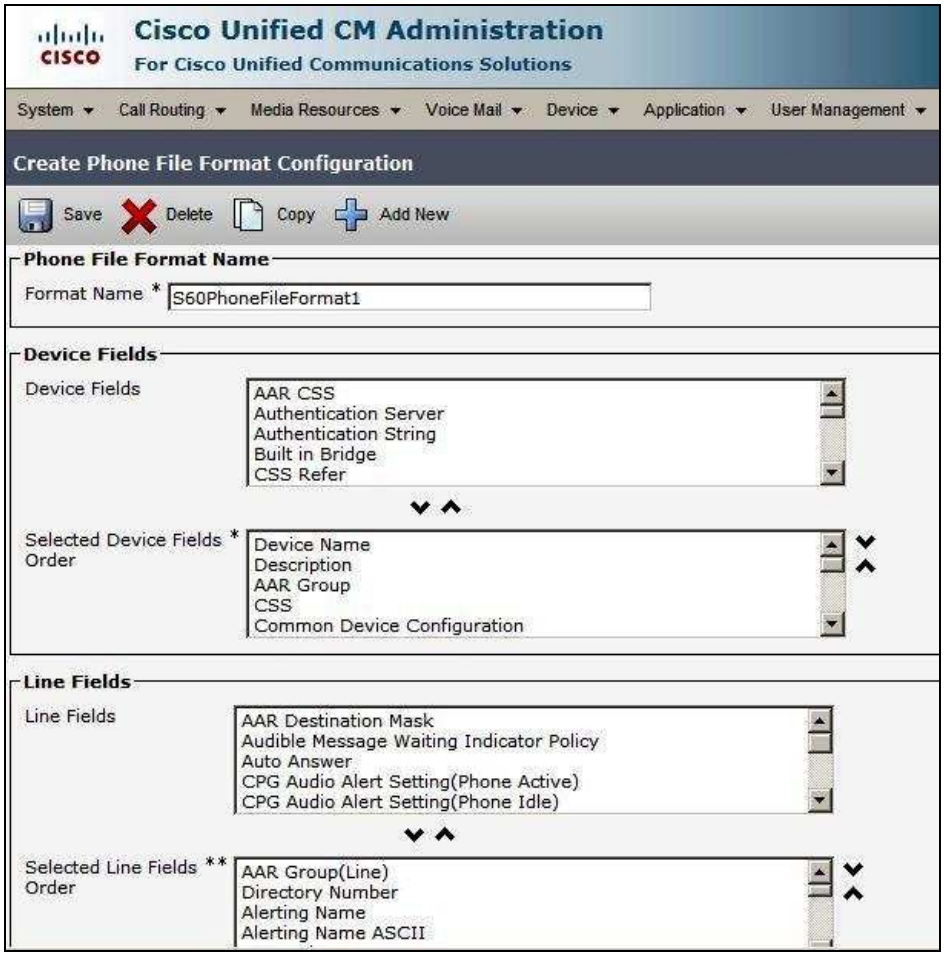
Browse to the BAT Phone File page by selecting **Bulk Administration > Phones > Phone File Format > Create File Format** and click the **Add New** button. The important part of this configuration is ensuring that we add all of the necessary fields, which have been outlined below.

Phone File Format Configuration order for **Device** Fields
- Device Name
- Description
- AAR Group
- CSS
- Common Device Configuration
- Device Pool
- Device Presence Group
- Security Profile
- Device Subscribe CSS
- Location
- MLPP Domain
- Device Mobility Mode

Media Resource Group List
Owner User ID
User Hold Audio Source

Phone File Format Configuration order for **Line** Fields
AAR Group(Line)
Directory Number
Alerting Name
Alerting Name ASCII
Busy Trigger
ASCII Display
External Phone Number Mask
Forward All CSS
Forward All CSS Activation Policy
Forward All Destination
Forward Busy External CSS
Forward Busy External Destination
Forward Busy Internal CSS
Forward Busy Internal Destination
Forward No Answer External CSS
Forward No Answer External Destination
Forward No Answer Internal CSS
Forward No Answer Internal Destination
Forward No Answer Ring Duration
Forward No Coverage External CSS
Forward No Coverage External Destination
Forward No Coverage Internal CSS
Forward No Coverage Internal Destination
Forward Unregistered External CSS
Forward Unregistered External Destination
Forward Unregistered Internal CSS
Forward Unregistered Internal Destination
Forward on CTI Failure CSS
Forward on CTI Failure Destination
Hold Reversion Notification Interval
Hold Reversion Ring Duration
Line CSS
Line Description
Line Network Hold Audio Source
Line Presence Group
Line Text Label
Line Text Labe ASCII
Line User Hold Audio Source
MLPP CSS
MLPP No Answer Ring Duration
MLPP Target
Maximum Number of Calls
Monitoring Calling Search Space
Partition
Voice Mail Profile
Call Pickup Group

The phone file template is used when we export the phones from the database.



Once the phone file template has been created, you will want to export your current phones. There are several types of Nokia ESeries that could be in your database including E51, E60, E61, E61i, E65, and E70's. Each device type is assigned a unique base MAC address which we can use for searching for Nokia devices, which otherwise will appear as Cisco 79XX phones.

To search for all possible Nokia device types search for the following base MAC addresses:

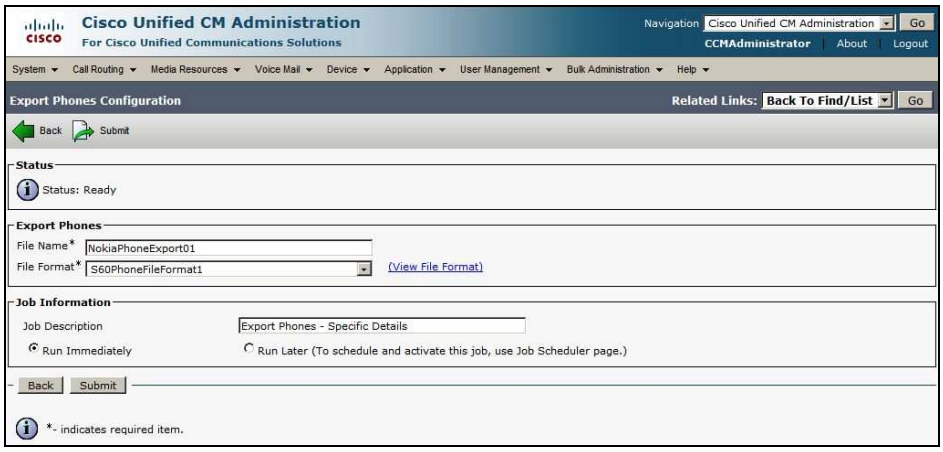
E51	001adc
E60	0015de
E61	0013fd
E61i	00194f
E65	001979
E70	0017b0

1.8.1.3. Exporting Nokia Devices

Next, browse to **BAT > Phones > Export Phones > Specific Details**. Here we will perform the search using the criteria above. Notice in the figure below that we are searching for Device Name, CONTAINS, and OR. This will allow the search to find all potential Nokia devices.

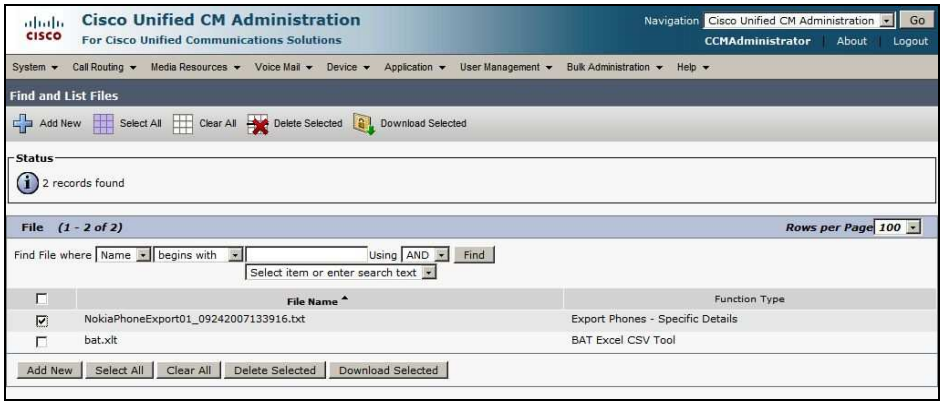
BAT > Phones > Export Phones > Specific Details

After you have searched and found the devices press **Next** to export them. You will notice now that we can apply the Phone File Format created in earlier steps.



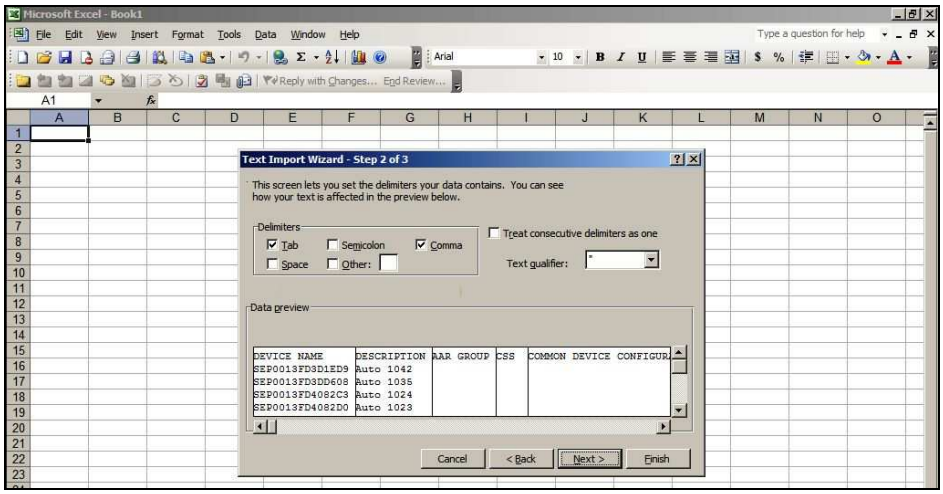
Submit your query to generate the phone file. This file will be used later for importing the devices back into the database.

To view the file that was created browse to **BAT > Upload/Download files**. Here we should find a .txt file that can be downloaded locally and imported into Excel.



Next we will open this file in Excel as a comma delimited file.

1.8.1.4. Using Excel to Modify Phone Data



Open MS Excel and then open the .txt file of exported data. When attempting to open the file MS Excel will recognize that this file could be a imported with delimiters and will prompt you how to open the file. You should open the file and select **"Delimited"** and then select **"Comma"** from the delimiters as shown above.

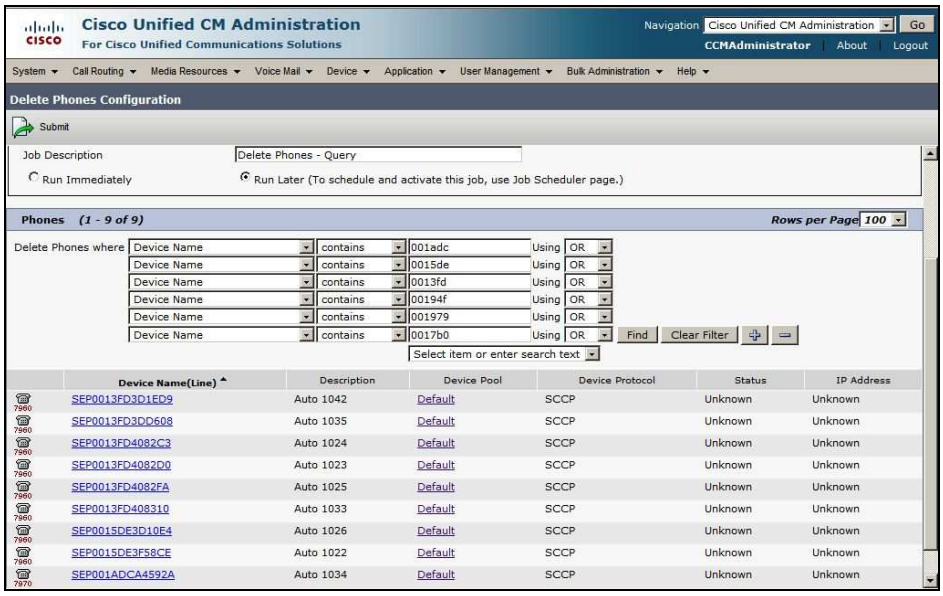
Now that we have the phones successfully exported and into a table format for importing we can modify it appropriately. We need to make the following changes:

Device Security Profile	"Nokia S60 – Standard SCCP Non-Secure Profile"
Maximum Number of Calls field	"3"

Save this file as a .csv file type for importing. Browse back to **BAT > Upload/Download** and upload the new .csv file.

1.8.1.5. Deleting Phones from the Database

Next, we are going to delete the phones from the database using BAT. To delete phones browse to **BAT > Phones > Delete Phones > Query**. We will use the same search criteria that we used before to delete the phones. Notice in the next figure we have searched and found nine Nokia devices in the database.

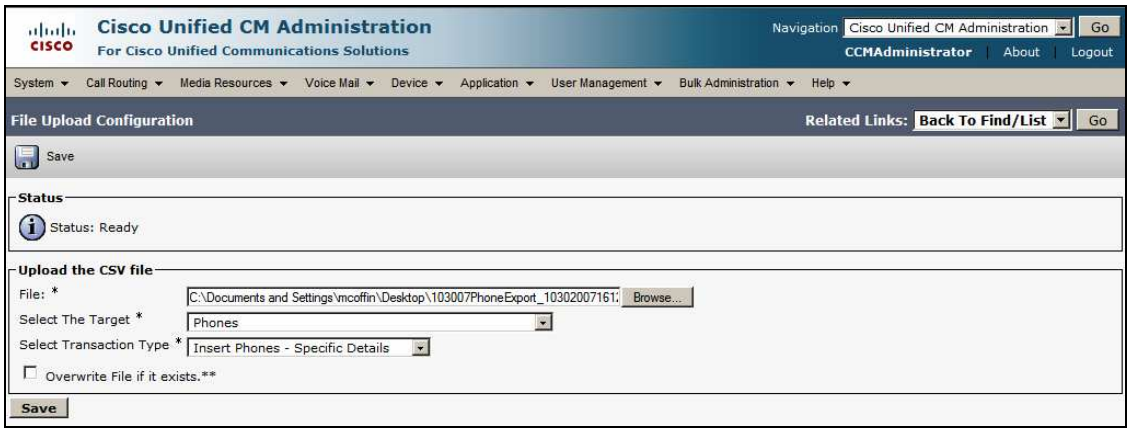


After running this job all 9 phones will be deleted.

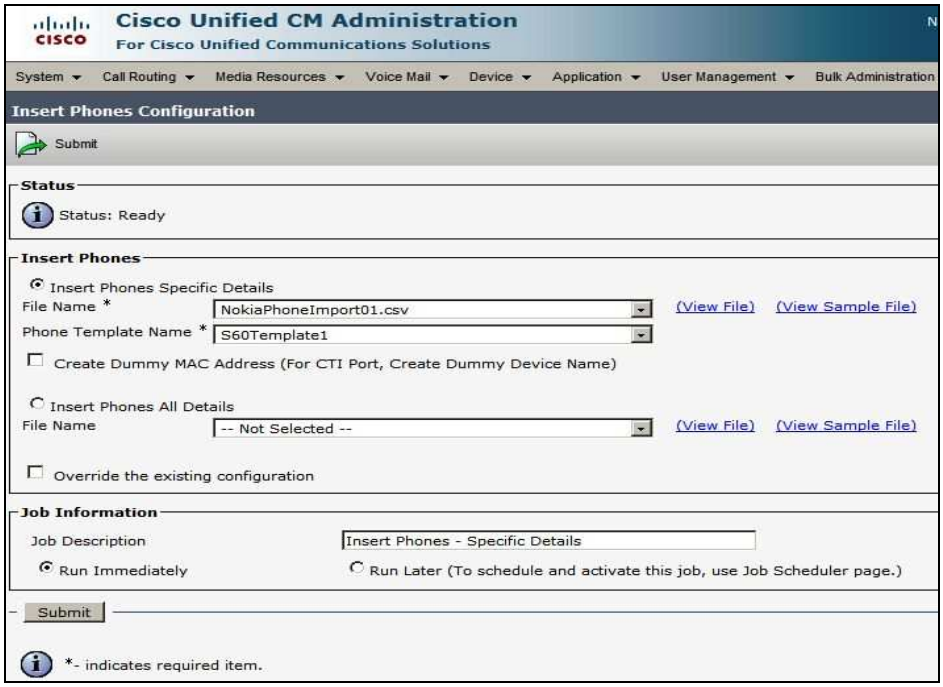
Note: If auto-registration has not been disabled the S60's may re-register back to CUCM as 79xx devices.

1.8.1.6. Importing Devices

To import the phones we are going to use the uploaded .csv file and the template that was created earlier, both of which should be available from the drop downs. Browse to **BAT > Upload/Download Files** to add the .csv file that was recently created, then click on the **Add New** button.



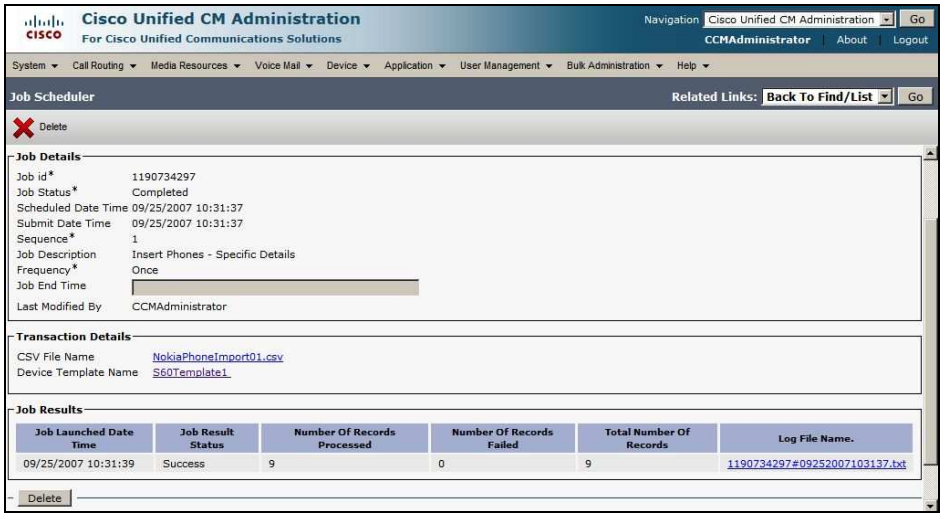
Next, browse to **BAT > Phones > Insert Phones**



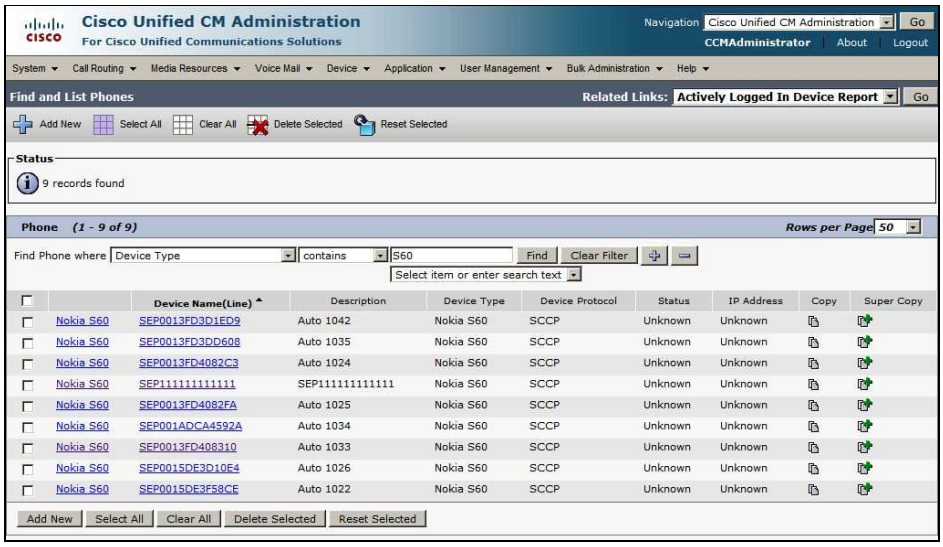
Once this job is run the phones will be added back to the database. If they are turned on and authenticated to the WLAN they may start registering back to CUCM.

1.8.1.7. Validating Insert

BAT allows us to validate that the insert worked by viewing the details of the job. To view the job browse to **BAT > Job Scheduler** and search for the recently Completed job. Click on the job ID to view if it was successful. If it failed, click on the Log File Name to view the details of why it failed.



To verify the phones are in the database you can perform a phone search, this time using Device Type as Containing S60. You should see the same number of phones as previously.



The steps above should be used as a simplified example. To learn more about BAT see the link below:
http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/bat/6_0_1/t03phtmp.html

1.8.2. Migration Steps for CUCM Version 5.x

The steps needed for migrating device types in CUCM 5.x are very similar to those in 6.x, but they have been outlined below as well. Installation of the .cop file is the same in 5.x as 6.x, and the same device type (Nokia S60) is added to the device list.

In this example we have 4 Nokia E61's registered as 7960's to a CUCM 5.1(3). Once the .cop file has been installed we can begin migrating from the Cisco device types to the S60's.

Note: If ICC has been installed on the Nokia dual-mode it will auto-register as a Cisco 7970 device.

1.8.2.1. CUCM Version 5.x Overview

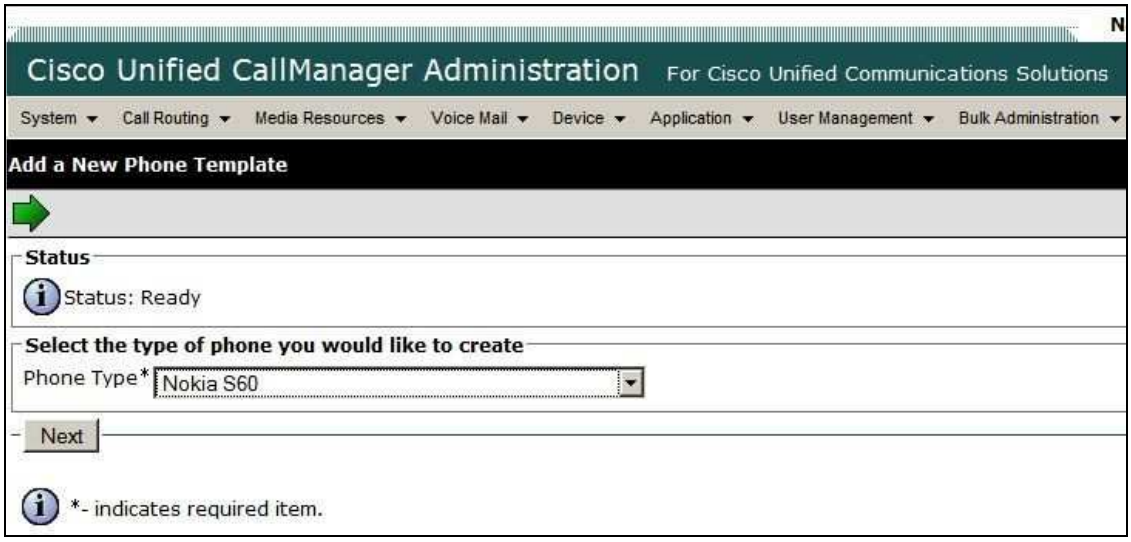
At a high level these are the steps needed to migrate from 7960 / 7970 device types to S60 device type:

- Create the S60 phone template
- Create the Nokia phone file
- Export the current device data
- Modify the exported data for insertion
- Delete the current devices
- Import the new devices data
- Validate the devices can now register

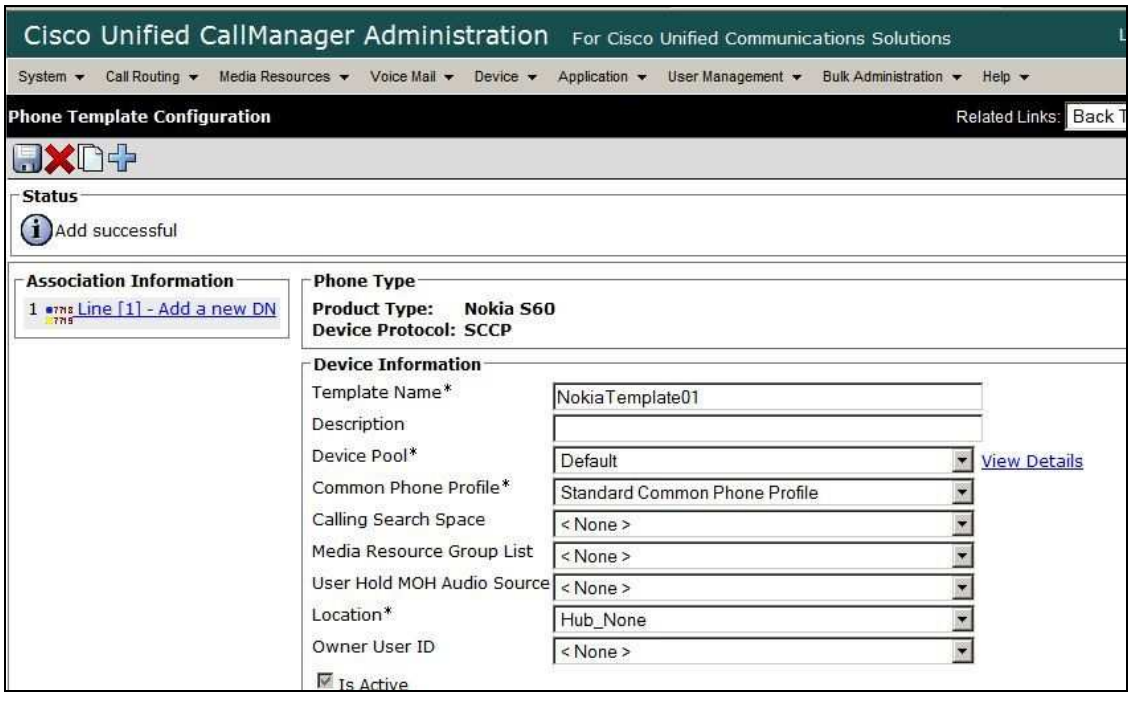
Note: When performing the steps above it is necessary to temporarily turn off auto-registration. If auto-registration is not turned off your Nokia devices may attempt to re-register as 7960's or 7970's before you have re-inserted them.

1.8.2.2. Creating the S60 Phone Template

Browse to **Bulk Administration > Phones > Phone Template** from CUCM Administration screens and click on **Add New**. Select **Nokia S60** as the device type and press **Next**.



Once the fields have been filled in appropriately click the Save button. This will save the template and also allow the Line information to be added. If the Line configuration is not completed the insert will not be done correctly.



1.8.2.3. Phone File Configuration

Next we are going to add the Phone File for exporting. To add this file browse to **Bulk Administration > Phones > Phone File Format > Create File Format** and click **Add New**.

The Device selected fields order will be:

Device Name
Description
AAR CSS
CSS
Device Pool
MLPP Domain
Media Resource Group List
Device Subscribe CSS
Device Presence Goup
Owner User ID
User Hold Audio Source
User ID

The Line selected fields order will be:

AAR Group
Directory Number
Alerting Name
Alerting Name ASCII
Busy Trigger
Call Pickup Group
Forward All CSS
Forward All Destination
Forward Busy External CSS
Forward Busy External Destination
Forward Busy Internal CSS
Forward Busy Internal Destination
Forward No Answer External CSS
Forward No Answer External Destination
Forward No Answer Internal CSS
Forward No Answer Internal Destination
Forward No Answer Ring Duration
Forward No Coverage External CSS
Forward No Coverage External Destination
Forward No Coverage Internal CSS
Forward No Coverage Internal Destination
Forward on CTI Failure CSS
Forward on CTI Failure Destination
Line CSS
Line Description
Line Network Hold Audio Source
Line Presence Group
Line Text Label
Line User Hold Audio Source
MLPP CSS
MLPP No Answer Ring Duration
MLPP Target
Maximum Number of Calls

Partition
Voice Mail Profile

Maximum Number of Lines = **2**

Click **Save** when finished.

1.8.2.4. Exporting Current Phone Data

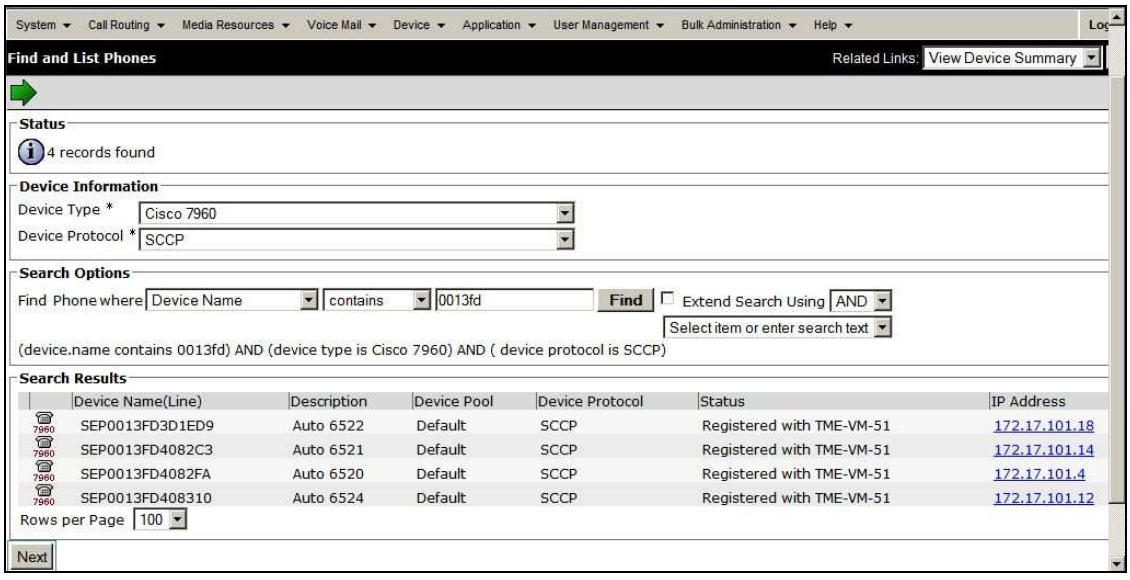
To export the information currently in the database, browse to **Bulk Administration > Phones > Export Phones > Specific Details**.

Here you must choose the Device Type and the Protocol for exporting. If you are dealing with clients on the ICC 1.0 version this will be 7960; however, if you have ICC version 1.1 clients this will be 7970. Here too we will be using the base MAC address as our search criteria, which have been outlined below:

E51	001adc
E60	0015de
E61	0013fd
E61i	00194f
E65	001979
E70	0017b0

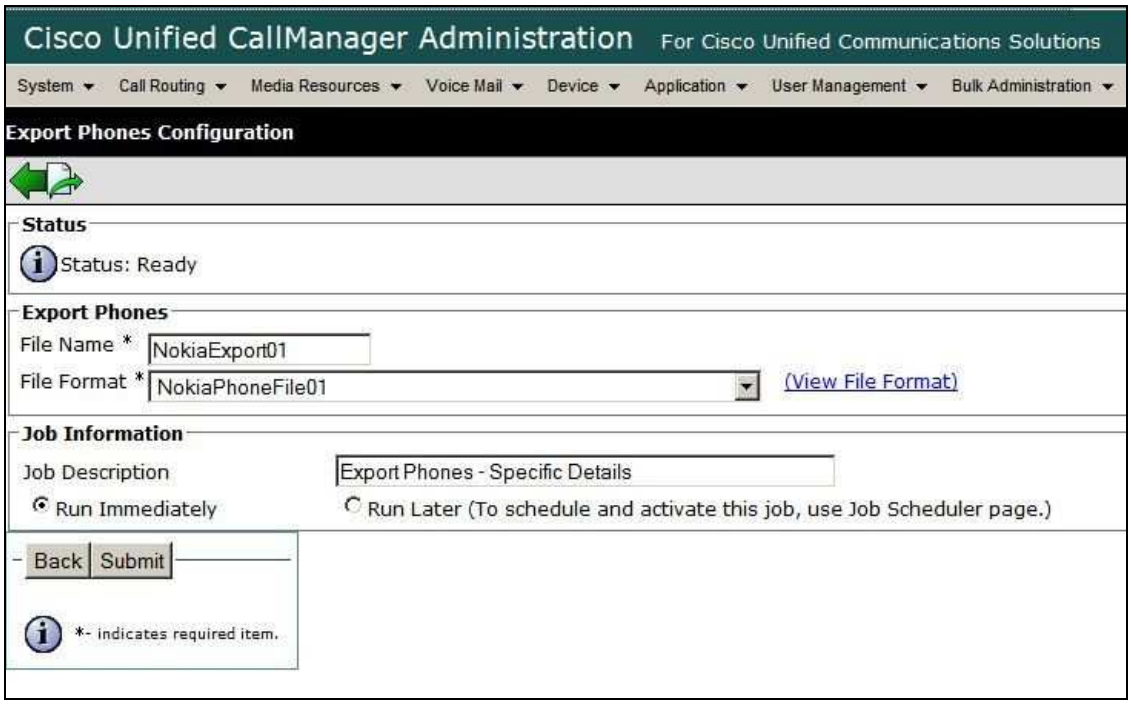
Note: The UI of CUCM 5.x does not allow for multiple search criteria so you will need to perform individual searches for each of the device types in your organization.

In our example we have 4 E61's starting with the base MAC address 0013fd.



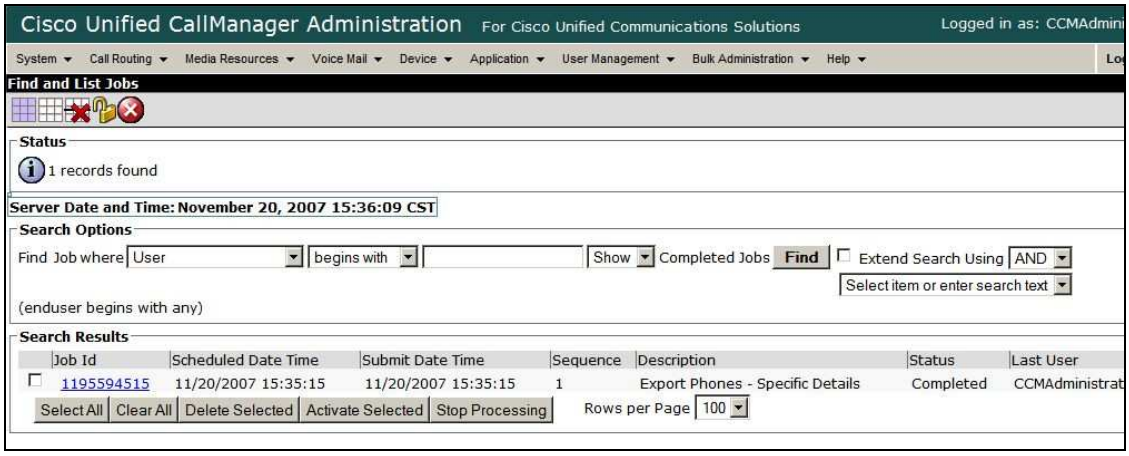
Click the **Next** button.

Now we export that data using the NokiaPhoneFile that was created in the previous steps.

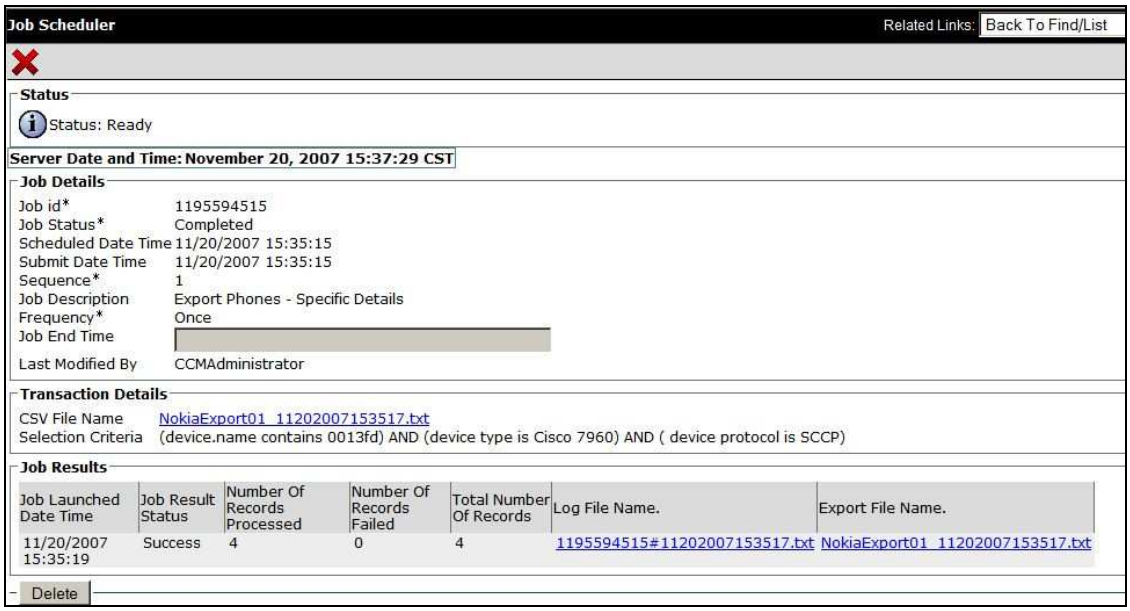


Click on **Submit** to run the job.

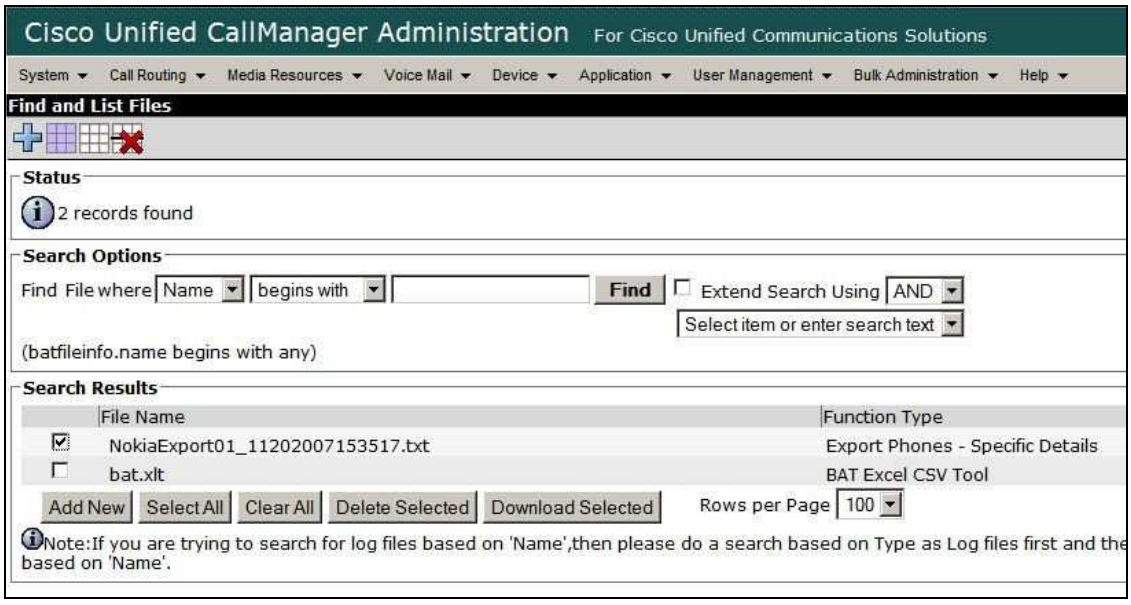
Browse to **Bulk Administration > Job Scheduler** to view the results of your export.



Click on the **Job Id** to view details of the results.

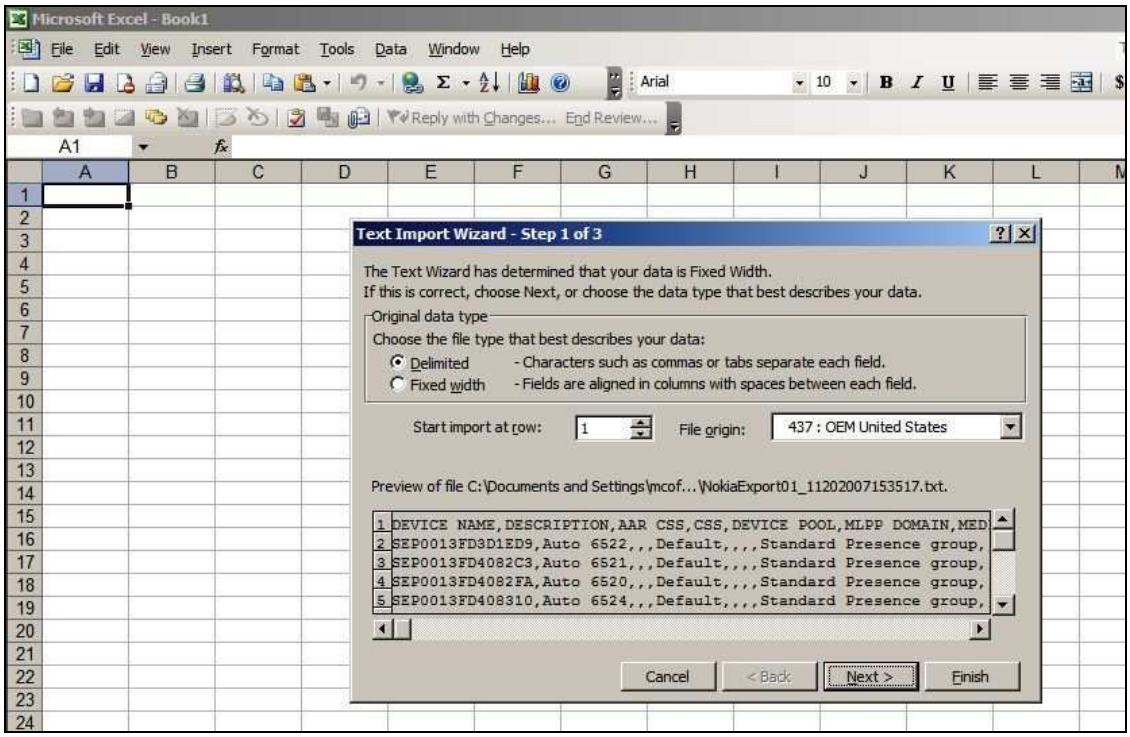


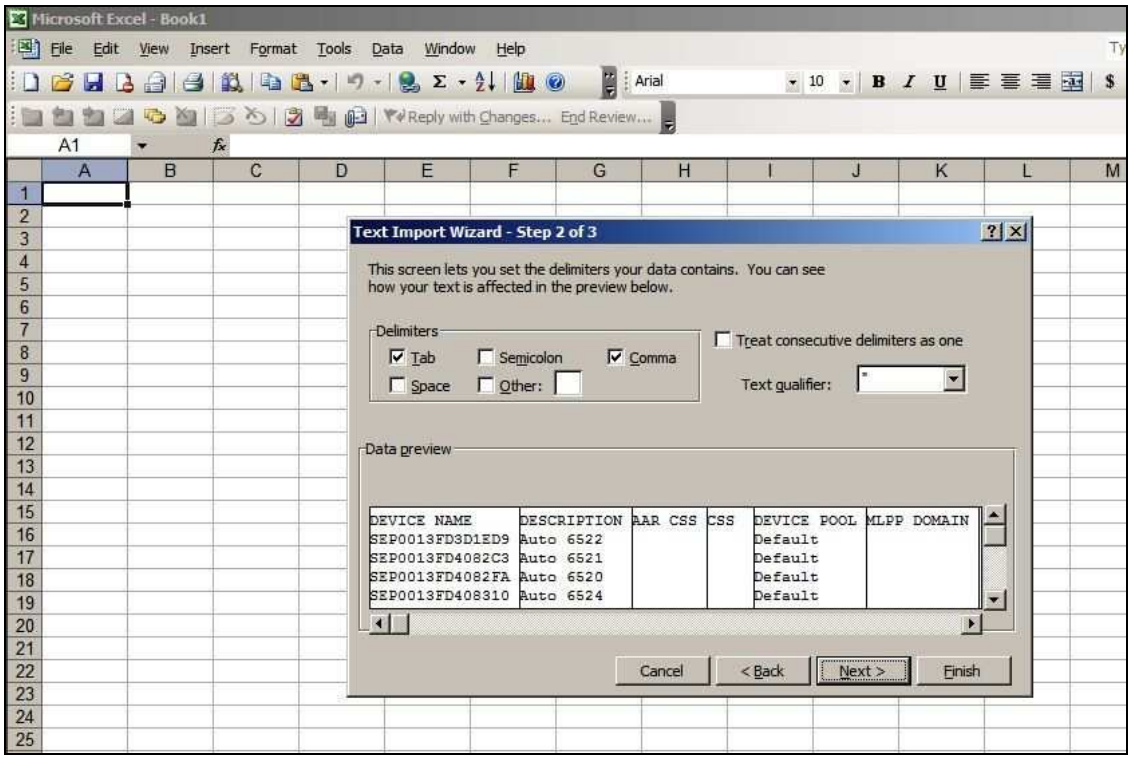
Now that we know the data has been successfully exported we can download the file for modification. To download the .txt file browse to **Bulk Administration > Upload/Download Files**, click on the check box next to the recently created file and select **Download Selected**.



1.8.2.5. Using Excel to Modify Phone Data

Save this file and open MS Excel. Once Excel is open we are going to import this comma delimited file. In Excel choose **File > Open > (NokiaExport.txt file).** When opening the file you should be prompted with the Text Import Wizard about how to open the file. Choose **Delimited > Next > Comma > Next > Finish.**





Next we are going to modify the data in a couple ways as shown below:

Device Name = Remove “SEP” from the front of the MAC addresses
Maximum Number of Calls = “3”

Be sure to check your data file for “Cisco 7960” or “Cisco 7970” and replace with “Nokia S60”.

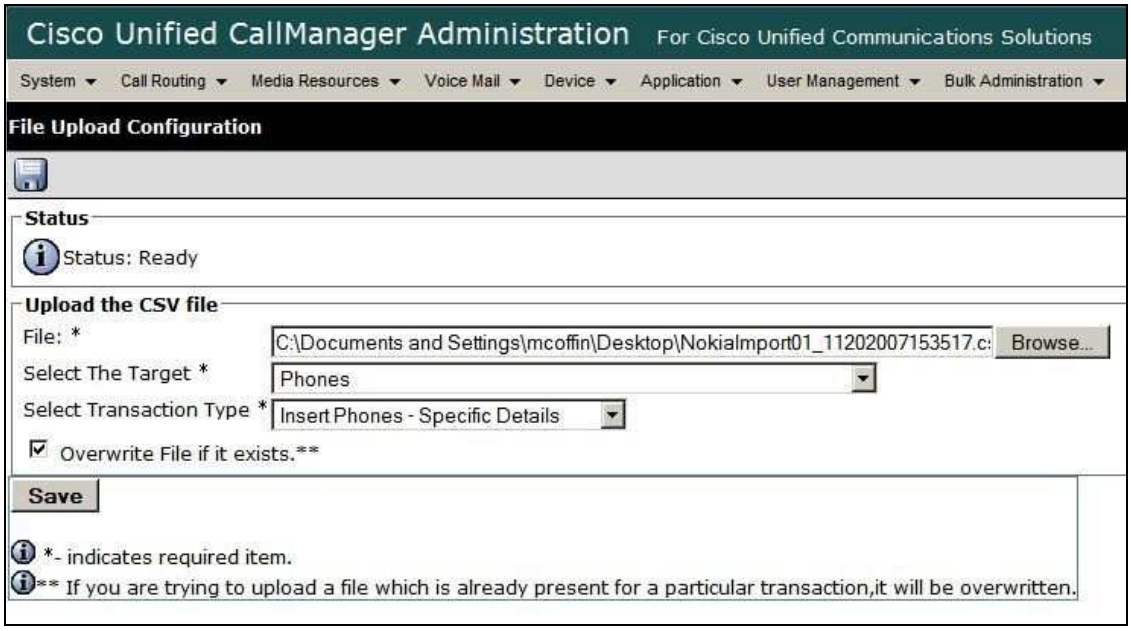
Now that this data has been updated we need to save this as a .csv file and upload it back to CUCM.

Note: When saving the file in Excel change the Save As Type to “CSV (comma delimited) (*.csv)”. If you get an error message indicating the features may not be compatible click on **Yes**.

1.8.2.6. Uploading Data for Re-Insertion

Back in CUCM we need to upload this file. Browse back to **Bulk Administration > Upload/Download Files**. Click on the **Add New** button to upload the file as below.

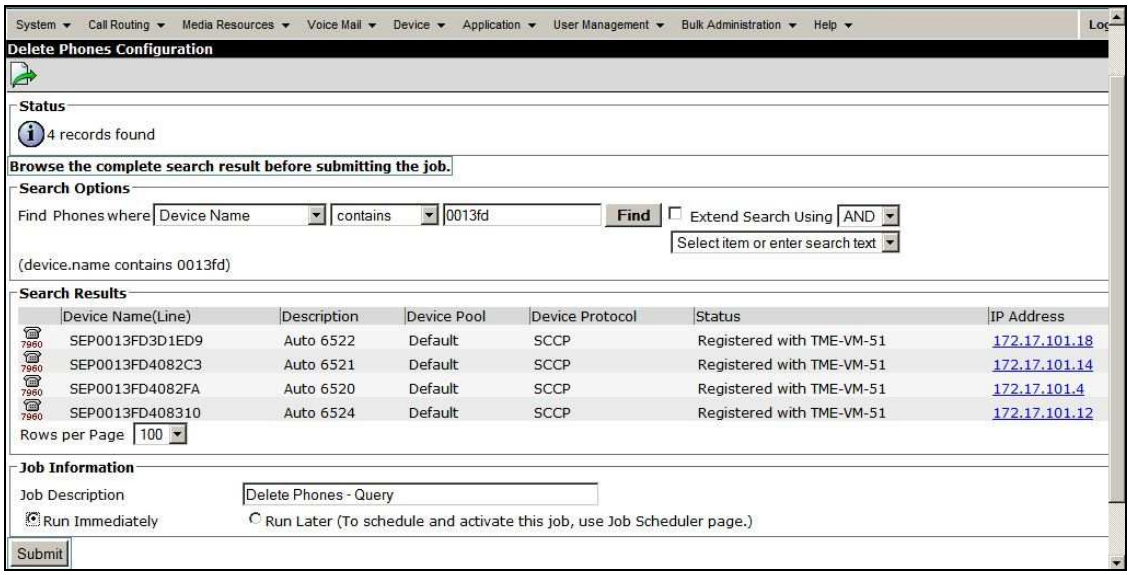
File: (newly created .csv file)
Select The Target: Phones
Select The Transaction Type: Insert Phones – Specific Details



1.8.2.7. Deleting Phones via BAT

Now we can delete the current devices from the database. This can be done two ways. If you have a small number of phones you can simply search for them from **Device > Phones** and delete those that are known to be Nokia’s. If you have a large number you can use BAT.

We will outline the steps needed to use BAT for deleting. First browse to **Bulk Administration > Phones > Delete Phones > Query**. Here we will use the same search criteria as above (base MAC addresses) to search for the Nokia devices.

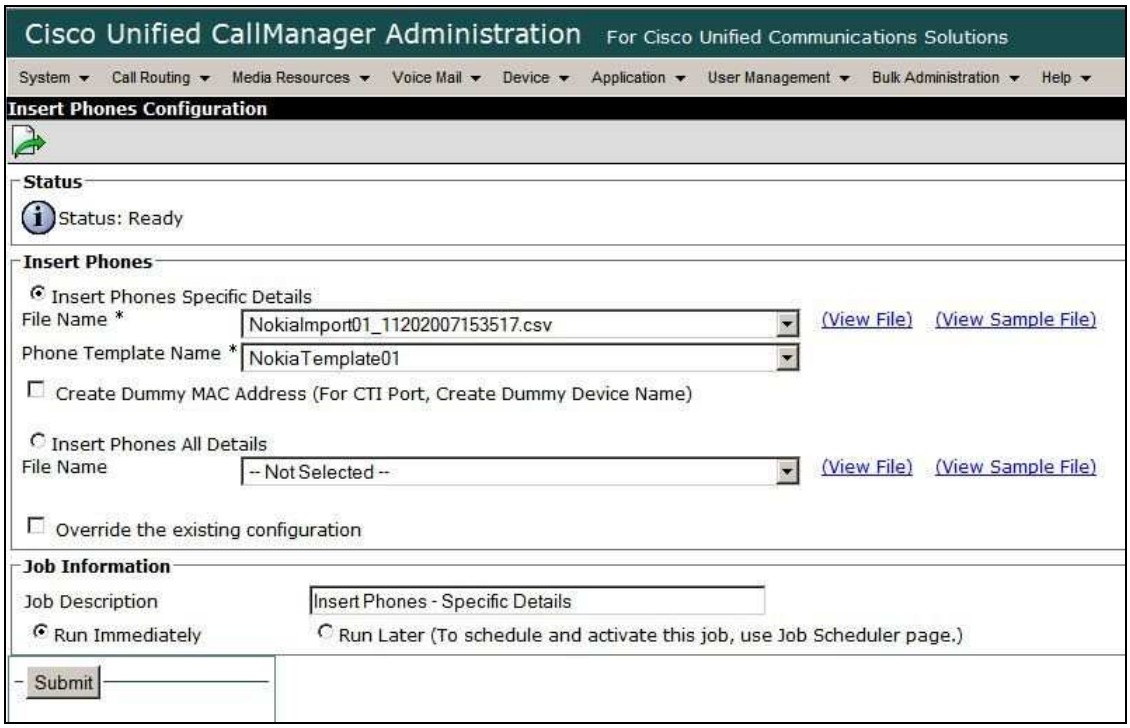


Once the **Submit** button is selected the phones will be deleted.

Note: If auto-registration has not been turned off this is where it should be done. Your Nokia dual-modes should unregister for CUCM at this point.

1.8.2.8. Re-Importing Nokia Device Data

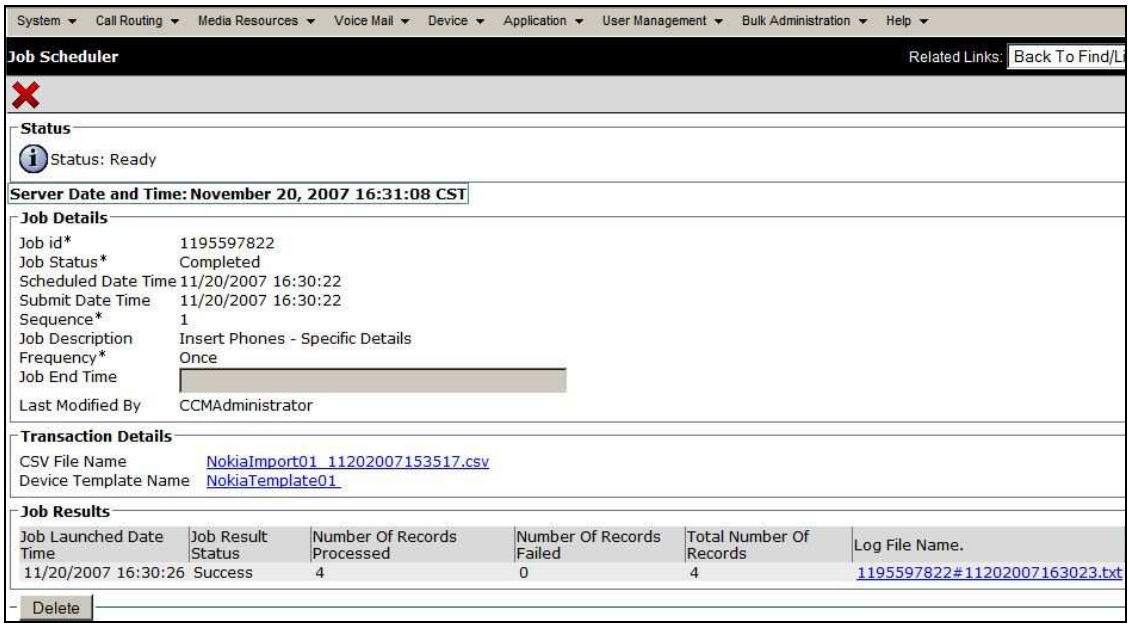
Next we are going to import the phones back into the database. To insert the phones via BAT browse to **Bulk Administration > Phones > Insert Phones.** You should see the .csv file uploaded previously which should be tied to the Phone Template that was created earlier as well.



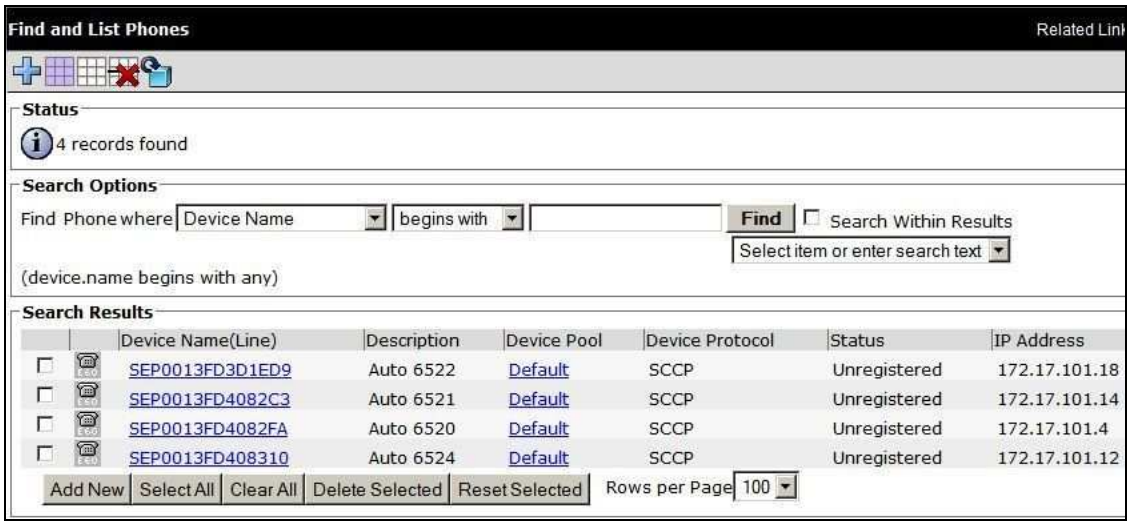
Click on **Submit** to begin the process.

1.8.2.9. Validating Data Insertion

To review the status of the insert browse to **Bulk Administration > Job Scheduler** and find the **Job Id** of the insert. The **Job Result Status** should show **Success**; however, if it does not the Log File can be used to determine the reason for failure.



The final steps are to search for the new Nokia S60 devices and attempt to re-register them to CUCM. Here we have performed a generic search to verify the devices are indeed in the database.



1.8.3. Migrating Steps for CUCM Version 4.x

Phones registered to CUCM version 4.x need to be migrated to the S60 device type as well; however, the process is different due to differences in the administration interface and BAT capabilities.

1.8.3.1. CUCM Version 4.x Overview

Essentially the process is very similar as CUCM 6.x, but we have provided a step-by-step example to help administrators. Again, this can be done on a phone-by-phone basis, but BAT can be used to help speed the migration process.

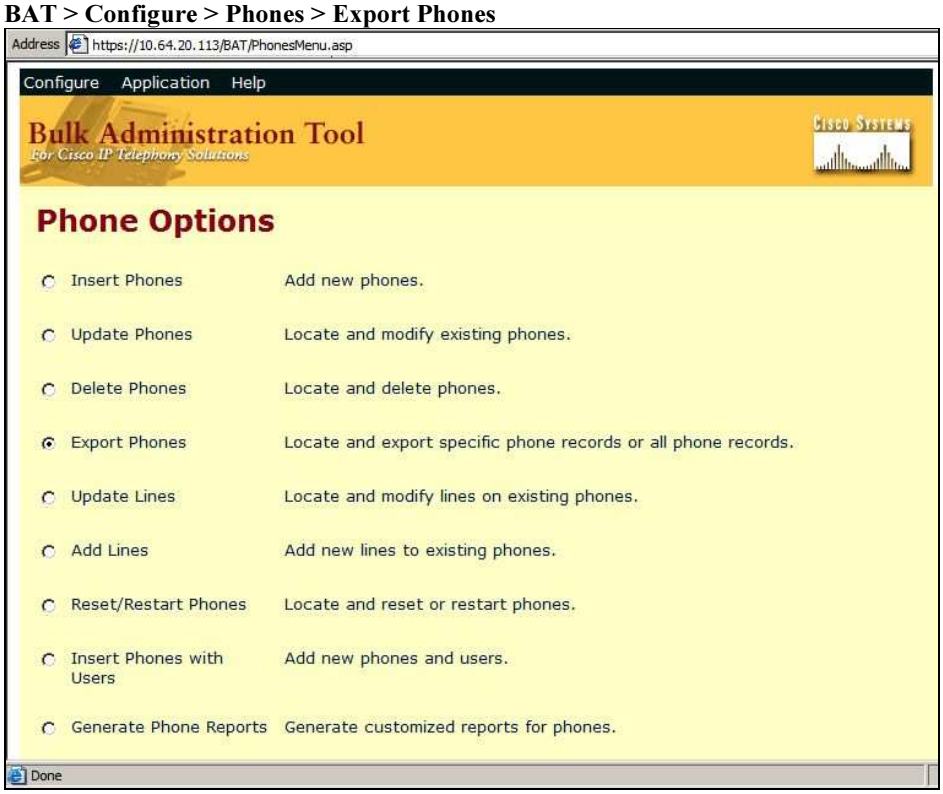
In our example we have 8 Nokia ESeries devices registered to CUCM, 2 E60's and 6 E61's, all registered using the 7960 device type. To make the upgrade to 1.1 successful, we need to migrate these phones to the S60 device type.

1.8.3.2. Creating CUCM 4.x Phone File Format

In 5.x and higher CUCM allows users to customize the exported data via phone file formats. However, in 4.x and lower versions this was not the case. The only two options are All Phone Details and Default Phone. All Phone Details can only be used when migrating all devices of a single type. For example, if I wanted to export all info on 7971's, this could be done and re-imported later without having to modify the fields. However, in this case we are changing device types so this cannot be done directly.

Instead we are going to export the data we can using Default Phone to populate the .csv file, and manually add the additional info needed to complete the insertion. To export the data browse to **Configure > Phones > Export Phones** and click **Next**.

BAT > Configure > Phones > Export Phones



1.8.3.3. Exporting Current Phone Data

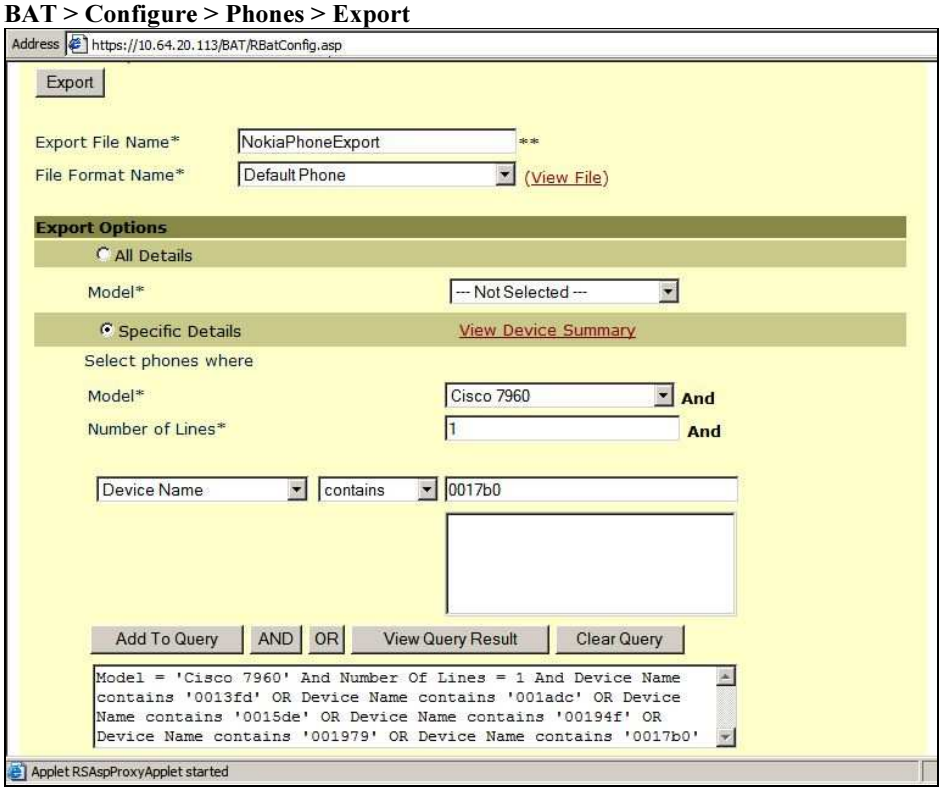
To export all the phones we will search for all 7960's containing base MAC addresses. These base addresses are the following:

E51	001adc
E60	0015de
E61	0013fd
E61i	00194f
E65	001979
E70	0017b0

Below is the output from our query (exported files are sent to c:\BatFiles\Export\Phones):

1,0013FD3D1ED9,Auto 5041,,,5041,,,,,,,,
1,0013FD3DD608,Auto 5038,,,5038,,,,,,,,
1,0013FD4082C3,Auto 5040,,,5040,,,,,,,,
1,0013FD4082D0,Auto 5039,,,5039,,,,,,,,
1,0013FD4082FA,Auto 5037,,,5037,,,,,,,,
1,0013FD408310,Auto 5036,,,5036,,,,,,,,
1,0015DE3D10E4,Auto 5034,,,5034,,,,,,,,
1,0015DE3F58CE,Auto 5035,,,5035,,,,,,,,

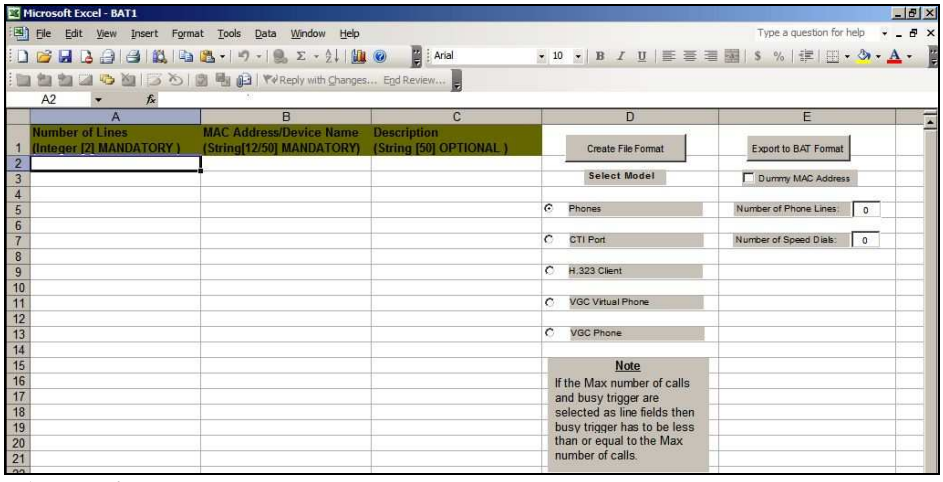
BAT > Configure > Phones > Export



The structure of the query can be seen in the picture above. Be sure to use "OR" rather than "AND" while building the query or you may not get the results desired. Use the View Query Result button to verify the structure of your statement, and then click on the Export button. This file is saved in the C:\BatFiles\Export\Phones folder.

1.8.3.4. Creating S60 Phone Template

Now that we have this data we are going to create a new S60 device template. To create this template retrieve the BAT.xlt file from the server, located at c:\CiscoWebs\BAT\ExcelTemplate\BAT.xlt. Once downloaded, run the file by double-clicking on it.



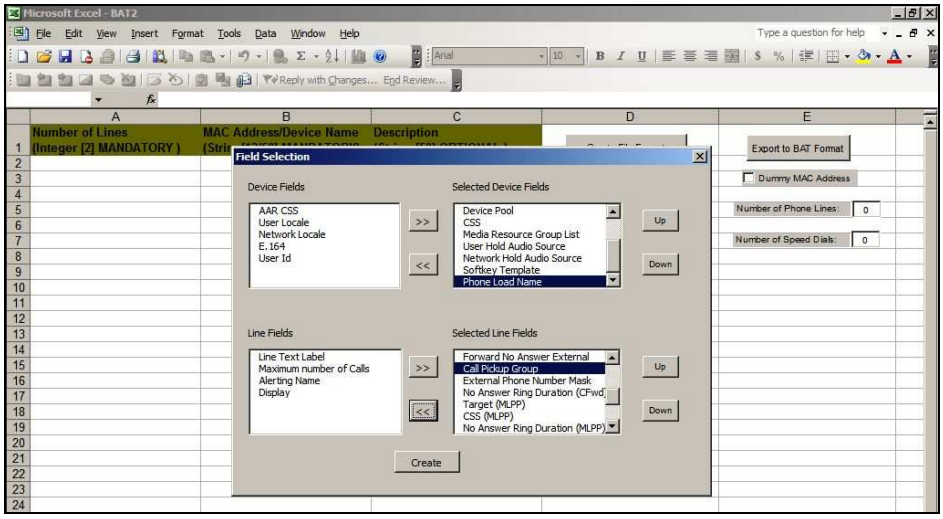
BAT.xlt File

Next we are going to click on the Create File Format button to customize our file. Notice that we have added most fields; however, there are some listed at the device level that have been removed:

At the Device level:
AAR CSS
E.164
Phone Load Name
Network Locale
User Locale

At the Line level:
Display
Alerting Name
Maximum number of calls
Line Text Label

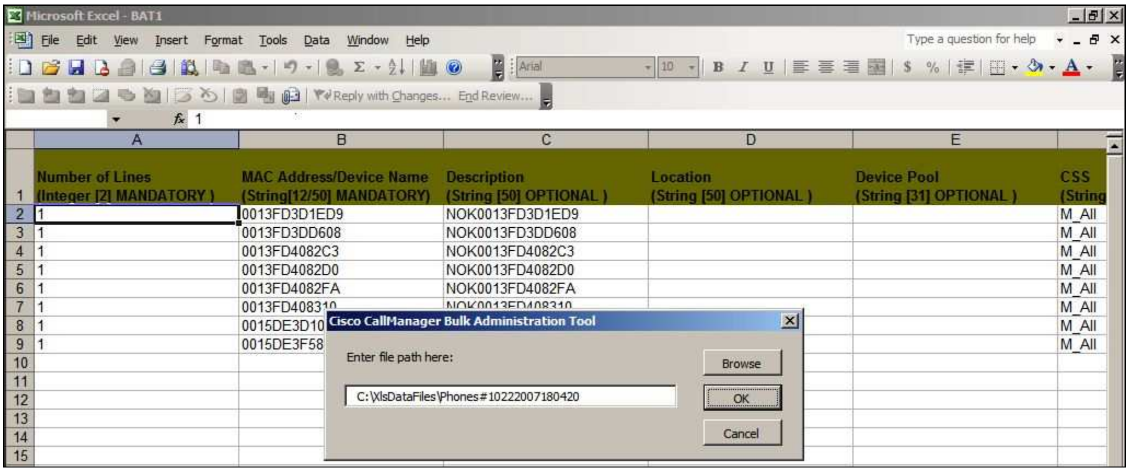
Note: Be sure that the BAT.xlt file and the Phone File created later are done in the same fashion.



Press the Create File Format button and press Yes to overwrite. Unfortunately, at this point the process becomes manual. We must copy out the info from the text file into the following fields created:

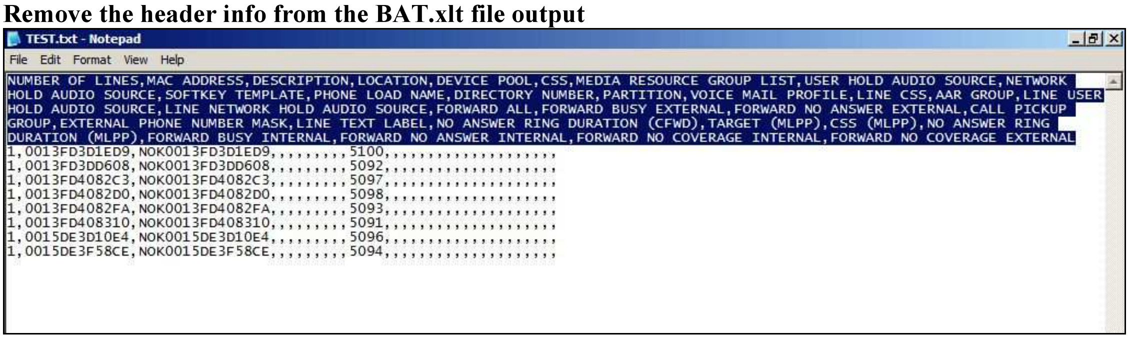
Number of Lines
MAC Address/Device Name
Description
Directory Number

After populating the fields click on the Export to BAT Format button. If the data has been entered correctly you will be asked where to save the file.



The file that is created contains the format needed for inserting into the database, however, we need to remove the column headings that are inserted. Open up the file and remove all data above the phone information, as shown below.

Remove the header info from the BAT.xlt file output

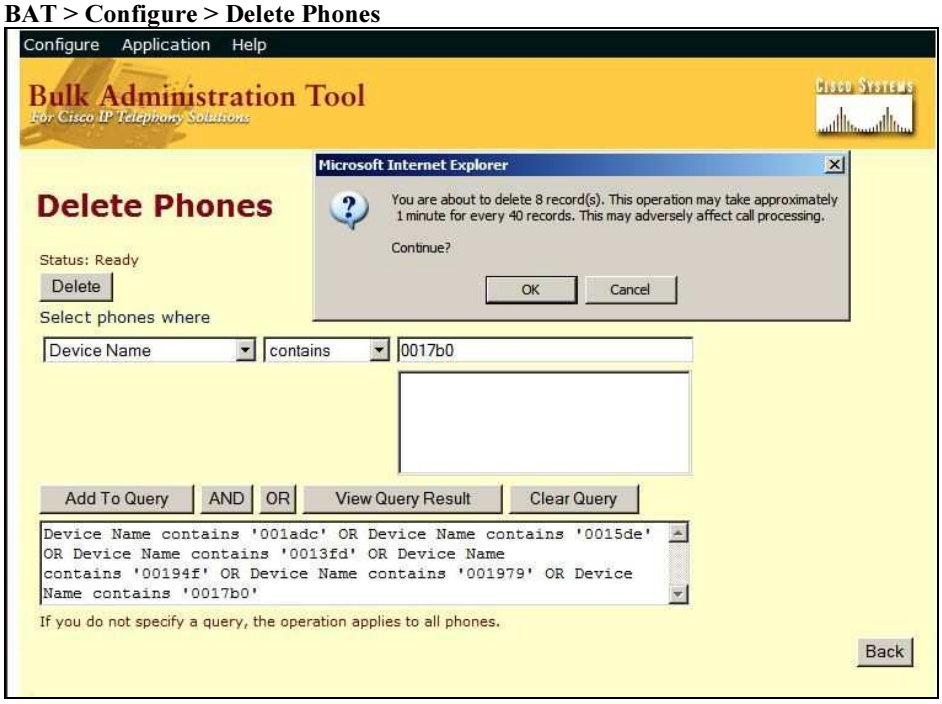


This file should be uploaded to the C:\BatFiles\Phones\Insert folder on the CUCM server. At this point we can delete the phones from the database.

1.8.3.5. Deleting Devices via BAT

Deleting the phones can be done via BAT as well. Browse to **Configure > Delete Phones** from the BAT administration screen. We will be searching the database for only those devices falling within Nokia's MAC address ranges using the same query as above.

BAT > Configure > Delete Phones



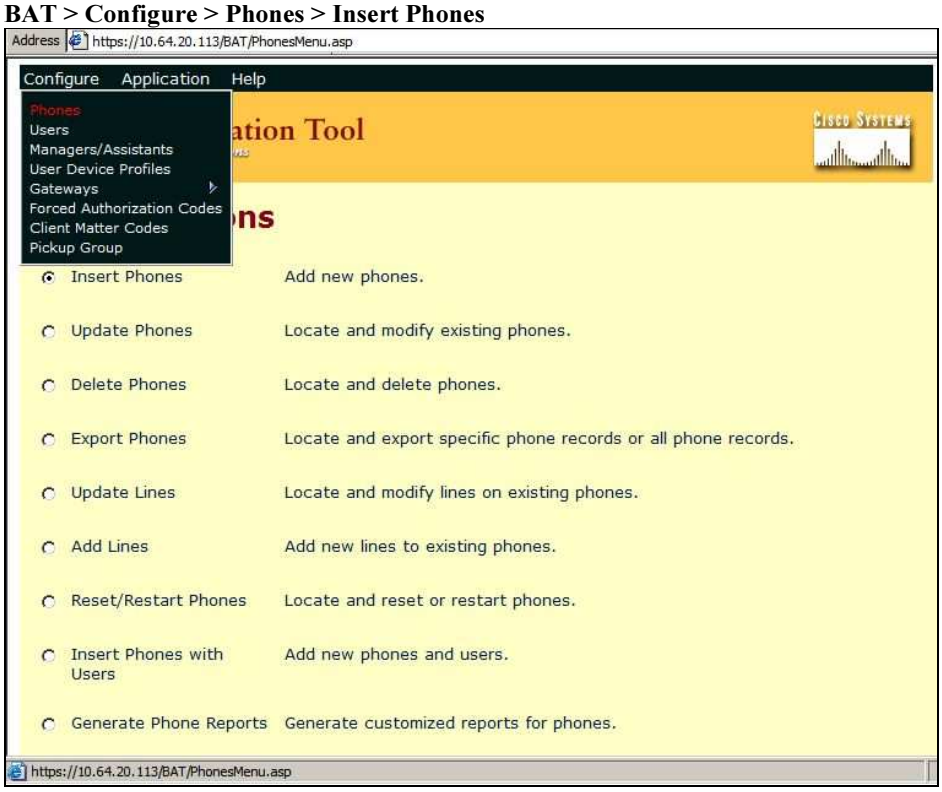
All Nokia's registered as 7960's should now be deleted from the database. If you do not have Auto-registration disabled they may being to re-register, which will cause the BAT insert to fail and require the steps above to be run again.

Note: It is recommended that you turn OFF auto-registration during this process. If auto-registration is not turned off your Nokia devices may re-register before the migration is complete.

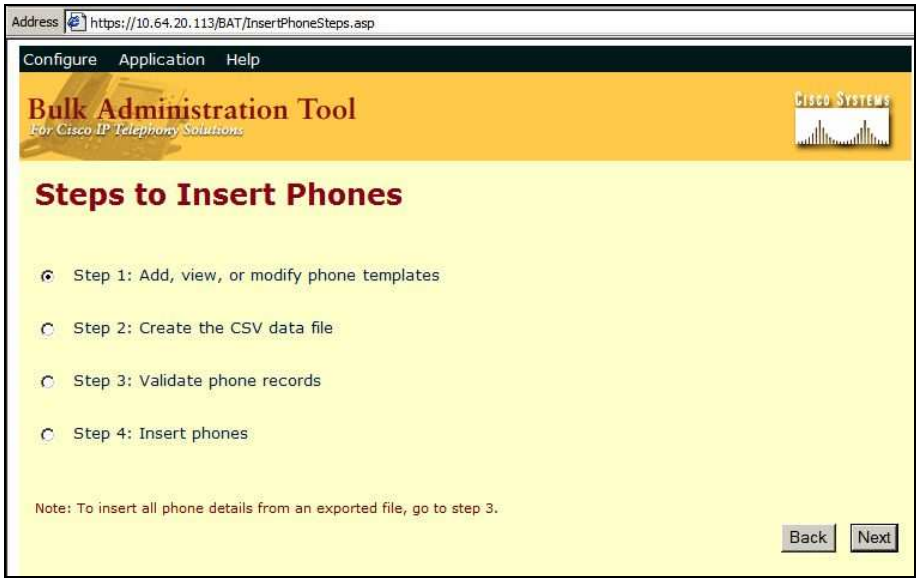
1.8.3.6. Inserting Phones via BAT

Now we can begin to add the phones back to the database. As before, our first step is to launch BAT and create the phone Template.

BAT > Configure > Phones > Insert Phones

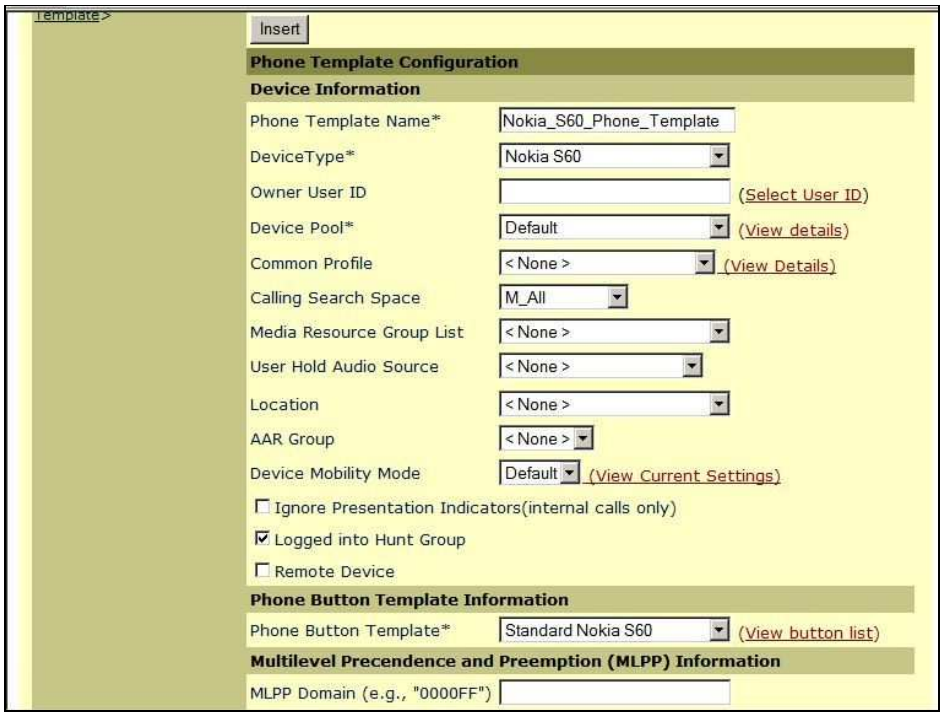


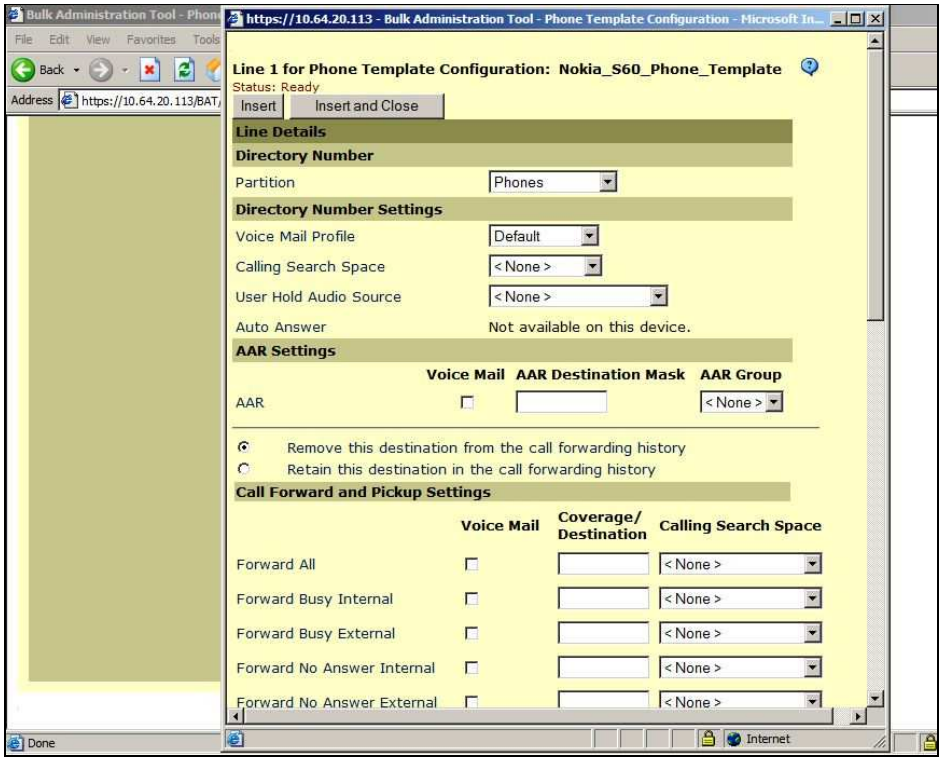
Select Insert Phones to begin the process. Notice that the process is broken down into 4 basic steps and that the application will step you through the process.



1.8.3.7. Creating S60 Phone Template

To begin creating the phone template for the S60's click on Step 1 and press Next. Here we will configure both the template for the device and the lines. Be sure to configure the Line info as well.



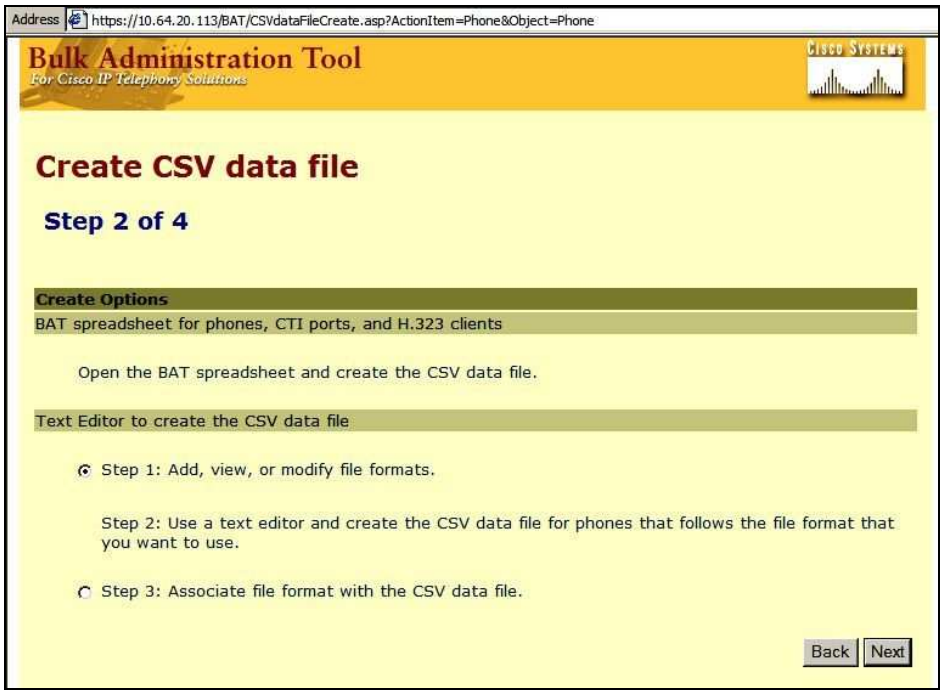


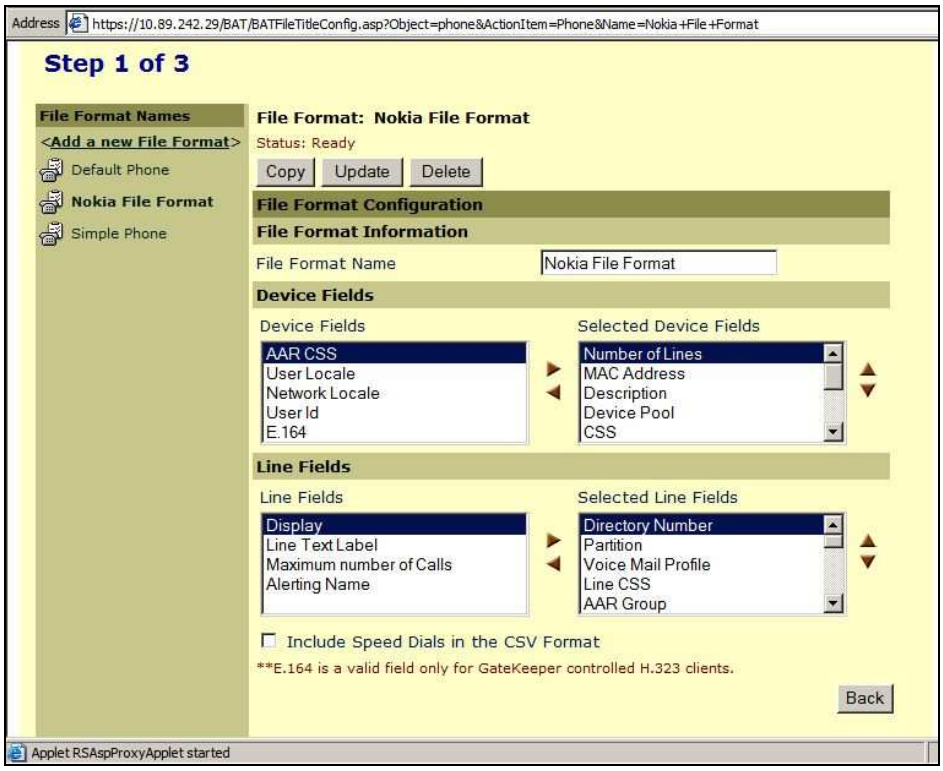
Click Back and move to Step 2. Notice that the first part of the step is to create the CSV data file. This is the file created by the BAT.xlt file, which should have been copied to the C:\BatFiles\Phones\Import directory earlier.

Note: Always use the BACK button provided on the web page, not your browsers.

1.8.3.8. Creating the Phone File Format

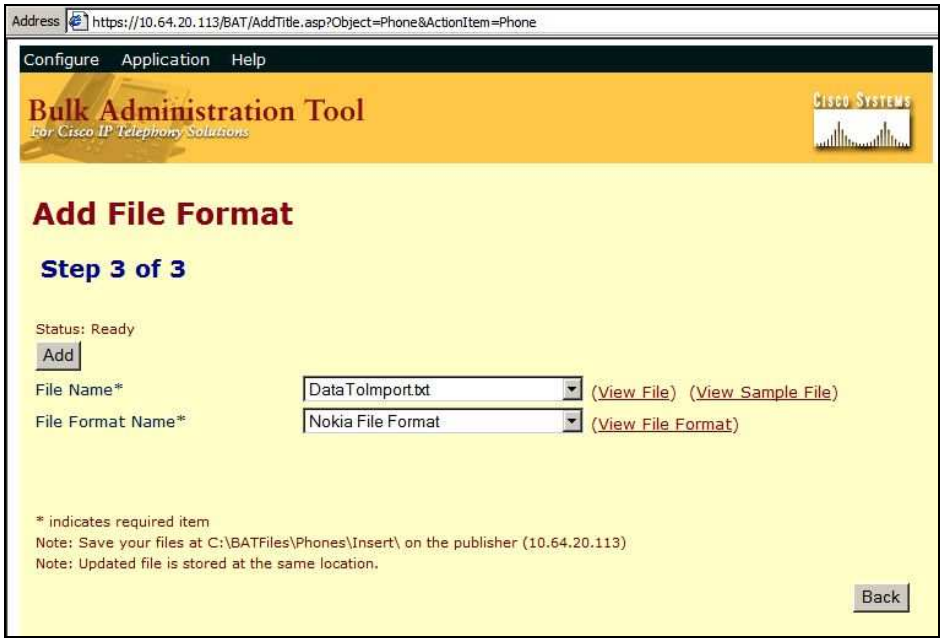
The next step is where we create the File Format. In this step we create a Nokia File Format to add the appropriate fields for that device.





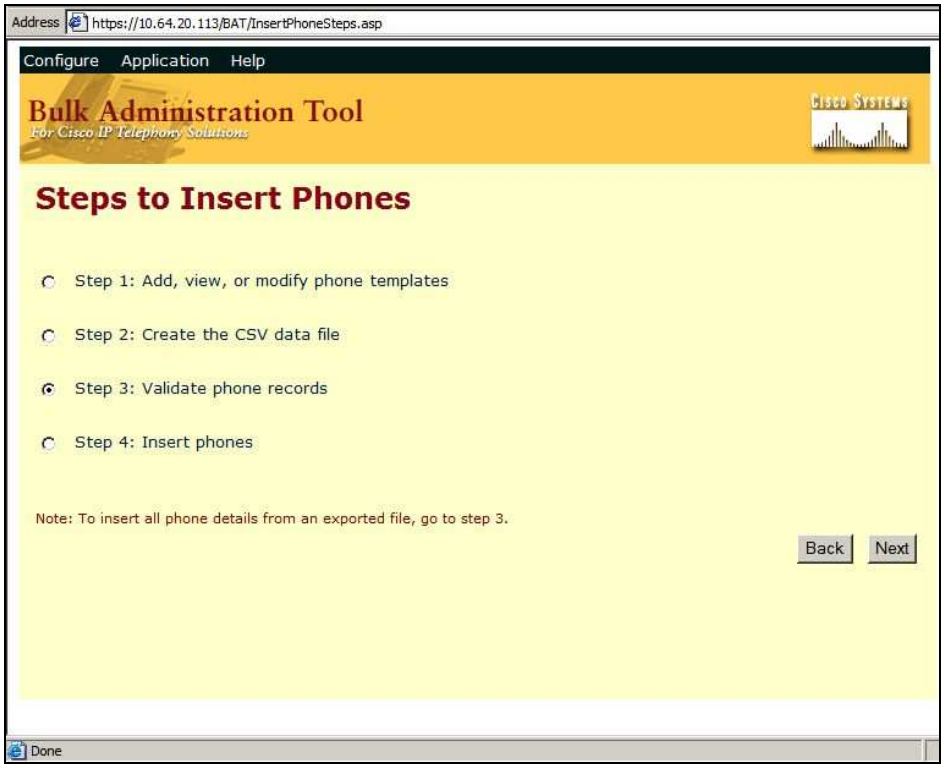
This file should be created with the same options as the BAT.xlt file created earlier, with certain device and line level fields removed. This creates the headers for the data we will be associating in the next step.

Press Back and move to Step 3of the Create CSV data file page. Here we are going to associate the data that was copied from the BAT.xlt program with the phone file that was just created.

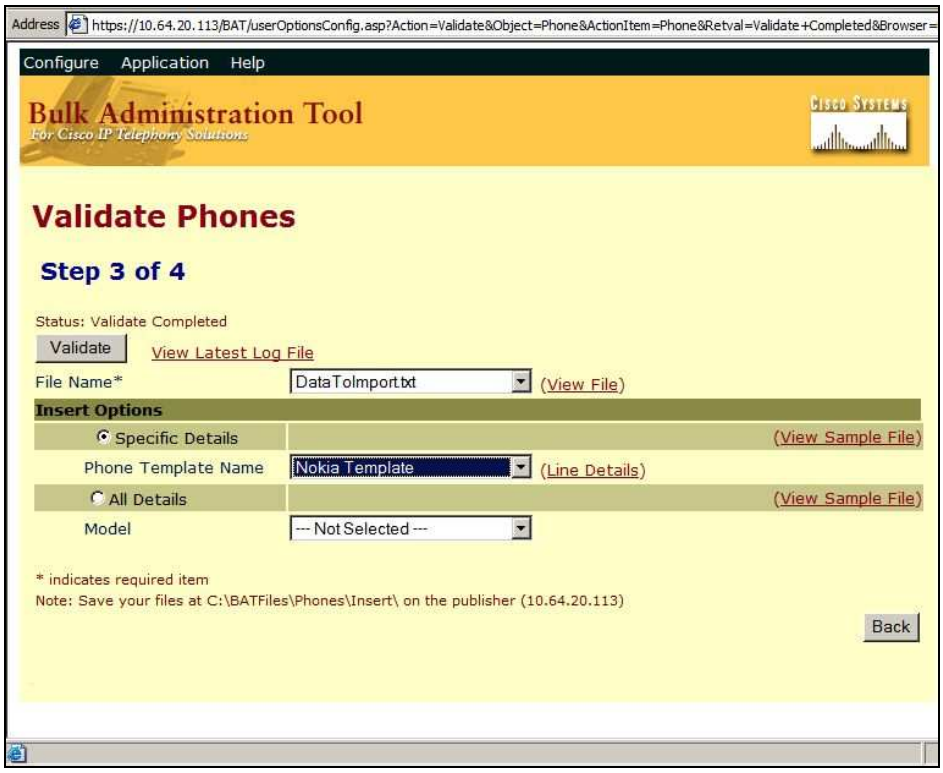


1.8.3.9. Validating the BAT Data

Click the **Add** button to update the data file with the headers. After is done successfully click Back and move to the Validation step.



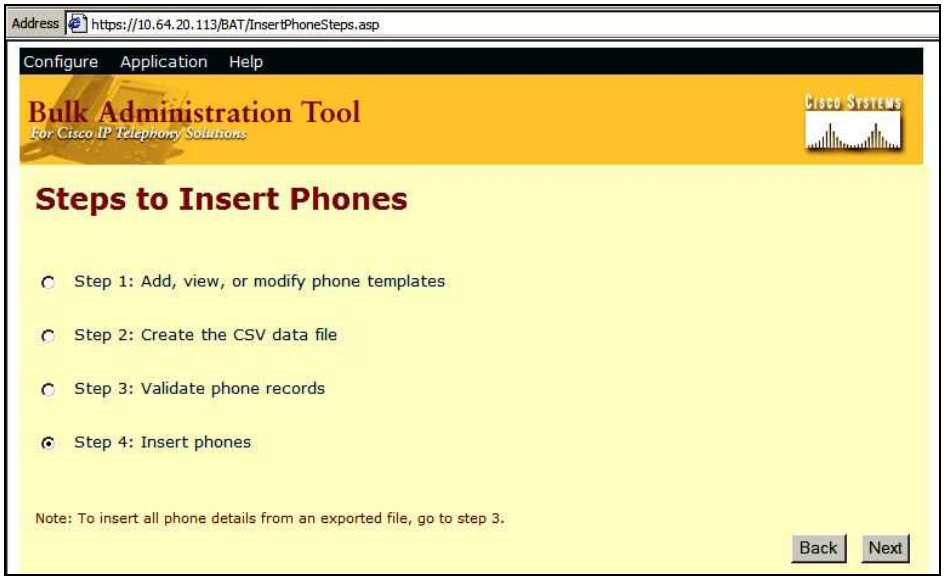
This will validate that the data in the file is correct for the header type. For example, if you have an entry in the Partition field that is not present in the database, the validation will fail.



Notice that after clicking on the Validate button the status has changed to "Validate Completed" and a log file is available to view. If validation fails this log file can be useful for troubleshooting.

1.8.3.10. Inserting and Verifying Phones

Next we move to Step 4 of the process, inserting the phones. Click the Back button from the Validation screen to move to this step.



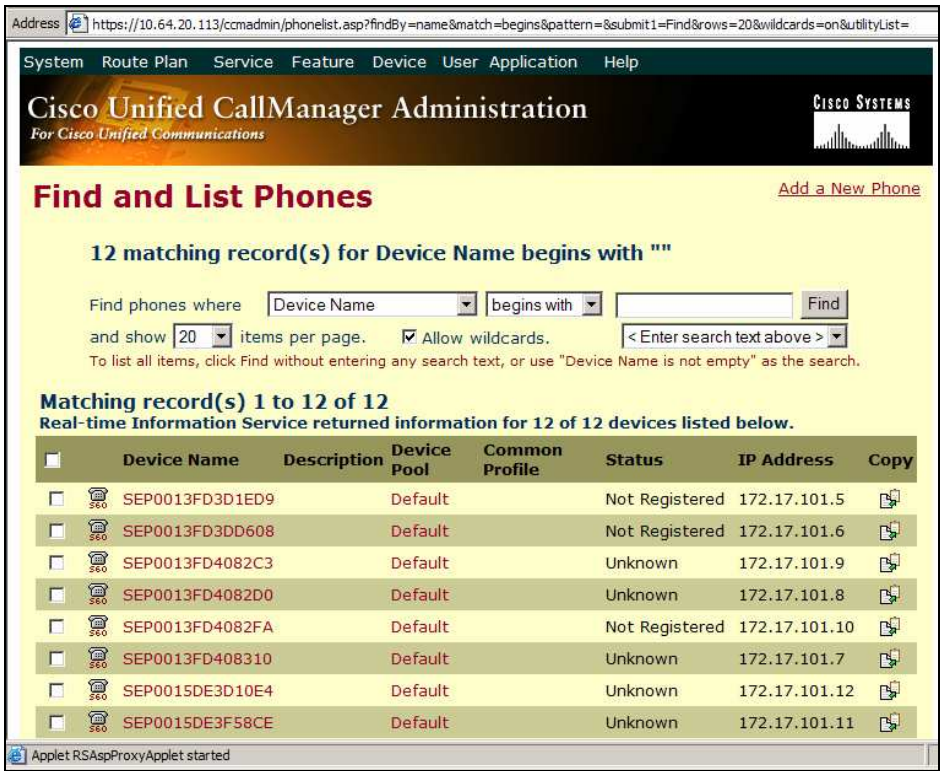
Inserting the phones works in much the same way as validating them except that this time the database will be populated once finished.

Note: If you have large numbers of devices to insert you may want to schedule time after peak hours to perform the operation.

Choose the same file and template as before and click Insert to being the process.

After completing you should get a message indicating that the insert was successful. If you got an error message, a log file will be created for review.

Now that the phones have been reinserted we can go to the CUCM administration screen and search for our phones. You should see them show up correctly as “S60” devices.



1.9. Further Reading

To review configuring QoS on Cisco access points refer to the links below:

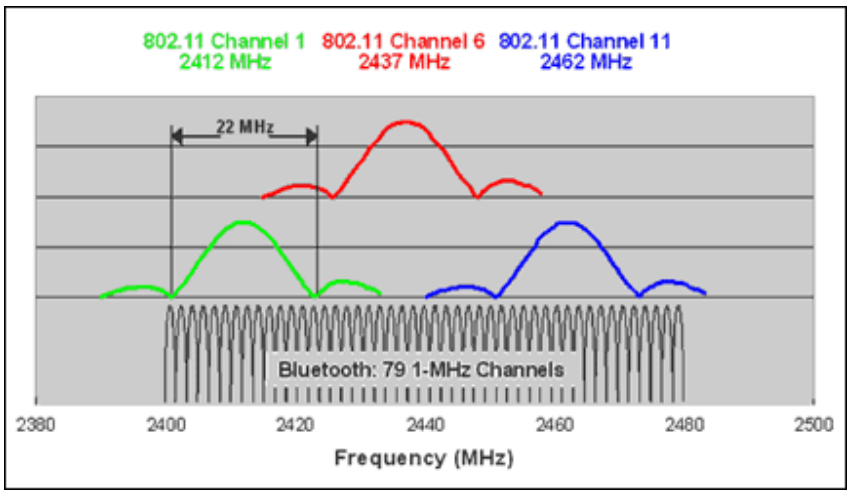
For controller based configurations see:
http://www.cisco.com/en/US/partner/products/ps6366/products_configuration_guide_chapter09186a008052d9e9.html

For IOS based access points see:
http://www.cisco.com/en/US/partner/products/hw/wireless/ps430/products_configuration_guide_chapter09186a0080606d2f.html

For further reading on WMM see the Wi-Fi Alliance white paper here:
http://www.wi-fi.org/files/uploaded_files/wp_1_WMM%20QoS%20In%20Wi-Fi_9-1-04.pdf

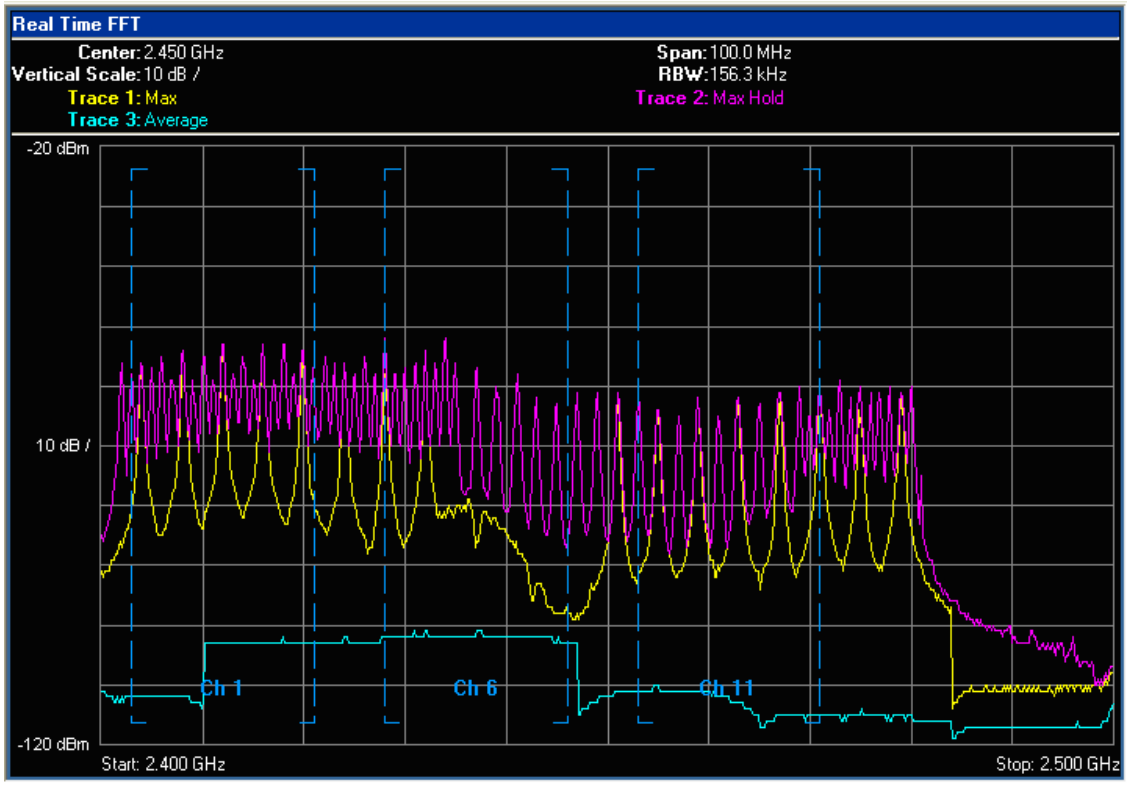
To review Cisco's Cisco Compatible Extensions (CCX) program see the link below:
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html

1.10. Appendix: A



This shows that Bluetooth and 802.11b/g shares the same frequency band.

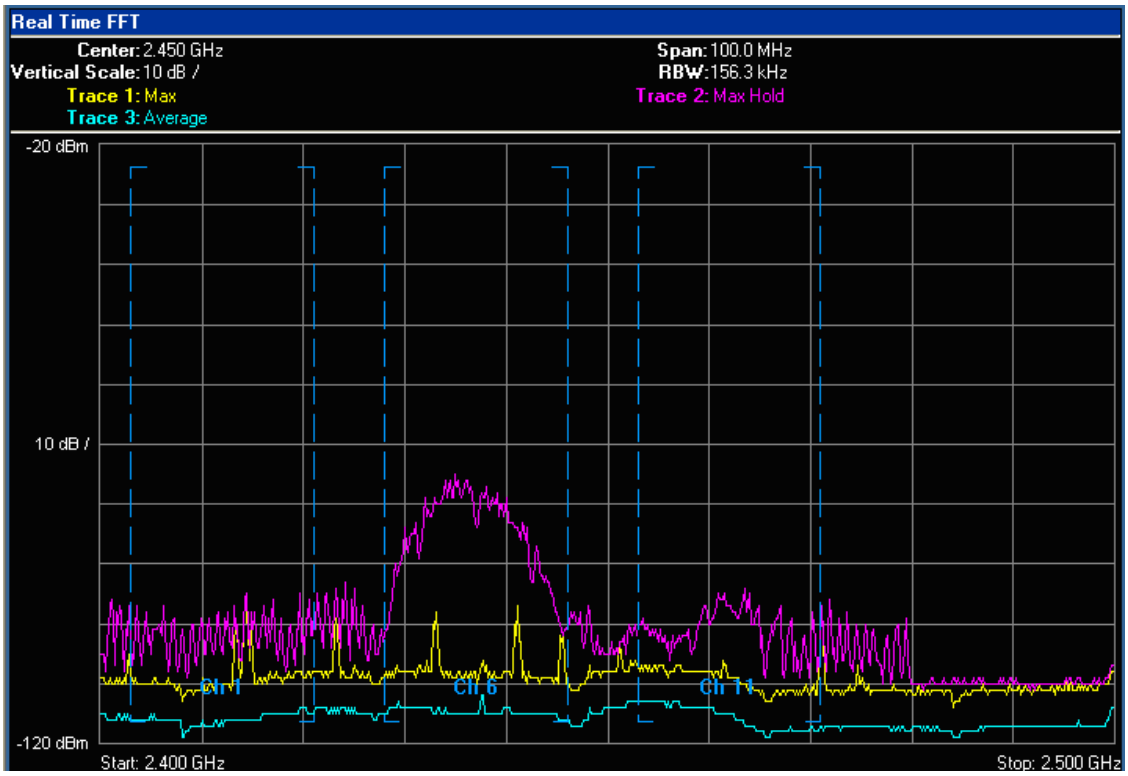
Bluetooth (BT) signal pattern in the 802.11b/g 2.4GHz spectrum of a typical BT earpiece.



Bluetooth (BT) signal pattern in the 802.11b/g 2.4GHz spectrum of a typical BT earpiece.

The PINK is the Max Hold line or the line that shows the maximum transmit power that was reached during the test. The YELLOW shows the maximum transmit power in the last sample period of ten seconds. The TURQUOIS shows the average transmit power over the period of the test. The vertical dashed lines separate the 3 non-overlapping 802.11b/g channels Ch1, Ch6, and Ch11. The charting is from 2.400GHz on the left to 2.500GHz on the right. From the right edge of the Ch11 vertical blue line is part of the 802.11 spectrum used in Europe and Japan. This capture was done with an access point and clients configured for the North American regulator domain. This graph shows that the Bluetooth earpiece was easily transmitting outside of FCC regulations.

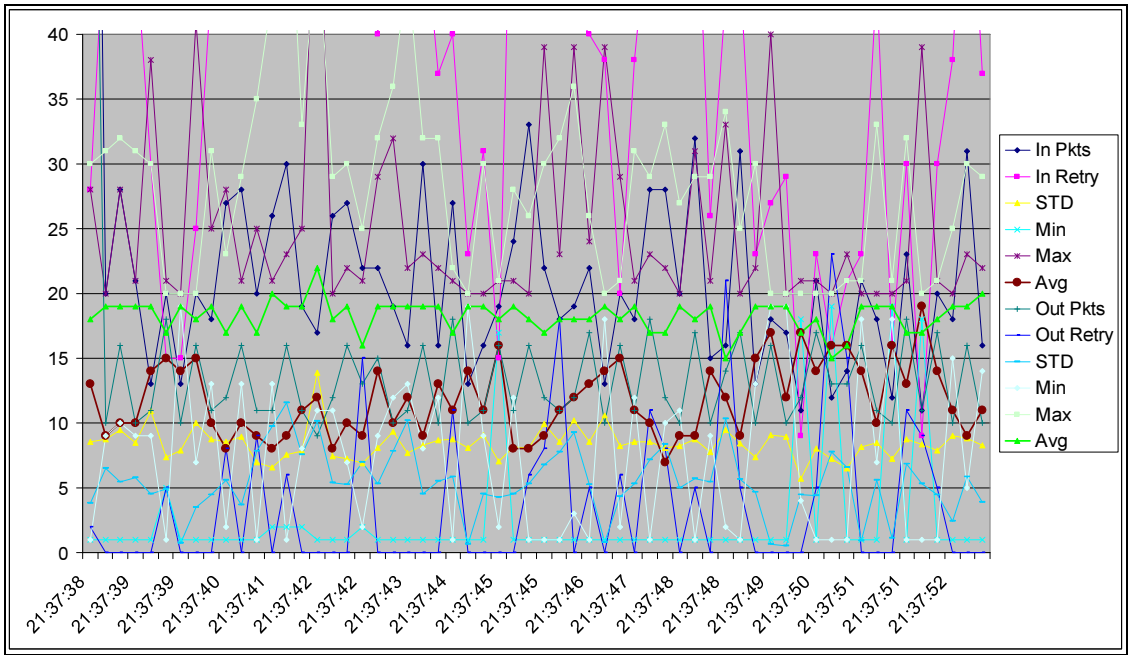
Notice that the BT signal is very narrow. BT transmits data on a single MHz of frequency. Stops the transmission, then moves to another frequency in the 802.11 2.4GHz band then transmits data. This is continual repeated. The 802.11b and 802.11g signals are sent of a combined 22MHz of frequency. The radio stays on that 22MHz of frequency. That grouping of 22MHz is the referred to as the channel. The Max Hold line shows how strong the BT while in search mode. The signal level is above that of a 50mW (17dBm) OFDM 802.11g radio. A signal of this strength and duration will cause the Nokia phone to drop VoWLAN call.



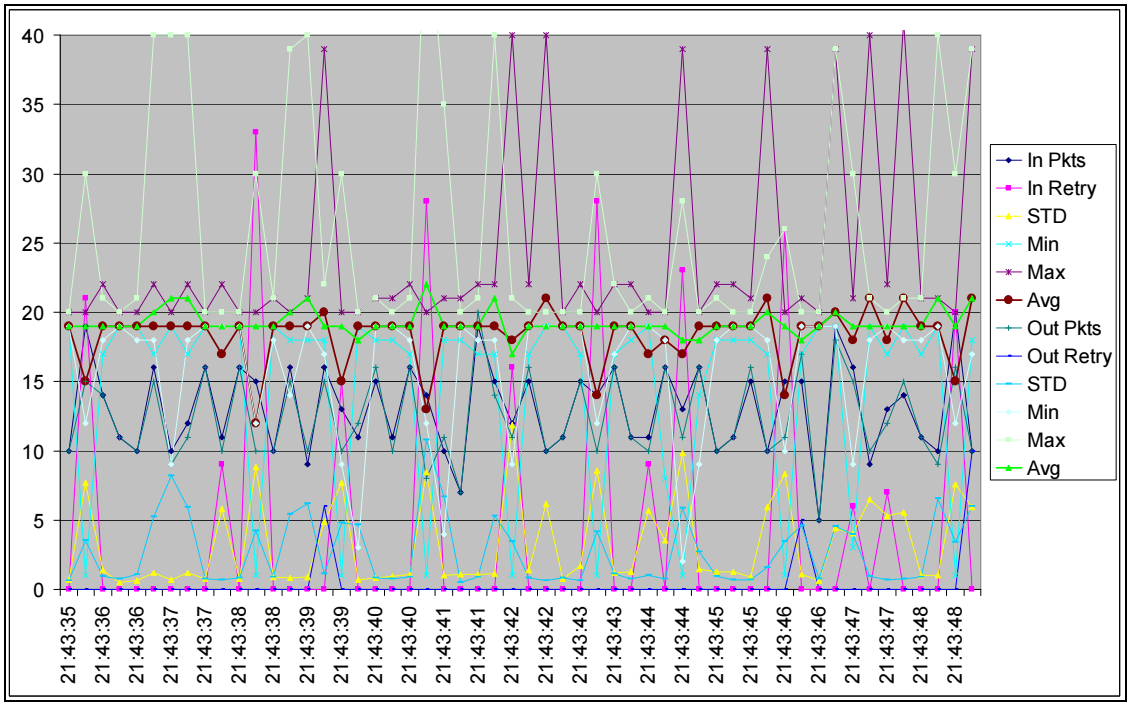
This chart shows an active call on channel 6 with a connected BT earpiece.

Notice the dome shaped Max Hold line in the center of the chart. That is the typical spectrum representation of the 802.11b or 802.11g signal with the signal strongest right in the middle of the 22MHz of frequencies that make up channel 6. BT is sharp pointed signals shown in the channel 1 and channel 11 area of the spectrum. The earpiece has connected to the phone and is not in the high transmit power mode that it was in while searching for the phone. At this time because the call was dropped when the earpiece was in search mode a new call was started. The call had poor voice quality. The yellow line in side of the dome is the BT radio transmitting during the call on channel 6. The chart was captured at the split second that BT was transmitting instead of the phone or access point transmitting.

1.11. Appendix: B

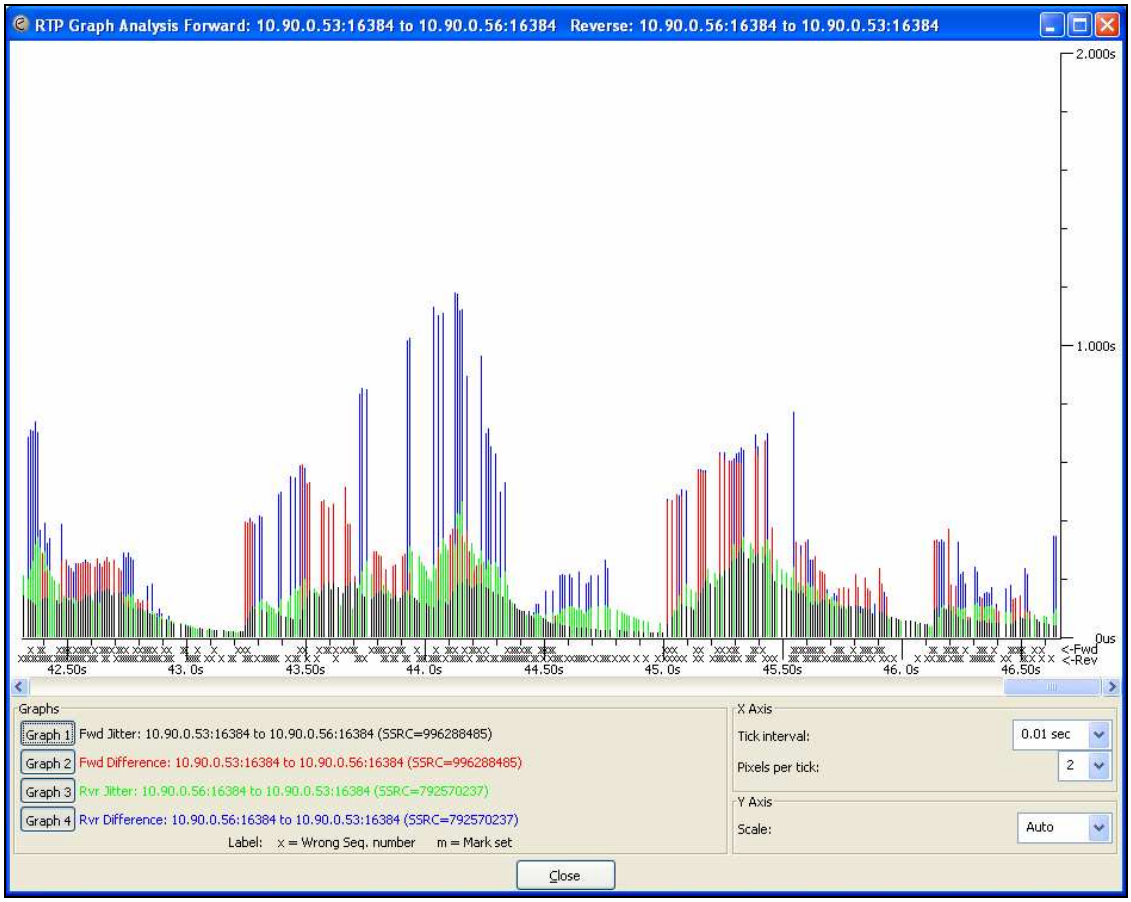


Same call with BT earpiece.



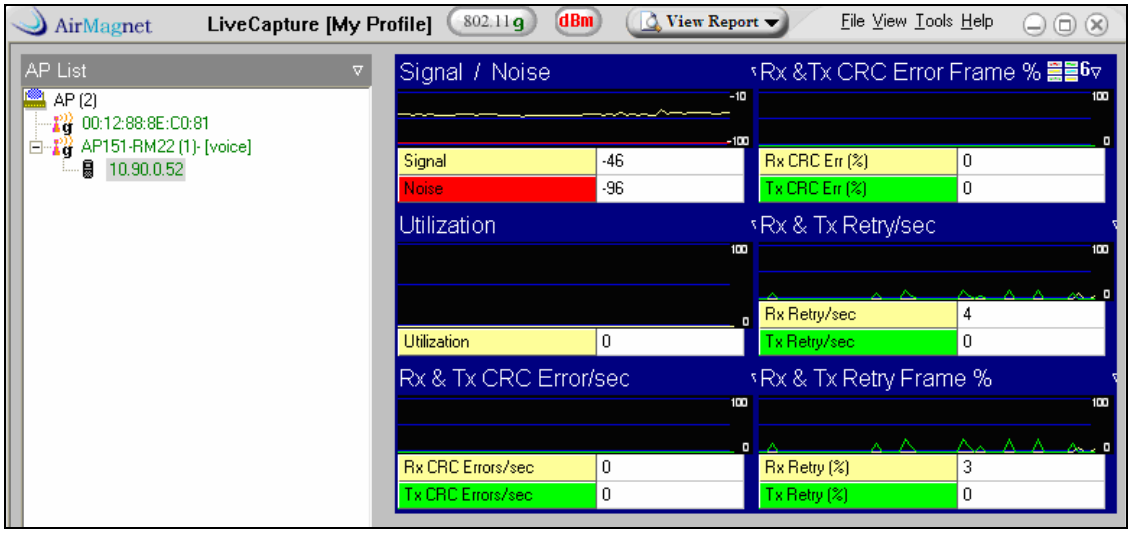
Same call without BT earpiece.

The ‘In Pkts Avg’ line and the ‘Out Pkts Avg’ lines are very close to each other.

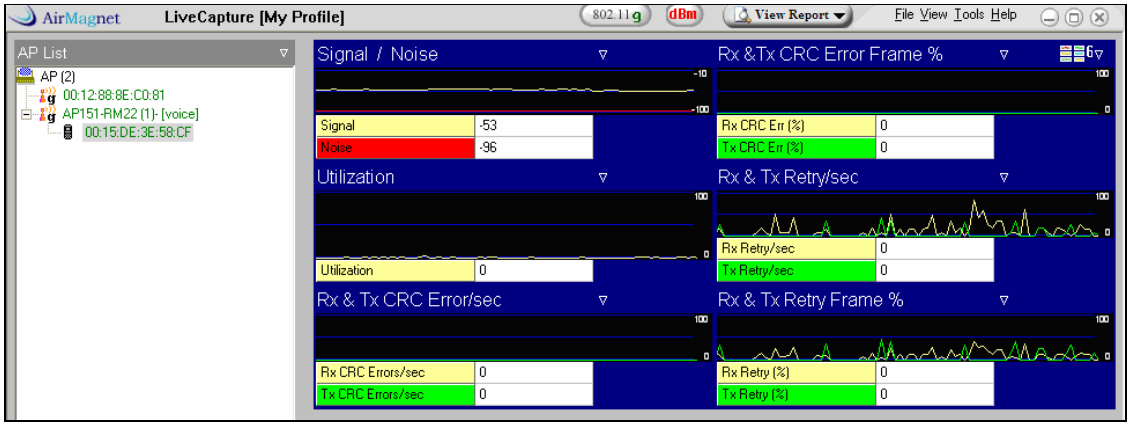


This is an Ethereal jitter analysis of three simultaneous phone calls each using a BT earpiece. All 3 calls were on the same AP and were calls to other Nokia phones on this access point.

1.12. Appendix: C.



The signal level is -46dBm when the antenna of the phone is not obstructed.



With the hand over the antenna the signal strength was lowered to -53dBm.

The signal level shown in this testing is very high. The AirMagnet capture tool was only 3 feet away from the Nokia phone. This shows that a significant difference in signal strength can be caused by hand and head position relative to position of the phone. Also note that this test was done in a low multipath environment. Multipath can also create a 4 to 6 dB swing in signal strength in a distance as little as one foot.

This series of tests was performed on the Eseries models with similar results for all.

1.13. Appendix: D.

AP and Antenna Placement

This section gives examples of both proper and improper placement of access points (APs) and antennas.

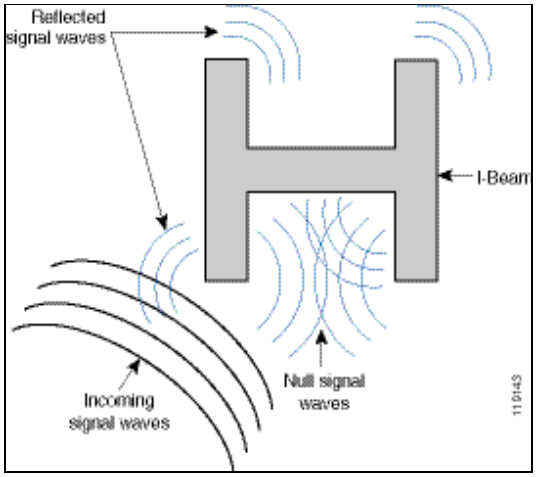
Improper AP and Antenna Placement

Figure D-1 shows improper placement of an AP and antennas close to an I-beam, which creates distorted signal patterns. An RF null point is created by the crossing of signal waves, and multipath distortion is created when signal waves are reflected. This placement results in very little coverage behind the AP and reduced signal quality in front of the AP.

Figure D-1 Improper Placement of Antennas Near an I-Beam

Figure D-2 shows the signal propagation changes or distortions caused by an I-beam. The I-beam creates many reflections from both received packets and transmitted packets. The reflected signals result in very poor signal quality because of null points and multipath interference. However, the signal strength is high because the AP antennas are so close to the I-beam.

Figure D- 2 Signal Distortions Caused by Placing the Antennas Too Close to an I-Beam

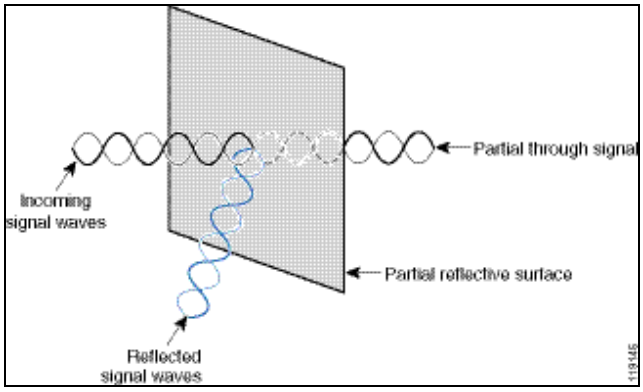


The AP and antenna placement in Figure D-3 is better because it is away from the I-beams and there are fewer reflected signals, fewer null points, and less multipath interference. This placement is still not perfect because the Ethernet cable should not be coiled up so close to the antenna.

Figure D-3 AP and Antennas Mounted on a Wall, Away from I-Beams

Figure D-4 shows the signal propagation caused by the wall on which the AP is mounted.

Figure D-4 Signal Reflection Caused by a Wall



The preceding examples also apply when placing APs and antennas in or near the ceiling in a standard enterprise environment. If there are metal air ducts, elevator shafts, or other physical barriers that can cause signal reflection or multipath interference, Cisco highly recommends that you move the antennas away from those barriers. In the case of the elevator, moving the antenna a few feet away will help eliminate the signal reflection and distortion. The same is true with air ducts in the ceiling.

Conclusion

A survey conducted without sending and receiving packets is not sufficient. The I-beam example shows the creation of null points that can result from packets that have CRC errors. Voice packets with CRC errors will be missed packets that adversely affect voice quality. In this example, those packets could be above the noise floor measured by a survey tool. Therefore, it is very important that the site survey not only measures signal levels but also generates packets and then reports packet errors.

1.14. Appendix F: Configuring the Nokia E-Series for EAP-PEAP

This is an example of the basic steps needed to configure the Nokia E-Series with the CA Certificate provided and configure the appropriate settings for the access-point using EAP-PEAP authentication.

1.14.1. Converting the CA certificate

Some certificates may need a binary conversion before they will be accepted by the Nokia phones. If your certificate does not work see the steps below.

1. The CA certificate is the root certificate installed on the ACS server. This certificate is needed by the Nokia for their PEAP implementation. To convert the certificate **open the certificate by double-clicking on it**.
2. Select the **Details** tab.
3. Find the **Copy to File** button and select it.
4. Click the **Next** button to begin.
5. Ensure that **DER encoded binary X.509** is selected.
6. Press the **Next** button.
7. Name the file and press **Next**.
8. Click the **Finish** button.
9. You should get a message that the export was successful.

1.14.2. Installing the certificate on the Nokia E-Series

Once you have a properly formatted certificate it needs to be installed on the Nokia phone. There are several methods of accomplishing this, but one of the easiest is using the Infrared (IR) port. The IR port on the Nokia is at the bottom of the phone and it should be aligned with the IR port on your laptop.

Turning on the IR port of the Nokia

1. Press the **Menu** button.
2. Find the icon labeled **Connect** and select it.
3. Select the **Infrared** icon and select it. You should get a message that the port is activated.
4. Position the IR port of the Nokia (at the bottom of the phone) in front of your laptop IR port.

Transferring files to the Nokia

Once you have the Nokia aligned in front of your IR port you should see an icon that will allow you to transfer files. You need to find the certificate from above and send it to the Nokia. The file will be sent to the Inbox of the Nokia.

Installing the certificate

1. There should be a New Message indication on the Nokia. Click the **Show** option.
2. Highlight the new message and open it. You should have the option to **Save** it. Press the **Save** softkey.
3. If you get a message that the certificate may not be secure select **Save**.
4. Click the **OK** softkey.
5. At the Certificate uses page put a check mark in both **Internet** and **Online cert. checking**.
6. Press the **OK** softkey.
7. You should see a message that says **Certificate Saved.**

1.14.3. Configuring the Access-Point

An access-point (AP) must be configured to associate to the IT network. This AP can be used for both web browsing and association to Cisco Communications Manager.

You should consult with your local IT staff for the SSID that has the best coverage in your area. You can also check to see what SSID your laptop is using by hovering over the Cisco Aironet Client Utility which will be in your system tray.

> **Note:** On the Nokia phone there are two ways to edit a field. You can either select the **Options** softkey and go to **change**, or you can use the **toggle button** and press it.

Access-Point Configuration

1. From the Idle screen press the **Menu** button.
2. Find the **Tools** icon and select it.
3. Find the **Settings** icon and select it.
4. Scroll down to the **Connection** heading and select it.
5. Select the **Access Points** heading.
6. Find the **Options** softkey and select this. Highlight **New access point** and **toggle to the right** for more options. Select **Use default settings**.
7. Change the **Connection name** to be a name of your preference.
8. Scroll to **Data bearer** and change it to **Wireless LAN.**
9. Scroll to **WLAN netw. Name**, change to **Enter manually** and enter **your SSID** as the WLAN network name.
10. Scroll to **Network status** and select **Hidden**, unless you are broadcasting you SSID.
11. Scroll to **WLAN netw. Mode** and make sure it is set as **Infrastructure**.
12. Scroll to **WLAN security mode** and change it to **802.1x**.

1.14.4. Configuring for EAP-PEAP

13. Scroll to **WLAN security sett.** Ensure that **WPA** is set to **EAP.** Scroll down to **EAP plug-in settings** and select it to change the settings.

Under the EAP plug-in settings we need to do three things. First, make sure that **EAP-PEAP** is enabled, move EAP-PEAP to the **highest priority,** and set all other EAP types to **disabled**.

14. To enable EAP-PEAP scroll down and highlight it, then press the **Options** softkey. Click the **Enable** selection.
15. To raise the priority of EAP-PEAP highlight it and press the **Options** sofkey, then select **Raise priority**. Do this until EAP-PEAP is in the number one position at the top.
16. To disable the other EAP types highlight them, press **Options**, and select **Disable**.
17. When you are done with the steps above press the **Options** softkey and select **Configure.**

Configuring the EAP-PEAP settings

> **Note:** The next section is where most of the EAP configuration is done. The fields **must** be done exactly as indicated below.

18. Leave the **User certificate** field as **(not defined)**.
19. Scroll to **CA certificate** and select it. You should find the certificate that was saved in steps 1-7 from above. If you do not see your certificate from the list it was not saved in the proper format.
20. Scroll to **User name in use** and change it to **User-configured**.
21. Scroll to **User name** and select it. Here you will use the following format for username if using Active Directory: **<username>@domain.com**. (case sensitive only – use up arrow key to change case)
22. Press the **OK** button when finished.
23. Scroll to **Realm in use** and change to **User-configured**. Here we will use the following format: **directory.com**. (Case sensitive - use up arrow key to change case).
24. Scroll down to **Allow PEAPv2** and change it to **No**. The only PEAP version that should be allowed is PEAPv0.
25. Use the Scroll button to go to the **EAP** tab by pushing to the **Right**.
26. Here we want to do two things: move **EAP-MSCHAPv2** to the highest priority, and **disable** all other options. Reference steps 14 – 16 for instructions on how.
27. Once EAP-MSCHAPv2 is enabled and at the top of the list in the number one position, highlight **EAP-MSCHAPv2** and press the **Options** softkey. Select **Configure**.

Configuring EAP-MSCHAPv2

28. Select the **User name** option and enter your **Cisco User ID** (Lower case only - use up arrow key to change case.).
29. Prompt password should say **No**.
30. Enter your Active Directory password.
31. Press the **Back** sofkey when finished.

Configuring the EAP Cipher

32. Once you have finished the EAP-MSCHAPv2 settings and pressed back, use the scroll button to press **Right** and find the **Cipher** tab.
33. Ensure that **ALL** cipher options are enabled. There are two that are not enabled by default at the very bottom of the list: RSA, RC4, MD5 and RSA, RC4, SHA – **Enable these.**
34. Press the **Back** button when finished. Continue pressing the **Back** button until you are back at the **Access Points** list. You should now see your access-point in the list.

To test your configuration you can open a web browser and point it to the new access-point.