Village Telco
Small Enterprise / Campus Network
SECN-6

User Guide

Acknowledgements

Note: This document is intended to be read in conjunction with SECN-6 firmware.

Table of Contents

1. Introduction

The VillageTelco Small Campus Enterprise Network (VT SECN) firmware is designed to allow a collection of Mesh Potato (MP02) and similar devices (eg various TP-Link, Ubiquity, Dragino, GL-iNet devices) with firmware based on OpenWrt, to provide a data and telephony network for a small campus or enterprise.

The intended use is typically for a small/medium size organisation which needs to set up a number of workpoints spread over a limited geographic area, with workpoints being equipped with a telephone and a networked PC, and to do this wirelessly without using conventional LAN cabling.

On a slightly larger scale, the system may also be used to provide networking for a a small community, with shared access to network resources such as web server, file server and Internet access.

The meshed devices utilise an OSI Layer 2 protocol (batman-adv) and collectively simply act as one large switch, transparently connecting all the attached devices together.

Each MP02-Phone device can provide a telephone connection, an Ethernet cable connection, and a WiFi Access Point. MP02-Basic, TP-Link, Ubiquity, Dragino, and GL-iNet devices can provide mesh nodes without the wired telephone connection.

PCs and other networked devices may be connected to the Ethernet port of a mesh node, or connect wirelessly to the WiFi Access Point of each node.

The WiFi Access Point in each mesh node is encrypted with WPA by default in order to provide some protection from abuse of the data network as long as the pass phrase/key is kept confidential.

The Access Points may be configured to use the same SSID and password, in which case the WiFi 'cell' will effectively cover the same area as the mesh, and WiFi client devices may 'roam' throughout the cell. Alternatively, the Access Points may be individually configured so as to provide discrete WiFi cells.

If one or more of the mesh nodes is connected via its Ethernet port to a LAN with a router / DHCP server and Internet access, any device connected to a mesh node, either by Ethernet cable or by WiFi, will be able to access the Internet via the LAN router.

Similarly, networked devices such as printers or storage devices may be attached to the LAN via a mesh node device. Attached devices will appear on the LAN and will be visible to each other.

MP02-Phone devices provide a telephone port which may be called from another MP02 telephone by dialling the IP address of the required device. Abbreviated dialling is also supported so that a call may be made by dialling just the last octet of the required IP address.

Support is also provided for Softphone applications running on Smartphones, PCs or other devices, so that calls can be made between softphone devices and MP02 Phone devices.

To use telephony off the local mesh, individual mesh node devices can be configured to access a SIP/VoIP Service Provider account for outgoing and incoming calls.

Configuration and management of individual mesh node devices is possible via web browser or terminal sessions with access to the underlying OpenWRT Linux operating system and software.

2. A Simple Mesh Set Up

In this simple mesh network we will set up a network of two MP-Phone devices so that phone calls can be made between them, then connect one MP to a Local Area Network with Internet access so that a laptop can connect wirelessly to the virtual Access Point and access the LAN and Internet.

Step 1

Flash the MP02-Phone devices to the SECN firmware.

(See following section for details of how to flash the devices.)

Step 2.

Set the unique IP address for each MP device.

Switch on one device and access its Web interface in your browser at the IP address 10.130.1.20

Change the IP address on the Basic page to 10.130.1.21

Click on the Save button. Wait for the page to refresh switch off the device.

Switch on the second device and repeat the process, but set the IP Address to 10.130.1.22, click on Save, wait for screen refresh and switch off the device.

Switch on both devices and wait several minutes for them to start up fully.

Connect a telephone to each device.

Lift the receiver and check for dial tone on each device.
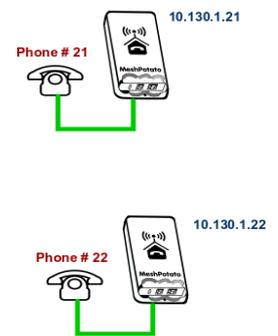
Step 3

Make a phone call.

After the MP devices have fully rebooted , pick up the phone on the '*21*' MP, check for dial tone and dial *22*. The other phone should start to ring after a few seconds.

Repeat the other way around.

Step 4

Attach the mesh network to your LAN.

Connect the MP '21' to a spare port on your LAN router with an Ethernet cable. The diagram shows the LAN using an IP address range of *192.168.1.xxx*, but the actual range used will not matter

 Note:– Because the mesh utilises an OSI Layer 2 protocol, it will work with any LAN address range. The MP addresses do *not* have to be in the same subnet as the LAN in order for the mesh to carry LAN data traffic.

Step 5

Attach a laptop via WiFi.

Your laptop should be able to see a WiFi Access Point called VT-**SECN-AP** secured with WPA encryption. Connect to this Access Point with a WPA password of '*potato-potato*' and using
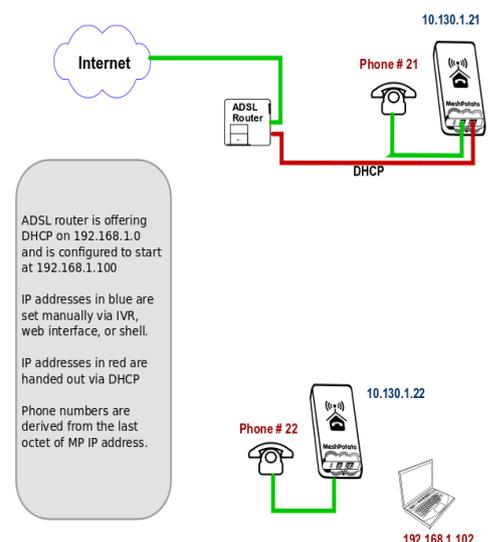
Automatic assignment of IP address (DHCP).

Your laptop should acquire an IP address in the range offered by your LAN router, and you should be able to access the Internet.

You should be able to make calls between the MP devices while accessing the Internet on the laptop.

You can connect another PC to the '*22*' MP using an Ethernet cable and it will similarly acquire an IP address from the router.

The laptop and PC should be able to access any other devices on the LAN, such as printers or network storage devices just as if they were connected directly to the LAN.

3. Example Networks

Following are examples of practical networks built around MP devices operating in a mesh.

Network 1

In this network, MP devices have been assigned static IP addresses that are part of the LAN address space, *192.168.1.xxx*, and appropriate Gateway and DNS addresses.

This means that the MP administration interfaces (SECN web interface and *ssh* command line) will be accessible from any workstation connected to the LAN.

When a workstation is attached to the mesh network either by Ethernet cable or WiFi, it will acquire an IP address from the router in exactly the same manner as if it was connected directly to the router.

The router address space must be managed so that there is no conflict between the statically assigned MP addresses and those for any other device on the network. In this example the router offers DHCP addresses starting at *192.168.1.100*, while the MPs have been assigned static addresses below this range.

Phone calls may be made between MP devices either by dialling the last octet of the required MP address (e.g. '10'), or by dialling the full address (e.g. '*192*168*1*10*').
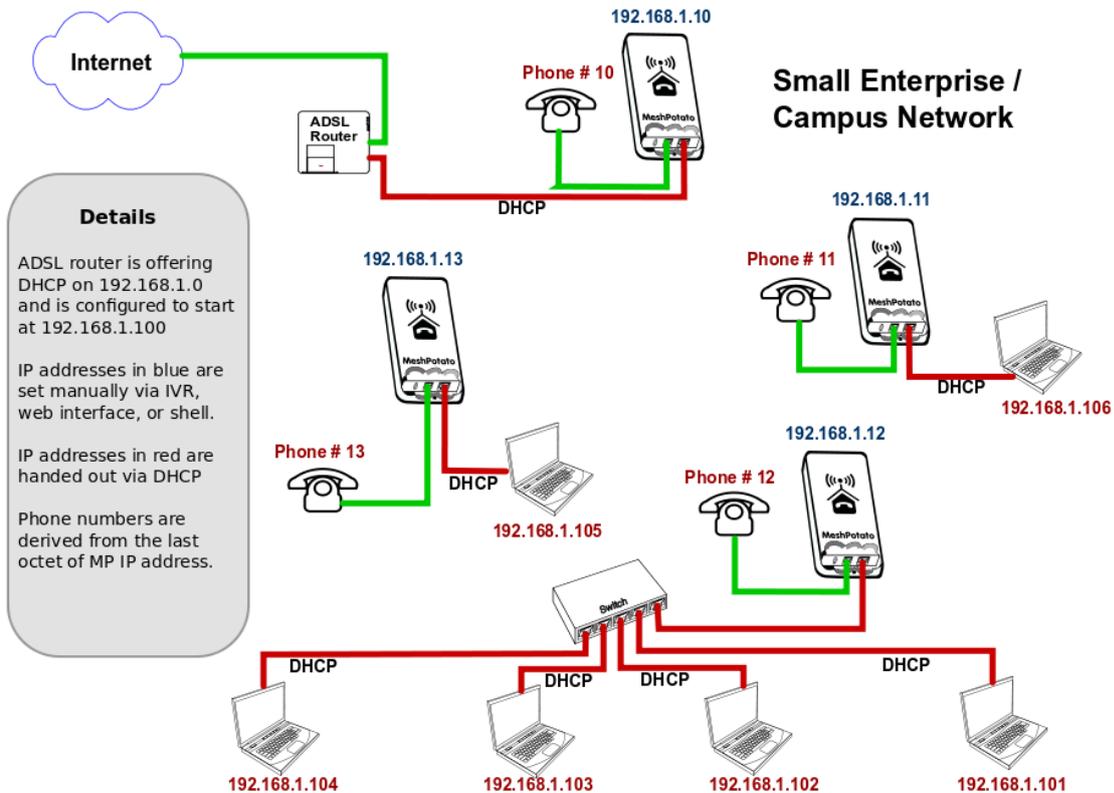
Network 2

In this network, MP devices have been assigned static IP addresses that are not part of the LAN address space. Instead they have been assigned IP addresses in the default address space 10.130.1.xxx.

This means that the MP administration interfaces (SECN web interface and *ssh* command line) will not be accessible from workstations connected to the LAN with IP addresses assigned in the LAN address space.

Administration of the MP devices may be undertaken from a workstation assigned a static address in the same range as the MP devices and attached via Ethernet cable or WiFi to any MP device in the network.

When a workstation is attached to the network either by Ethernet cable or WiFi, it will acquire an IP address from the router in exactly the same manner as if it was connected directly to the router.

In this example there is no need to manage the LAN address space to allow for the MP addresses as they are allocated in a completely different address space (*10.130.1.xxx*).

Phone calls may e made between MP devices either by dialling the last octet of the required MP address (e.g. '10'), or by dialling the full address (e.g. '*10*130*1*10*').
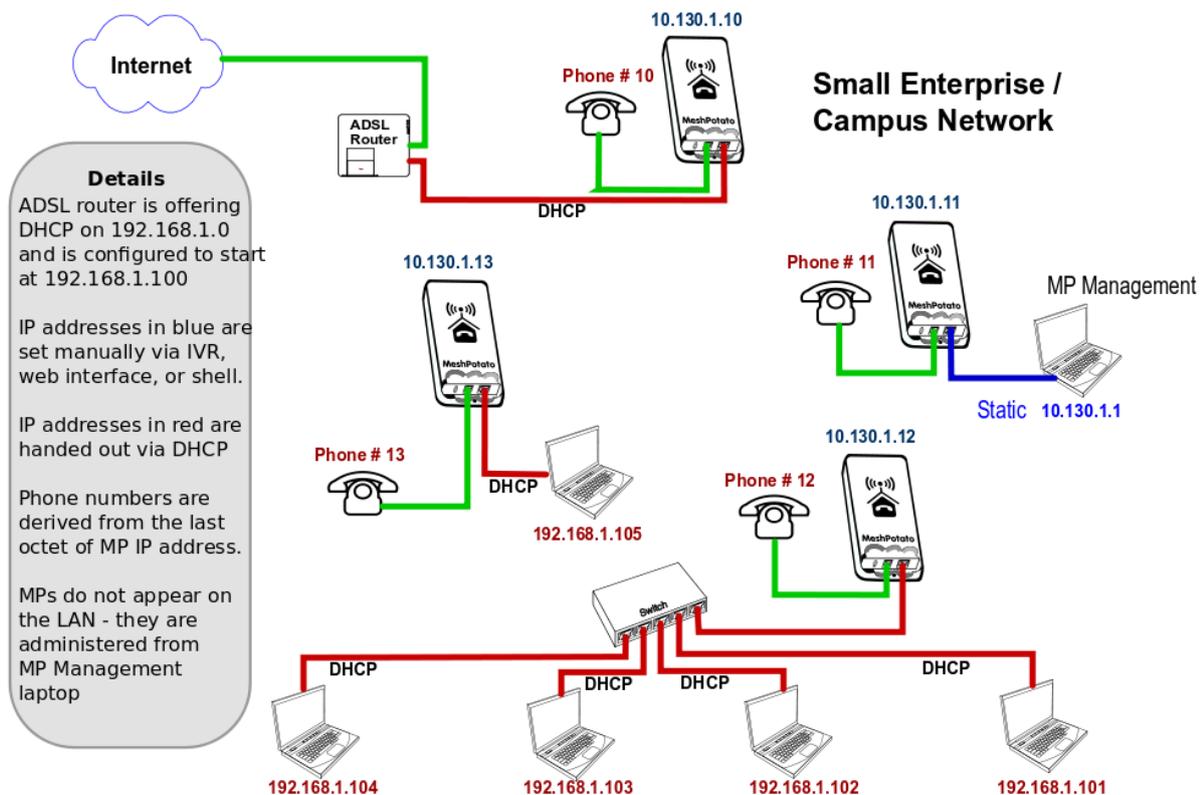
4. Setting Up SECN Devices

This section describes how to set up MP, TP or Ubiquity devices for use on your mesh network.

The first step is to install the SECN firmware on the device.

After installing the firmware, three different methods are available to configure the device:

- **Web Based Setup** using the SECN web browser interface.
- **Command Line Setup** using a *ssh* terminal session and command line.

4.1 Installing the SECN Firmware

Installing Firmware on MP02

If you have purchased a new MP-02 device, it should be delivered from the factory with the VT SECN firmware installed, however you may wish to upgrade the firmware to a different version.

Installing from the SECN Web interface

The SECN web interface provides a screen that allows you to easily upgrade the firmware using a *sysupgrade* firmware image.

To get to the SECN Web interface connect your PC to the device and connect to it at its IP address (10.130.1.20 by default). Point your browser to the IP address and you should see the web interface. If the root account password has been set, you will be prompted for the login credentials.

Go to the *Advanced/Firmware* page and click on the *Browse* button to locate the firmware file on your PC.

The firmware file should be accompanied with a file of *md5sum* values. Open this file and select the md5sum that corresponds to the firmware file and enter it into the field on the web page.

Click on *Upload* button to upload the file to the SECN device. The md5sum will be checked and if it matches the *Upgrade* button will appear. Click on this button to start the upgrade process, which will take several minutes to complete, after which the *SECN Basic* web page will appear.

The new firmware version will be displayed in the top right of the screen.

Installing OpenWrt or SECN Firmware on TP Link or Ubiquity Devices

If you want to flash an OpenWrt base firmware (such as SECN) on to a new TP Link or Ubiquity device running the original factory firmware, you will need to use the *factory* version of the firmware file, rather than the *sysupgrade* version of the file.

This is required only for the first time the device is flashed to the OpenWrt based firmware.

Use the IP address and web interface of the manufacturer's firmware to load the new firmware file, just as if you were installing an upgrade of the manufacturer's own firmware.

OpenWrt publishes generic firmware images for all supported devices on the OpenWrt Downloads page. You can select a Stable firmware such as "Barrier Breaker 14.07" to install on a new device.

The device will restart on the default IP address of 192.168.1.1 and will give you the LuCI web interface, from which you can flash a *sysupgrade* file.

NOTE: If you are flashing from OpenWrt LuCI to another firmware such as SECN, **make sure** that you *untick* the checkbox that preserves settings, otherwise the new firmware will attempt to use the configuration setting of the old firmware, which will likely be incorrect for the new firmware.

If this happens accidently, you will find that the device appears on the old IP address, and you can access the device via telnet or web interface to change the settings manually, or just reflash the device.

Installing with the *sysupgrade* Utility

To install firmware with the ***sysupgrade*** utility on a device whch already has an OpenWrt based firmware installed, it is necessary to copy the required ***sysupgrade.bin*** file to the device using the ***scp*** command from within a ***ssh*** session on your PC. You may also use ***sftp*** to browse the devices's file system in Nautilus or with WinSCP.

A device flashed with SECN firmware will only provide terminal access via ***ssh*** by default using the login account of ***root*** once the system password has been set.

If you are re-flashing a TP device that already has the VT SECN or other OpenWrt firmware version loaded, follow the process outlined below using the ***sysupgrade*** version of the firmware.

If you are using a new MP it will operate with IP addresses of ***10.130.1.20*** (LAN) and ***172.31.255.254*** (Fallback). To use one of these addresses, configure your PC Ethernet networking profile with a static address to be able to access either of these addresses, and connect directly with an Ethernet cable to the MP device.

For example, to use the MP Fallback IP address, set the PC network profile to:

IP: ***172.31.255.253*** Netmask: ***255.255.255.252*** (Note restricted IP and Netmask values)

From a terminal session on your PC, transfer the required *.**bin*** file to the MP using the ***scp*** command e.g

```
scp ./openwrt-filename-sysupgrade.bin   root@172.31.255.254:/tmp
```

This will place the file in the ***/tmp*** directory on the MP device. Note that the contents of ***/tmp*** are stored in volatile RAM and thus will be lost on a system restart.

From the ***ssh*** session install the firmware with the command:

```
sysupgrade -n -v  ./openwrt-filename-sysupgrade.bin
```

The flashing process will begin and may take several minutes, after which the MP device will restart.

Note that the ***-n*** flag causes previous configuration settings ***not*** to be retained i.e. the device will operate with the default settings after the flash. This may be an issue for remotely accessed devices – see later section for discussion on this.

It is recommended **not** to try to save settings as the new firmware may not be compatible with the previous configuration files.

After the MP device has restarted and the WiFi led has started to flash, allow up to three minutes for the flashing process to complete. After that you should be able to connect to the MP device with web browser or ***telnet/ssh*** on the default LAN or Fallback IP addresses.

Factory Firmware Reset

Pressing and holding the the hardware reset button for between 10 and 20 seconds will restore both the default configuration and the firmware as it was installed.

Any files that have been added or modified will be removed or restored respectively.

Firmware Recovery

A number of additional mechanisms are available to recover the device in the event of a bad flashing operation or an erroneous configuration set up.

1. Uboot

The MP02 has an advanced Uboot which supports Web Interface, Serial Console, and NetConsole methods of connection.

The web Interface mode may be used to reflash the device firmware with a suitable sysupgrade firmware image

To switch to the web mode, hold the button down, switch on the power and wait for one long flash and **THREE** short flashes, then release the button. At this point the LEDs will flash quickly for a second to indicate that the web mode has been selected.

The web page is then available at IP address 192.168.255.1

This web page allows you to reflash the device with new a firmware sysupgrade file.

For more detailed information see:

   http://wiki.villagetelco.org/Uboot_and_OpenWrt_Failsafe_on_the_MP02

2. OpenWrt Failsafe

Once a device has been flashed with a copy of OpenWrt firmware, there is a Failsafe mechanism provided which makes it relatively easy to recover from many 'bad flash' scenarios without having to resort to opening the device and accessing the serial port.

The Failsafe Mode may be activated by pressing the reset button on the device while the power power up sequence is happening.

For the MP02 the correct time to push the Reset ('toggle') button is 10 seconds after applying power. Apply power, time ten seconds, and then push the button for one or two seconds.
The device should then be in Failsafe mode and you can telnet to it on 192.168.1.1

After connecting with telnet, the filesystem you see is what will be restored if you just proceed with the 'firstboot' command.

Check /etc/config/network to see what IP will be used.
Enter "firstboot" at the prompt to reset the router to default.
Restart with "reboot -f" or by power cycling (simple 'reboot' command will not work)
The device will come up on the original IP address(es).

For further information see:

http://wiki.villagetelco.org/OpenWrt_Failsafe_Mode_and_Flash_Recovery

3. Serial Port Access

MP02 Serial Adapter

A Serial Port adaptor board is available for the MP-02. This adapter board plugs in to the header between the power connector and the Ethernet connectors on the main MP-02 board, with the serial connector facing away from the board.

The adaptor board provides RS-232 level signals via a DB-9 connector. The connector is designed to be connected to the serial port on a PC via a straight DB-9 M-F serial cable.

USB Serial Adapters

Many routers have serial port access provided via logic level pins on the board.
These are typically labelled Tx, Rx and Gnd.

A USB Serial adapter may be used to provide access to the serial port via these pins.

Using the Serial Port

To use the serial interface on the router, a Serial Terminal program is required on your PC.

Install a suitable serial terminal program, e.g. GtkTerm for a Ubuntu PC.

Set the configuration to be:
```
 - 115kbps
 - no parity
 - 8 bits
 - 1 stop bit
 - No Flow Control
```

On a Linux PC, the serial port will typically be /dev/ttyS0 for a serial port, or /dev/ttyUSB0 for a USB serial adapter.

For Further information see:

http://wiki.villagetelco.org/Serial_Port_Access_and_Firmware_Recovery_for_MP-02

http://wiki.villagetelco.org/Serial_Port_Access_and_Firmware_Recovery_for_TL_WR842ND

http://wiki.villagetelco.org/Serial_Port_Access_and_Firmware_Recovery_for_TL_MR3020

4.2   Set-up Using SECN Web Interface

Basic SECN Configuration

The Basic SECN Configuration screen may be accessed by pointing your web browser to the IP address of the MP device. A newly flashed device will not have a root password set and thus the web interface will not require authentication.

For a newly flashed device you may use the default IP address of 10.130.1.20 or the Fallback IP address of 172.31.255.253 To use either of these addresses you will need to configure networking on your PC to be able to access these subnets.

The Basic SECN Configuration screen allows you to set up just the key parameters for Network Address, Gateway, WiFi Access point, a SIP/VoIP phone service, set the password for the root account, and configure the web server security.

A link is provided at the top of this screen to allow access to the Advanced SECN configuration screen if required.

Network Configuration

The network configuration parameters that can be set up are the IP Address for the MP device and the IP address for the Gateway (router) device on the local network which provides access to the

Internet.

The Internet Access button will test whether there is access to the Internet and will display a message indicating success and the WAN port mot..

WiFi Access Point Configuration

The WiFi configuration allows you to set the Station ID (SSID), Passphrase and radio Channel for the MP device.

The Station ID must be comprised of alphanumeric characters (plus dash and underscore). This is the name of the WiFi Access-point that will be seen from a WiFi client device attempting to connect.

The Passphrase will be required to allow a client to connect if WiFi encryption is being used. The Passphrase must be comprised of alphanumeric characters (plus dash and underscore) and must be a minimum of eight characters in length.

Note that as this is the only security that prevents wireless access to your network, you should change the default password and make it suitably strong by using a combination of upper and lower case letters, and numbers.

By default the SECN firmware operates using WPA1-PSK encryption on the WiFi access point. You may change the encryption if required on the Advanced screen.

VoIP Configuration

The VoIP configuration allows you to set up a SIP/VoIP service to make calls beyond the local mesh if you wish. Typically this is via a commercial VoIP service provider that provides access to the standard telephone network.

Note: For this to work, the MP device must be correctly configured to operate on a network which provides Internet access for the device through the specified Gateway. In particular, the MP must be configured with an IP address in the same subnet as the Gateway IP address.

The settings are used to update the **/etc/asterisk/sip.conf** file via the **potato.sip.conf** file.

When you establish an account with a SIP/VoIP provider, you will be given a User Name and Password, as well as the URL of the SIP server on the Internet. Enter these details in the relevant fields on the screen. The Password will only be displayed when first entered.

The Dialout Code is used to distinguish between calls to be made on the local mesh, and those to be routed out to the SIP/VoIP provider. The specified digit needs to be dialled before the required external number. The available digits are #, 0 and 9.

The SIP Enable checkbox allows you to enable or disable the external SIP service while keeping the saved settings.

After entering the required settings, click the Save and Restart Asterisk button. If the MP can successfully contact the SIP server and register, the registration status will be shown below the Dialout control. Note that registration may take some time and the status may not show immediately. You can click the Refresh button to check the status after a period of time.

Password

These fields allow the password to be changed for the root account by default.

After entering the password in both fields, click on the Set Password button to make the change.

A status line at the bottom of the page will indicate whether the change was successful.

Web Server

These controls provide access security configurations to be applied to the web based configuration screens. The options can be applied in any combination and require a restart to become effective.

The Limit IP Address checkbox restricts access only to the Fallback IP address **172.31.255.254** with Netmask **255.255.255.252**

A connecting PC will need to be set to an IP address of **172.31.255.253** in order to gain access.

The Enable SSL checkbox makes access to the unit only available using SSL, thus encrypting data over the link.

When used for the first time, the unit generates a self-signed certificate, which the web browser on a connecting PC will flag and require the user to accept the certificate before allowing access.

When SSL is enabled, the required URL is: https://<ip-address>

Saving and Rebooting

The Refresh button will simply refresh the field values from saved values in memory and check the registration status of the SIP/VoIP service.

The Save button writes the various field values on the screen into memory, but does not change the operation of the MP device.

The Save and Restart Asterisk button will save all field values and restart the Asterisk telephony subsystem. This usually takes about 10 seconds to complete, but may take longer if Internet access is not configured correctly.

The Save and Reboot button will save the field values and restart the MP device using the newly saved values. Note that a restart is required to effect changes to the Network, WiFi and Web Server security settings, and will take around two minutes to complete.

Advanced SECN Configuration

The Advanced SECN Configuration screen may be accessed by clicking on the link at the top of the Basic SECN Configuration page.

This screen allows you to set up basic and additional parameters for Network, WiFi, a SIP/VoIP phone service, Softphone support and DHCP server.

Links are provided at the top of this screen to allow access to the Basic SECN and Wireless Status configuration screens if required.

Network Configuration

The network configuration parameters that can be set up are the *IP Address* and *Netmask* for the MP device, the IP address for the *Gateway* (router) device on the local network, which provides access to the Internet, and the IP address of the *DNS* server to be used for name resolution.

Radio Configuration

The *Tx Power* parameter may be used to adjust the power of the device radio transmitter. It is set by default to a of 17dBm. Normally this should not need to be adjusted but doing so may be useful in certain circumstances. The reported power is also displayed.

The **HT Mode** control allows selection of the hardware modes supported by the device

eg for 802.11gn set the mode to HT20, for 802.11g, set the mode to None.

Country Code sets the wifi parameters for the selected regulatory domain e.g. AU, US, DE…

Chan BW sets the wifi channel bandwidth to a narrow setting of 10 or 5MHz if required.

Class sets the distance parameter for the wifi link e.g Class 5 is suitable for a 2.25km link.

WiFi Access Point Configuration

The WiFi configuration allows you to set the SSID (Station ID), **Passphrase**, **Encryption** and radio **Channel**, and the maximum number of connections for the MP device.

The **SSID** is the name of the WiFi Access-point that will be seen from a client device attempting to connect and must be comprised of alphanumeric characters, dash and underscore.

The **Passphrase** will be required to allow a client to connect if WiFi encryption is being used. The passphrase must be comprised of alphanumeric characters (plus dash and underscore) and must be a minimum of eight characters in length. Note that as this is the only security that controls access to your network, you should change the default password and make it suitably strong by using a combination of upper and lower case letters, and numbers.

The **Encryption** control allows you to select from WPA1, WPA2, WEP or Open encryption on the WiFi Access-point.

The **AP Connections** control sets the maximum number of WiFi associations that will be supported. This may be used to manage the load on APs in an extended WiFi cell arrangement, or to disable the AP.

WiFi Mesh Configuration

The Mesh Wireless configuration allows you to set a number of parameters for the mesh interface including: **IP Address, Netmask, Mesh ID, Mesh Gateway**. These values are written into the configuration files **/etc/config/network** and **/etc/config/wireless**.

The interface used for the mesh wireless protocol has an IP Address and Netmask. These are set to default values of **10.10.1.20** and **255.255.255.0** and normally do not need to be altered. These settings are not used for the Batman-adv mesh protocol, and so all MP devices on the mesh may remain on the default IP address.

The mesh IP address can be used to access the MP device for maintenance in the same way as the Network Address or the Fallback Address described previously. If it is intended to use this address for maintenance access, it should be set to a unique value to avoid any potential IP address conflict.

The **MeshID** parameter sets the station identification used by devices on the mesh, and should be set the same for all devices in a mesh cell. This parameter may be used to set up separate mesh cells if required.

The **Mesh Gateway** parameter determines whether the device will act as a Gateway in the Batman-adv mesh routing protocol. This setting is only needed if there is more than one gateway device on the mesh. A device which is connected to a LAN in order to provide Internet access for example, should be set to Server mode to assist routing requests efficiently through the mesh. Devices requiring access through a Gateway should have this set to Client mode.

Asterisk Configuration

The VoIP / SIP configuration allows you to set up a SIP/VoIP service to make calls beyond the local mesh if you wish, and to optionally support Softphone operation on devices attached to the mesh.

Typically VoIP / SIP operation is via a commercial VoIP service provider that provides access to the standard telephone network.

Note: For this to work, the MP device must be correctly configured to operate on a network which provides Internet access for the device through the specified Gateway. In particular, the MP must be configured with an IP address in the same subnet as the Gateway IP address.

The settings are used to update the **/etc/asterisk/sip.conf** file via the included **potato.sip.conf** file.

When you establish an account with a SIP/VoIP provider, you will be given a *User Name* and *Password*, as well as the URL of the *SIP Host* and *Registrar* server on the Internet. Enter these details in the relevant fields on the screen.

The *Enable Asterisk Nat* checkbox may be used to enable Asterisk use behind a NAT firewall. Normally this is not required for a LAN behind a simple router/NAT firewall providing Internet access, but may be required, for example, if the MP is behind a second NAT firewall. If used, the External NAT IP field should be set to the upstream network IP address of the NAT router to which the MP is connected.

The **Dialout Code** is used to distinguish between calls to be made on the local mesh, and those to be routed out to the SIP/VoIP provider.

The default is *Auto* which will make a SIP/VoIP call if the number of digits dialled is more than six.

Alternatively, a specific digit may be used to designate SIP/VoIP calls. The specified digit is required to be dialled before the required external number. The available digits are #, 0 and 9.

The **SIP Enable** checkbox allows you to enable or disable the external SIP service while keeping the saved settings.

The **Register** checkbox determines whether the device will register with the SIP host. Registration is required in order to receive incoming calls, and some providers require registration for outgoing calls as well.

The **Softphone Support** control is used to set the mode of operation of the MP device in conjunction with other devices such as cell phones or laptops attached to the network typically via WiFi.
See later section for details of Softphone operation.

NOTE: One device only on the mesh may be set to Master mode, and this device will automatically be configured to use the reserved IP address of .252 on the LAN segment in use.

The **Codec** settings may be used to control the Codecs available to be used for calls. Normally this will not need to be changed, however some SIP/VoIP providers do require specific codecs to be used, in particular for calls outside their immediate domain.

After entering the required settings, you may click the Save and Restart Asterisk button for the changes to be made effective. If the MP can successfully contact the SIP/VoIP server and register, the registration status will be shown alongside the Sip Status label.

Note that registration may take some time and the registered status may not show up when the screen is first refreshed. You can click the Refresh button to check the status.

DHCP Server Configuration

The DHCP configuration allows you to set up a DHCP server to operate on the device. This may be used, for example, to ensure that devices attaching to the mesh network are able to obtain an IP address via DHCP in the event that here is no service available from a gateway device, perhaps due to the absence of an uplink to a remote router device.

Note: Care must be taken in setting up the configuration of the DHCP server to ensure that there is no conflict between multiple DHCP servers that are visible to devices attached to the network. Normally only a single DHCP server is enabled on a network.

The DHCP server provides IP address leases and a range of network information to clients in response to a DHCP Discovery request. The settings for the DHCP server that can be configured from the MP device web interface are outlined below.

The **Enable DHCP Server** checkbox allows the server in the MP device to operate when it is checked. By default the DHCP server is not enabled.

The **Starting and Ending IP** fields set the range of addresses that will be handed out by the DHCP server. Care must be taken to ensure that this range does not overlap the range of any other DHCP server on the network.

Lease Term sets the time period in seconds that IP address leases are valid.

Max Leases sets the maximum number of concurrent leases that will be handed out.

DNS defines the Domain Name Server IP addresses that will be handed out to clients as part of the DHCP protocol.

Domain Name sets the network name that will be handed out to clients as part of the DHCP protocol.

Subnet Mask sets the network mask that will be handed out to clients as part of the DHCP protocol.

Router sets the IP address of the network gateway that will be handed out to clients as part of the DHCP protocol.
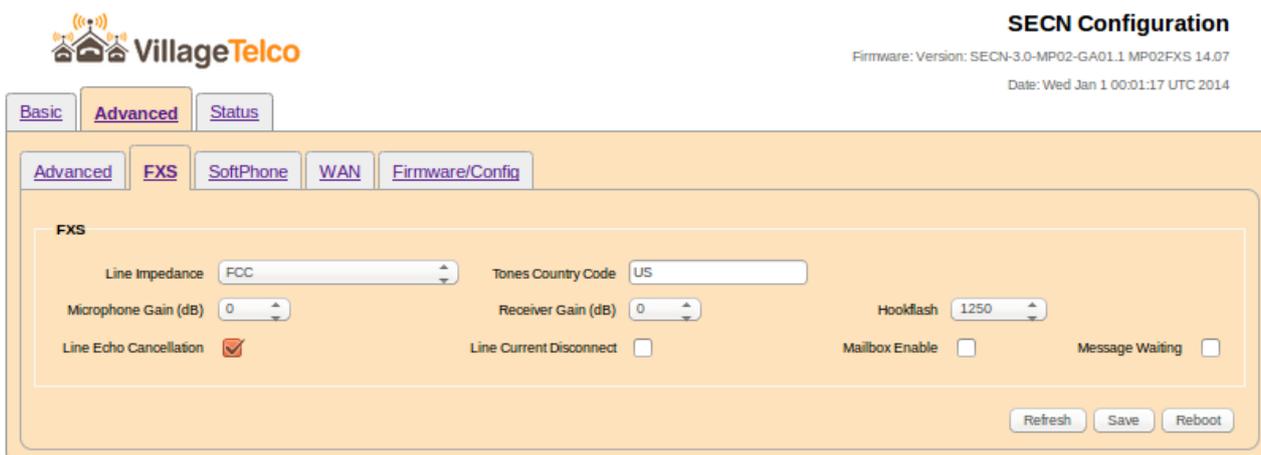
FXS Setup

This page will be present on the MP02-Phone device equipped with an FXS board providing the analogue telephone interface.

It allows changes to the operation of the FXS module to suit local network and telephone characteristics.

Line Impedance

Several standardised line impedance options are provided. The default is FCC for use in the US.

Setting the correct impedance for you local telephone network will assist with achieving correct levels and echo cancellation.

Tones Country Code

Use the standard two letter country code to set ring tone, dial tone etc to match the local conventions.

Microphone Gain / Receiver Gain

Set values to suit the analog telephone in use.

Hookflash

Set the duration of hokflash (mSec).

Line Echo Cancelation

Enable the echo cancellation software.

Line Current Disconnect

Tick this box to change to LCD mode.

Mailbox Enable

Enable the Asterisk mailbox feature.

Softphone Setup

This page allows the setting up of Softphone accounts, and displays a list of existing accounts.

To set up a new Softphone account enter the required data fields as below.

An existing account may be edited to change its Display Name or Password by entering the account number and the Name and Passsword Details.

The list of existing accounts is displayed in the lower panel of the page.

Softphone Number

This is a number in the range 300 to 399 which will be used to dial the Softphone device.

Softphone Name

This is a display name for the account.

Password

Enter the account password twice for confirmation

WAN Configuration

Reference: http://wiki.villagetelco.org/SECN_WAN_Options

WAN Port

The WAN Configuration page allows the SECN router to be configured with one of its network ports acting as a WAN port, with Network Address Translation (NAT) in operation between the WAN port and the other network ports attached to the internal bridge.

By default, the WAN interface is *Disabled* when the firmware is first installed.

Note that for all WAN Modes other than WiFi Relay Mode, Network Address Translation (NAT) will be operating between the LAN and WAN sides of the SECN device i.e. it is acting as a router.

Client devices connecting to the LAN side via WiFi or Ethernet will usually need to get an IP address assigned, so it is usual to enable the DHCP server on the LAN side of the SECN device. This can be done on the Advanced configuration page.

The following WAN Modes are supported:

> **Ethernet WAN Mode**
>
> Selecting *Ethernet* for the WAN interface will make the Ethernet port act as a WAN port.
>
> On devices (e.g. TP Link routers) with multiple Ethernet ports, the port designated as the WAN port (often coloured differently to the others) will be made the WAN port, with the others remaining connected to the internal bridge. In WAN Disabled mode, this port will be inactive.

WiFi WAN Mode

Selecting **WiFi WAN Mode** for the WAN interface will disable the WiFi Mesh interface, and makes the router act as a WiFi Station (Client) that will attach to an upstream WiFi Access Point as specified in the **WiFi WAN Host Settings** section.

Note: Because the WiFi mesh interface is disabled in this mode, the device can **not** be part of the mesh network.

In this mode of operation, the SECN device operates a WiFi Station (Client) interface as the WAN port. This allows the SECN device to connect to a host WiFi Access Point to provide upstream network access.

The SECN device will appear as a single WiFi client to the upstream host Access Point, while providing network access for a number of local client devices connected to it. The SECN device will operate its own local Access Point and Ethernet connections on the LAN side to allow client devices to connect.

This mode of operation may be useful, for example, where there is a community WiFi Access Point providing Internet Access, and a classroom or residence with a number of client devices.

Instead of connecting each individual client device directly to the community WiFi Access Point, it is possible to use the SECN device as a single WiFi Client, located in a position where it has a strong signal, and to provide access for local clients via the Ethernet or WiFi Access Point on the SECN device.

The local clients attached to the SECN device operate in their own private network address range, while having access to upstream network resources such as Internet gateway and file servers, via the main WiFi link.

The **WAN WiFi** port may use DHCP or Static IP address settings to match the upstream network.

To connect to the upstream Access Point, the WiFi WAN Host settings for SSID, Passphrase and Encryption must be set to match the upstream host Access Point (see Note below).

The status of the connection to the WiFi host is displayed on the Status page in the Node Signal Strength section.

NOTE: In this mode the WiFi Access Point on the LAN side of the SECN device will not operate unless the WAN side WiFi connection has been successfully established to the upstream host.

WiFi Relay Mode

In this mode of operation, the SECN device operates as a WiFi Relay using a WiFi Station (Client) interface connected to an upstream WiFi Access Point.

Within the device, traffic between the WAN side WiFi Station (Client) interface and the LAN interface of the SECN device is routed using the **relayd** package, which provides a pseudo-bridge between the two network interfaces.

The WAN side WiFi Station interface is set up to connect to an upstream WiFi Access Point by configuring the appropriate SSID, Passphrase and Encryption parameters.

Other devices connected to the SECN node via Ethernet or WiFi will be transparently connected to the upstream device, just as if they were attached to it directly.

This means that DHCP requests from a connected device will normally be handled by the upstream device. The DHCP service on the SECN node should thus **not be enabled** for normal operation in this mode.

 The SECN configuration interfaces (SSH or HTTP) will be available on the device's LAN IP address, by default 10.130.1.20

Note that this LAN address **must** be in a **different** IP subnet to that of the upstream Access Point, or the **relayd** software will not operate correctly.

The SECN device itself will have access to upstream network resources. For example if the upstream Access Point provides Internet access, then the clock on the SECN device will be set automatically by the NTP process.

NOTE: In this mode the WiFi Access Point on the LAN side of the SECN device will not operate unless the WAN side WiFi connection has been successfully established to the upstream host.

Mesh WAN Mode

This mode is similar to the **WiFi WAN** mode described above, but instead of a simple point-to-point WiFi connection to the host, the WAN interface forms part of a mesh network, with each node of the mesh able to pass data to other nodes. The SECN device will operate its own local Access Point and Ethernet connections on the LAN side to allow client devices to connect.

This mode of operation may be useful, for example, where there is a community WiFi Mesh Network providing Internet Access.

Instead of connecting each individual client device directly to the community WiFi Mesh, it is possible to use the SECN device as a single mesh node, located in a position where it has a strong signal, and to relay the data stream to local clients via the SECN device WiFi Access Point or Ethernet port.

In this mode of operation the local clients operate in their own private network address range, while having access to upstream network resources such as an Internet gateway, file servers and printers, via the mesh network.

The Mesh settings for MeshID, IP Address and Netmask are located on the SECN Advanced configuration page, and these must be set up to match the host mesh.

It is preferable to set the IP Addressing mode to Static for Mesh WAN mode due to potential timing issues with DHCP requests as the mesh initially starts up. Static IP address parameters should be set to match with the upstream gateway node on the mesh.

Note that on single radio devices, enabling Mesh WAN mode will always enable the Mesh interface, even if it has been disabled manually on the Advanced page, or by a previous WiFi WAN mode setting. For dual radio devices the mesh interface must be enabled manually on the required radio.

USB Modem WAN Mode

In this mode of operation, a USB Modem may be plugged in to the SECN device in order to provide Internet access.

Client devices attached to the SECN device via its LAN interfaces (Ethernet, WiFi o mesh) may then access the Internet through this shared connection.

The settings for the USB modem appear on the WAN configuration page, along with some status information showing details of the USB device connection. The process for setting up the USB Modem connection is outlined below.

USB Ethernet Modem WAN Mode

This mode supports modern USB Modems that use an Ethernet / HTTP configuration interface.

To access the interface, enter the URL for the modem. The web interface will be displayed in the dialog box on the page.

WAN / LAN

If this checkbox is ticked, the Ethernet port labelled **WAN** will be added to the **br-lan** bridge and thus act as a second **LAN** port.

Port Forwarding

This facility allows you to forward the LAN side SSH (port 22) and HTTPS (port 443) ports to the WAN side of the router on ports 2222 and 4433 respectively.

The facility is enabled by ticking the checkbox on the WAN configuration page.

With Port Forwarding enabled, the SECN router can be accessed via the web or command line interfaces for remote management from the WAN side using the Primary or Secondary IP addresses.

Note that the Primary IP address may have been assigned automatically by an upstream DHCP server. However the Secondary IP address is static.

Command Line Access

SSH is enabled when the root password has been set.

To connect via SSH to the default Secondary WAN IP address, use the command:

```
$ ssh -p 2222 10.0.1.20
```

Web Access

SSL is enabled when the "Enable SSL" checkbox on the SECN Basic configuration page has been ticked, and the device restarted.

To connect via HTTPS to the default Secondary WAN IP address, use the URL:

> https://10.0.1.20:4433

Primary WAN IP Address

By default, when it is enabled, the WAN interface operates as a DHCP Client and gets its Primary IP address, Gateway and DNS Server IP addresses from an upstream DHCP server.

There is an option to change to use a Static address by selecting from the ***WAN IP Mode*** list.

Note that for ***Mesh WAN*** mode, using DHCP may be problematic as it takes some time on start up to establish the mesh connections, and the DHCP request from the node may time out before the link is established. It is preferable to use Static IP addressing for the Mesh WAN mode where possible.

Secondary WAN IP Address

In the Ethernet and Mesh WAN modes there is a Secondary IP address that operates on the WAN interface.

This static address may be used to access the router for remote management from the WAN side.

WAN IP Mode

This setting determines whether the WAN interface will operate as a ***DHCP*** client, obtaining its IP address from the network to which it is connected, or whether it will have a ***Static*** IP address.

Static Network Settings

These settings are used to configure the WAN interface if ***Static*** mode is selected.

WiFi WAN Settings

These settings are used to specify the details of the Access Point to which the device will attach if ***WiFi WAN*** or ***WiFi Relay*** mode is selected, including the ***SSID, Encryption*** mode and ***Passphrase***.

USB Modem Settings

These settings are used to configure the USB Modem for devices that have a USB port.

> *USB Modem Service*
>
> Select the value corresponding to your wireless broadband service, either UMTS or XXX
>
> *Vendor ID and Product ID*
>
> These settings need to match the values for the modem hardware. If a modem is plugged in and the device restarted, the values will be displayed in the status line ***USB Device Detected.***
> These are four character hexadecimal values.
> Note that there may be multiple values shown for devices with more than one USB port, and you need to select the values corresponding to the modem, and enter them into the appropriate fields.
>
> *Service APN*
>
> This is the APN value for the wireless broadband service and will be provided by the service provider.
>
> *Dial String*
>
> This is the dial string for the wireless broadband service and will be provided by the service provider.
>
> *Username, Password*
>
> These values may be required by your service provider. If not required, leave them blank.

PIN Number

If the PIN Number has been activated for your modem, enter the value here.

USB Serial Port

The USB Serial Port number is specific to the USB modem device.
For example, Huawei devices generally use 0, and Sierra Wireless generally use 2.
Once the **Product** and **Vendor ID** values are correctly set, and the the device is restarted with the USB modem installed, the USB Serial ports detected will be displayed in the status line at the bottom of the page.

When the USB modem settings have been correctly entered and the device restarted with the modem installed and the Wireless Broadband service is available, the connection status will be displayed in the status line at the bottom of the page.

Setting Up a USB Modem Connection

The process for setting up a USB 3G modem in the SECN WAN configuration screen is as follows:

- Plug in the USB Modem and then power up the SECN device
- Go to SECN Advanced / WAN page and select WAN Mode 'USB Modem'
- Scroll down to USB Modem section and look to see if the device has been detected in the status area.
- Get the Vendor and Product IDs from the detection string and copy them into the required fields.
- Select the USB Modem Service type. UMTS is default for 3G services.
- Set the Service APN field as per your telco service provider eg in Australia it is 'telstra.internet' for the Telstra telco.
- Select the USB Serial Port. (Google is your friend to find this out for your particular USB modem. Otherwise trial and error - 0 and 2 are common values).
- Username, Password and (SIM card) PIN fields can be left blank unless your Service / SIM card has been configured to require them.
- Click on the 'Save' button and check the settings when the screen refreshes.
- Power cycle the device.
- Check to see if the USB Serial Ports have been detected in the status area. This means that the device ID parameters are correct.
- Check to see if the modem has connected to the service provider in the USB Modem Status line. This depends on the USB Serial port setting being correct, and also on the PIN, Username and Password if these settings are required by your SIM card and service provider.
- If you have to try different settings, it is best to save the settings then power cycle the device, otherwise the USB modem may not initialise correctly.

The simplest set up is with no PIN number on the SIM card, and no Username/Password on the service. In this case it is just a matter of getting the correct APN and USB Serial port setting.

Firmware / Configuration Page

Firmware Upgrade

This page allows you to upload a 'sysupgrade' firmware file in order to reflash the device.

After selecting *Firmware Upgrade*, browse for and select the new firmware file.

It is preferable to also enter the MD5 checksum of the file to ensure that it has not been corrupted, but you may choose to skip this feature by checking the *Ignore Checksum* box.

Select *Upload File to Server* to transfer the fie and checksum to the device.

The file will be uploaded and the MD5 checksum calculated and compared to that supplied.

If the checksum comparison is correct, you may select whether to preserve the current device configuration (eg IP address, SSIDs, passwords etc), then select *Upgrade Firmware* to begin the flash process.

A screen will be displayed showing the time remaining for the upgrade to be completed. This is typically five minutes, and it is important not to disrupt the process during this time.

Configuration Save

This facility generates a gzipped tar archive file of a range of device configuration files in order to backup the state of the device configuration.

The configuration files included in the archive are specified in */etc/backup.conf*

The file may then be downloaded by clicking on the **Download Configuration File** link and saved for future use. The archive may be unpacked and the individual files edited if required. Files may be added to or deleted from the archive if required.

Configuration Load

This facility loads a gzipped tar archive file into memory, checks the md5sum, and unpacks the archive file if the user requests.

This is normally used to restore a set of configuration files previously saved by the **Configuration Save** facility.

It may also be used to upload and unpack an arbitrary archive file containing any appropriate files, and so may be used to install patches.

The archive file is first uploaded to the **/tmp** directory and the md5sum checked, before offering the user the ability to unpack the archive.

Saving and Rebooting

The Refresh button will simply refresh the field values from saved values in memory and check the registration status of the SIP/VoIP service.

The Save button writes the various field values on the screen into memory, but does not change the operation of the MP device.

The Save and Restart Asterisk button will save all field values and restart the Asterisk telephony subsystem. This usually takes about 10 seconds to complete, but may take longer if Internet access is not configured correctly.

The Restore Defaults button will reset all the configuration settings to the default values of a newly flashed device.

The Save and Reboot button will save the field values and restart the MP device using the newly saved values. Note that a system restart is required to effect changes to the network settings and will take around two minutes to complete.

4.3   Advanced Command Line Set-up

Advanced Command Line Set-up utilises access to the OpenWrt Linux operating system on the device and permits full access to all configuration facilities as well as adding and configuring additional software packages.

Access to the device for Advanced Set-up is by means of a command line from a *telnet* or *ssh* terminal session.

Connecting to the device

When first flashed with new SECN firmware, the device supports a *telnet* connection as there is no root password set.

Connect to the MP with *telnet* using the MP device's Fallback address: 172.31.255.254

Set PC network to: IP: 172.31.255.253 Netmask: 255.255.255.252

Alternatively the default *br-lan* IP address 10.130.1.20 may be used with Netmask 255.255.2555.0

Once the telnet connection has been made, set the root password with the *passwd* command, logout with the exit command, then reconnect with *ssh*.

Setting the device Network Addresses

Setting the br-lan Bridge IP Address

Set the unique IP address for the br-lan interface of the MP device by using the uci command, or by directly editing the network configuration file.

From the command line:

```
uci set network.br-lan.ipaddr=103.130.1.xxx    (Where xxx is unique to each device)
uci commit network
```

Editing the **/etc/config/network** file:

```
config 'interface' 'lan'
        option 'type' 'bridge'
        option 'ifname' 'eth0 bat0 wlan0'
        option 'proto' 'static'
        option 'netmask' '255.255.255.0'
        option 'gateway' '10.130.1.1'      # Default Gateway router address
        option 'dns' '8.8.8.8'
        option 'ipaddr' '10.130.1.xxx'     # Where xxx is unique to each device
```

Setting the mesh IP Address

You may wish to change the mesh IP address, however this is not required for basic mesh operation.

From the command line:

```
uci set network.mesh_0.ipaddr=10.10.1.xxx           (Where xxx is unique to each MP)
uci commit network
```

Editing the **/etc/config/network** file:

```
config 'interface' 'mesh_0'
        option 'proto' 'static'
        option 'ipaddr' '10.10.1.xxx'
        option 'netmask' '255.255.255.0'
        option 'mtu' '1532'
```

Set the Access Point SSID and WPA Passphrase

From the command line:

```
        uci set secn.accesspoint.ssid="VT-SECN-AP"
        uci set secn.accesspoint.passphrase="potato-potato"
        uci commit secn
```

Editing the **/etc/config/secn** file:

```
config 'secn' 'accesspoint'
      option 'encryption' 'WPA2'
      option 'ssid' 'VT-SECN-AP'
      option 'passphrase' 'potato-potato'
      option 'ap_enable' '1'
```

Modifying Asterisk Operation

Setting up External SIP / VoIP Operation

To add external VoIP support, use the SECN web configuration interface or modify the *secn* configuration file.

From the command line:

```
        uci set secn.asterisk.host=sip.myhost.com
        uci set secn.asterisk.reghost=sip.myhost.com
        uci set secn.asterisk.fromdomain=sip.myhost.com
        uci set secn.asterisk.secret=mysecret
        uci set secn.asterisk.username=myusername
        uci set secn.asterisk.fromusername=myusername
        uci commit secn
```

Editing the **/etc/config/secn** file:

```
config 'mesh' 'asterisk'
      option 'fromdomain'   'sip.myhost.com'
      option 'host'         'sip.myhost.com'
      option 'reghost'      'sip.myhost.com'
      option 'secret'       'mysecret'
      option 'username'     'myusername'
      option 'fromusername' 'myusername'
      option 'codec1'       'gsm'
      option 'codec2'       'ulaw'
      option 'codec3'       'alaw'
      option 'enablenat'    ''
      option 'externip'     '0.0.0.0'
      option 'proxy'        ''
      option 'softph'       'CLIENT'
      option 'dialout'      'Auto'
      option 'enable'       'checked'
      option 'register'     'checked'
```

5. Overview of SECN Operation

This configuration uses Batman-advanced for the mesh rather than Batman as used in earlier firmware versions. Batman-advanced uses a different mesh protocol to batman and so the two will not interoperate on the same mesh.

The MP device provides two physical network interfaces, Ethernet cable and wireless, which are configured as follows:

- The eth0 interface operates on the MP Ethernet cable connection.
- Two wireless interfaces, *wlan0* and *wlan0-1*, are set up on the wireless interface radio0.
- Batman-adv is configured to run on the wlan0-1 meshpoint interface using the batctl command and generates the bat0 interface.
- The second wireless interface, wlan0, is set up to operate as a WiFi Access Point.
- The bat0, wlan0 and eth0 interfaces are bridged (br-lan) together in each device and assigned a static IP address, and thus, due to the operation of the mesh via bat0, all the wlan0 and eth0 interfaces of all the MPs in the mesh are similarly bridged.
- The default IP address used for the br-lan interface is 10.130.1.20

The mesh will operate in a stand-alone configuration, simply connecting attached devices together and providing telephony between devices. Alternatively the mesh may be interconnected to a LAN to provide access to additional resources, including Internet connectivity.

If one of the devices is connected via Ethernet cable to a LAN router, then all WiFi and Ethernet interfaces connected to the meshed devices will have access to the LAN resources.

If there is a DHCP server running on the LAN (eg in the router/gateway) then devices configured as DHCP clients connected to the mesh node devices via WiFi or Ethernet will acquire an IP address just as if they were connected directly to the LAN.

Note that there is *no* DHCP server running in a stand-alone mesh arrangement by default, and so in this case, attached devices would need to be statically configured for their IP address in order to connect. Alternatively one of the meshed devices may be configured to provide a DHCP service.

5.1   IP Address Range for MPs

It should be noted that the IP address used for the br-lan bridge in the MP devices needs to be configured during setup, and may or may not be made to lie in the IP address space used on the LAN to which the mesh may be connected. Operation is essentially the same in both cases, but care must be taken to manage the address space in the former case to avoid conflicts with LAN addresses.

IP addresses assigned to MP devices are static. If the IP addresses used for the MP devices lie in the same address space as the LAN, then the DHCP server and other devices on the LAN must be appropriately configured so that the addresses assigned to the MP devices are left free in order to avoid IP address conflicts. In this arrangement, the MP devices will appear on the LAN just as any other device with a static IP address, and they may be accessed for management via browser or ssh terminal session.

Conversely, if the IP address range used for the MP devices is separate to that used on the LAN, the MP devices will not appear on the LAN and there is no need to reserve the address space. In order

to access the MPs for management in this configuration, it is necessary to configure a PC with a static address in the same range as the MPs, and attach via Ethernet cable or WiFi.

The default IP address assigned to the br-lan interface in the MPs is 10.130.1.20 which is unlikely to conflict with the default address range of commodity routers.

If it is desired to have the MPs appear on the LAN, the br-lan IP address should be assigned accordingly during set up.

The address assigned to the br-lan interface for each MP must be changed to be unique, so that each device can provide a separate telephone number. This IP address assignment may be made by a number of methods including web interface or manipulation of the **/etc/config/network** file.

5.2   Batman-Adv Operation

Batman-adv is a "OSI layer 2" routing protocol which is implemented as a kernel module in the Linux kernel. Since Linux 2.6.38 batman-adv is an official part of Linux.

When you assign at least one active physical network interface to batman-advanced, it will create the virtual bat0 interface. In the SECN firmware the wlan0-1 (meshpoint) interface is assigned to the batman-adv kernel module.

Because batman-adv operates entirely on MAC layer (OSI layer 2), wlan0-1 doesn't need any Layer 3 configuration. Only its Layer 2 MAC address is required. The MAC address is configured during production, so we don't need to configure it. All we need to do is make sure to switch wlan0-1 on. To sum it up: wlan0-1 is the link-local transport interface for the batman-adv mesh.

Batman-adv itself bridges all bat0 interfaces in all the mesh devices to a big, smart, virtual switch. This means that all bat0 interfaces in the mesh are link-local, even if they are multiple wireless hops away.

Despite being virtual, bat0 acts like a real, physical, network interface connected to a big switch. As such you can run all kinds of network protocols on it, like IPv4, IPv6, ARP, IPX – or whatever protocol that can communicate over a network interface that is connected link local (which means directly connected, like a straight Ethernet cable connected between two computers, or a bunch of computers connected to a switch).

In the SECN firmware the bat0 interface itself is again assigned (or rather enslaved) to a bridge in each machine. bat0 is part of the bridge named br-lan, together with wlan0 and eth0.

eth0 is the LAN port of the MP, and wlan0 is an Access-Point interface, operating in WiFi infrastructure mode (as opposed to "Station" mode used e.g. by a laptop or smartphone)

Hence all eth0 and wlan0 interfaces in all devices running the SECN firmware are part of one big wireless bridge. The wlan0-1 meshpoint interface does the low level work to carry the traffic link-locally from hop to hop and batman-advanced takes care about the routes that the MAC packets have to take.

Note: It is not possible to add IP settings to an interface which is encapsulated in a bridge - you can only assign IP settings to the bridge interface itself. eth0 is part of the bridge br-lan, together with wlan0, bat0 (the batman-adv virtual interface, which is routed by the mesh routing protocol using MAC addresses). Hence you can not assign any IP settings to eth0, wlan0 or bat0 - only to br-lan.

BATCTL Command

The following description is taken from the man page published by OpenMesh.org at:

> http://downloads.open-mesh.org/batman/manpages/batctl.8.html

Syntax

```
batctl [batctl-options] command [command-options]
```

This command offers a convenient way to configure the batman-adv kernel module as well as displaying debug information such as originator tables, translation tables and the debug log. In combination with a bat-hosts file batctl allows the use of host names instead of MAC addresses.

B.A.T.M.A.N. advanced operates on layer 2. Thus all hosts participating in the virtual switched network are transparently connected together for all protocols above Layer 2. Therefore the common diagnosis tools do not work as expected. To overcome these problems batctl contains the commands ping, traceroute, tcpdump which provide similar functionality to the normal ping(1), traceroute(1), tcpdump(1) commands, but modified to Layer 2 behaviour or using the B.A.T.M.A.N. advanced protocol.

Commands of particular interest include the following:

```
originators|o    [-w [interval]][-n][-t]
```

Once started batctl will display the list of announced gateways in the network. Use the "-w" option to let batctl refresh the list every second or add a number to let it refresh at a custom interval in seconds (with optional decimal places). If "-n" is given batctl will not replace the MAC addresses with bat-host names in the output. The "-t" option filters all originators that have not been seen for the specified amount of seconds (with optional decimal places) from the output.

```
gw_mode|gw       [off|client|server] [sel_class|bandwidth]
```

If no parameter is given the current gateway mode is displayed otherwise the parameter is used to set the gateway mode. The second (optional) argument specifies the selection class (if 'client' was the first argument) or the gateway bandwidth (if 'server' was the first argument). If the node is a server, this parameter is used to inform other nodes in the network about this node's internet connection bandwidth. Just enter any number (optionally followed by "kbit" or "mbit") and the batman-adv module will guess your appropriate gateway class. Use "/" to separate the down- and upload rates. You can omit the upload rate and the module will assume an upload of download / 5.

> default: 2000   →   gateway class 20
>
> examples: 5000   →   gateway class 49
>
>   5000kbit
>
>   5mbit
>
>   5mbit/1024
>
>   5mbit/1024kbit
>
>   5mbit/1mbit

If the node is a gateway client the parameter will decide which criteria to consider when the batman-adv module has to choose between different internet connections announced by the

aforementioned servers.

bat-hosts file

This file is similar to the **/etc/hosts** file. You can write one MAC address and one host name per line. batctl will search for bat-hosts in **/etc**, your home directory, and the current directory. The found data is used to match MAC address to your provided host name or replace MAC addresses in debug output and logs. Host names are much easier to remember than MAC addresses.

Batman-adv and Gateways

The batman-adv package for the MP supports configuring advanced batman-adv gateway and gateway client parameters via UCI.

Note: You need this if you want to use more than one gateway in the mesh. In this case set the gateway MPs mode to Server and the other MPs mode to Client

Gateway settings for Server and Client mode are provided in the SECN web interface on the Advanced page.

Settings may be made from the command line as follows.

An example how to configure batman-adv gateway bandwidth:

```
root@MP-2:/# uci set batman-adv.bat0.gw_mode=server
root@MP-2:/# uci set batman-adv.bat0.gw_bandwidth=384kbit/128kbit
root@MP-2:/# uci commit
root@MP-2:/# /etc/init.d/batman-adv restart
```

Setting the downlink/uplink speed of the gateway like in this example is optional, if you want to override the default value.

For more info check out http://downloads.open-mesh.org/batman/manpages/batctl.8.html

An example how to configure a MP as batman-adv gateway client:

```
root@MP-2:/# uci set batman-adv.bat0.gw_mode=client
root@MP-2:/# uci commit
root@MP-2:/# /etc/init.d/batman-adv restart
```

By default the clients will connect to the gateway with the 'best' access (qualified by the TQ route metric, which measures route quality) in the mesh. As long as no other gateway has a TQ route metric which is more than 20 counts better than the currently selected gateway, the clients will stick to the current gateway. If another gateway is more than 20 TQ counts better, the clients will switch the selected gateway. You can, of course, tweak this threshold.

If you want to do some fancy - experimental - setup like dynamically changing the announced gateway bandwidth, in order to balance the load of the gateways, you can change the clients gateway selection algorithm.

Example:

```
root@MP-2:/# uci set batman-adv.bat0.gw_mode=client 1
root@MP-2:/# uci commit
root@MP-2:/# /etc/init.d/batman-adv restart
```

This setting will configure the clients to select the gateway in order to find the best compromise of TQ route metric and announced gateway speed. A 100Mbit/100Mbit gateway is useless if the TQ

route metric is small.

For more detailed info check out the batctl man page at open-mesh.net

5.3 Telephony Operation

Overview

MP02-Phone devices provide an RJ11 port to which a telephone may be connected, and each MP device runs a copy of the Asterisk application to provide the telephony facilities. Asterisk allows phone calls to be made between devices by means of Voice over IP (VoIP) and Session Initiated Protocol (SIP).

5.4 Asterisk Operation

The operation of Asterisk is controlled to a number of configuration files, two of which are of particular interest for MP devices - **/etc/asterisk/extensions.conf** and **/etc/asterisk/sip.conf**

The **extensions.conf** file sets up the dial plan while the **sip.conf** file defines the channels to be used for making calls.

Operation of Asterisk can be monitored from the MP command line by executing the commands:

```
#  asterisk -r
#  asterisk -vvvvvrddd     Launches with Verbose Lev 5 and Core Debug Lev 3.
```

Some useful commands in the Asterisk shell include:

```
CLI> exit                 Return to the command shell
CLI> help                 Displays a list of available commands
CLI> core set verbose 5   Set verbose level to 5
CLI> sip reload           Reload sip.conf configuration
CLI> dialplan reload      Reload extensions.conf dialplan
CLI> show dialplan defaultDisplay current dial plan
CLI> sip show registry    Display sip registrations
```

Making Calls to MP Devices

To dial an MP device using the full IP address, dial the IP number substituting the * character for the dots between octets in the address. To dial an MP with address 10.130.1.21, dial

> 10*130*1*21

The SECN firmware includes a facility for making on mesh calls using abbreviated dialling by using just the last octet of the MP device's IP address. When an abbreviated number dial string is detected, the full IP address is generated by pre-pending the rest of the address.

The IP address used for on mesh abbreviated dialling is set up during the start up process by the script /bin/generate-extension.sh, using the MP device's own br-lan IP address as reference.

To dial an MP device using abbreviated dialling, simply dial the last octet of the unique IP number assigned to the required MP. This can be dialled as 1, 2 or 3 digits, and may include leading 0 eg

5, 05, 005   (device address 10.130.1.5)
25, 025   (device address 10.130.1.25)

105   (device address 10.130.1.105)

Debugging Asterisk Operation

Asterisk provides a comprehensive interactive console mode to allow you to monitor its operation.

If Asterisk is already running, invoke the console mode with the command:

```
root@MP-2:/# asterisk -vvvvvrddd
```

This will run the console with Verbosity set to Level 5, and Core Debug set to level 3, which generally gives good visibility of what is happening. It does not interfere with the operation of Asterisk.

An extensive set of commands is available from the Asterisk CLI command line.

To see a list of these commands type: help

To exit the console mode, type: exit

If Asterisk is not already running, you can start it up with console mode running with the command:

```
root@MP-2:/# asterisk -vvvvvrgcddd
```

This can be useful for monitoring the start-up behaviour of Asterisk.

Asterisk and Network Settings

Asterisk has some very particular requirements around network settings, specifically:

Network DNS Address

Firstly, during Asterisk start-up, it will test for the presence of a ping response from the DNS nameserver address specified in the /**etc/resolv.conf** file. It may wait for a period of many seconds for a response, which will affect the start up delay for the whole device. This delay can be seen in the Asterisk console. In the MP device firmware, the Asterisk start-up script temporarily uses the local host address for the DNS setting to ensure fast start-up.

Secondly, for external SIP / VoIP operation, Asterisk will use the nameserver value in **/etc/resolv.conf** to resolve the URL of the SIP / VoIP host server on the internet. If there is no valid DNS service operating on this address, or the DNS address is not accessible from the MP device, Asterisk will fail to register the SIP / VoIP service and will complain of a DNS error in the Asterisk interactive console output.

Network Gateway Address

Asterisk requires that the network gateway address specified in **/etc/config/network** be in the same IP subnet range as the MPs IP address, even if there is no device actually present at this address.

If the gateway address is not in the correct subnet, Asterisk will fail to place even on-mesh calls and will complain of a 'Bad file descriptor' error in the interactive console output.

Note: Care must be taken when setting these addresses manually from SECN web interface or command line.

Access to SIP/VoIP Server

If Asterisk cannot access the network and see the external VoIP host during startup, calls through the service will fail, even if Asterisk is able to register with the service after startup. Calls to mesh

devices will work correctly in this scenario, leading to confusion over the status of Asterisk.

This is particularly relevant to MP devices that are connected to the LAN / Internet only via the mesh, as the start up order and timing of scripts in **/etc/rc.d** are designed to ensure the mesh is running correctly before Asterisk tries to start.

Sample Asterisk Console Outputs

1. Calls between MP02 at 10.130.1.20 and MP02 at 10.130.1.85 on the mesh network.

```
Outgoing Call to MP02-085 from MP02-020


    -- Starting simple switch on 'DAHDI/1-1'
    -- Executing [085@incoming-local:1] Dial("DAHDI/1-1", "SIP/4000@10.130.1.085") in
new stack
  == Using SIP RTP CoS mark 5
    -- Called SIP/4000@10.130.1.085
    -- SIP/10.130.1.085-00000000 is ringing
    -- SIP/10.130.1.085-00000000 answered DAHDI/1-1
       > 0x7dcc68 -- Probation passed - setting RTP source address to 10.130.1.85:14022
  == Spawn extension (incoming-local, 085, 1) exited non-zero on 'DAHDI/1-1'
    -- Hanging up on 'DAHDI/1-1'
    -- Hungup 'DAHDI/1-1'


-------------------------------------------------

Incoming call from MP02-085 to MP02-020

  == Using SIP RTP CoS mark 5
    -- Executing [4000@incoming-analog:1] Dial("SIP/10.130.1.85-00000001", "dahdi/1")
in new stack
    -- Called dahdi/1
    -- DAHDI/1-1 is ringing
    -- DAHDI/1-1 is ringing
    -- DAHDI/1-1 answered SIP/10.130.1.85-00000001
       > 0x7d88b0 -- Probation passed - setting RTP source address to 10.130.1.85:17624
    -- Hanging up on 'DAHDI/1-1'
    -- Hungup 'DAHDI/1-1'

```

2. Call to a PSTN number 07-3399-1234 via SIP / VoIP Service

```
MP2-20*CLI>
    -- Starting simple switch on 'DAHDI/1-1'
    -- Executing [0733991234@incoming-local:1] Dial("DAHDI/1-1",
"SIP/0733596620@sipaccount,120,r") in new stack

  == Using SIP RTP CoS mark 5
    -- Called SIP/0733991234@sipaccount
    -- SIP/sipaccount-00000001 is making progress passing it to DAHDI/1-1
    -- SIP/sipaccount-00000001 answered DAHDI/1-1
       > 0xc1b058 -- Probation passed - setting RTP source address to
125.213.160.71:24516

  == Spawn extension (incoming-local, 0733991234, 1) exited non-zero on 'DAHDI/1-1'
    -- Hanging up on 'DAHDI/1-1'
    -- Hungup 'DAHDI/1-1'

MP2-20*CLI>
```

3. Dmesg / logread output

```
Off-hook / On-hook event
[ 7572.480000] dragino2_si3217x: Going off hook
[ 7572.480000] dragino2_si3217x: DAHDI_TXSIG_OFFHOOK
[ 7572.480000] dragino2_si3217x: ioctl DAHDI_TONEDETECT, not supported
[ 7572.490000] dragino2_si3217x: Linefeed status was 0x11, is now 0x2
[ 7573.280000] dragino2_si3217x: Going on hook
[ 7574.530000] dragino2_si3217x: DAHDI_TXSIG_ONHOOK
[ 7574.530000] dragino2_si3217x: Linefeed status was 0x11, is now 0x1

Outgoing call
[ 7719.100000] dragino2_si3217x: Going off hook
[ 7719.100000] dragino2_si3217x: DAHDI_TXSIG_OFFHOOK
[ 7719.100000] dragino2_si3217x: ioctl DAHDI_TONEDETECT, not supported
[ 7719.110000] dragino2_si3217x: Linefeed status was 0x11, is now 0x2
[ 7731.430000] dragino2_si3217x: DAHDI_TXSIG_KEWL
[ 7731.440000] dragino2_si3217x: Linefeed status was 0x11, is now 0x0
[ 7731.660000] dragino2_si3217x: Going on hook
[ 7731.940000] dragino2_si3217x: DAHDI_TXSIG_ONHOOK
[ 7731.950000] dragino2_si3217x: Linefeed status was 0x00, is now 0x1

Incoming call
[ 7794.470000] dragino2_si3217x: ioctl DAHDI_TONEDETECT, not supported
[ 7794.480000] dragino2_si3217x: DAHDI_TXSIG_START
[ 7794.480000] dragino2_si3217x: Linefeed status was 0x11, is now 0x4
[ 7796.490000] dragino2_si3217x: DAHDI_TXSIG_OFFHOOK
[ 7796.500000] dragino2_si3217x: Linefeed status was 0x44, is now 0x2
```

5.5   Softphone Support

Softphone Support is provided in order to be able to allow devices such as cell phones and laptop PCs equipped with softphone applications to join the MP telephone network and to make and receive calls on the network, and to an external SIP/VoIP service if configured.

Setting up the Devices

Softphone Support is enabled by the control in the VoIP / SIP section of the Advanced SECN Configuration screen. The available modes are Off (default), Master and Client.

In order to support Softphones on a network over the mesh, one, and one only, device on the network is set to Master mode. The copy of Asterisk running on the Master device is used to route softphone calls around the network.

The Master device will automatically have its IP address last octet set to .252

This address is reserved by default in a SECN network as a 'well known' network address for the Softphone server.

Other MP devices on the network that are to be able to make calls to softphone equipped devices must have their Softphone Support control set to Client.

Note that after setting the mode in the configuration screen, the device has to be restarted for the changes to take effect.

Configuration of Softphone Accounts

Softphone accounts are defined in the file **/etc/asterisk/softphone.sip.conf**

Setting up softphone accounts may be done using the *Softphone* tab on the SECN Advanced web interface.

To create a softphone account, enter the required softphone number (300 – 399), a Name for display purposes, and a password (twice for confirmation).

Once an account is set up on an attached softphone device, it may be called using the three digit numbers (300 through 399).

Note that setting of the allowed codec(s) is critical to the operation of some softphone clients.

Testing of the SECN Softphone facility has be primarily undertaken using the CSip Simple application, however many other applications are available.

Setting up the DHCP Server

Telephony on the SECN MP network relies on the IP addresses of the devices attached to the network to route calls to the correct device. MP devices typically have statically assigned IP addresses for this purpose. This allows an MP network to operate without the need for any master device controlling the telephony system, thus providing maximum robustness.

This is not the case with Softphone Support described here. Softphone devices are 'registered' with the Softphone Master device, and the presence and correct operation of this device is essential for softphone operation. It is in effect a single point of failure.

Furthermore, the softphones do not rely on their IP address to determine their phone number; the

phone number is part of the registered account for the device.

However a device which attaches to the network may not have a static IP assigned and will expect to get an IP address from a DHCP server on the network. When a cell phone or similar device equipped with a softphone application is attached to the network it is generally configured to receive an IP address from a DHCP server.

Where a MP network is attached to a LAN, there will usually be some device on the LAN running a DHCP server that will hand out a suitable IP address to an attaching device. As long as the MP static addresses are on the same sub net range as the DHCP addresses, all will be well.

Where a MP network is operating in a stand alone manner, not attached to a LAN, there will be no device present to hand out IP addresses. For this reason, a DHCP Server is provided in the firmware so that an MP device can perform this function.

The DHCP Server may be configured from the DHCP Server section of the Advanced SECN Configuration web page.

Care should be taken to avoid IP address conflicts, and conflicts between multiple DHCP servers on the same network. The range of addresses used for the DHCP server should be outside the range used for statically assigned addresses used for the MP devices.

Setting up the Softphone Clients

The Softphone function has been tested with the CsipSimple application, however there are many other applications that will work satisfactorily.

For a CSipSimple client, the setup is as follows:

1. Start up CSipSimple and go to the CSipSimple settings.

2. Create a SIP account (e.g. softph300).

3. Set the Password to match the account entry e.g. "mypassword300"

4. Set the Server (or Proxy) to the IP address of the Softphone Master MP (ie .252 on the IP sub net)

CSipSimple should show successful registration to the softphone server.

The Asterisk console on the node will also show that the Softphone has correctly registered with the *sip show peers* command.
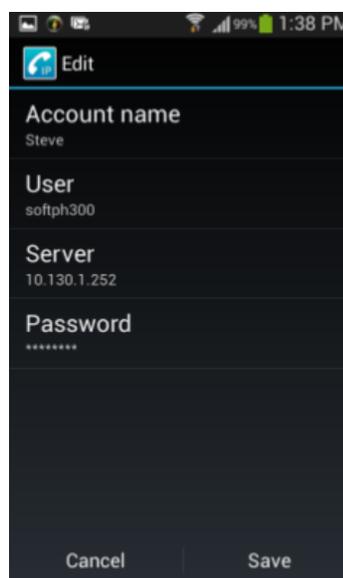
Making Calls to and from Softphones

To make a call from a softphone equipped device to an MP device simply dial the last octet of the MP's IP number in the usual manner.

To make a call from an MP device to a softphone device, simply dial the three digit number corresponding to the account entry e.g. "300"

Calls to softphone clients are only supported from MP devices with Softphone Support set to

"Client", and from the Softphone Master device.

Softphone devices may make calls to an external SIP/VoIP provider if this has been configured on the Softphone Master device.

Softphone Set Up Tutorial

1. Install the SECN firmware on your router.
The router will appear on IP address 10.130.1.20

2. Connect to the router and point your browser to the admin page at the above IP address.

3. Go to the Advanced page

4. Scroll down to the Asterisk section and tick the Enable Asterisk box.

5. Select 'MASTER' from the Softphone Support list box.

6. Go down to the DHCP Server section and tick the Enable DHCP box

7. Scroll down and click on the Save button.
Wait for the page to refresh and check that the settings have been entered correctly.
On the Basic page, check that the IP address of the device has been set to 10.130.1.252

8. Go to the Softphone page and create two new softphone accounts as follows:

Softphone Number: 301
Softphone Name: User1   (this is for display purposes only)
Password: mypassword1

Click on the Save button, wait for the page to refresh, and check that the new entry has been created in the list at the bottom of the page.

Repeat for '302', 'user2', mypassword2'

9. Reboot the SECN device and it will appear on the new IP address 10.130.1.252
Connect to the device at this new IP address.
Go to the admin Advanced and Softphone pages and check that the settings are all ok.

10. Install the CSipSimple app on two suitable Android devices.

11. Connect the Android devices to the wifi Access Point of the SECN router.
Default settings are:
SSID: 'VT-SECN-AP'
Password: 'potato-potato'

12. Set up a newCSipSimple account on the Android device with the following parameters:

Account Name: User1   (display usage only)
User: softph301
Server: 10.130.1.252
Password: mypassword1

13. Check that the account registers correctly.

14. Repeat for the second Android device using account details 'User2', 'softph302', 10.130.1.252, 'mypassword2'

15. Make test calls between the devices by dialling '302' from the first Android device, and '301' from the second device.

5.6   USB File System

The SECN firmware supports USB flash memory storage on devices that are equipped with USB ports.

Examples of these devices include theMP02, TP-Link WR703N, MR3020, MR11U, WR842ND and WDR3500/4300, and GL-iNet devices for which SECN firmware has been ported.

A USB drive with a single partition will be auto-mounted on startup to **/mnt/sda1**

END OF DOCUMENT