

Village Telco
Small Enterprise / Campus Network
SECN-2.0

User Guide





SECN User Guide by T L Gillett is licensed under a
[Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).
Based on a work at www.villagetelco.org.

Acknowledgements

This work would not have been possible without the contributions of many people associated with Village Telco.

In particular I would like to acknowledge the considerable contributions made by Elektra both in providing technical guidance and in building the software, as well as writing the text for sections of this manual.

Much input has also been provided by Keith Williamson, particularly in relation to development of the Softphone Support and DHCP features, and in building many test versions of the firmware.

I would also like to acknowledge the ongoing support and encouragement provided by Steve Song as a founder of the Village Telco project.

Note: This draft document is intended to be read in conjunction with SECN-2.0 firmware.

Table of Contents

1. Introduction.....	1
2. A Simple Mesh Set Up.....	2
3. Example Networks.....	4
4. Setting Up MP Devices.....	6
4.1 Installing the SECN Firmware.....	6
Installing MP Firmware with the Potato-Flash Utility	
Installing with the sysupgrade Utility	
4.2 Minimum Set-up.....	10
Set the br-lan IP Address	
4.3 Set-up Using SECN Web Interface.....	12
Basic SECN Configuration	
Advanced SECN Configuration	
WAN Configuration	
Firmware Upgrade - MP-1 and AR23	
Firmware Upgrade - TP and AR71 Devices	
4.4 Advanced Set-up.....	27
Connecting to the device	
Setting the device Network Addresses	
Modifying Asterisk Operation	
Dial Plan for SIP / VoIP	
5. Overview of SECN-1 Operation	30
5.1 IP Address Range for MPs.....	30
5.2 Batman-Adv Operation.....	31
BATCTL Command	
bat-hosts file	
Batman-adv and Gateways	
5.3 Telephony Operation.....	34
Overview	
Interactive Voice Response (IVR) Commands	
IVR Command Summary	
5.4 Asterisk Operation.....	35
Making Calls to MP Devices	
Debugging Asterisk Operation	
Asterisk and Network Settings	
5.5 Softphone Support.....	39
Setting up the Devices	
Configuration of Softphone Accounts	
Setting up the DHCP Server	
Setting up the Softphone Clients	
Making Calls to and from Softphones	
5.6 USB Extended File System	42
Extended filesystem for additional packages	
Installing web content	
Using a VFAT USB for web content from Windows	

1. Introduction

The VillageTelco Small Campus Enterprise Network (VT SECN) firmware is designed to allow a collection of Mesh Potato (MP) and similar devices (eg various TP-Link 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 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 MP device provides a telephone connection, an Ethernet cable connection, and a WiFi Access Point. TP devices provide mesh nodes without the telephone connection. PCs and other network devices may be connected to the Ethernet port of a mesh device, 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 will '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 either by Ethernet cable to an MP or by WiFi, will be able to acquire a DHCP address on the LAN and connect to the Internet via the router.

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

Each MP device provides a telephone port which may be called from another MP 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.

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 telephone IVR commands (MP only), 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 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 MP 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.

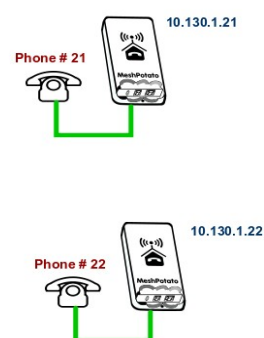
When the MP devices are rebooted, connect a telephone.

Lift the receiver and check for dial tone.

Dial **2662**, enter the pin **1234**, and when the announcement has finished dial **21**. Wait to hear the number being read back, then reboot the device when prompted.

Repeat the process with the second MP, but dial **22** and wait for it to reboot.

The MP devices are now set to IP addresses **10.130.1.21** and **10.130.1.22** respectively. It may be useful to label the devices as '21' and '22'



Step 3

Make a phone call.

After the MP devices have fully rebooted (allow a couple of minutes after the WiFi light starts to flash), 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.

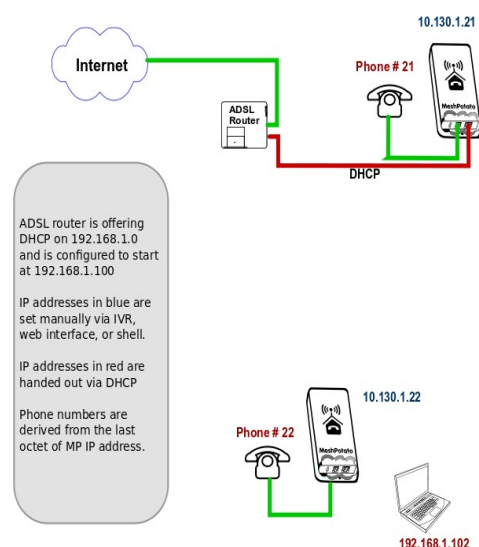
Connect the MP '21' to a spare port on your router with an Ethernet cable. The diagram shows the LAN using an IP address range of **192.168.1.xxx**, but the actual range used will not matter

*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

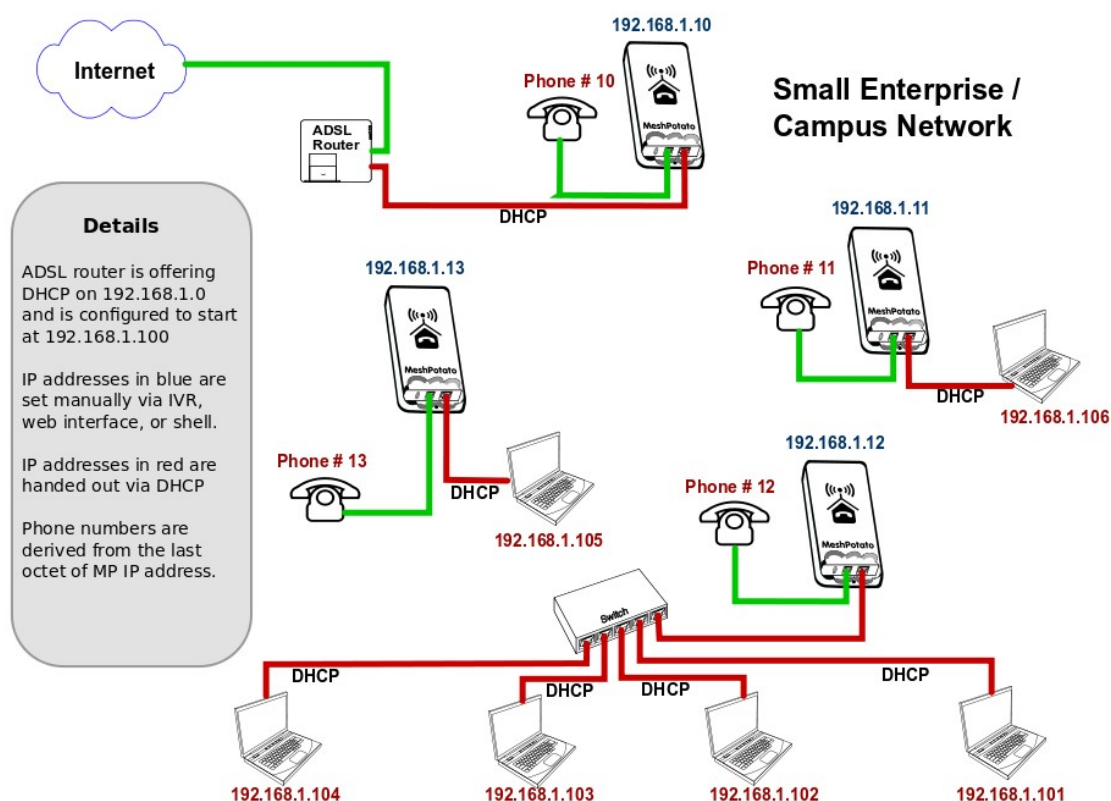
In this network, MP devices have been assigned static IP addresses that are part of the LAN address space, **192.168.1.xxx**, and appropriate Gateway and DNS addresses.

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.

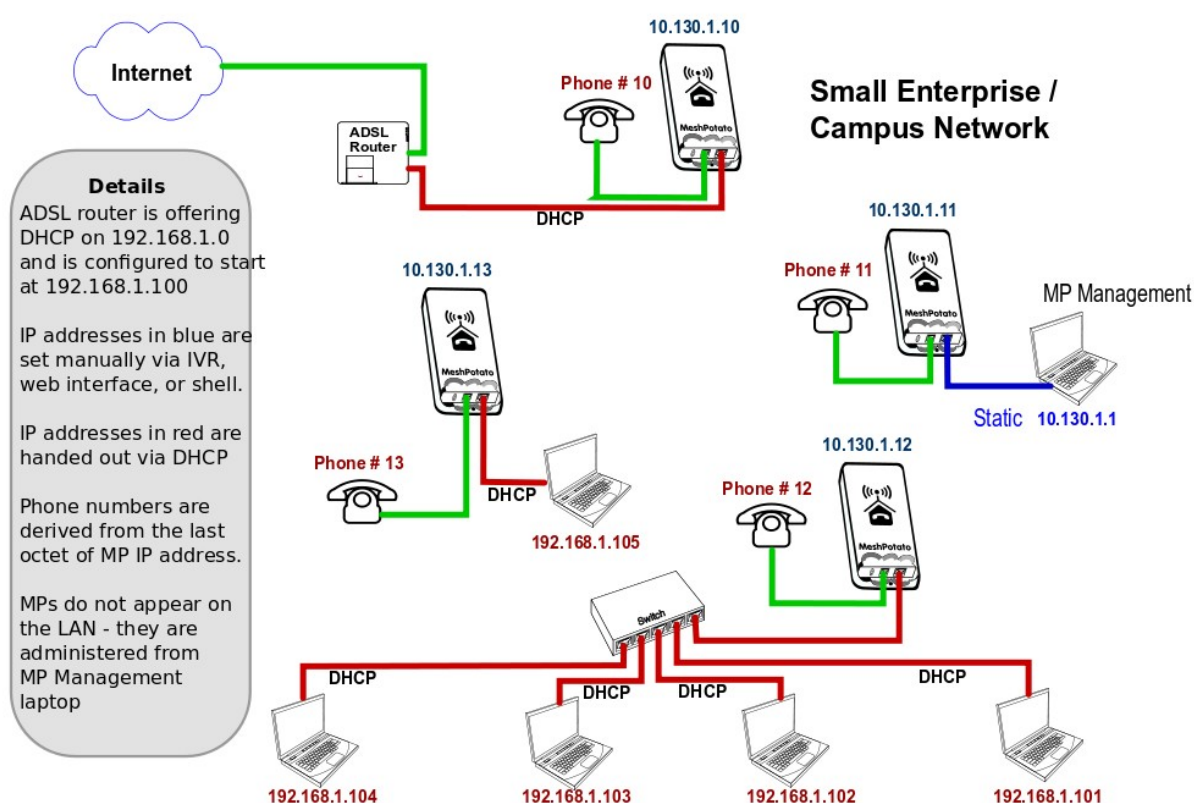
This means that the MP administration interfaces (SECN web interface and *ssh* command line) will not be accessible from workstations connected to the LAN with IP addresses assigned in the LAN address space.

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 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. '10*130*1*10').



4. Setting Up MP Devices

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

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

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

- **Minimum Setup** using telephone Interactive Voice Response (IVR – MP only)
- **Basic Setup** using the SECN web browser interface.
- **Advanced Command Line Setup** using a *ssh* terminal session and command line.

4.1 Installing the SECN Firmware

If you have purchased a new MP-1 device, it may be delivered from the factory with VT firmware version rv233 installed. To operate with the SECN configuration, you will need to flash the MP with the appropriate SECN firmware. Similarly you may wish to upgrade the SECN firmware version.

There are two methods for installing the firmware:

- Use the *Potato-Flash* utility on a Linux PC connected to the MP via Ethernet cable.
- Use the *sysupgrade* utility from the command line on the MP/TP device.

Using the *sysupgrade* utility has the advantage that the firmware can be installed on the MP/TP 'over the air' without the need to connect with an Ethernet cable, which may avoid the need to physically recover the device from an installation.

NOTE: *Early MP devices may not be immediately suitable for flashing with the sysupgrade utility until they have been flashed at least once with the potato-flash utility. This is due to an incorrect memory layout from a different flashing program. If possible, use the potato-flash utility as the preferred way to flash the MP device.*

To check the status of your MP, run the command:

```
cat /proc/mtd
```

The correct output looks like:

```
dev:      size      erasesize  name
mtd0: 00030000 00010000 "RedBoot"
mtd1: 000b0000 00010000 "vmlinux.bin.17" Note that mtd1 contains the Linux kernel
mtd2: 006f0000 00010000 "rootfs"
...
```

An incorrect output may look like this:

```
dev:      size      erasesize  name
mtd0: 00030000 00010000 "RedBoot"
mtd1: 006f0000 00010000 "rootfs" Note that mtd1 does not contain the Linux
kernel
mtd2: 00410000 00010000 "rootfs_data"
...
```

Installing MP Firmware with the Potato-Flash Utility

These instructions assume that you are running Ubuntu or other Linux distribution on your PC. If this is not the case, use one of the other methods to flash the device.

1. Set up the *potato-flash* application on your PC

Download the potato-flash file from:

<http://villagetelco.org/download/utilities/>

Save the file into */usr/local/bin*

Make the file executable:

```
chmod +x /usr/local/bin/potato-flash
```

2. Download the firmware

Download the required firmware from:

<http://villagetelco.org/download/firmware/secn/>

Download the *.squashfs* and *.lzma* files for the required firmware version and save to a working directory.

3. Set up networking on your PC

This step will ensure that *potato-flash* has proper access to the PC Ethernet network port.

Connect the MP directly to your PC with an Ethernet cable **with the MP power off**.

In Ubuntu Gnome desktop, right click on the Network Manager icon and deselect ***Enable Wireless***

Left click on the Network Manager icon and ***Disconnect*** any ***Wired Network*** that is active.

4. Flash the MP

Following is a brief description of the flashing process. Refer to the general instructions in ***Upgrading Mesh Potato Firmware HowTo*** on the Village Telco Wiki for more detail.

- Connect the MP directly to your PC with an Ethernet cable with the MP power **off**
- Execute potato-flash:

```
$ sudo potato-flash eth0 <filename>.squashfs <filename>.lzma
```

- Assuming the Ethernet port on the PC is *eth0*.
- Note that the order of the *.squashfs* and *.lzma* files is mandatory in the command.
- Enter your password when prompted.
- Wait for the program to start looking for the MP device - a series of dots will appear on the screen.
- Switch the power **on** to the MP.
- Wait for the flashing process to complete and for the MP to fully restart.
This may take a couple of minutes. This is a good time to have a coffee.
- Wait for three minutes after the MP WiFi led starts to flash to ensure that flashing process is complete. Some early MP devices may take quite a long time (10mins +) to load and flash.

Sample MP Potato Flash Session

```
$ sudo potato-flash eth0 openwrt-atheros-root-rv238.squashfs openwrt-atheros-vmlinux-rv238.lzma
Reading rootfs file openwrt-atheros-root-rv238.squashfs with 3801088 bytes ...
Reading kernel file openwrt-atheros-vmlinux-rv238.lzma with 720896 bytes ...
Note: The device has to be connected directly (not via switch/hub)
Device detection in progress.....
```

<<< *Turn the power to the MP device ON at this point* >>>

```
.....device detection: non-arp packet received..
Peer MAC: 00:09:45:58:1c:e7
Peer IP : 192.168.1.184
Your MAC: 00:ba:be:ca:ff:ee
Your IP : 192.168.1.0
Connecting to Redboot bootloader
WARNING: UNPLUGGING POWER WHILE FLASHING MIGHT DAMAGE THE BOOTLOADER
HOWEVER: IF YOU SEE NOTHING SHOWING UP BENEATH THIS LINE
FOR MORE THAN A MINUTE, START AGAIN...
A flash size of 8 MB was detected.
rootfs(0x006a0000) + kernel(0x00100000) + nvram(0x00000000) sums up to 0x007a0000 bytes
Setting IP address...
Initializing partitions...
Now uploading kernel...
Sending kernel, 1408 blocks...
Flashing kernel...
Loading rootfs...
Sending rootfs, 7424 blocks...
Flashing rootfs...
Flashing process completed...
Restarting device...
```

Installing with the *sysupgrade* Utility

To install with the *sysupgrade* utility on the MP or TP device, it is necessary to copy the required *.img* file to the MP/TP using the *scp* command from within a *ssh* session on your PC. You may also use *sftp* to browse the unit's file system in Nautilus or with WinSCP.

An MP/TP 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 flashing a new TP device running the original factory firmware, you will need to use the '*factory*' version of the firmware *.img* file, rather than the one *sysupgrade* version of the *.img* file.

This is required only for the first time the device is flashed to the VT SECN firmware. Use the IP address and web interface of the manufacturer's firmware to load the new firmware file.

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)

Alternatively you may set the MP device address to work on your LAN. Connect a telephone to the MP and dial the IVR command **C-O-N-F** (2663) and follow the prompts to set the IP number to one that lies in your normal LAN address range and is not already in use. The device will then reboot. Connect the MP device to an Ethernet port on your LAN and it will be accessible by any PC on the LAN.

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

```
scp ./openwrt-atheros-root-rv287.img 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 ./<filename>.img
```

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 setting after the flash. This may be an issue for remotely accessed devices – see later section for discussion on this.

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 **ssh** on the default LAN or Fallback IP addresses.

You may also use the IVR **C-O-N-F** (2663) command to change the MP device address to work on your LAN.

4.2 Minimum Set-up

The Minimum Set-up process uses the telephone IVR facility to simply set a unique IP address for the br-lan bridge interface in order to allow telephone calls to the device using the IP address. Even with this minimal configuration, the MP mesh network may be connected to a LAN and will provide WiFi and Ethernet connectivity for PCs and other devices to the LAN and Internet.

The default setting for the br-lan IP address when the device is flashed is 10.130.1.20 and you should change at least the last octet of the address in order to make the address unique on the mesh to support telephone dialling.

In a simple mesh arrangement, all MP devices on the mesh are assigned addresses in the same address range (ie only the last octet of the address is changed) so telephone calls can be made to all devices on the mesh with abbreviated dialling using just the last octet of the MP device's bridge IP address.

If you are intending to connect the mesh to a LAN, you may choose to assign addresses from the LAN address space to the MP devices so that they will appear as static IP devices on the LAN.

In this case, just set the IP address of the MP device to the required IP address on the LAN.

You will need to ensure that the address that has been assigned will not be used by any other device on the LAN in order to avoid IP conflicts.

Set the *br-lan* IP Address

Connect a telephone to the MP device and check that you have dial tone.

Use one of the methods below to set the device address.

Set Abbreviated Address:

- Pick up the telephone, check for dial tone and dial 2662
- Enter the IVR Pin number (default 1234)
- Follow the voice prompts and enter the required number for the device as 1 – 3 digits
- e.g 21. This will set the last octet of the MP device IP address e.g. 10.130.1.21
- The number entered will be read back to you and a prompt to reboot the MP.
- The command will fail if the IP is in use (ping) or out of range (.1 to .254).

Set Full IP address:

- Pick up the telephone, check for dial tone and dial 2663 (C-O-N-F)
- Follow the voice prompts and enter the IP number in the form 10*130*1*21
- (For an IP address of 10.130.1.21)
- The number entered will be read back to you and a prompt to reboot the MP.
- The command will fail if the IP is in use (ping).

After the device has rebooted, you should be able to make a call to the device using either the full IP number, or abbreviated dialling using just the last octet of the address.

Note: When the *br-lan* address is set using IVR, the device's *gateway* address will be automatically be set to an address in the same subnet with the last octet set to 1 e.g 10.130.1.1 to ensure correct operation of Asterisk.

If you plan to connect the mesh devices to a LAN and you use this method to set up the MP to have

an address in the LAN address space, then the MP will expect to find your LAN router at the ***x.y.z.1*** address. If your router has a different address, you may use the 4283 (G-A-T-E) IVR command to change the ***gateway*** address as required after setting the IP address.

4.3 Set-up Using SECN Web Interface

Basic SECN Configuration

VillageTelco **SECN Configuration**
 Firmware: Version 2.0 MeshPotato-1
 Date: Wed May 1 10:00:47 AEST 2013

Basic **Advanced** **Status**

Network

IP Address Gateway Find Gateway

WiFi Access Point (WPA1)

Station ID Passphrase Channel

VoIP / SIP Configuration

User Name Password
 SIP Host Dialout Code
 SIP Enable ☐ SIP Status **Not Registered**

Password

Enter Password Repeat Password

Web Server Security and Timezone

Limit IP Address ☐ Enable SSL ☐ Time Zone

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.

Alternatively you may wish to first set the IP address of the MP so that it appears on your LAN subnet by using the phone IVR menu as described in the previous section. If doing so, make sure that you assign an IP address that does not conflict with other devices on the network.

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 Find Gateway button will attempt to locate the Gateway device by sending a DHCP Discover request on the network. If a device responds to the request, then the address of the responding device will be shown in a status message at the bottom on the page. Enter the required Gateway device address in the field and click on the Save button.

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

VillageTelco

SECN Configuration
Firmware: Version 2.0 MeshPotato-1
Date: Wed May 1 10:00:47 AEST 2013

[Basic](#) [Advanced](#) [Status](#)

[Advanced](#) [WAN](#) [Firmware](#)

Time: 10:00:47 up 15:52, load average: 3.40, 1.18, 0.58 TZ: AEST-10

Network

IP Address Gateway
DNS Netmask

Radio

Channel US/Can (11 ch) ☐ Tx Power 1-20
Wifi Mode Chan BW

WiFi Access Point

SSID
Passphrase Encryption AP Connections

WiFi Mesh

IP Address Netmask
SSID BSSID
Gateway Mode Encryption

Asterisk 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

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 [US/Can \(11ch\)](#) checkbox sets the regulatory domain for North America to limit the number of available channels to 11 in accordance with FCC regulations. When this mode is active and channel 12 or 13 is selected, the channel setting will be set to Channel 1.

The [SSID](#) 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 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 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 ath0 interface including: [IP Address](#), [Netmask](#), [SSID](#), [BSSID](#), [Transmit Power](#), and Country Code. These values are written into the configuration files `/etc/config/network` and `/etc/config/wireless`.

The [ath0](#) 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 OSI Layer 2 Batman-adv mesh protocol, and so all MP devices on the mesh may remain on the default IP address.

The [ath0](#) 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 [SSID](#) and [BSSID](#) parameters set the station identification for the MP on the mesh and should be set the same for all devices in a mesh cell. These parameters can be used to set up separate mesh cells if required.

Note: It is a requirement of the current OpenWrt operating system that the [BSSID](#) must commence with an even number eg 02, 04, 06 etc.

The [Tx Power](#) parameter may be used to adjust the power of the device radio transmitter. It is set by default to the maximum value of 17. Normally this should not need to be adjusted but doing so may be useful in certain circumstances such as testing.

The [Encryption](#) control may be used to enable encryption on the mesh, if the device supports it.

The [MP Gateway Mode](#) 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.

The [WiFi Mode](#) control allows selection of the hardware modes supported by the device

eg 802.11G and 802.11N-G.

WiFi Mesh

IP Address

10.10.1.20

Netmask

255.255.255.0

SSID

vt-mesh

BSSID

02:CA:FF:EE:BA:BE

Gateway Mode

OFF

Encryption

OFF

Asterisk Configuration

Enable Asterisk

☒

Softphone Support

OFF

Codec1

gsm

Codec2

ulaw

Codec3

alaw

SIP Enable

☐

SIP Register

☐

Dialout Code

#

SIP Status

Not Registered

SIP Registrar

sip.myhost.com.

User Name

myuser

SIP Host

sip.myhost.com.

Password

Enable Asterisk NAT

☐

NAT External IP

0.0.0.0

DHCP Server

Enable DHCP Server

☐

Authoritative

☐

Starting IP

10.130.1.200

Ending IP

10.130.1.240

Subnet Mask

255.255.255.0

Gateway Router

192.168.1.1

Lease Term (secs)

7200

Max Leases

40

Domain

lan

Refresh

Save

Restart Asterisk

Restore Defaults

Reboot

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 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 there 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.

WAN Configuration

Date: Wed May 1 10:14:41 AEST 2013

Basic **Advanced** Status

Advanced **WAN** Firmware

WAN Configuration

WAN Port: Note: If a WiFi WAN port is selected, Mesh and AP interfaces are disabled on that port.

WAN IP Mode:

Static Network Settings

Static IP: Gateway:

Netmask: DNS:

WiFi WAN Host Settings

SSID: Encryption:

Passphrase:

USB Modem Settings

USB Modem Service:

Vendor ID: Product ID:

Service APN: Dial String:

Username: Password:

PIN: USB Serial Port:

USB Device Detected: **USB2.0 Hub Vendor=05e3 ProdID=0608**

USB Serial Ports Detected

USB Modem Status

WAN Port

WAN Configuration allows the 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**.

Ethernet WAN

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

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

Note: Because the WiFi mesh interface is disabled in this mode, the device will **not** be part of the mesh network. This is a limitation of the OpenWrt wireless drivers at this time.

USB Modem WAN

Selecting ***USB Modem*** for the WAN interface allows the use of common USB modems

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 mode is selected, including the ***SSID*** and ***Encryption*** mode and ***Password***.

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 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.

Firmware Upgrade - MP-1 and AR23

For the Mesh Potato 1 and Ubiquiti devices based on the AR23 chipset, this page allows you to upload the 'root' and 'vmlinux' firmware files in order to reflash the device.

After selecting *Firmware Upgrade* and *Proceed with upgrade*, browse for and select the new firmware files, then select *Upload files to server*.

The files will be uploaded and the flash process started. 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.

[Return to Configuration](#)

Upgrade your Mesh Potato firmware

If you click "Proceed with Upgrade" the upgrade process will begin by closing down any non-essential running programs. This includes telnet, sshd, hostapd, ntpd and others. This is done in order to free sufficient ram for the upgrade. If even you do not proceed after the next stage, you will still need to reboot in order to restore full functionality to the Mesh Potato.

[Proceed with upgrade](#)

Shutting down telnetd...
Shutting down sshd...
Shutting down ntpd...
Shutting down asterisk...
Shutting down wireless AP...
Shutting down misc...
Free memory is...

	total	used	free	shared	buffers
Mem:	13240	12112	1128	0	1016
-/+ buffers:		11096	2144		
Swap:	0	0	0		

Upgrade your firmware

Filename (vmlinux) [Browse...](#)

Filename (root) [Browse...](#)

[Upload Files to Server](#)

Progress

0%

Please be patient. There may be a delay even after the progress bar reaches 100%

Firmware Upgrade - TP and AR71 Devices

For TP Link, Ubiquiti and other devices based on AR71 and compatible chipsets, 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 file and checksum to the device.

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

[Return to Configuration](#)

Upgrade your firmware

Filename:

Ignore Checksum? ☐

Paste checksum:

Progress: 0%

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.

[Return to Configuration](#)

Upgrade your firmware

Filename:

Ignore Checksum? ☐

Paste checksum:

Progress: 100%

You uploaded **openwrt-ar71xx-generic-tl-wr703n-v1-squashfs-sysupgrade.bin**.

The checksum of the uploaded file is: c8904bb9a201b99969734c2c74194900
 The checksum you submitted is: c8904bb9a201b99969734c2c74194900
 Congratulations your checksums match. The file uploaded correctly.

Preserve existing configuration?
☐ Yes
☒ No

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.

4.4 Advanced Set-up

Advanced Set-up utilises access to the 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 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 [255.255.255.0](#)

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 MP)
uci commit network
```

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

```
config 'interface' 'lan'
    option 'type' 'bridge'
    option 'ifname' 'eth0 bat0 ath1'
    option 'proto' 'static'
    option 'netmask' '255.255.255.0'
    option 'gateway' '10.130.1.1'                # Default router address
    option 'dns' '8.8.8.8'
    option 'ipaddr' '10.130.1.xxx'               # Where xxx is unique to each
device
```

Setting the **ath0** IP Address

You may wish to change the **ath0** IP address, however this is not required for basic mesh operation.

From the command line:

```
uci set network.wifi0.ipaddr=10.130.1.xxx      (Where xxx is unique to each MP)
uci commit network
```

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

```
config 'interface' 'wifi0'
  option 'ifname' 'ath0'
  option 'proto' 'static'
  option 'ipaddr' '10.10.1.xxx'
  option 'netmask' '255.255.255.0'
  option 'mtu' '1527'
```

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: (MP file example)

```
config 'mesh' 'accesspoint'
  option 'wpa_key_mgmt' 'WPA-PSK'
  option 'encryption' 'WPA1'
  option 'ssid' 'VT-SECN-AP'
  option 'passphrase' 'potato-potato'
  option 'ap_enable' '1'
```

NOTE: On the MP device running SECN-1.1 firmware, the secn config file parameters are used to automatically generate the hostapd configuration file. Do not edit the hostapd configuration file as it will be overwritten on startup or on use of the web interface.

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' '#'
    option 'enable' 'checked'
    option 'register' 'checked'
```

Dial Plan for SIP / VoIP

The dial plan for external SIP / VoIP operation is defined in the configuration include file */etc/asterisk/potato.extensions.conf* as follows:

```
; Send incoming calls to the MP
exten => s,1,Dial(MP/1)
; Make outgoing calls using [sipaccount] details
; Dial # for access, and then required number string
exten => _#.,1,Dial(SIP/${EXTEN:1}@sipaccount,120,r)
```


5. Overview of SECN-1 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/ath0` and `wlan0-1/ath0-1`, are set up on the wireless interface `wifi0`.
- Batman-adv is configured to run on the `wlan0-1/ath0-1` interface using the `batctl` command and generates the `bat0` interface.
- The second wireless interface, `wlan0/ath0`, is set up to operate as a WiFi access point.
- The `bat0`, `wlan0/ath0` and `eth0` interfaces are bridged (`br-lan`) together in each MP and assigned a static IP address, and thus, due to the operation of the mesh via `bat0`, all the `ath1` 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 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 telephone IVR, 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-1 firmware **ath0** is assigned to the batman-advanced kernel module. **ath0** is the wireless interface operating in multipoint-to-multipoint mode (ad-hoc).

Because batman-adv operates entirely on MAC layer (OSI layer 2), **wlan0-1/ath0-1** 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/ath0-1** on. To sum it up: **ath0** is the link-local transport interface for the batman-advanced 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/ath0** and **eth0**.

eth0 is the LAN port of the MP, and **wlan0/ath0** is an access-point interface, operating as a Master in WiFi infrastructure mode (as opposed to Client mode used e.g. by a laptop or smartphone)

Hence all **eth0** and **wlan0/ath0** interfaces in all devices running the SECN firmware are part of one big wireless bridge. The **ath0** 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/ath0**, **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/ath0** 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

Amongst performance improvements and faster handover of clients, the batman-adv package for the MP now supports configuring advanced batman-adv gateway and gateway client parameters via UCI.

Note: You only 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

MP 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).

Interactive Voice Response (IVR) Commands

The MP Asterisk configuration includes several telephone extension numbers that allow interaction with the device using Interactive Voice Response (IVR) system. These numbers include:

2661		Read out the mesh wireless interface IP address
2664		Read out the bridge (br-lan, eth0, wifi AP) network interface IP address
7774	RSSI	Read out the rssi signal strength
2426	CHAN	Set wireless channel
2662		Set the unique network IP address of the MP device - Last octet.
2663	CONF	Set the unique network IP address of the MP device - Full IP.
4283	GATE	Set the IP address of the network gateway used by the MP device.
6749	MPGW	Set the mesh batman-adv gateway mode of the MP device.
7466	PINN	Set IVR PIN number. Default pin is 1234
9434	WIFI	Set WiFi passphrase.
3427	DHCP	Enable DHCP temporarily on br-lan to offer Fallback IP.
9322	WEBB	Enable / Disable the web interface
73738	RESET	Restore factory default configuration settings.
9999		Restart Asterisk.

IVR Command Summary

Commands which change the system configuration require the entry of the IVR PIN number for security. The initial IVR PIN number is set to 1234 This should be changed before deployment.

Commands which have a variable number of input digits will wait for a timeout period after the last digit has been input to complete the command. The command may be terminated immediately by keying in the # digit after the last command digit has been entered.

Commands which require the MP device to be restarted to take effect (e.g. network settings) will include a message advising this fact.

The 2661 and 2662 commands simply read out the IP addresses used by the MP device on the mesh and on the wifi and ethernet network carried on the mesh, respectively.

The RSSI command 7774 will read out the signal strength of neighbouring MP devices. This is intended to assist with adjusting the MP device's location and orientation for best signal from its neighbours on the mesh.

If the mesh has batman-adv gateways set up the RSSI command will list the signal strength values for each neighbour which is selected as a next hop towards a gateway as follows:

Gateway nexthop ... 1 ... 34, Gateway nexthop ... 2 ... 22,

In the absence of gateways the RSSI command will read out the signal strength values for all

neighbours as follows:

Neighbour 1.....36, Neighbour 2.....42, Neighbour 3.....28

Other useful terminal commands for monitoring signal strength are:

wlanconfig ath0-1 list	Lists signal data for nearby devices on the mesh.
wlanconfig ath0 list	Lists signal data for devices attached to the MP's WiFi AP.
batctl o	Lists nearby devices on the mesh.
batctl gw server	Enable batman-adv gateways on the fly

The CHAN command 2426 sets the wireless channel used for the mesh and wifi interfaces.

The CONF command 2663 is used to set the unique network address of the MP device using the full IP number. The 2662 command changes only the last octet of the IP address. If the MP device is attached to a network and the specified IP address is already in use, the commands will fail.

The GATE command 4283 sets the IP address of the network gateway that the MP can use to access IP addresses beyond the local network, such as Internet addresses.

The MPGW command 6749 sets the batman-adv gateway mode of the MP. This setting is used to assist with efficient routing of traffic on the mesh. If more than one MP on the mesh is connected to a gateway, these MP devices should have their gateway mode set to Server, with other MP devices set to Client. If only one MP device on the mesh is connected to a gateway then it is useful to announce this device by setting its gateway mode to Server.

The PINN command 7466 sets the four digit IVR PIN number, which should be changed from the default 1234 before the device is deployed in the field.

The WIFI command 9434 sets the encryption passphrase used for secure wifi access as a numeric string. A minimum of eight characters is required and the passphrase should be changed from the default before field deployment.

The DHCP command 3427 activates a DHCP server temporarily on the device so that if you connect a PC via Ethernet or WiFi it will be automatically given an IP address corresponding to the MP Fallback address. This avoids having to set up a static IP on the PC to connect. The facility can be activated and de-activated with this command, and it is deactivated automatically on a reboot.

The RESET command 73738 restores the device to the original factory default settings.

The Restart Asterisk command 9999 can be useful to ensure that the telephony sub-system is initiated correctly after the mesh network starts up and Internet access becomes available for registering external SIP providers. Restart time for Asterisk is a few seconds, after which dial tone will be available.

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 default Display 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 MP's 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.

When the MP device's unique IP address is set from the IVR, the Gateway addresses will be set to be in the same IP subnet with the final octet set to '1' e.g. 10.130.1.1

By default, the IVR function will set the DNS address to a public server address at 8.8.8.8

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. Call from MP at **192.168.1.32** to MP at **192.168.1.22** on the mesh network.

```
MP-32*CLI>
-- event_offhook
--   AST_STATE_DOWN:
-- start mp_new
-- event_dtmf 2
-- event_dtmf 2
-- event_digit_timer
--   extension exists, starting PBX 22
-- Executing [22@default:1] Dial("MP/1", "SIP/4000@192.168.1.22") in new stack
```



```
-- Called 4000@192.168.1.22
-- SIP/192.168.1.22-00587578 is ringing
-- Asked to indicate 'Remote end is ringing' condition on channel MP/1
MP-32*CLI>
```

2. Call to a PSTN number 0733991234 via SIP / VoIP Service

```
MP-32*CLI>
-- event_offhook
--   AST_STATE_DOWN:
-- start mp_new
-- event_dtmf #
-- event_dtmf 0
-- event_dtmf 7
-- event_dtmf 3
-- event_dtmf 3
-- event_dtmf 9
-- event_dtmf 9
-- event_dtmf 1
-- event_dtmf 2
-- event_dtmf 3
-- event_dtmf 4
-- event_digit_timer
--   extension exists, starting PBX #0733991234
-- Executing [#0733991234@default:1] Dial("MP/1", "SIP/0733991234@sipaccount|120|r")
-- Called 0733991234@sipaccount
-- Asked to indicate 'Remote end is ringing' condition on channel MP/1
MP-32*CLI>
```

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`

By default there are ten accounts set up for softphones defined as `softph300` through `softph309`

Once assigned to particular attached softphone devices, these devices may be called using their three digit numbers 300 through 309.

The list of softphone accounts may be extended as required, and the individual passwords changed as required by manually editing the configuration file.

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

It has been found for example that SipDroid will operate correctly only when ulaw is the only allowed codec.

A section of the `/etc/asterisk/softphone.sip.conf` file is shown below for reference.

```
[softph300]
type=friend
secret=Pa55uu0rd300
context=default
host=dynamic
disallow=all
;allow=gsm
allow=ulaw
;allow=alaw
dtmfmode=rfc2833
qualify=yes
canreinvite=no
nat=yes
```

Setting up the DHCP Server

Telephony on the SECN-1 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 a 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 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

For a Sipdroid client, the setup is as follows:

1. Start up Sipdroid and go to the Sipdroid settings.
2. Create a SIP account with Authorization Username set to one of the account entries in the file **softphone.sip.conf** (e.g. softph300),
3. Set the Password to match the account entry e.g. "Pa55uu0rd300"
4. Set the Server (or Proxy) to the IP address of the Softphone Master MP (ie .252 on the sub net)

Sipdroid should show successful registration to the softphone server.

The screenshot shows the Sipdroid settings interface. At the top, there's a status bar with signal strength, Wi-Fi, battery, and time (1:01). Below the status bar, the title bar says 'SIP Account'. The settings are as follows:

Authorization Username	▼
Password	▼
Server or Proxy	▼
Domain	▼
Username or Caller ID	▼
Port	▼
Protocol	▼

Additional text visible in the form:

- Server or Proxy: pbxes.org
- Domain: Leave empty if same as server
- Username or Caller ID: Leave empty if same as authorization username
- Port: 5061
- Protocol: TCP

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.

5.6 USB Extended File System

The SECN-1.1 firmware supports additional USB flash memory storage on devices that are equipped with USB ports. Examples of these devices include the TP-Link WR703N, MR3020, MR11U and WR842ND devices for which SECN-1.1 firmware has been ported.

USB drives on these are automounted to **/mnt** as normal unless they are labelled with one of two special volume names: SECN-Extended and WEBSITES. These labels enable two special purpose USB configurations which are used to support additional installed program packages and local web server content for the SECN-1.1 firmware.

Extended filesystem for additional packages

The first pre-defined USB configuration requires the USB drive to be formatted as ext3 and have a volume label of "SECN-Extended". Formatted and labeled this way, the USB drive will be automounted to **/user** instead of **/mnt**

There is a file "**SECN-extended.tgz**" available with the firmware which contains an extended filesystem for the device, including a pre-installed copy of Asterisk configured for use with SECN to support telephony in the same way as the MP-01 devices, including softphone support, but without the built-in ATA.

To set up a USB memory for this configuration, format the USB as ext3 e.g.

```
$ mkfs.ext3 /dev/sda1
```

then label the drive "SECN-Extended" so that it gets automounted under **/user** e.g.

```
$ e2label /dev/sda1 SECN-Extended
```

Note: PLEASE be sure that you run mkfs only on your intended USB drive.

A good way to check is to run:

```
$ cat /proc/partitions
```

and verify the drive's device node.

Alternatively you may use an application such as Gparted to format and label the USB device.

After formatting and labelling the USB flash drive, unpack the "**SECN-extended.tgz**" file into the root of the drive. The extended filesystem drive is now ready for use on the TP-Link SECN 1.1 device. With the TP-Link device turned off, insert the USB flash drive, and power up. If you have followed the steps correctly, the USB drive will be automounted to **/user**.

Simply enter the mount command to verify.

Note: As of this writing, due to a bug in the OpenWRT automount feature, inserting the above drive in the TP-Link device while it is running will result in it being mounted to **/mnt** instead of **/user**. This won't hurt anything, but until you reboot, the features available on the extended filesystem won't be available due to the incorrect mount point.

Installing additional packages

Other packages may be installed into this flash memory space with the command:

```
root@MP-2:/# opkg install -d usb <package-name>
```

Installing web content

There is a directory called **/websites** on this USB ext3 file system which may be used to store web content.

This directory appears as **/user/websites** and is symlinked to **/www/websites** on the device, so the content may be accessed through the web server at:

`http://<ip-address>/websites`

Using a VFAT USB for web content from Windows

The second pre-defined USB configuration is formatted as the normal FAT32 (vfat) file system and has a volume label of "WEBSITES". This was done to more easily allow Windows users to capture websites to a USB drive since Windows support of the ext3 formatted drive is limited.

This volume is mapped to **/www/websites2** and so the web content will appear at:

`http://<ip-address>/websites2`

If you want to simply capture websites on a FAT32 USB drive (vfat), give it a volume label of "WEBSITES" and it will automount at boot up to **/www/websites2**.

To capture websites on a USB drive under either Linux or Windows, a good free utility is HTTrack Website Copier.

There are both Linux and Windows versions at: <http://www.httrack.com>

END OF DOCUMENT