NTNU – Trondheim
Norwegian University of
Science and Technology

Utilizing Mesh Potatoes in Emergency Situations

Esther Bloemendaal & Ida Malene Hassel Øveråsen

Submission date: June 2014
Responsible professor: Norvald Stol, ITEM
Supervisor: Sjur Eivind Usken, Aarbakke Innovation AS

Norwegian University of Science and Technology
Department of Telematics

Abstract

The Village Telco organization aims to provide affordable communication by means of data and voice services where no other companies are able or willing to do so. Village Telco provides a “plug-and-play” solution with low cost voice and data service. This solution is delivered using an inexpensive fixed mesh WiFi delivery system called Mesh Potato. Village Telco’s solution can be applied anywhere in the world where people wish to take control of their own communications infrastructure. Mesh Potato networks can be deployed either as a stand-alone solution or as an extension to existing technologies. Village Telco’s solution has been deployed in several countries around the world. The installed communities vary from 10, to several hundreds of Mesh Potatoes.

We directed our studies toward the use of Mesh Potatoes in mobile situations. We have looked at different scenarios covering everything from emergency situations and natural disasters, to festivals and temporary refugee camps. Keith Williamson, a Village Telco volunteer, has created a "go box" using the first generation of the Mesh Potato. We wanted to take his solution further and developed a mobile and stand-alone kit that could be used in all the different scenarios mentioned. The prototype we developed is slightly different from the "go box". We have used the second generation Mesh Potato and the box includes everything necessary for quick roll-out; solar panel, battery, different cables and easy to use manuals for configuration.

We established that many of the descriptions found on the Village Telco wiki were not clear and difficult to use. Hence a big part of our work consisted in simplifying these descriptions. We created manuals for connecting the Mesh Potato to different uplinks in order to provide Internet access to the network. Four test persons, both with and without technical knowledge, tested the manuals. The test process gave us valuable feedback, which led to improvements in the manuals. We have looked at the process of roll-out, and stated possible simplifications and improvements in order to make the roll-out as quick as possible. Hence we have named our solution the Quick User-friendly Internet-providing Communication Kit (QUICK) box.

We believe that our work and theoretical research has contributed to and enriched the Village Telco community. Our prototype can be further developed and introduced to relief organizations as well as to others who express an interest in a mobile communications kit.

Sammendrag

Village Telco er en organisasjon som har som mål å tilby en billig "plug-and-play"-løsning for data- og taletjenester på steder hvor ingen andre har muligheten, eller er villig til å tilby det. Denne løsningen blir levert ved å benytte et rimelig "fixed mesh WiFi" leveringssystem kalt Mesh Potato. Village Telco sin løsning kan bli anvendt hvor som helst i verden der mennesker ønsker å ta kontroll over sin egen kommunikasjonsinfrastruktur. Mesh Potato nettverk kan bli distribuert enten som en frittstående løsning, eller som en utvidelse til en allerede eksisterende teknologi. Village Telco sine eksisterende distribusjoner inneholder alt fra 10 til flere hundre Mesh Potatoes.

Vi har rettet vårt arbeid mot bruken av Mesh Potatoes i mobile situasjoner. Vi har sett på forskjellige scenarier, alt fra krisesituasjoner og naturkatastrofer, til musikkfestivaler og midlertidige flyktningleirer. Keith Williamsom, en av de som jobber frivillig for Village Telco, har tidligere laget en boks omtalt som "go box". I denne boksen benyttes den første generasjonen av Mesh Potato. Vårt ønske var å videreutvikle denne løsningen, og lage en mobil og frittstående løsning som kan bli brukt i alle de tidligere nevnte scenarier. Prototypen vi har laget er noe annerledes fra Williamson sin "go box". Vi har benyttet den andre generasjonen av Mesh Potato, og vår boks inneholder alt som er nødvendig for at den skal kunne rulles ut raskt; solcellepanel, batteri, nødvendig kabler og brukervennlige manualer for konfiguering og oppsett.

Vi har fastslått at mange av brukermanualene/beskrivelsene som finnes på Village Telco sin wiki er lite forklarende og vanskelig å forstå. Dermed ble en stor del av vår opppgave å forenkle disse beskrivelsene. Vi har laget manualer som beskriver hvordan man kobler en Mesh Potato til forskjellige aksessnettverk for å få Internettilgang. Fire testpersoner, både med og uten god teknisk forståelse, har testet manualene. Testprosessen ga oss verdifulle tilbakemeldinger, og dette førte til forbedringer av manualene. Vi har sett på prosessen rundt utrulling av boksen vi har laget, og kommet med forslag til hvordan denne prosessen kan utrulles raskest mulig. Vi endte derfor med å kalle løsningen vår for "QUICK" boks.

Vi tror og mener at vårt arbeid og forskning har bidratt positivt til Village Telco-samfunnet. Vår prototype kan videreutvikles og introduseres for hjelpeorganisasjoner, og for andre mennesker som har en interesse av denne mobile kommunikasjonsløsningen.

Preface

This study was carried out as a Master's thesis on behalf of the Department of Telematics (ITEM) at the Norwegian University of Science and Technology (NTNU), in cooperation with Village Telco. This report is the final result of our Master's thesis and is worth 30 ECTS points. The study was conducted between January and June 2014. The project description was outlined in cooperation with our supervisor Sjur Eivind Usken from Aarbakke Innovation AS.

We would like to thank Sjur Eivind Usken who has guided us throughout this period, and contributed with helpful ideas, feedback and support. We would also like to thank our professor Norvald Stol for his feedback and support. We would also like to thank the Village Telco community, especially Steve Song and Keith Williamson, for taking the time to answer our questions and for helping us along the way. Also a thanks to Marte Berg Innset for the collaboration on the background chapter. Finally, we would like to thank everyone who helped us test the prototype of the QUICK box.

Trondheim, June 4, 2014

Esther Bloemendaal

Ida Malene Hassel Øveråsen

Contents

List of Figures

List of Tables

List of Acronyms

2G Second Generation of Mobile Telecommunications Technology.

3G Third Generation of Mobile Telecommunications Technology.

4G Fourth Generation of Mobile Telecommunications Technology.

ADSL Asymmetric Digital Subscriber Line.

AODV Ad hoc On-Demand Distance Vector.

AP Access Point.

ATA Analog Telephony Adapter.

B.A.T.M.A.N. Better Approach To Mobile Adhoc Networking.

CDMA Code Division Multiple Access.

DSL Digital Subscriber Line.

FXS Foreign eXchange Station.

GSM Global System for Mobile Communications.

IME Information Technology, Mathematics and Electrical Engineering.

IP Internet Protocol.

ISDN Integrated Services Digital Network.

ISIF International Society Innovation Fund.

ISOC Internet Society.

ISP Internet Service Provider.

ITEM Department of Telematics.

IVR Interactive Voice Response.

kbit/s Kilobit Per Second.

LAN Local Area Network.

MANET Mobile Ad hoc Network.

Mbit/s Megabits Per Second.

MNO Mobile Network Operator.

MP Mesh Potato.

MP01 Mesh Potato Version 1.

MP02 Mesh Potato Version 2.

MR Mesh Router.

M.Sc. Master of Science.

NGO Non-Governmental Organization.

NRC Norwegian Refugee Council.

NTNU Norwegian University of Science and Technology.

OLSR Optimized Link State Routing Protocol.

P2P Peer-to-Peer.

PLMN Public Land Mobile Network.

POTS Plain Old Telephone Service.

PSTN Public Switched Telephone Network.

QUICK Quick User-friendly Internet-providing Communication Kit.

SECN Small Enterprise/Campus Network.

SIP Session Initiation Protocol.

SPUD Simple Unified Dashboard.

SSH Secure Shell.

SSID Service Set Identification.

TTL Time To Live.

VoIP Voice over Internet Protocol.

VSAT Very Small Aperture Terminal.

WISP Wireless Internet Service Provider.

WMN Wireless Mesh Network.

Chapter 1
Introduction

1.1 Motivation

Until now the Mesh Potato has mainly been permanently deployed in villages where the existing telecommunications systems are limited, non-existent or too expensive. In many scenarios there is a need for a solution that can easily and quickly provide people with telephone communication and Internet access. It may be necessary to communicate both within a community and with the outside world. The use of Mesh Potatoes as a mobile solution has not yet been fully explored. There are many scenarios where it would be useful to have a mobile communications solution. These scenarios range from natural disasters, post-conflict situations and temporary refugee camps, to the use at festivals, when a mobile tower is non-functioning or during blackouts. Communications technology, like the Mesh Potato, could be revolutionary in such situations.

With our portable solution, we hope to expand the Mesh Potato's potential. We want to create a solution that is quick and easy to deploy, thus making it more usable in emergency situations. This does not only benefit the locals, but also makes the job easier for relief organizations. We want to provide communication where there currently are none or the existing ones are not functioning. We believe that with the QUICK box time would be spared and lives can be saved.

Easy to use communications are extremely important in crisis situations, both communication within a community and outgoing communication with the rest of the world. Today's society relies on technology to disseminate information efficiently. A mobile communications system therefore creates the opportunity for people to disseminate essential information rapidly, where no other communications system is available.

1.2 Problem Description

As our main problem description shows, the initial approach in our Thesis was to look into refugee camps and how the Mesh Potatoes could be utilized in these situations. We started contacting different Norwegian relief organizations, but found it hard to establish a good connection with any of them. We also saw that the field was enormous and too much for us to grasp with the limited amount of time we had at our disposal. A deciding factor was also that we saw the need to visit a camp in order to understand how refugee camps work, and what the need in terms of communication would be. Everyone we were in contact with maintained that no two camps are the same, or are run in the same way. Often camps are run by the local government, with help from the different relief organizations. Different countries have different laws and regulations, and these also have to be taken into consideration. Since we were unable to establish a cooperation with a relief organization early in the process, we decided to direct our focus in a slightly different direction. We therefore chose to look into the use of the Mesh Potato in different scenarios, with the main focus on quick roll-out and Internet access.

Our main focus is to provide the people with Internet access, since it is crucial to communicate with the outside world during an emergency situation. In order to get the Internet into the mesh network formed by the Mesh Potatoes, at least one of the Mesh Potatoes must be connected to the Internet. The type of access network available depends on the individual location. In some locations there might exist stable landlines, in other places not. Other options could then be to use satellite or cellular networks to provide the network with Internet access.

Our idea is to construct a QUICK box that consists of a Mesh Potato, a rechargeable battery, a charge regulator and a solar panel to charge the battery. All of these components are placed inside a robust and waterproof suitcase, all packed together and ready to go in any situation, at any time, anywhere in the world.

Based on our motivation we researched and conducted a study in order to answer the following research questions:

1. How are the Mesh Potatoes set up?

2. How can a QUICK box be developed? What components, set-ups and configurations are necessary?

3. What type of uplinks can we connect the Mesh Potato to? And how can this be done easily?

4. How to make the roll-out process as quick as possible? What measures can we do in advance to make it as easy and fast as possible to connect the QUICK box to an up-link providing Internet access?

5. In what kind of situations could there be a need for a portable QUICK box?

1.3 Methodology

Our studies have mainly consisted of researching, and looking into the technologies used by the Mesh Potato. Before we could start to answer the questions in our problem description, it was important to obtain knowledge, and an understanding, of the company, Village Telco, how it all started as well as their vision. We conducted informal Skype interviews with several of the founders of Village Telco, which gave us a good insight into how it all started, how Village Telcos are created and what their motivating factors are. When conducting informal conversational interviews, there are no, or few, predefined questions in order to keep the conversation as open and as flexible as possible. Conversational interviews are a good way to establish a personal connection as well as rapidly gather information [4].

In addition to having knowledge about the company and it's vision, it is important to gain an understanding of the technologies which are employed. This provides an opportunity for conducting further research and testing. After this initial theoretical learning process, we started looking at how the Internet can be provided to mesh networks.

The theoretical insight gave us ideas as to how to expand the Mesh Potato's area of usage. We looked at specific scenarios in need of a communications system,

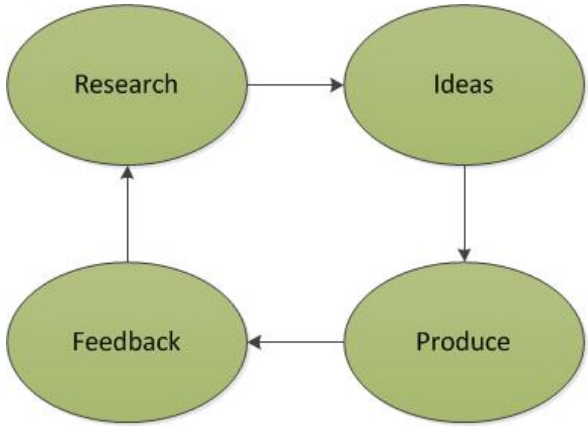


Figure 1.1: Method for constructing the QUICK box.

and this brought forward the idea of creating a QUICK box that could be applied for roll-out in different scenarios. The idea of the box is developed on the basis of previous work conducted by others. This work provided the foundation for our idea and development of the box. The prototype is provided with manuals describing how to connect an Mesh Potato (MP) to different uplinks. These manuals were tested on technical and "non-technical" people. The testing provided us with valuable feedback, which led to an improvement of the manuals.

We also further developed the miscellaneous set-up descriptions provided by Village Telco. This became a big part of our assignment. Many of the existing descriptions are outdated and hard to understand, and also not valid for the second version of the Mesh Potato.

1.4 Limitations

Our main limitation was the amount of time we had available to finish our Masters thesis, since we only had 21 weeks at our disposal. When entering a new field it takes some time to understand the technology used. None of us have much experience with the different technologies used, and it took us some time to learn. Another limitation is money. We tried to get funding, from Engineers Without Borders, to visit an area recently affected by a natural disaster. Unfortunately they had no funding available at the moment. This restricted our research so it became more theoretical and less practical. We were therefore unable to test our solution and manuals on the actual end users. Instead we have conducted tests on people in our local community. These had both technical and "non-technical" backgrounds, all of them from the younger generation. In order to develop our solution further, it should be tested in a more realistic setting, as well as on a wider range of people.

Chapter 2
Background

This chapter is written in cooperation with Marte Berg Innset, a fellow student at NTNU, who also writes her thesis in collaboration with Village Telco. This chapter will describe the invention of Village Telco and the Mesh Potato. Further we will describe some of the Village Telco network deployments and the relevant technologies.

2.1 Village Telco

The Village Telco concept was developed in June 2008 during a workshop at the Shuttleworth Foundation in Cape Town, South Africa. The main goal was to develop an inexpensive system to provide affordable telephone communication in rural and under-served areas [5]. The workshop included participants like open hardware pioneer Dawid Rowe, and the developer of the Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.) protocol, Elektra (for more information about B.A.T.M.A.N. see section 2.5.6) [6]. The purpose of the workshop was to develop a business model, as well as a prototype for a Village Telco. Initially, the idea was to use low cost Voice over Internet Protocol (VoIP) headsets. At that time it was the most viable and convenient way to deliver telephone services to the customers. The wireless VoIP telephones have small antennae, and this would lead to problems in the development. The nodes could not be more than 100 meters away from each other in order to have a reliable connection. This required more nodes in order to cover a desirable area. This factor drastically increased the start-up costs for a village. In order to keep the costs down, it was also important to keep the number of Access Points (APs) down. A mesh network has a larger range, and one suggestion was to use a small mesh device like an Open Mesh AP and connect a Session Initiation Protocol (SIP) phone to it. This solution would solve a lot of the problems regarding range, antenna and number of APs, but the idea was still expensive. The challenge was to create something that would be simple enough to configure and scale by local entrepreneurs with limited technical skills. The two key cost factors that emerged in the scale-up of a Village Telco were the cost of the customer's phone and the power

supply. It was clear that the power supply was the most important factor, and that they had to look at other, and cheaper options regarding the customers phones [6]. During the debating, Rael Lissos took an Analog Telephony Adapter (ATA) and an Open Mesh AP, held them together and said: *"We need these two devices in one"*. This point was the birth of the Mesh Potato, fully based on customized open hardware and open software design. The name "Mesh Potato" comes from combining the words mesh, Plain Old Telephone Service (POTS) and ATA. "Patata" is the Spanish word for potato, hence the name Mesh Potato. The Mesh Potato is a mesh enabled WiFi device, with the possibility of connecting an inexpensive regular phone and IP device [7].

2.2 Mesh Potato

The first generation of the MP is shown in Figure 2.1. This device was designed to be used in rural areas. It can be deployed and run anywhere in the world, relying only on a small, but stable, power supply. The Ethernet port, the Foreign eXchange Station (FXS) port, and the power port are robust and designed to handle all weather conditions, poor power conditions, lightning and static electricity. In addition to this, the Mesh Potato Version 1 (MP01) comes in a waterproof box for outdoor mounting [8].

The MP combines the features of a 802.11bg WiFi router with an ATA [9]. The ATA converts the signal from a standard telephone, into the digital signal needed to connect to the Internet and use the SIP protocol [5]. The device is based on the Atheros chipset and runs OpenWrt (see section 2.5.1 for more information) and B.A.T.M.A.N. (see section 2.5.6 for more information). Each MP01 provides a single fixed telephone line to the end user. The MPs are connected together via a mesh

Figure 2.1: The first generation Mesh Potato, MP01.

WiFi network, and configure themselves automatically to establish a Peer-to-Peer (P2P) network, greatly extending the range of the network over AP mode WiFi. This enables the phone calls to be made independent of landlines and telephone towers, and creates a basis for the "plug-and-play" solution.

As mentioned, the MP is based on open hardware, as well as open software design. Everything is kept open in order for any third party to test, set standards, and give feedback. The key goals during the development was to minimize the binary blobs (a closed source binary-only driver that has no publicly available source code [10]), minimize closed software and make the hardware open.

The mesh network can be connected via a backbone link to the rest of the world using VoIP gateways. No cell phone towers, no landlines, and no telecommunication companies are required. A Village Telco is a community owned telephone service, allowing a local entrepreneur to roll out the Village Telco system only needing a server and the desired amount of MPs. The mesh network is self-healing and self-organizing, meaning if one node goes down, B.A.T.M.A.N. routes the calls through other available nodes in the network [11]. In order to provide Internet access to the mesh network, one of the MPs must be provided with Internet access. The Internet signal is then carried through the network from one Mesh Potato to another.

Mesh Potato Version 2

The first generation of the Mesh Potato has sold more than 2500 copies, and is deployed all over the world. In order to keep up with time, the constant technical development and the demand from the users, a new version of the Mesh Potato was introduced. The second generation became available to users in August 2013. This device comes in a smaller box, as shown in Figure 2.2, and is sold at half the price of the first generation. One of the biggest differences is that the second generation has two Ethernet ports and is built on a new, and faster, chipset. It is also operating on a new and more extensive firmware.

Figure 2.2: The second generation Mesh Potato, MP02.

The second generation comes in three variants, where just the first one, Mesh Potato Version 2 (MP02)-Basic, is available on the market. In May/June 2014 Village Telco will release MP02-Phone. This variant will be almost identical to the MP02-Basic. The only difference is that MP02-Phone will have a FXS daughterboard, which enables the possibility to connect a phone to the MP. Village Telco will also release an advanced variant of the second generation. This MP02 - AWD will be a full outdoor unit which is designed for rugged use and will have a PoE/TL adaptor which will carry voice, data and power. Time of release for MP02-AWD is still unannounced.

2.3 Village Telco Network Deployments

Village Telcos can be found in different places all around the world, from Brazil, Puerto Rico, South Africa and Nigeria, to Nepal. The first Village Telco network was established in Dili in Timor-Leste. This section will present some of the villages that exist today. Figure 2.3 show where some of the Village Telco deployments are located. Since the villages are not deployed by Village Telco itself, but by local entrepreneurs, there does not exist a complete overview of all operating Village Telcos.

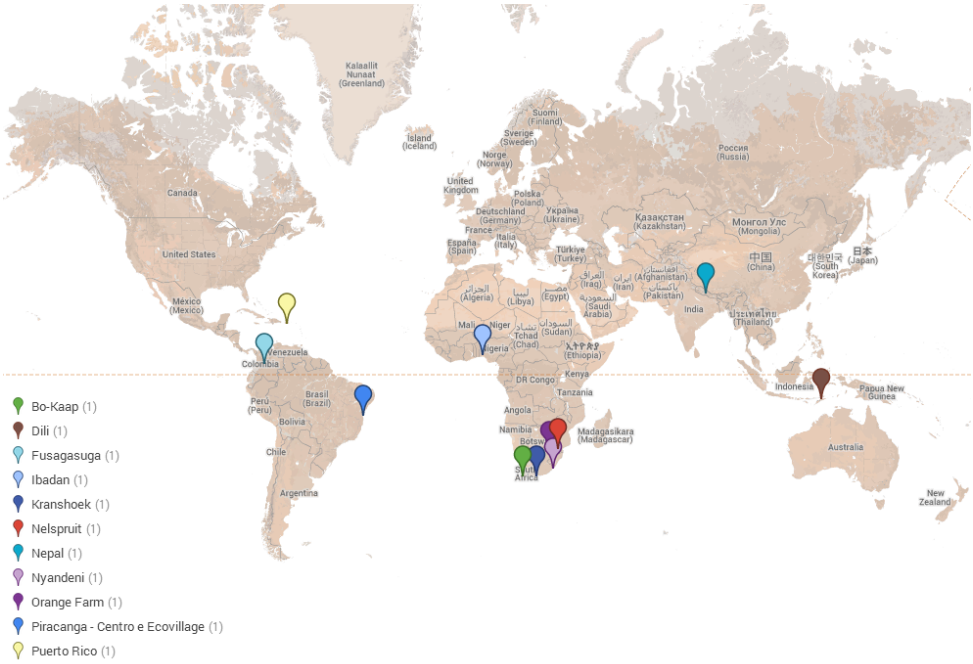


Figure 2.3: World map of Village Telco deployments

The information about the villages that are presented in the following sections is gathered from the Village Telco website [12] and from a questionnaire that was sent out on Village Telco's mailing list in February 2014 by Marte Berg Innset. The full questionnaire is not published due to reasons regarding anonymity.

2.3.1 Dili, Timor-Leste

Dili is the capital of Timor-Leste, one of the poorest countries in Asia [13]. Dili has 193 000 (2010) inhabitants. Over 70% of Timor-Leste's population lives in rural areas [14]. Timor-Leste gained its independence from Indonesia in 2002, but the telecommunications infrastructure was destroyed in the process.

Telecommunications in Timor-Leste

There exists some infrastructure for fixed and mobile telephony in Timor-Leste. However, the services are expensive and the regular Timorese can not afford to use the services on a regular basis. After the independence of Indonesia, Timor-Leste's telecommunications sector has expanded, especially the mobile telephone sector. Figure 2.4 and Figure 2.5 show number of subscriptions/users per 100 people in Timor-Leste for cellular telephony and Internet.

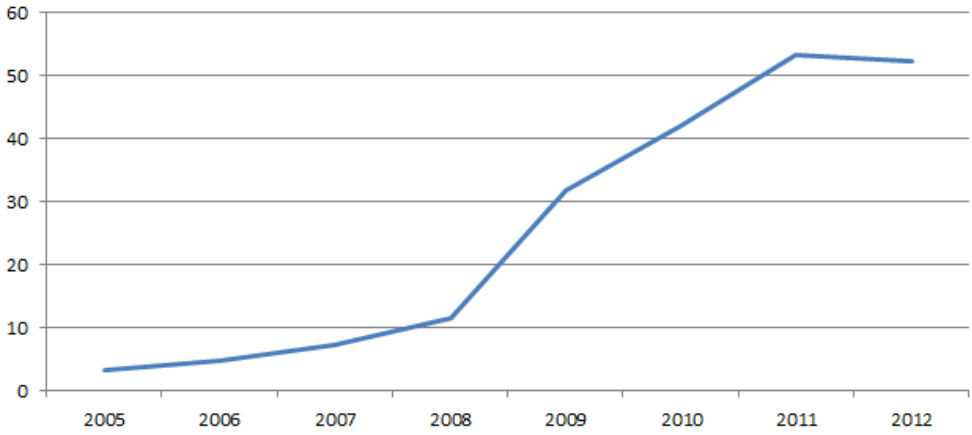


Figure 2.4: Number of cellular subscriptions per 100 people in Timor-Leste

Figure 2.5 shows that less than 1% of the population uses the Internet. The main reason for this is the high costs of the services, in combination with the low income of Timor-Leste's inhabitants.

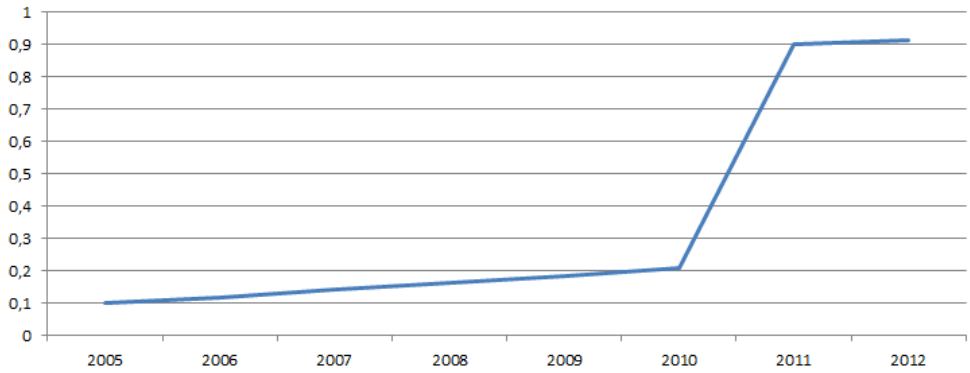


Figure 2.5: Number of Internet users per 100 people in Timor-Leste

Telephony

From 2002 to 2013, Timor Telecom (owned by Portugal Telecom) had a monopoly in Timor-Leste. Portugal Telecom signed a contract with the government in 2002 to invest $29 million to rebuild and operate the phone system, and gave them an exclusive license in the market until 2017 [15]. The contract was renewable, but in 2012 Portugal Telecom agreed with the government to end the monopoly earlier than planned [16]. In 2013 two new competitors entered the market, which led to rapid changes in the marked. In addition, the government is in the process of setting up a new independent regulatory authority for the telecom sector.

Internet

There is only one Internet Service Provider (ISP) in Timor-Leste, Timor Telecom [15]. The Internet traffic is expensive due to the fact that international traffic goes via Very Small Aperture Terminal (VSAT) connections, which also accounts for most of the national traffic [13]. It is not possible to send a Internet Protocol (IP) packet from one side of Dili to the other without sending the packet overseas via VSAT connections.

The Deployment

The Village Telco deployment in Dili is planning to build a 100-node network. The project is a collaboration between Rowotel [1] and Fongtil [2]. The project was funded by International Society Innovation Fund (ISIF) and Internet Society (ISOC) community grants.

[1] A business operated by David Rowe that focus on open telephony software and hardware.

[2] The umbrella organisation for Timor-Leste's local, national and international Non-Governmental Organizations (NGOs).

The project has three main goals [13]:

- Train the inhabitants of Dili to roll out a Village Telco network and educate them in the necessary technologies (mesh WiFi, VoIP, mesh node installation and maintenance).
- Deploy a 100-node Village Telco network to build a local telephone network.
- Use the mesh WiFi network to provide a community IP backbone across metropolitan Dili to encourage local IP traffic and local content.

In May 2012, the project had 60 operating nodes. The network is a public resource, giving anyone in Dili access to the bandwidth. Fongtil both trains people in how to set up the MPs, and maintains the network.

Business Model

The business model for the Village Telco deployment in Dili is based on free internal calls, in addition to pre-paid usage charging.

2.3.2 Orocovis, Puerto Rico

Orocovis is a village in Puerto Rico with about 25 000 inhabitants. Orocovis is a rural and low-income town, the average annually income in the town is less than $14 000. In order so survive, most families require financial assistance in the form of government funding.

In the village there is a landline telephone infrastructure that needs to be repaired and upgraded. The village is situated in a mountainous terrain, which is an obstacle for cellular telephony. Most of the cell phone users have to travel 30 to 40 minutes to get a stable cell phone connection [17, 18].

The Deployment

In 2012, Jose Soto rolled out and funded a Village Telco network in Orocovis. Jose Soto is the president of CoquiTel, a small Wireless Internet Service Provider (WISP). CoquiTel is a project created to improve the infrastructure, especially in the rural areas of Puerto Rico. The desired output of the project was to create and maintain the infrastructure, and simultaneously stimulate the local economy and provide adequate resources for students, patients in the medical care institutions, etc.

The network consists of 146 MPs and is still growing due to the expansion to other villages close to Orocovis [17]. The initial roll-out consisted of 45 MPs, and

took between eight and ten months to set-up. Initially, the main focus of the project was telephony, but later this changed to Internet connectivity. The reason for this change is that the project gained access to a microwave link with large capacity.

Business Model

The business model of Orocovis is based on post-pay unlimited data plans and phone plans. 85% of the service is Internet and 15% is telephony.

2.3.3 Mataffin-Macadamia, Nelspruit South Africa

Mataffin-Macadamia is located in Nelspruit in north-east of South Africa. Mataffin-Macadamia is a secure retirement estate, and the inhabitants are of the middle/upper class. The estate consists of over 250 homes spread across a 17-hectare village.

The Deployment

Mataffin-Macadamia offers telephony and Internet access by using Village Telco's technology [19]. So far, there are 45 MPs installed in the village.

Business Model

Mataffin-Macadamia is a for-profit project. Their business model can be divided in three, and offers:

1. Free internal calls.
2. National and international calls via VoIP at about 35% below incumbent telco (post-pay).
3. Two Internet access levels: Low usage (about $26 per month) and high usage ($49 per month)(post-pay).

2.3.4 Summary Developments

There are several Village Telco networks in the world today. This section has presented three of them. The three villages were chosen due to their differences. The networks are deployed in different type of areas and are used by people from different social conditions. Two of the deployments offers free internal calls, while the last one focuses on Internet connectivity. All the networks, presented in this chapter, are driven by local entrepreneurs with one person as the driving force.

2.4 The Evolution of the Telecommunications Industry

Communication started in ancient times with visual signals, such as smoke signals, called optical telegraphs [20]. The first telephone was produced by Alexander Graham Bell in 1875, and the first regular telephone call was made in 1878 [21]. This section will focus on the evolution of the telephony this century, especially the introduction of VoIP services.

2.4.1 Evolution of Telephony

In the period between 1999 to 2003 telecommunications was one of the leading growth sectors in the world economy [20]. The mobile phone became more popular and cheaper to purchase. The coverage of the Mobile Network Operators (MNOs) expanded.

Up until 2003, when Skype launched their freemium VoIP[3] service, a call was usually done over the Public Switched Telephone Network (PSTN) or the Public Land Mobile Network (PLMN). In 2003, Internet services such as e-mail and instant messaging had existed for several years. However, the household Internet connections did not have the capacity to transfer audio with good enough quality and latency [22]. As the Internet access became faster and more accessible for the end users, VoIP services emerged.

One of the advantages of VoIP services is that international calls can be made without paying toll charges. This had an impact on the pricing of telephone services, and allowed VoIP service providers to charge a smaller amount for international calls than traditional telephony. Another advantage is that IP networks can carry 5 to 10 times the number of voice calls over the same bandwidth than circuit-switched services.

The introduction of VoIP services, such as Skype, forced the traditional telephony providers to change their revenue streams and business models. Telenor[4] changed their pricing strategy from usage charging to flat rate and bundle pricing strategies.

2.5 Relevant Technologies

This section covers some of the most relevant technologies used to develop and run the Mesh Potatoes. In order to understand how the Mesh Potato works, it is important to have a certain knowledge about the underlying technologies.

[3] Real-time transmission of voice signals using the Internet Protocol (IP) over the public Internet or a private data network. Also known as IP telephony.

[4] Telenor dominates the Norwegian market space for telecommunication services.

2.5.1 OpenWrt

OpenWrt is an embedded open-source operating system for routers distributed by Linux [23]. It is extensible and can easily be modified to suit any application, since it offers a file system with a package manager. OpenWrt provides (1) Free and open-source, (2) Easy and free access, and is (3) Community Driven [23]. This means that the source code is free and available to everyone, and that everyone is able to contribute to it.

2.5.2 Telnet and SSH

Telnet is a TCP/IP protocol that enables the opportunity to remotely connect to a computer/device. In order to do this, telnet client software is necessary. The client becomes a virtual terminal, and through command line prompt one can remotely work with files and data [24].

Secure Shell (SSH) offers the same services as telnet, but is a more secure alternative. With SSH all data sent to and from the server is encrypted [25].

2.5.3 Mobile Ad Hoc Networks

Mobile Ad hoc Networks (MANETs) are networks that do not rely on an underlying and fixed infrastructure, in other words "infrastructure-less" (as shown in Figure 2.6). The structure of MANETs change dynamically. Key factors describing MANETs is that they are self-configuring, self-organizing, self-discovering, and self-healing [27]. The members of the network are mobile and free to join, or leave, the network at any time [26]. MANETs are based on multi-hop forwarding. Each node acts not only as a

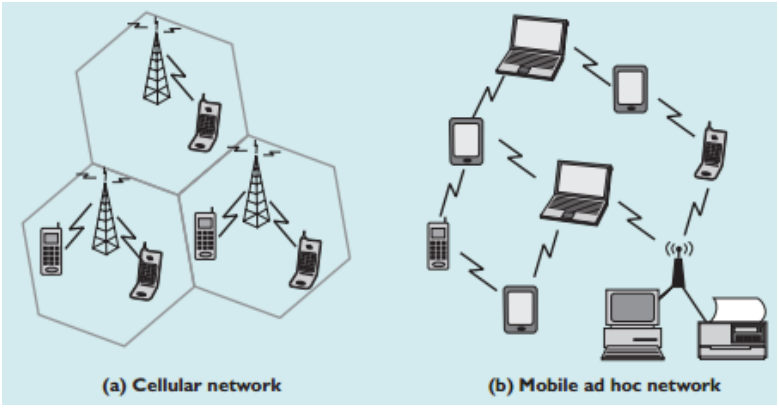


Figure 2.6: Cellular network vs. MANET. This figure illustrates the difference between a regular cellular network and a mobile ad hoc network [26].

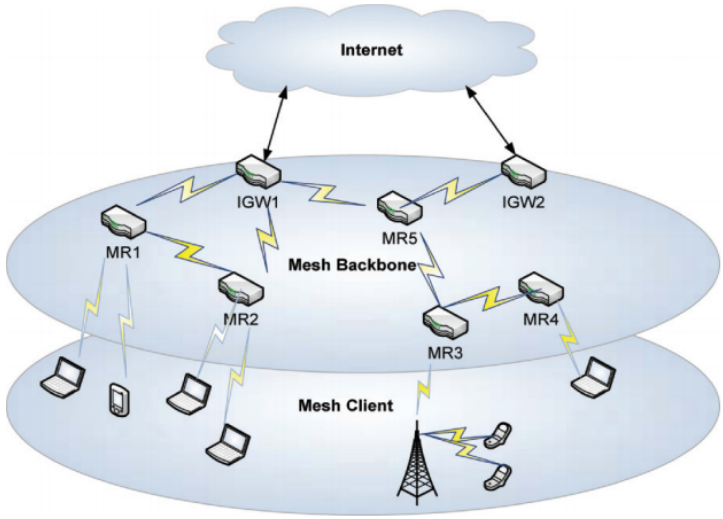


Figure 2.7: Example of a Wireless Mesh Network. This figure illustrates the architecture of a typical WMN [27].

host, but also as a router. The nodes themselves establish and maintain routes, and forward packets to other nodes if necessary. This enables communication between nodes that are originally not within each other's range [26]. MANETs are suited for use in situations where there is no fixed underlying infrastructure. A MANET can operate as a stand-alone solution, but can also be connected to the Internet.

2.5.4 Wireless Mesh Networks

A Wireless Mesh Network (WMN) is a type of MANET [27]. The objective of a WMN is to serve a larger number of users with high bandwidth access. As mentioned before, MANETs are "infrastructure-less" and they have self-configuring, self-organizing, self-healing and self-discovering features. WMNs share all these characteristics, except from the infrastructure part. WMNs are often a collection of routers called Mesh Routers (MRs). These MRs are usually stationary, and can be employed for different use. One MR could, for example, be connected via cable to the Internet, and then become an Internet gateway. This MR can then provide Internet connectivity to the other MRs in the mesh network. A wireless mesh network consists of two parts; the backbone of the mesh (the MR) and the clients of the mesh [27]. An example of a WMN architecture is shown in Figure 2.7.

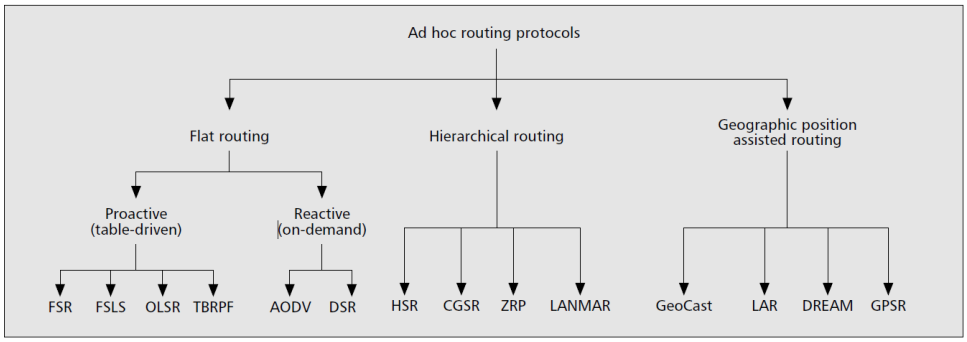


Figure 2.8: Different groups of ad hoc routing protocols [29].

2.5.5 Routing Protocols

Ad hoc networks and mesh networks pose several challenges when it comes to routing and routing protocols. One challenge is that the routing protocols must be able to adapt quickly due to topology changes. It is important that a routing protocol does not cause excessive overhead (extensive use of computer resources). Figure 2.8 shows the different groups of the existing ad hoc protocols. Under the category flat routing, there are two types of routing protocols; proactive and reactive. *Proactive routing protocols* (e.g. OLSR) are table driven [28]. Every network node has a routing table data forwarding. To obtain stability, each node broadcasts and modifies the routing table periodically. Proactive routing protocols are suitable when there are few nodes in the network. The routing table is periodically updated, hence the overhead exceeds the desired value when there are a high number of nodes in the network. Contrary to the proactive routing protocols, *reactive routing protocols* (e.g. AODV) are on demand (meaning they only establish a route when it is requested). Since they are "on demand", the overhead is significantly lower. These protocols utilize flooding. The network is flooded with the Route Request (RREQ) in order to set up the route. The reactive routing protocols do not have an up-to-date routing table like proactive routing protocols [28]. Routes are only set up to nodes they communicate with, and these routes are only kept alive while they are needed [26].

2.5.6 B.A.T.M.A.N

Better Approach To Mobile Adhoc Networking (B.A.T.M.A.N.) is the routing protocol utilized in the networks formed by the MPs. B.A.T.M.A.N. is a proactive routing protocol for wireless ad hoc networks, including MANETs [30]. This protocol was developed as an alternative to Optimized Link State Routing Protocol (OLSR) [31]. As mentioned before, routing protocols must be able to adapt quickly to topology changes. B.A.T.M.A.N. was designed to be a more efficient routing protocol in this

area, since it employs a new method for discovering routes. The nodes in the network broadcast an OGM periodically, as shown in Figure 2.9. An OGM is a Originator Message which contains:

- The address of the node
- Sequence number
- Time To Live (TTL)

The address and the sequence number enables identification of a packet and duplicate detection.

Information about the nodes that are accessible via single-hop or multi-hop are maintained and updated [30]. Every node updates its routing table each time it receives an OGM. The routing table includes information about [31]:

- **Originator Address:** This is the source address of the node that sent the OGM.
- **Current Sequence Number:** The sequence number of the last OGM. This is used to discover if there are any duplicates or any outdated information.
- **Sliding Window:** A list of sequence numbers that is stored for each originator and each previous hop, i.e. for the neighbour node that forwarded or originated the OGM, as shown in Figure 2.9. This is used to decide which next hop is best for each destination.

When a node receives an OGM it will decrease the TTL, and then forward it to the neighbour nodes. The same OGM can arrive at a node, but from different paths. In this case, only the first copy is preserved.

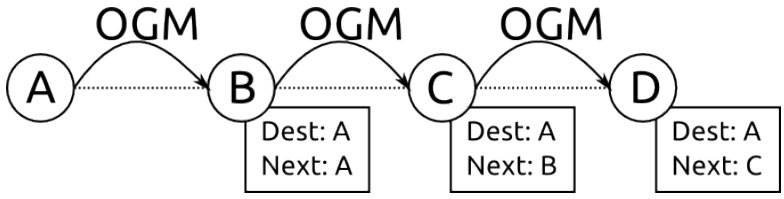


Figure 2.9: Originator Message (OGM) used in B.A.T.M.A.N [31].

Simple Unified Dashboard for mesh networks

Simple Unified Dashboard (SPUD) for mesh networks is a tool for visualization made for B.A.T.M.A.N. mesh networks, and for the users of the networks [32]. SPUD is, like the name indicates, a dashboard based on PHP which is designed to be simple. It communicates with the B.A.T.M.A.N. visualization server. The dashboard makes it possible to monitor the link status of the networks, by displaying real time wireless link status. Other features are client management and customization. The software is written in CakePHP and for visualization SPUD uses Google Maps API 1.3 [32].

2.6 Uplinks

In 2011, the UN declared Internet access a human right [33]. This says something about the extent of the Internet, and the importance of connectivity. Internet access can be provided through different types of uplinks. An uplink connects a device or a Local Area Network (LAN) to a larger network [34]. The type of access network that is available depends of the location. In some places there might exist a stable landline, in other places not. Then an option could be to use cellular networks or satellite. The availability of the different uplinks is not the only thing that varies. The uplink speed and the price also varies from place to place, and between the different types of uplinks. In the following sections, we will look at some of the uplinks available, and how Internet access can be provided for a mesh network.

2.6.1 Internet access via Telephone-line

The most common way of getting Internet access is via a landline. The telephone lines are often used for this purpose, since they can be converted to broadband. Because of this characteristic the landline can be used for phone calls and the Internet simultaneously [35]. The line is usually in the form of twisted pairs (copper lines). These lines support broadband up to 51 Megabits Per Second (Mbit/s) (with VDSL), and are often in the form of ADSL, or other digital subscriber line of type x (xDSL) technologies [36]. Internet access via telephone lines can be provided as a stand-alone solution, or it can be provided together with television or/and phone service. The latter option is usually cheaper. Internet access is highly reliable via landlines in comparison with cellular networks and satellite [37]. We will now describe some technologies used for receiving Internet access via a telephone line; dial-up Internet connection, ISDN, and DSL.

Dial-up Internet connection

Dial-up is an analogue technology that utilizes the telephone line. A telephone wall jack is used as a fixed point of connection, and the computer is connected to a voiceband modem. With this technology, the data is transmitted over the same

frequencies used for phone calls. Hence, if you only have one telephone line, you cannot take a phone call and use the Internet at the same time [38]. The absolute maximum speed is 56 Kilobit Per Second (kbit/s). Along with the digital era, better Internet technologies were introduced; Integrated Services Digital Network (ISDN) and Digital Subscriber Line (DSL).

ISDN

ISDN is a fixed Internet connection, which also utilizes the telephone line. When using ISDN, as with dial-up, a telephone wall jack is used as a fixed point of connection. ISDN utilizes an ISDN terminal adapter instead of a voiceband modem. This ISDN terminal adapter sends out digital signals. The data speed varies between 64 kbit/s - 128 kbit/s. The speed of the data is symmetric, which means upstream and downstream data rates are the same. In contrary to dial-up, ISDN allows voice calls and transmission of data simultaneously. ISDN is faster than dial-up, but the speed is nothing compared to the speed obtained using DSL [38].

DSL

DSL is a digital high-speed technology for Internet access that allows simultaneous voice and data transfer. Like dial-up and ISDN, DSL also utilizes the telephone line. The signals are modulated in order to be transferred on non-voice frequencies. DSL is an always-on technology, and in this way differs from the previous technologies which have been mentioned. Only a small part of the telephone line is used for voice signals. The DSL technology allows utilization of an unused frequency spectrum of a telephone line, and does not convert between analogue and digital signals, hence making it possible to transmit data faster. When the voice and data signals arrive at the telephone company's local switching station, they are separated and routed differently: voice to the regular telephone system and data to the ISP, and then to the Internet. A connection must be within approximately 5 kilometres of a switching station in order for DSL to work. The speed depends on many factors. Data can be transported up to 6 Mbit/s (with a distance of approximately 2 kilometres from the station). The relevant factors that have an impact on the speed is the distance to the switching station, and the quality of the telephone line. As mentioned earlier, there are different types of DSLs. The most common is Asymmetric Digital Subscriber Line (ADSL), where the downstream speed is faster than the upstream speed [38].

2.6.2 Cellular Network Technologies

It is getting more and more common to use cellular technologies for broadband. Around 2011 the number of mobile broadband subscriptions grew to twice as many as the number of fixed-broadband subscriptions. In developed countries it is common to have a fixed-broadband connection, and use a mobile-broadband network in addition

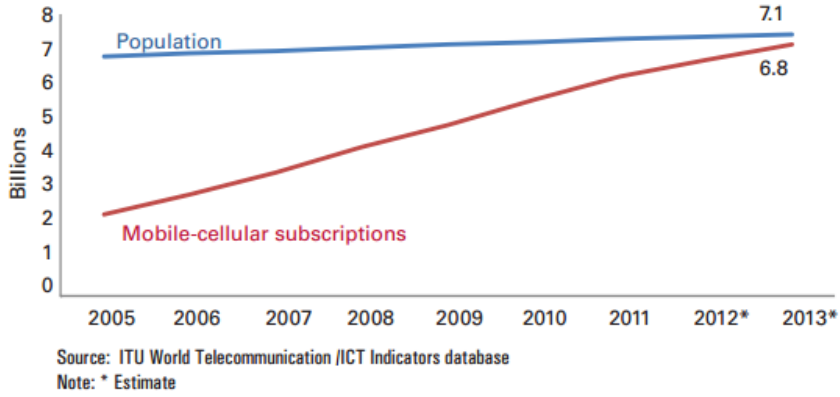


Figure 2.10: Number of mobile-cellular subscriptions The figure shows that the growth of mobile-cellular subscriptions have increased drastically during the last decade, and show that there are almost as many as there are people in the world [39].

to the fixed. In developing countries, on the other hand, it is not a given that access to a fixed-broadband connection is available. In these cases mobile-broadband can be the only method of access available. In 2011, 90 % of the world's population had Second Generation of Mobile Telecommunications Technology (2G) coverage, and 45 % had Third Generation of Mobile Telecommunications Technology (3G) coverage [40]. By 2013, the number of mobile-cellular subscriptions had reached a high level, and were approaching the number of total world population, as shown in Figure 2.10. From 2011 to 2013, the number of mobile broadband subscriptions more than doubled in developing countries [39].

Through mobile network technologies, high-speed Internet access can be provided via portable devices. In order to get mobile broadband, there must be a cellular network (Global System for Mobile Communications (GSM) or Code Division Multiple Access (CDMA)) service available. The key technologies when talking about mobile broadband is 3G and Fourth Generation of Mobile Telecommunications Technology (4G) [41]. With 3G the average speed is 0.5 to 1.5 Mbit/s, and with 4G the average speed is 2 to 12 Mbit/s. These vary, due to different versions of each technology, underlying service and so on. Like with everything else, the actual and realistic speed differs from the peak speed [42].

2.6.3 Satellite

Internet access from satellite is offered by satellite Internet providers [37]. Satellites orbit the Earth, and get their signals from a land-based Internet connection. To get Internet broadband via satellite a satellite dish is needed. The main advantage

of using satellite is that it provides an universally available Internet access [43]. Since it is universally available, it is equipped for use in rural regions where there are no landlines or other options for Internet connection. There are also certain disadvantages in connection with using the Internet via satellite. Since it is a shared medium, privacy concerns arise, and the speed is dependent on simultaneous use. Also the connection can be affected by bad weather, unlike wired connection. Hence satellite is not as reliable as cable.

2.6.4 Summary Uplinks

Table 2.1 sums up the advantages and disadvantages of using the different uplinks described in the previous sections.

Table 2.1: Advantages and disadvantages - Uplinks [1].

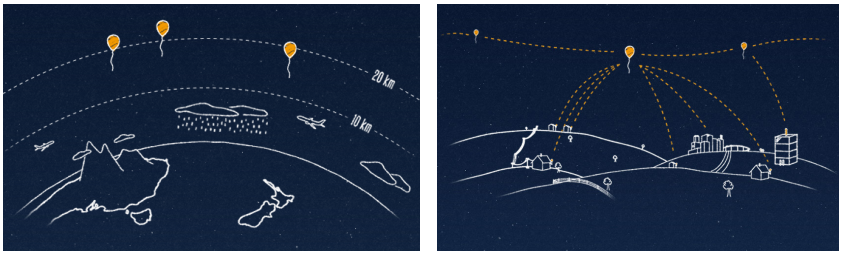
Uplinks	**Advantages**	**Disadvantages**
Landline/xDSL	High reliability, cost effective, good speed.	Low availability in rural areas.
Cellular networks	High availability, fitted for "on the move"-use.	Expensive, slower than xDSL.
Satellite	High availability.	Unreliable, expensive, slower than landline.

2.7 Future Internet Access Methods

Different methods of distributing the Internet is always under development. The uplinks previously described are well established. In many parts of the world these uplinks are not fully developed, or not affordable to the average person. Large technology companies, like Google, are experimenting with different ways of distributing Internet access.

2.7.1 Google's Internet Balloons

Two thirds of the world's population is not connected to the Internet. Project Loon, a Google project, is a network of high altitude balloons travelling in the stratosphere. This network aims to provide cost effective, reliable and inexpensive Internet access for everyone, world wide. The project started in June 2013 as an experiment in New Zealand [44].



(a) The Balloons are situated in the stratosphere. **(b) Connecting to the Internet**

Figure 2.11: Project Loon: Balloon-powered Internet for everyone.

The balloons are 15 meters in diameter. They travel at an altitude of 20 km, in the stratosphere, twice as high as aircrafts and weather, this is shown in Figure 2.11a. At this altitude there are many layers of wind, each varies in direction and speed. By regulating which wind the balloons are flying in, it is possible to control their position, and steer them in the desired direction. Figure 2.11b shows that people can access the Internet shared by the balloons by having a special antenna attached to their house. From this antenna the signal bounces to one balloon which again bounces through the other balloons and down to the local ISPs on Earth. This creates a network in the sky.

A specially designed control system is used in order to control the altitude of the balloons. The system is managed remotely from the ground. By either pumping helium in, or letting helium out of the balloons, one can decide in what layer of air the balloon should be in. Letting helium in or out is not the only way to decide whether the balloon should go up or down, but it is the only way to do so on a huge scale. A GPS is attached to each balloon in order to keep track of the precise locations of the balloons and to record how the winds are changing. Enormous amounts of data are collected in this way, and some of this information is given to meteorologists. The balloons fly at almost the same speed as the wind.

The balloons contain specially designed antennae and radio systems in order to receive signals from Project Loon only, and to achieve high bandwidth over long distances. Satellites stay in the same place and at the same altitude, which means that a satellite dish can be mounted in a fixed position. This is not the case with the balloon antennae, since they are in constant movement, vary in altitude and distance from the antenna. A dish pointing in a fixed direction would therefore not work.

Since the balloons are in constant movement, it is important to make sure that there is always a balloon available and one ready to move in when another moves out, so that the connectivity is always available (can be compared to soft handover in

GSM). Without this feature the project would not be of much value. Every balloon contains information about all the other balloons in order to spread out nicely. Think of it as a flock of birds, they always look at the one next to them and space out accordingly.

The balloon works as a communication tower in the sky. The balloons are solely run on solar power. The solar panels catch the sunlight that is available during the day, as well as charging up the lithium-ion battery to last through the night. In the stratosphere the temperature is -70 degrees Celsius. These extremely cold conditions are not ideal for lithium batteries. In order to make sure that the batteries does not loose their effective capacity, it is important that they are kept warm. The battery pack is insulated to reflect the heat that comes from the other electrical components. When it comes to lifetime, the goal is that the balloons stay alive for 100 days, or 3 laps around the globe.

When balloons are on their way up and down, the air traffic control in the specific country has to be contacted since the balloons are moving through the country's airspace. Project Loon requested permission to land on Norwegian soil according to Teknisk Ukeblad, a Norwegian science magazine. This permission was approved [45].

The area of usage is enormous. The balloons can be utilized where there is no Internet infrastructure, either because it is too expensive or just not available. Examples of situations like these are emergency situations, during/after natural disasters and when cell phone-towers are down. Project Loon is an ongoing project with extensive testing taking place. The project is utilizing what everybody have in common, namely the sky, in order to reach out to areas where Internet access has not yet been available. It is expensive to have enough balloons in the sky in order to have good enough coverage. Also, the speed is not high. Even though a specialized antenna is required to get access, one is approaching a breakthrough which means that the whole world will be connected [46, 47].

Although this solution is not an option for distributing the Internet as of today, it could be a good option in the near future. The solution is affordable and easily compatible with our QUICK box solution presented later in this report.

Iridium

Iridium satellite consultation is a large group of satellites providing data and voice services to specialized satellite phones. The consultation exists of 66 active satellites in orbit. Iridium are considered to be low-orbit satellites and are situated in an altitude of 781 km. The Iridium network is unique in the way that it covers the whole globe, including oceans, airways and poles. The low-orbit satellite differs from the balloons in the way that the satellites travel at an altitude almost 40 times higher

[48]. To be able to utilize the satellite one would need a specialized satellite phone or a satellite dish in order to receive signal. With the balloons there are only need for an antenna to receive the signal. But then again the balloons does not offer a voice service. The balloons are intended as a cheaper, easier and simpler solution to the satellites.

2.8 Apple's Mesh Network

In March 2014 a new iOS app was released, FireChat. FireChat utilizes Apple's Multipeer Connectivity Framework introduced in iOS7 [49]. This app enables the possibility to chat with people "off-the-grid" [50]. Applications that communicates through this framework creates a mesh network similar to the one created by the Mesh Potatoes.

The Multipeer Connectivity framework provides support for discovering services provided by nearby iOS devices using peer-to-peer WiFi, infrastructure WiFi networks and Bluetooth to communicate. This communication could either be message-based data, streaming data or resources such as files [51]. These technologies have a short range, but this range can be greatly extended by a chain of users that creates a mesh network, see section 2.5.4 for more information about mesh networks. AirDrop is a product that have been on the market for a while and also utilizes mesh networking. The main difference is that FireChat is fully decentralized and peer-to-peer. When there are multiple users in one area, FireChat relay messages in the same way as the Internet, from node to node, just in this case it is from phone to phone. This, not only, enables two users to chat with each other without Internet connection, but also far beyond WiFi and Bluetooth range from each other, using the chain of users (phones). For example if Bob is connected to Alice, and Alice is connected to Carol, Bob and Carol can send messages to each other. This chain can be indefinitely long. As long as no device goes out of WiFi range, all the devices can communicate with each other.

This new framework will mainstream wireless mesh networking, and open for a future way of spreading Internet access. This could for example be in a hotel basement, a cave or in rural areas where there are no cell phone-coverage. There are many benefits with the use of mesh networks. Mesh networks does not require a centralized infrastructure, meaning there are no need for all the devices to be connected to the Internet (as a router). Another benefit is that the mesh network is really easy to set up - everybody just uses the app FireChat (or similar applications like AirDrop), the network is created and everybody is connected. Simple as that!

The possibilities for this feature are enormous, both in the area of usage, and in the creation of new applications. In many countries, Internet and mobile broadband

connection is extremely expensive. People might afford a used cell phone, but not the cost to connect. With this new feature, Internet connectivity can be spread through the mesh network needing only one node (phone) to have Internet access. This way of spreading connectivity can open the possibility for people in rural areas, like slums and small villages, to stay connected. Not only rural areas can benefit from this new mesh-networking feature. Young people that do not have a phone can use an iPad, or a similar device, to talk with their friends. Teens or others with restricted cell contracts could get in contact with their friends by, for example, connecting through the neighbour's phone. Since FireChat enables communication without the use of the Internet, it can be a useful tool to communicate privately and also to send sensitive data.

It is not only Apple that is seizing the enormous potential in main-streaming mesh networking. Google has expressed that they are working on a home mesh network [52]. FireChat and AirDrop is just the beginning.

Chapter 3
Refugees and IDPs

Our initial approach for the thesis was to look into refugee camps, focusing on Norwegian relief organizations. The aim was to get an understanding of how refugee camps are run and how the communication is, both within the camp, and to the outside world. We wanted to look into how the Mesh Potatoes could be utilized to improve the communication. We conducted research trying to get an overview and a general understanding. In addition to this, we carried out interviews with people from Norwegian organizations, namely the Norwegian Refuge Council and CARE. These interviews gave us more information and a better understanding of the area. They also showed us that refugee camps is an extremely comprehensive area, and the differences in the unique camps are enormous depending on country and government law, size of the camp, lifetime of the camp and so on. Some countries have well established Internet and cellular network infrastructure, and people are equipped with smart phones and laptops. In other countries this is far from the case, and their only way of receiving news is by radio or mostly by word-of-mouth. In addition to this, many camps are under strong technological restriction because of country law.

Since the differences are so big, it is hard to find general information, simply because there are no general information. No camps are equal, and it is hard to compare them. This made it hard to decide in what direction to focus. A research, as the one first intended, would require a close collaboration with a relief organization, and for them to give full focus both to us and our research. It was difficult to create a stable connection and collaboration with one of the Norwegian help organizations. A collaboration like this would require a lot more time than what we had at our disposal.

During our research and work in the first months we could see our report going in a different direction. The area initially chosen became to big to grasp. We decided to direct our focus onto natural disasters, and how a QUICK box can be used to quickly get Internet access and to help coordinate relief work (more information about this in chapter 4). This chapter contains the research we conducted on refugee camps. We

will go through some general statistics to get an idea of the life in the camps and the development over the last few years. In addition to this we will present summaries of the interviews with the Norwegian Refugee Council and CARE.

3.1 Definitions

It is fairy common to think of every person that is displaced as a refugee, but this is not the case. It is important to separate between a refugee and an internally displaced person.

Refugee

The definition of a refugee is a person who has been forced to leave his/hers homeland because of, for example, war, violence or persecution. A refugee often has a justifiable fear of persecution for reasons as religion, political opinion, race, nationality or membership in a certain social group. For these reasons they are not able to, or afraid to, return to their homeland. The leading reasons for refugees fleeing their home country is war and ethnic, religious and tribal violence [53].

Internally Displaced Person

An internally displaced person (IDP) is a person that has been forced to leave his/her home for some reason and are a refugee in his/her own country. The main distinction between an IDP and a refugee is that the person has not crossed any country borders. Unlike refugees, the IDPs are not protected by any international laws, nor able to receive all types of aid. During the last years the number of IDPs have drastically increased, mostly due to the conflicts between countries [53].

3.2 Statistics

We have looked at some of the global refugee statistics presented by UNHCR from 2010 and 2012. The following section will enlighten some of these statistics.

In 2010, the majority of the refugees came from Afghanistan, Iraq and Somalia [2]. In both 2010 and 2012 Pakistan was the country which hosted the most refugees. By the end of 2012, 45.2 million people were displaced by force. According to UNHCR this is the largest number seen in 20 years. The report for 2012 show that 55 % of the registered refugees came from countries affected by war, e.g Syria, Afghanistan, Sudan, Iraq and Somalia. The crisis in Syria has been a major factor for displacement. The whole of 647,000 people have be forced out of the country [3]. Table 3.1 shows the drastic increase of Syrian refugees from 2010 to 2012.

An observation made is that the number of Somali refugees has increased from 770,154 refugees in 2010 to 1,136,100 refugees in 2012. There has been an ongoing conflict in Somalia ever since the Siade Barre regime collapsed in 1991. This conflict have resulted in the displacement of many Somalis. The number of displaced persons is constantly changing. In 2011-2012 there was a famine in Somalia, and this caused not only many deaths, but the displacement of many people [54]. This is one of the reasons for the increase of Somali refugees from 2010 to 2012.

In contrary to the increase of Somali refugees between 2010 and 2012, the number of Iraqi refugees had decreased from 1,683,579 refugees in 2010 to 746,400 refugees in 2012. Before the Syrian civil war started in 2011, there were many Iraqi refugees who had fled to Syria due to the invasion led by the U.S. When the Syrian civil war began, the situation reversed. Many Syrian people sought shelter in Iraq, and many of the Iraqi refugees returned to their homeland. This is one reason for the drastic decrease of Iraqi refugees from 2010 to 2012. Although many Iraqi refugees went back to Iraq, they remained displaced. This situation has brought the number of Iraqi IDPs up to approximately 2.8 million [55].

Table 3.1: Refugee statistics - Comparing 2010 and 2012 [2, 3]

Information	**2010**	**2012**	**% variation**
Number of people forcibly displaced worldwide	43.7 million	45.2 million	+ 3.4%
Number of refugees from Afghanistan	3,054,709	2,585,600	÷ 18%
Number of refugees from Somalia	770,154	1,136,100	+ 47.5%
Number of refugees from Iraq	1,683,579	746,400	÷ 125%
Number of refugees from Syria	18,452	728,500	+ 3848%
Number of refugees hosted by Pakistan	1,900,621	1,638,500	÷ 13.8%
Percentage of refugees that are female	47%	48%	+ 1%
Percentage of refugees that are children (below 18)	47%	46%	÷ 1%
Number of individual asylum applications lodged by unaccompanied or separated children	15,500	21,300	+ 37.4%

3.3 Interview with Norwegian Refugee Council

We had a Skype interview March 12, 2014, with Katrine Wold from the Norwegian Refugee Council (NRC). The aim of the interview was to hear about her work in

refugee camps and how the situation in the refugee camps are today, with main focus on means of communication. Katrine Wold has been working for NRC for many years, and also has a background from United Nations (UN). She has worked in emergency and crisis situations abroad. She is specialized in camp management and coordination. In recent years she has been responsible for education, and have had the main focus on youth. We asked her which refugee camps NRC is working in, but she could not give us a clear answer on this question. The reason for this is that NRC works in over 24 countries and have, as of 2013, reached out to 4.4 million people. She makes it clear that there is a difference between internally displaced persons (IDPs) and refugees. An official refugee must cross a boarder, or else you are internally displaced. NRC works both with refugees and IDPs, and also with people who are affected by having refugees in their local area. NRC does not only help with operational issues in the camps, but they mainly offer services that the refugees need. When dealing with refugees, there exists international laws and regulations. These also states what kind of human rights exists. Everyone have rights! The vast majority of countries have acknowledged the UN refugee commission, which has been formed by the international society, UN, and authorities via UN's forums. The commission is an important premise when working with refugees. It is important to know which rights you have as a humanitarian worker, and which rights the refugees have.

We ask her how communication within the camp is conducted. She takes Kenya as an example. NRC has been working in the largest refugee camp in the world, Dadaab Kenya, for many years. The authorities have the main responsibility for what is going on in the camp. They often ask the international community (e.g. NRC) for help. Wold states that it is important to establish a good communication and information flow between the different organizations working together in the camp. This communication takes place by, for example, establishing coordination meetings. These meetings includes the relief organizations working in the camp, and the authorities. The goal is not to make a permanent home for the refugees, but to make the camps a safe place to live temporarily, and to help them move on (either go home or find another place to live). Living in camps is a temporary life situation. She states the different types of communication; internally between the workers in the camp and communication with the refugees. It is important to establish transparent coordination mechanisms, in other words ensure good forums where the refugees can communicate and inform the workers in the camp what their needs are. This can only be achieved by recognizing that refugees are not a large mass, but individuals with different needs and with different life situations. The humanitarians and authorities try to establish some sort of local elections. This means that the refugees can choose representatives who's job is to be in communication with the primary humanitarian managers in the camp. The reason for this is that it is impossible for the humanitarians to talk to 500 000 people. The communication between the representatives and the managers must be done either through meetings,

or in an informal manner. Overall, this creates a communication pattern in the refugee camps. Wold states that there are few places without mobile coverage, and that the majority of the refugees own a mobile phone. Mobile phones are often used as a tool when goods (access to money, food etc.) are distributed to the refugees. They can "add credit" to their card, and use this as payment. This an up-and-coming way of doing distribution. Mobile phones are also used to collect information, for example by sending the refugees surveys on their mobile phone.

In general, Wold states that methods of communication can be via mouth, radio, billboards, data communication, but this all depends on which camp and what is allowed in the camp. The law in the refugee camps depends on the national authorities. In some camps it is allowed to establish a data communication center, but in other camps this is illegal. It is important that the refugees get informed of the current situation upon arrival, and of what rights they have. The distribution of this information takes place primarily by someone called the camp management agency. They have the daily coordination responsibility for activities taking place in the camp. It must be made clear to the refugees where they can obtain different types of services, and also what is expected of the refugees. It is important that the refugees at an early stage get the opportunity to contribute positively in the camp, or else they can end up with something called "dependency syndrome" (they feel incompetent and get totally dependent on external assistance).

Another question we asked her is how the refugees get registered in the camps. Here she states the importance of distinguishing between official and unofficial camps. The definition of a camp is that people are gathered together and live there. Registration is only done in official camps. When refugees are registered they get an ID card. This ID card is very valuable, because it indicates that you, as a refugee, have access to the goods that are available in the camp. The registration procedures can vary, but most often there exists computer systems for the registration.

3.4 Interview with CARE - Dadaab Refugee Camp

We got in contact with Mary Muia from CARE. She is a program assistant at CARE International in Dadaab, Kenya. We sent her a questionnaire with questions about Dadaab refugee camp, with focus on means of communication. The following section contains information both from different articles and from the answers of the questionnaire. See Appendix A for the full questionnaire.

Dadaab is the largest refugee camp in the world, and is located in Kenya, Africa [56]. It was created in 1991 by the government of Kenya and UNHCR to host Somali refugees displaced by civil war [57]. Over the years, the camp has also hosted other nationalities, from the Horn of Africa, the Great Lakes and East African regions.

These people constitute less than two percent of the camp population. In April, 2013, there were 423,496 registered refugees in the Dadaab camp. 51 % of these were female and 58 % were younger than 18 years old. Also in 2013, UNHCR and its partners decided to conduct a verification exercise to ascertain the current population. The reason for this was that many of those who had arrived in 2011 due to the famine had returned home. As of February, 2014, the current population stands at 369,294. The lead agency for this camp is the UN High Commission for Refugees (UNHCR) [56]. In addition to UNHCR, major international humanitarian agencies like CARE, Save the Children and the International Rescue Committee are active helpers in the Dadaab refugee camp. These agencies provide the refugees with critical services (e.g. food, housing, sanitation and medical help). This is an extremely challenging task in refugee camps, especially when they reach this size. During the recent years, the terror group Al Shabaad (Somali-based) have intensified their misdeeds in, and around, the Dadaab refugee camp. This has made the situation even tougher for the refugees and the relief agencies. Muia states that the biggest challenges in the camp are lack of space to accommodate everyone, and the lack of funding to take care of all the needs of the refugees. Another challenge is the language barrier between the humanitarian staff and the refugees. Many of the staff members neither speak nor understand the Somali language, and as many as 95.6% of the refugees are Somali.

Muia explains how the registration process is handled; when a new refugee enters the camp, the refugee reports to a UNHCR reception desk. There the refugee is given a temporary registration, while pending full registration. Upon arrival, the refugees are given information about available services, and which agency is handling what service. Immunizations, medical attention, emergency food supply, tarpaulins, sleeping mats, jerrycans for fetching water and kitchen sets are issued on arrival. This is to help them start their new lives in the camp.

To improve the situation in Dadaab, communication is crucial. In 2011, a group consisting of people from NetHope, Inveneo and the USAID Global Broadband and Innovations Program gathered to discuss ways to improve the means of communication in Dadaab [56]. NetHope is a consortium of over 30 international NGOs [58]. NetHope works with improving connectivity, with the help of information technology, among relief agencies. The aim of this project, called DadaabConnect, was to bring forward more reliable Internet, and find ways for agencies to communicate better internally [56]. The group put together teams that travelled to Kenya to investigate the conditions in the refugee camps, and to find out what they could implement. It was clear from the feedback they got that a better communication system was needed, and that it would make the humanitarian work much easier. It would improve both the coordination and the security in the camp. Improvements of these aspects gives the humanitarian agencies better working conditions, and makes it easier for them to help the refugees with critical services. Inveneo started working with Cisco's

Tactical Operations (TacOps) to install and configure a local high-speed network [59]. They also engaged in a partnership with a local Kenyan mobile and landline telecommunications service provider called Orange. The reason for this was that they wanted to extend the Dadaab compound with new data services. This could be done by using Inveneo's long-distance Wi-Fi solutions. The data services that were added included services requested from the Dadaab aid community. "DadaabNet", a high-speed network, was created in cooperation between Inveneo and TacOps. This network connected the NGOs locally, and made it possible for the agencies to easier communicate internally (VoIP telephony, file sharing etc.). Following this, in March 2012, they started the training of technicians. These technicians were people from Orange, from the technical staff of the NGOs and from Inveneo's staff. The training took place both in classrooms and in the field, in order to give the technicians a wide understanding. The results from DadaabConnect has been great. The humanitarian agencies has gotten better working conditions, due to the improvements in means of communication. Other positive outcomes is that the network is more reliable and cost effective.

We asked questions about means of communication within the camp, and with the outside world. Muia did not specifically mention the project described above. She states that CARE as an organization has invested in communication systems in cooperation with ISPs in the capital city of Kenya, Nairobi. Through this cooperation, the camp staff are assured to get Internet access for both official and social purposes. Several Kenyan telecommunications companies have set up equipment in the camp area, and the camps are therefore provided with access to mobile communication and Internet. Unfortunately, Internet and telephone service outages are fairly common. In addition to mobile communication and the Internet, there are radio station services and access to digital television. CARE use telephone services to reach out to refugee staff. 50% of the refugees have access to mobile phone services. Posters and radio are also commonly used to reach out. Word-of-mouth (e.g. over speakers) is also a communication technique employed. There are two main telecommunication providers in Dadaad, hence little competition. The lack of competition makes the prices higher. We asked Muia how the refugees can afford having their own mobile phone, when the costs are so high. She says that many refugees have been in the camps for a long time, and therefore have had the time to establish small businesses which gives them some profit. Others get money sent from their relatives.

3.5 Life in Camps for Refugee Women

In this section we will shortly present some of the most relevant answers found in research done by Mari Maasilta, a Swedish post doctoral researcher. She has looked at the use of oral and mediated communication by women living in refugee camps in Eastern-Africa.

Women are in general in a more vulnerable position when living in a camp, especially if they are single mothers. They may be solely responsible for taking care of the children, in addition to sick and elderly family members, maintaining the household, preparing food, acquire water, and securing firewood. Collecting firewood for cooking is a necessity, but it forces women to walk far away, hence making them vulnerable for sexual assault. They often have to turn to prostitution and other unhealthy and dangerous means in order to survive [60].

The means of communication vary greatly in the different camps. Some have Internet connection and satellite TV, other barely have access to a radio. Even though radios are the most common media for communication, it is not given that all citizens in a camp have access to one. Often people gather around the few radios that exists in a camp. One issue that limits the usage is the batteries, since they are very expensive and hard to acquire. The use of cell phones are increasing. Even though the prises are extremely high it does not stop people from calling relatives in Europe and other places in the world [60].

Information walls and word-of-mouth is often used in order to spread practical information within the camp and about camp activities. Word-of-mouth is also used in order to retrieve information about the world outside the camp. People visiting the camp were used as sources for information. Earlier studies have shown that social connections with neighbours works as an important medium to transport information, resources and services between individuals. This kind of networking has been used to find lost family members in big camps, as well as get financial help from abroad [60].

Chapter 4
QUICK Box

The main purpose of our study was to create an easy way to utilize the Mesh Potatoes in emergency situations and other situations where there are need for cheap and instant communication. Our main focus has been on providing Internet access to the mesh network formed by the MPs, and on the aspect of quick roll-out of the network. Internet access may be a vital way of communication in emergency situations, or just convenient in other situations. The process of setting up a mesh network providing Internet should be done quickly, since time is a crucial factor to consider in emergency situations. In this chapter we will describe parts of the set-up techniques for the Mesh Potatoes. Further on we will present our QUICK Box, which is a box including an MP, a solar panel, a battery, a charge regulator, manuals for connecting the MP to different uplinks, a manual describing how to get started with the box, necessary cables, a USB-stick containing script and a CD with Linux Ubuntu. A box ready to go in any situation. We will describe how we made this box, and similar work that has been conducted previously on this area. At last we will describe some situations where there is a need for a mobile communications system.

A big part of our work has been gathering of information, and make the existing information more understandable for the common user. The existing user guides tend to be advanced and not adapted to end users. Therefore we found it necessary to make the descriptions easier and more user friendly.

4.1 Set-up of the Mesh Potato

The set-up process of the Mesh Potato includes, among other activities, installing firmware, allocating IP addresses and providing Internet access to the network. The firmware used in the MPs is called Small Enterprise/Campus Network (SECN) Firmware [61].

4.1.1 Configuring the Mesh Potato

Configuring a Mesh Potato is the process of allocating a unique IP address to the MP. Each of the MPs are assigned a static IP address (10.130.1.20), this addresses is not part of the LAN address space. In order to change the IP address of the MP, the MP must be connected via an Ethernet cable to a PC running Linux. The PC must be on the same subnet as the MP in order to establish contact. When the PC is on the same subnet, the MP's web interface can be accessed via a browser. In the web interface, the IP address can easily be changed. This description works for both MP01 and MP02. One difference is that the user can change the IP address of the MP01 by using Interactive Voice Response (IVR) commands (see page 28 in Appendix C). A second variant of the MP02 is in development. This variant has a telephone jack port (FXS daughterboard), which will allow for IVR commands on the MP02 as well.

Execute the following commands in the Linux terminal:

1. Set the PC to be in the same subnet as the MP, by writing the following command in the terminal:

```
$ ifconfig eth0 10.130.1.120 netmask 255.255.255.0
```

2. Open a browser and type in "10.130.1.20". The web interface will then appear. This verifies that contact with the MP is established.

3. In the web interface, under network, change the IP address field to "192.168.1.x", where x is the unique number for the specific MP. This number should be between 1-254. In order to set the change, press "Save" and "Reboot" in the interface.

Change from telnet to SSH

To remotely configure the MP from a PC, telnet or SSH is used. Telnet is the default option, but SSH is a far more secure option and is highly recommended. In order to enable SSH, some steps must be conducted in the terminal:

1. Install SSH by entering the following command:

```
$ sudo su
$ apt-get install ssh
```

2. Execute the following command to telnet into the MP:

```
$ telnet <IP address of the MP>
```

3. The following command will enable SSH, and ask you to choose a password for SSH. You will be asked to enter this password two times:

```
$ passwd
```

4. SSH is now enabled. The next time you enter the MP, SSH must be used. To SSH into the MP enter the following command:

```
$ ssh root@<IP address of the MP>
```

4.1.2 Upgrading the Mesh Potato

The MP's firmware are under constant development. It is therefore advisable that the MP is running the latest version of the firmware. The process of upgrading the firmware is different on MP01 and MP02. The different methods are described below.

See the SECN User Guide, for respectively MP01 and MP02, in Appendix C and D for more details around the upgrading process.

Installing Firmware on Mesh Potato Version 1

Flashing is the process of updating or changing the firmware (SECN) on the MP. The most common way to perform the flashing process is by using the potato-flash application [62]. This is a specialised software application for the Mesh Potato. Potato-flash can be used regardless of previously installed firmware on the Mesh Potato [63].

1. Download the 64 bit potato-flash utility from `http://download.villagetelco.org/utilities/potato-flash/potato-flash-64bit/` to the folder `/etc/local/bin`.

2. Make the potato-flash file executable by writing the following command in the terminal:

```
$ cmod +x /usr/local/bin/potato-flash-x64
```

3. Download the rootfs file (`openwrt-secn1_1-GA01-MP01-root.suashfs`) and the kernel file (`openwrt-secn1_1-GA01-MP01-vmlinux.lzma`) from `http://download.villagetelco.org/firmware/secn/stable/mp/SECN-1.1/` to a folder, for example called, *mp_firmware* in the local directory. (Always choose the latest stable version of the firmware.)

4. Open the terminal and write the following commands:

   a) Enter root environment:

```
$ sudo su
```

b) Turn of network manager:

```
$ service network-manager stop
```

c) Bring up the interface connected to the MP:

```
$ ip link set eth0 up
```

d) Access the directory containing the .squashfs and .lzma files:

```
$ cd <the directory containting the .squashfs and
.lzma files>
```

e) Assign IP address to the interface:

```
$ ifconfig eth0 1.1.1.1
```

f) Before running the potato-flash utility, make sure that the MP is unplugged from its power supply, and that the MP is connected to the PC via an Ethernet cable.

g) Execute the potato-flash utility:

```
$ potato-flash-x64 openwrt-secn1_1-GA01-MP01-root.suashfs
openwrt-secn1_1-GA01-MP01-vmlinux.lzma
```

Briefly after the potato-flash is executed, dots will start to appear on the screen, as shown in Figure 4.1. When these dots appear, plug the power supply back into the MP. The process of upgrading the firmware will then start.

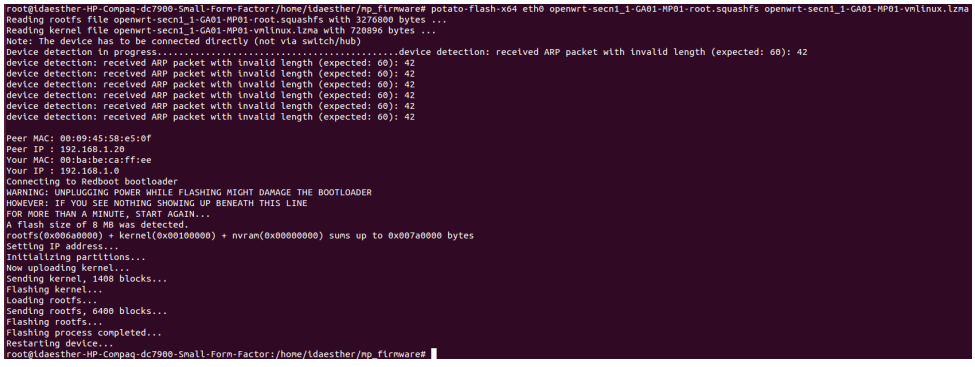


Figure 4.1: Flashing the Mesh Potato version 1. This figure shows the flashing process from when we first flashed our Mesh Potato version 1

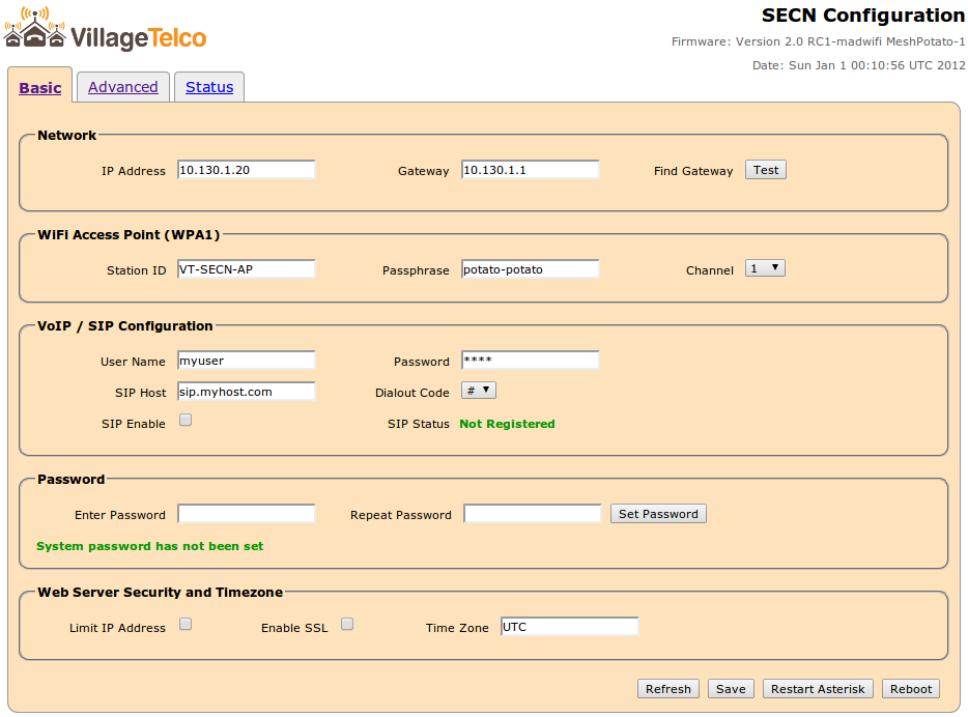


Figure 4.2: Web interface. Displays the MP's web interface.

Installing Firmware on Mesh Potato Version 2

The process of upgrading the MP's firmware is simplified with the MP02. With the MP01, command shell (terminal) must be utilized in order install or upgrade the firmware. With the MP02, firmware upgrade can be done from the SECN web interface (more information about the interface can be found in section 4.1.3). Extra functionality has been added to the interface from MP01 to MP02. Under "Advanced" in the interface an extra tab called "Firmware" is added. Under this tab the firmware upgrade can be executed. When the "Firmware"-button is pressed, a new windows pops up where you have to add the firmware file. The firmware for MP02 can be found here: http://download.villagetelco.org/firmware/secn/unstable/mp02/SECN-2.0/SECN-2.0-RC4/.

4.1.3 The SECN Web Interface

Village Telco provides a SECN web interface for configuration and management of individual MPs. This web interface can be accessed by entering the IP address of the MP in a browser, as shown in Figure 4.2. To be able to do this, the PC must be on the same subnet (exact same prefix) as the MP.

The web interface allows the user to alter different settings on the MP. The user can, for example, change the IP address of the device, set up the WiFi AP, conduct VoIP/SIP configurations, change/set password and configure web server security. The web interface also allows the user to alter more advanced settings. To get a detailed description of the web interface, see the SECN User Guides in Appendices C and D.

4.2 QUICK Box

The Mesh Potatoes and Village Telcos were created to get voice and data connection to areas where services like these are non-existent or too expensive for the average person. As of now, the MPs have been set up to create networks of different size in villages all over the world. We want to expand this solution by looking at its mobility and its usage on the go. We want to make a box that has high adaptability, enabling it to easily be used in several different scenarios, under different conditions and by different people, all with different needs. The box must be user friendly, so there are no room for misunderstandings or mistakes. The box should be ready to go in any situation. QUICK stands for Quick User-friendly Internet-providing Communication Kit.

Quick - The box should be easy to set-up, and include all manuals necessary to get started with the box, and to provide Internet access to the network. Scripting could be used in order to automate the set-up process.

User-Friendly - The manuals should be easy to use, both by technical and non-technical people.

Internet-Providing - There should be manuals explaining how to connect the MP to various types of up-links.

Communication - In today's society, and especially during emergency situations, it is crucial to have the possibility to communicate, both within a community, and with the outside world.

Kit - Our solution will be delivered in a mobile suitcase.

4.2.1 Previous/Similar work

Go Box

Something similar has been done before by Keith Williamson, a volunteer in the Village Telco community. His idea of utilizing the Mesh Potatoes in emergency situations started with his interest in amateur radios, and the use of radios in

emergency situations. He put together a "go box" by using a waterproof Pelican 1200 case. This case contained a bracket holding the Mesh Potato, a rechargeable Li-Ion or Li-Poly battery, telephone handset and a junction box to provide an on/off switch [64]. The QUICK box differ in some ways from the "go box" made by Williamson. The main difference between the "go box" and the QUICK box is the QUICK box is based on the MP02-basic, while the "go box" is created using MP01. Since the QUICK box is based on the MP02-Basic, it is not possible to add a phone to our solution. Another difference is that the QUICK box includes everything needed for an installation. The QUICK box is therefore more comprehensive than the "go box".

AfrikaBurn

AfrikaBurn is a "Burning Man" festival in Tankwa Town in the Karoo (South Africa) that is held once a year [65]. This is a festival with focus on art and freedom of expression. Instead of using money, the festival attendants are inspired to trade different types of goods with each other. A Village Telco has been established at this festival a few years now. Free-standing phone boots with Mesh Potatoes powered by solar panels has been set up at the festival area. The first year five phone boots were set up around the festival area. Since it were few numbers to call, the calling became sort of random. This gave a "ChatRoulette" like effect, only with phones instead. The second year some aspects were improved from the previous year. The boots had production MPs, no lighting and new sleeves. A netbook was brought with them, and this acted as a gateway [66, 67].

4.2.2 Key Components

The key components of the QUICK box is described in Table 4.1.

Table 4.1: The components of the QUICK box

Component	**Description and purpose**
Access point for Internet	Mesh Potato version 2.
Suitcase/box	A suitcase made of high quality plastic coated with aluminium foil. Strengthened edges and corners of aluminium and steel. It has a soft-padded interior. A solid handle for carrying. Dimensions: 455x330x152 (width, depth, height). Weight: 2,6 kg.
Power supply	A gel battery (12 V and 5 Ah). No need for maintenance. The battery acid is bound in a viscous gel. This prevents leakage, even when the battery is mounted horizontally. Long lifetime and safe to handle. The battery is fully closed, and do not need refill of battery water. No hydrogen gas or other gas might leak. When the battery is charging no gas or acid vapor is emitted, hence the battery can be placed in narrow or enclosed spaces. The battery withstands multiple discharges. The gel battery is ideal for seasonal or occasional use, since it have a slow self-discharge tempo, and a good ability to recover after deep discharging. Dimensions: 114x69x109. Weight: 2,16 kg.
Solar panel	Solar panel from Multicomp with item number: MC-SP10-GCS. Power rating: 10 W. Power Voltage Max: 17 V. Dimensions: 357x280x18.
Charge regulator	Regulator for 12 V solar panel. Protects the battery from overcharging and discharge. Capacity: 100 W / max. 7 A. Overcharging protection: 14.5 V. Discharge protection: <10,5 V. Three diodes shows charging, high voltage and low battery voltage.
Manuals	Different manuals for providing Internet access to the MP, and a manual explaining how to get started with the QUICK box.
CD with Linux Ubuntu	A CD with Linux Ubuntu is provided.
USB-stick	The USB-stick contains a script that can be run in order to provide Internet access to the MP via a PC.
Necessary cables	An Ethernet cable is provided in order to connect the MP to a PC, and an extra power cord is added in case there is a power outlet available.

4.2.3 Creating the QUICK Box

This section describes how we created the QUICK box from scratch. The box is delivered with a Mesh Potato that is pre-configured with an unique IP address. The suitcase contains a CD with Linux Ubuntu in case the user does not already have it installed. It is necessary to have Linux in order to execute all the configurations and set-ups provided in the box. The case also contains necessary cables and detailed descriptions on how to connect to the different up-links, in order to provide Internet access to the network. Figure 4.4 shows the box in the making.

Conjoining the components of the QUICK box. The key components that we used to construct the box was a charge regulator, a gel battery, a solar panel and an MP02. These components were conjoined as shown in Figure 4.3. The charge regulator is connected to all the components, and is used in order to not overcharge the battery. The charge regulator was initially built for another type of solar panel than the one we chose to use. This means that the concomitant plugs could not be used. These plugs were cut of and we soldered on new wires.

New wires were soldered on the charge regulator, one was connected to the MP's power cord, while the other two was connected to the battery and to the solar panel. Before connecting everything together we used a multimeter to measure the voltage

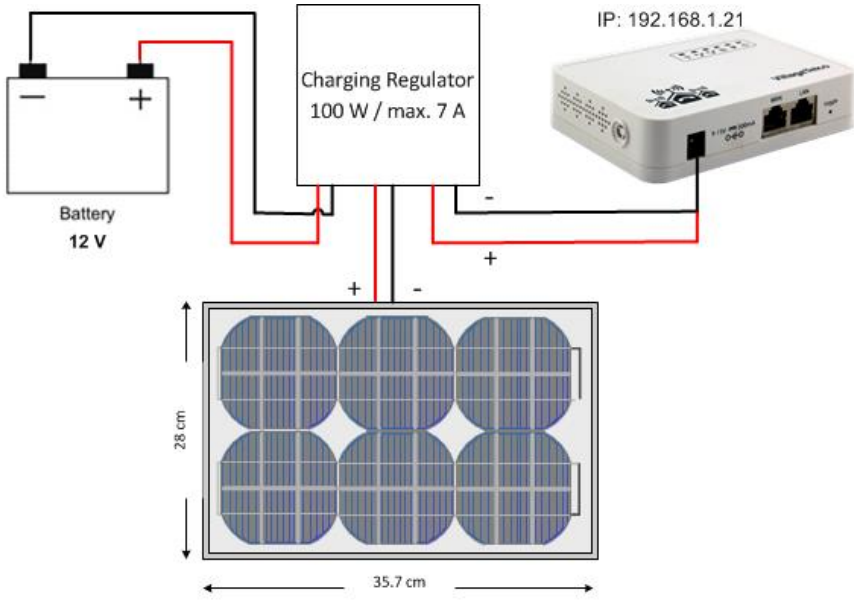


Figure 4.3: The composition of the QUICK box. This figure shows how the key components in the QUICK box is conjoined together.

Figure 4.4: Building the QUICK box.

of the solar panel. We placed the solar panel under a bright light (lamp) to see if it had any impact, which it did. We used the multimeter to check the battery as well, which was fully charged, with a voltage of a little over 13 V. We first connected the solar panel, then the battery, and at last the Mesh Potato. When everything was conjoined correctly, the MP turned on. Figure 4.5 shows our final prototype of the QUICK box.

Configuring and upgrading the QUICK Box. When the QUICK box is delivered, the Mesh Potato is already set-up and configured with an unique IP address, and running the latest version of the SECN firmware. The processes of upgrading and configuring the MP are described in sections 4.1.1 and 4.1.2. These descriptions are attached in the QUICK box.

Figure 4.5: Final prototype of the QUICK box. This figure shows the final prototype of the QUICK box including everything necessary for a quick roll-out. As shown, there is room for adding a telephone inside the box. This can be included with the MP02-Phone.

4.2.4 Battery and Charging Calculations

All the calculations done in this section is based on the components described in Table 4.1.

Charging with solar panel

How long it will take for the solar panel to charge the battery from a fully discharged state to a fully charged state, depends on how much sun there is. The following calculations are based on the peak value of the solar panel (10W).

The solar panel capacity is:

$$Amp = \frac{Watt}{Volt} = \frac{10W}{17V} = 0.59Ampere$$

When charging batteries it is important to take the charging factor into consideration. This factor is the ratio between supplied capacity and submitted capacity. The charging factor varies depending on battery type. For the gel battery used in the QUICK box the factor is roughly 1.2. The charging factor does not have an annotation. If the battery is completely discharged it will take:

$$Amp \times Hours = AmpHours \Rightarrow Hours = \frac{AmpHours}{Amp} = \frac{5Ah \times 1.2}{0.59A} = 10.17Hours$$

to fully charge it.

This calculation does not take into consideration that the solar panel might have to charge the battery while the MP is running. The effect from the solar panel to the battery will then decrease.

Charge while MP01 is running

The capacity from the solar panel with the MP01 running is:

$$Amp = \frac{Watt}{Volt} = \frac{10 - 2.5W}{17V} = 0.44Ampere$$

The time it will take to fully charge the battery from fully discharged condition will then be:

$$Amp \times Hours = AmpHours \Rightarrow Hours = \frac{AmpHours}{Amp} = \frac{5Ah \times 1.2}{0.44A} = 13.6Hours$$

Charge while MP02 is running

The capacity from the solar panel with the MP02 running is:

$$Amp = \frac{Watt}{Volt} = \frac{10 - 0.75W}{17V} = 0.54Ampere$$

The time it will take to fully charge the battery from fully discharged condition will then be:

$$Amp \times Hours = AmpHours \Rightarrow Hours = \frac{AmpHours}{Amp} = \frac{5Ah \times 1.2}{0.54A} = 11.1Hours$$

In South Africa in December, for example, the number of sun hours per day is approximately 14. In June the number of sun hours is approximately 10.5. These numbers are best case, since cloudy weather has not been taken into consideration. This means that it is possible to fully charge the battery in the course of a day, but this may not always be the case. The following calculations show how long the battery can provide the Mesh Potato with power when fully charged, without the solar panel charging the battery simultaneously.

With fully charged battery - MP01

This calculation takes into account that the solar panel is disconnected from the battery. With the components described in Table 4.1 the number of hours the MP01 can last with a fully charged battery is:

$$Amp = \frac{Watt}{Volt} = \frac{2.5W}{12V} = 0.208Ampere$$
$$Amp \times Hours = AmpHours \Rightarrow Hours = \frac{AmpHours}{Amp} = \frac{5Ah}{0.208A} = 24Hours$$

With fully charged battery - MP02

This calculation takes into account that the solar panel is disconnected from the battery. With the components described in Table 4.1 the number of hours the MP02 can last with a fully charged battery is:

$$Amp = \frac{Watt}{Volt} = \frac{0.75W}{12V} = 0.06Ampere$$
$$Amp \times Hours = AmpHours \Rightarrow Hours = \frac{AmpHours}{Amp} = \frac{5Ah}{0.06A} = 83Hours$$

As the calculations show, the MP02 use much less power and can therefore last on the battery almost four times longer than the MP01.

4.2.5 Possible Improvements

As mentioned, the QUICK box is fairly easy and simple, and leaves room for improvements. There should be an on/off switch in order to spare battery capacity. This on/off switch would be placed between the battery and the regulator. Unless a measuring instrument is available to check the voltage, there are no way for the user to know the remaining battery capacity. This might be very useful in situations where communication is vital and the hours of battery lifetime and sun hours are limited.

The battery used is a gel battery. They are less explosive than the lithium batteries, and are better suited to be placed into enclosed spaces that may get hot. The downside of the gel batteries is their weight, since they are very heavy. Our aim is to make a case that is portable, a lighter battery would be preferable. Under the requirement of being portable a factor to keep in mind is that it is not allowed to bring lithium batteries on airplanes. This means that if we chose to use a lithium battery in our solution, a regular person would not be allowed to bring the QUICK box on an airplane. When it comes to relief organizations, this might not be a problem since they transport equipment in their own airplanes, for example Hercules.

The MP02 is small (much smaller than the MP01), and a powerful solar panel does not take much space, so there is no need for a suitcase of the size we have used. A smaller case, that is lighter and easier to handle, would make the solution even more portable.

Our main focus was to make something that worked and that was safe. We did not focus on aesthetics and appearance. This is therefore also an area with room for improvements.

4.3 Different Scenarios Where a Quick Roll-out Might be Necessary

Everyday there occur situations in the world that might affect the modern communication system, or causes a need for one. These situations can range from big natural disasters, like the tsunami in Japan, to temporary refugee camps. Also more festive situations, like a music festival, can utilize a quick roll-out communication system. The following sections describes some of the scenarios where the QUICK box might be useful.

4.3.1 Natural Disasters

A natural disaster is defined as: *any event or force of nature that has catastrophic consequences, such as avalanche, earthquake, flood, forest fire, hurricane, lightning,*

tornado, tsunami, and volcanic eruption [68].

All over the world relief organizations are ready to help if an unexpected situation occurs. These groups of people have the equipment, knowledge, experience and funding to help people in desperate need. Where are their help needed? Or if they hear about the disaster and the first respond team is in place, how do they report back about the situation? How do they communicate with each other to work more effectively and help the ones in desperate need? There is no doubt that there is a need for a simple, fast, and reliable communication system.

When a natural disaster strikes, it is hard to know the extent of it, which again makes it difficult to predict how the communication systems would be affected. This unpredictability makes it important to always have a back-up plan to the back-up plan. History shows that cell phone service is not a reliable service during an emergency situation. During 9/11 the system became heavily overloaded, and when hurricane Katrina hit, 70% of the cell phone towers were knocked down. People might think that if they live in a big metropolitan they will be safe, but this is not necessarily the case [69]. In addition, these examples are from the western world. The western communication systems tend to be more robust initially, compared to the ones in developing countries.

When looking at the developing world, which unfortunately is often more exposed to natural disasters, the situation is different. According to [70, 71] developing countries are in an larger extent affected by natural disasters than the developed world. The reason for this can be explained by the economic status of the country, both in how the country is prepared for a disaster and in how fast they can rebuild and recuperate after a natural disaster. Developing countries often lack the infrastructure needed to quickly and efficiently provide aids to the ones affected. According to Baxter [71], a natural disaster could set back a developing country many years in development.

People are extremely dependent on having the ability to communicate when natural disasters occur. It is crucial to have the possibility to inform others about the current situation and about what is needed at the disaster area. Time can be the difference between life and death in situations like these. Employing QUICK boxes could be a good solution in situations like these.

In the next sections, two examples of recent natural disasters, respectively from a developed country, and an underdeveloped country. The examples shows how the situation was handled, and if there were emergency communications systems available.

Hurrican Sandy

Hurricane Sandy hit big parts of the Caribbean, as well as the south-east parts of the Unites States at the end of October 2012 [72]. As many as 25% of the citizens in the affected areas lost cell phone coverage, and even more lost electricity. Communication is a challenge both during and after a natural disaster. It may also be difficult for first responders (like fire fighters, police, etc.) to communicate. No single communication system is fault free, and it is therefore smart to have a back-up communication system. Satellite communication was used, but the phones are expensive and the lines can be oversaturated if others are trying to connect to the network simultaneously. A small aperture terminal (VSAT) trailer was used to act like a satellite ground station. Finding a good spot for the trailer can be tricky, it requires clear view to the sky and it can not be placed too close to a tall building. The Red Cross launched an emergency preparedness application for smart phones. The application had a peak in downloads right before the hurricane hit, but when the commercial wireless network failed, they had to go back to the old way of spreading information; distributing paper files, going from house-to-house to check up on people, give information word-by-mouth and using bullhorns [73].

Philippines

November 8 2013 the typhoon Haiyan, a powerful tropical cyclone, struck and destroyed parts of south-east Asia, in particular the Philippines. Haiyan is the strongest hurricane in wind speed ever recorded. The hurricane had the highest number for casualties, killing over 6,268 people in the Philippines alone [74]. International humanitarians and the Philippine government were warned about the storm in advance, but nobody could anticipate its viciousness. Some of the first teams on the spot was communication experts. Their assignment was to help with coordination, and make sure information was spread as desired [75].

Numerous of relief organizations contributed with their help after the typhoon struck. They helped with everything from food and shelter, to collecting donations. The United Nations World Relief Programme were among the helpers, and they helped setting up emergency communication systems [76]. In addition to this, amateur radio operators helped with communication both during and after the disaster. Due to power outages, the existing communication systems were down and there were no cell phone signals. By using radio, they could help keep track of the storm, and give important information (about evacuations and flooding). The radio was also used to help people communicate with their loved ones [77].

4.3.2 Temporary Refugee and IDP camps

We got a better understanding of refugee and IDP camps after conducting interviews with different relief organizations (for interview with respectively the Norwegian Refugee Council and CARE, see section 3.3 and section 3.4). Not all refugee and IDP camps are as well established, like the one in Dadaab. Many camps are short-term, and are therefore in more need of a temporary communication system. In this case, setting up QUICK boxes in the camp to provide the refugees/IDPs with Internet access could be an option.

4.3.3 Festivals

Imagine you are at a music festival with your friends in a foreign country. There are thousands of people, and much activity. In a scenario like this, there are many reasons why an Internet connection would be beneficial. You could loose your friends, have to inform your friends about something urgent, inform the staff if an emergency situation occur and so on. Since it is very expensive to send text messages, make phone calls or use cellular networks abroad, it could be an idea to use the Mesh Potatoes to provide the people at the festival with Internet access. This could be set up by the organizers in advance. Although this adds an extra cost to the organizers, the people attending the festival can save a lot of money by refraining from using the expensive services available on their smart phones. The organizers could add an extra fee to prize of the festival pass, and it would probably still be beneficial for the people at the festival.

4.3.4 Breakdown of Mobile Towers

The 10th of June 2011 Telenor had problems with one of their servers in Oslo. This problem caused a down time of 18 hours and affected 3 000 000 Telenor users [78]. Not only was this the biggest problem Telenor have had since they opened their mobile network in 1993, but it was also the longest downtime and had the highest number of affected users recorded in Norway. In addition to this it all happened in a period with severe flooding in big parts of eastern Norway, and made it difficult to reach emergency numbers. The fact that the problems occurred during the flooding made the situation much worse [79].

Chapter 5
Roll-out of the QUICK Box

One area of focus has been the process of quick roll-out. There are many aspects that can be included in order to speed up the roll-out process and make the QUICK box as easy to use as possible. We will now present some of the main pointers, and ideas, to meet this requirement.

5.1 Scripting

A script is a list of commands that can be executed without the need of user interaction, in other words, to automate a process. In order to connect the mesh network to the Internet a list of commands must be executed. One idea to speed up the process of setting up the network is to create a script that automates this process. The QUICK box has a USB-stick containing a script for setting up an Internet connection via a PC. This script requires some user interaction, since the user has to start the script manually, and enter some variables. There is of course room for improvements in this area. The script could be made completely self-executable (not dependent on any user interaction). Additional scripts could also be included for other types of uplinks.

The script we have made simplifies the process of providing the Mesh Potato with Internet access via a PC and can be found in Appendix B (see section 5.5.3 for step-by-step description).

5.2 Distributing Numbers

The MP02 Basic does not have the ability to connect to a phone, hence the issue with telephone number distribution is irrelevant. During 2014 Village Telco will release a new version of the MP02, MP02-Phone. The MP02-Phone will be identical to the MP02-Basic, just with an FXS daughter board, allowing it to be connected to a phone. With the MP02-Phone the issue of number distribution reappears.

When a Village Telco is set up today, telephone numbers are distributed by updating a spreadsheet with name and number of the different users. These spreadsheets are printed out and delivered to everyone in need of it. This is a system that might seem cumbersome, but it serves its purpose. If new nodes are added to the network or any changes are made, new sheets have to be printed out and delivered to everyone. This way of spreading telephone numbers might be more difficult with the QUICK box. Even though the numbers are predefined, it is not set who is using the phones.

One option is to continue with the number distribution approach in use today, only in a smaller scale. The suitcase could contain five MP02s. All MP02s are marked with its own unique IP address. A list of the IP addresses of all the Mesh Potatoes in the suitcase will be attached. When setting up the network the names of the users can easily be filled in on each MP02. This will then serve as the telephone list.

Another approach could be to integrate the distribution of phone numbers as a new feature in the web interface. This feature would discover the other MPs in range of the network. All MPs would be displayed with the name of the Service Set Identification (SSID), the IP address, where the last octet serves as the telephone number, and the name of the residence or user. This name could be edited by the master user or by the user themselves. Each MP in the suitcase is pre-configured and set up. In this case the MPs also have to be set up with a password to enter the web interface. This ensures that only the specific user has access to the web interface of the given MP. Inside the web interface the user can see other MPs in range and also put in their name for the other users/MPs to see.

5.3 Training

The QUICK box is delivered pre-configured, with all the information necessary to set up a mesh network. It is recommended that the one who will be using the QUICK box has tested it and tried to set up the network in advance. This to make the process faster and easier when an emergency situation occurs, but it should not be necessary. The provided descriptions should be explanatory and easy enough for most people to use.

5.4 How to Create a Network

The following sections provide some explanation of specific aspects that should be taken into consideration when setting up a network consisting of MPs and the QUICK box.

Placing the Mesh Potatoes

The range of the MPs differs based on the terrain. If the terrain is hilly, and with many obstacles, the range shortens. It is also important to keep in mind where the MP/QUICK box is placed. To obtain a longer range, the MPs should be placed as high as possible. This could for example be on a roof top, on a telephone pole or on any other kind of tall object. With a clear view, the range could be up to 2 kilometres.

Stable power source

If there is a stable power source available, there would be no use for the battery and the solar panel in order to power the MP. The QUICK box provides an extra power cord for situations like these.

No stable power source

If there is no stable power source available, there will be a need for the battery and the solar panel that is included in the QUICK box in order to run the Mesh Potato. If the power is out, there is a high probability that most uplinks also will be unavailable. If this is the case, then satellite might be the only option. In order to use satellite, there must be a satellite dish available. Keep in mind that this satellite dish may be located far away, and that there might be a need for several MPs in order to spread the Internet access to the desired location. A need for several Mesh Potatoes in an area with power outage, indicates a need for several QUICK boxes, since the MP then becomes dependent on a battery and a solar panel to run.

5.5 Manuals

The following section contains manuals describing how to get started with the QUICK box, and how to connect it to different uplinks in order to provide Internet access to the network. All of the following manuals will be laminated, and included in the QUICK box.

5.5.1 Get Started - How to Use the QUICK Box

This is a description of how you set up and get started with the QUICK box.

Make sure that the QUICK box contains all these items:

- A Mesh Potato
- A battery
- A solar panel
- A charging regulator
- Ethernet cable
- A CD with Linux Ubuntu operating system
- A USB-stick containing a script called "scriptviaPC.sh"
- Descriptions on how to connect the Mesh Potato to different uplinks in order to provide Internet access.

The QUICK box is delivered with a pre-configured Mesh Potato, and a fully charged battery. The battery can be charged by placing the solar panel in sunlight.

Name of Mesh Potato (SSID): MP2_21.

IP address of the Mesh Potato: 192.168.1.21

Password: potato-potato

The password is the default password used on Mesh Potatoes, and it can be changed in the user interface for a more secure option. The SSID can also be changed there if that is preferable.

To set up the QUICK box:

1. Connect the wires to the battery (the red one to plus and the black one to minus). The Mesh Potato should then automatically turn on.
2. To provide Internet to the mesh network, follow the attached descriptions for the specific uplink type you have available.

In order to preserve the lifetime of the battery, it can be smart to disconnect the wires from the battery while the box is not in use. A fully charged battery has a lifetime of approximately 83 hours. This is when the solar panel is not connected to the battery. Take into consideration that the charging time when the battery is completely discharged is approximately 10 hours. If the MP02 is connected while charging, 1 hour is added to the charging time.

5.5.2 Manual for Connecting the MP02 Directly to Cabled Internet

One way to provide Internet access is by connecting the MP with an Ethernet cable to the jack port in the wall. The Mesh Potato is delivered pre-configured, with the IP address and the name of the network (SSID) stated in the "Get Started - How to Use the Box"-document included in the QUICK box. Figure 5.1 illustrates how the components are connected together in the following manual. The figure is provided to help the user get a better understanding of the network.

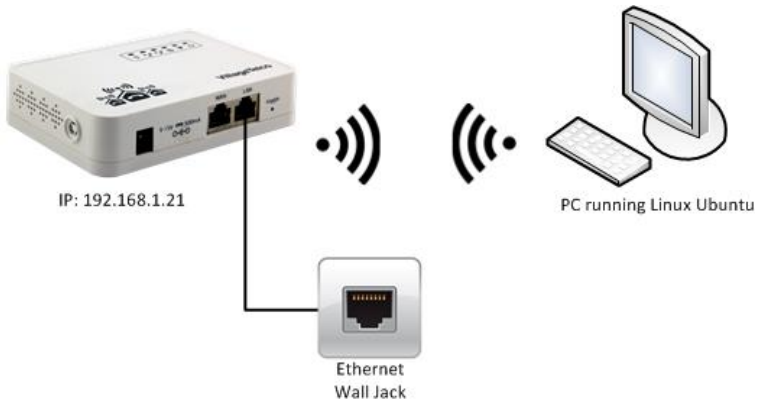


Figure 5.1: How the components are linked together during set-up for accessing the Internet from wall jack. This figure shows how the different components are set up when the manual for providing Internet access from a wall jack is carried out. As shown, the PC is connected to the MP via WiFi in order to perform the configurations on the MP.

1. Do the following steps to connect the PC via WiFi to the MP:

    a) Press the WiFi symbol in the top right corner of your Linux Ubuntu home screen, and press "Edit Connections".

    b) Under the tab "Wireless" choose the network called "vt-mesh" and press "Edit" like shown in Figure 5.2.

    c) In the field "BSSID" enter "02:CA:FF:EE:BA:BE", like shown in Figure 5.3a.

    d) Under the tab "IPv4 Settings" choose "Manual" in the "Method" drop-down menu, like shown in Figure 5.3b.

    e) Then press "Add" on the same page. Enter the following parameters, like shown in Figure 5.3b:

    Address: 10.10.1.245

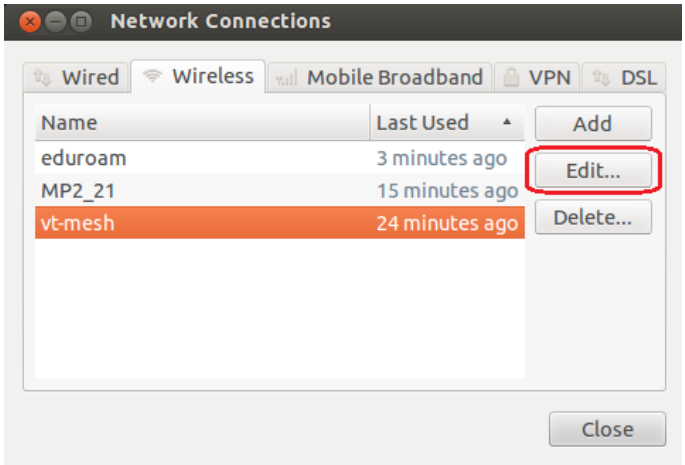
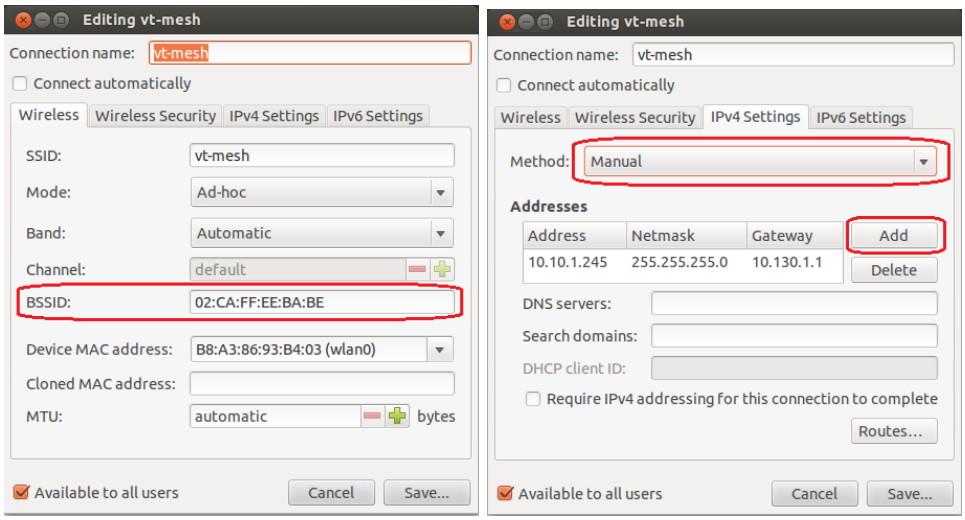


Figure 5.2: This figure shows the "vt-mesh" under Wireless Network Connections.

Netmask: 24

Gateway: 10.130.1.1



(a) The correct BSSID set. **(b) The correct parameters set under IPv4 settings.**

Figure 5.3: "Edit Connections" settings on Linux

f) Press "Save" on the "Editing vt-mesh"-window, and then "Close" on the "Network Connections"-window.

g) Then choose "vt-mesh" from the list of available networks. This list is found after pressing the WiFi symbol in the top right corner on your screen. The PC should then be connected to the MP via WiFi.

2. Connect an Ethernet cable from the LAN-port on the MP (make sure the MP is powered up) to the wall jack (cabled Internet).

3. Open the terminal window on the PC by pressing "Ctrl+Alt+t" and type in the following commands to telnet into the MP:

```
$ sudo su
$ telnet 10.10.1.20
```

We highly recommend that you enhance the security on the MP by enabling SSH instead of telnet. This has no impact on this set-up, and will not affect the ability to provide Internet access to the network. Description on how to enable SSH is found in section 4.1.1.

4. To verify that the previous command was executed correctly, a "picture" will appear in your terminal saying "Welcome to Village Telco". Execute the following command to finish the set-up:

```
$ udhcpc -i br-lan
```

5. A "Sending discover ..." appears, and a lease is obtained like shown in Figure 5.4.

```
root@MP2-26:/# udhcpc -i br-lan
udhcpc (v1.19.4) started
Sending discover...
Sending discover...
Sending discover...
Sending select for 129.241.209.242...
Lease of 129.241.209.242 obtained, lease time 302400
udhcpc: ifconfig br-lan 129.241.209.242 netmask 255.255.254.0 broadcast 129.241.209.255
udhcpc: setting default routers: 129.241.208.1
```

Figure 5.4: This figure shows the allocation of lease after executing "uchcpc -i br-lan".

6. After the lease is obtained, the MP is provided with Internet access. You can test this by connecting to the MP from, for example, your smart phone or a PC.

   - The name of the network: **MP2_21**
   - The password is: **potato-potato**

   Both the name and the password can be changed in the web interface.

5.5.3 Manual for Connecting the MP02 to the Internet via PC Getting WiFi from Landline or Cellular Network

If you have a PC that is able to connect to WiFi, there are different ways of getting wireless Internet access. You can connect to a wireless router with a landline connection, or you can establish a wireless connection to a device (for example a cell phone) that is acting as an access point (AP). You can set your smart phone to act as an access point. Most smart phones have this capability, allowing other devices to connect to it utilizing the cellular network to get Internet access. You can of course connect directly to this AP, but then the MP does not get Internet access, and can not spread it further to neighbouring MPs. The following set-up works for both types: either if you connect to a regular wireless router that gets Internet from for instance xDSL, or if you connect to an AP that has a cellular network (3G, 4G) available.

In order to perform this set up, a Linux PC connected to WiFi and an MP02 is required. The last octet (number) of the IP address of the MP, is a unique number for each MP. In the following example we use "x" as the last octet (the last number in the IP address). When carrying out the steps described in this manual, please replace the "x" with the last octet (number) written on your MP.

Figure 5.5 illustrates how the components are connected together in the following manual. The figure is provided to help the user get a better understanding of the network.

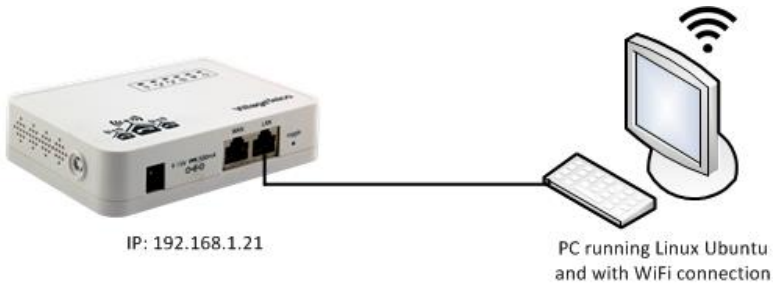


Figure 5.5: How the components are linked together during set-up for accessing the Internet via a PC. This figure shows how the different components are set-up when the manual for providing Internet access via PC is carried out. As shown the PC has a wireless Internet connection.

1. Connect the MP to the PC (make sure the MP is powered up) running Linux Ubuntu, with an Ethernet cable. The Ethernet cable must be plugged into the LAN-port on the MP.

2. Open Linux terminal by pressing "Ctrl+Alt+t" and install telnet, dns and iptables by entering the following commands:

```
$ sudo su
$ apt-get install telnetd
$ /etc/init.d/openbsd-inetd restart
$ apt-get install dnsmasq
$ apt-get install iptables
```

3. The Mesh Potato will be pre-configured with the IP address 192.168.1.x. In order to access the MP, the PC must be on the same subnet. If the PC has only one Ethernet port, this is most likely called eth0. If the PC has two or more Ethernet ports, make sure to change from eth0 to the correct port-name in the following command. Execute the following command to enter the PC into the same subnet as the MP:

```
$ ifconfig eth0 up 192.168.1.2
```

4. Open a browser on your PC and type in "192.168.1.x" in the URL field. Remember that x is equal to the last number of the IP address stated on the MP. The SECN Web Interface should now appear. This assures you that you have contact with the Mesh Potato. Changes in the interface will be described further down, so do not close this window.

5. If there is only one Ethernet port on the PC:

   <WIRELESS INTERFACE> = wlan0

   <INTERFACE CONNECTED TO MP> = eth0

   (It is not common, since most laptops only have one Ethernet port, but if there are two or more Ethernet ports on the PC, make sure to use the right ports in the following commands. In order to find out which ports are in use, execute the command "ifconfig" in the terminal. The ports in use will have a "inet addr" stated.)

   Go to the terminal and write the following commands in order to set up the ip tables correctly:

```
$ iptables --table nat --append POSTROUTING --out-interface
 <WIRELESS INTERFACE> -j MASQUERADE
$ iptables --append FORWARD --in-interface <INTERFACE
CONNECTED TO MP> -j ACCEPT
$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

- If you mess up in this step, accidentally write something wrong etc., the following commands will reset the ip tables, and you may try step 5 again.

```
$ iptables --table nat --flush
$ iptables --flush
$ iptables --delete-chain
```

6. Execute the following commands to telnet into the MP and configure the default gateway: (Note that the output of the command "route del default" may display "SIOCDELRT: No such process". This is because the MP does not have a default gateway. Ignore this notification.) Remember that x is equal to the last number of the IP address stated on the MP.

```
$ telnet 192.168.1.x
$ route
$ route del default
$ route add default gateway 192.168.1.2
```

   We highly recommend that you enhance the security on the MP by enabling SSH instead of telnet. This has no impact on this set-up, and will not affect the ability to provide Internet access to the network. Description on how to enable SSH is found in section 4.1.1.

7. Go back to the web interface and click on the "Advanced"-tab at the top of the page. Change the following parameters under "DHCP Server":

   - Tick the box "Enable DHCP Server".
   - Remove the tick from "Use device IP".
   - Change the address in "Gateway Router" to "192.168.1.2".
   - Press "Save" at the bottom of the page.

8. Internet access should now be available in the mesh network. You can test this by connecting to the MP from, for example, your smart phone or a PC.

   - The name of the network: **MP2_21**
   - The password is: **potato-potato**

   Both the name and the password can be changed in the web interface.

Script providing Internet access via PC

An alternative, and easier method in order to provide Internet access to the MP via a PC with WiFi, is running a script. A script is a list of commands that can be executed with less user interactions to automate a process. The script is provided on a USB-stick that is included in the QUICK box.

A few easy steps must be conducted to run the script:

1. Connect the MP to the PC (make sure the MP is powered up) running Linux, with an Ethernet cable. The Ethernet cable must be plugged into the LAN-port on the MP.
2. Plug the provided USB-stick into the PC.
3. Open the terminal on your PC by pressing "Ctrl+Alt+t".
4. Execute the following commands to enter the right directory (where the script is located):

   ```
   $ sudo su
   $ cd /media/MP-USB
   ```

5. Execute the following command to run the script (Follow the descriptions provided in the script from now on. This information will both be given in the terminal window and as pop-up windows. Make sure you read these carefully):

   ```
   $ sh scriptviaPC.sh
   ```

6. After completing the steps given by the script, Internet access should be available in the mesh network. You can test this by connecting to the MP from, for example, your smart phone or a PC.

   - The name of the network: **MP2_21**
   - The password is: **potato-potato**

   Both the name and the password can be changed in the web interface.

5.5.4 Manual for Connecting the MP02 to Satellite

If there is a satellite dish available, getting Internet access is fairly easy. Internet access via satellite does not use telephone lines or cable systems, but instead utilizes a satellite dish to get two-way data communication. To get Internet access via satellite you need a satellite dish, a modem (both for uplink and downlink), a coaxial cable between the dish and the modem, and an Ethernet cable from the modem to the laptop or MP.

Make sure that the cables are connected correctly. The coaxial cable must be connected from the satellite to the modem. There are two alternatives for where to plug in the Ethernet cable. The one end must be connected to the modem, and the other can either be connected to an MP or a PC.

If you choose to connect the Ethernet cable directly to the MP, the set-up in section 5.5.2 must be executed.

Another option is to connect the Ethernet cable from the satellite modem to a PC. One drawback with this approach is that the PC must have two Ethernet ports (one to connect to the MP, and one to the modem). If two Ethernet ports are available, the set-up for getting Internet access to the MP is identical to the set-up "Manual for Connecting the MP02 to the Internet via PC Getting WiFi from Landline or Cellular Network" (section 5.5.3). Although this is a set-up from a PC getting wireless Internet, it also works with a PC getting cabled Internet. Just make sure that the right interfaces (name of port) is chosen in step 3 and 5. To get an overview over available interfaces, the following command can be executed in the terminal window: "iwconfig".

Chapter 6
Testing the QUICK Box

In order to assure the quality of the manuals and the QUICK box, we conducted a test iteration. Testing is one of the most important parts of the process when developing a product. Using test persons with different technical background and knowledge, as well as different gender and age, provided us with valuable feedback and comments on issues that we in advance did not foresee.

Table 6.1: Key facts about the test participants

Test person	**Gender**	**Age**	**Technical knowledge**
Test person 1	Male	28	High
Test person 2	Female	25	High
Test person 3	Female	22	Low
Test person 4	Male	21	Low/medium

6.1 Test Procedure

The main focus when performing the tests was to assure the quality of the manuals we had created. We wanted to find out if the manuals were intuitive and user-friendly.

The tests were performed in our office, since the focus was on the manuals and not on the concept of the QUICK box. The test persons were given the different manuals, an MP, an Ethernet cable, a USB-stick containing the script and a stationary PC running Linux Ubuntu with WiFi connection. We gave them a short introduction to what our project consists of. After this introduction, the test persons started following the manuals, one at a time. In real life there will most likely only be necessary to run through one of the manuals. Every test person ran through all the manuals, in order for us to get as much feedback as possible. This gave the test

persons the opportunity to compare the different manuals. While the test persons were running through the manuals, we observed their actions. The test persons were allowed to ask questions, although it was desirable that the test persons tried themselves before asking. If we observed that the test persons performed mistakes, caused by lack of information or poor information in the manual, we stopped the test persons and guided them towards correcting the mistakes. After a manual was completed, the test persons assured that they were able to connect to the Internet via the MP, and were asked to answer a few questions regarding their experience. The questions concerned their previous use, and knowledge, of Linux and how this affected their test experience, how easy they felt it was to follow the manual, and if they had any suggested improvements. While the questions were asked, the MP was rebooted and set up ready for the next manual. The same procedure was followed for all three manuals.

The test was first performed on test person 1 which is considered a person with high technical knowledge. This test showed that the manuals were lacking a lot of crucial information. We chose to correct the shortcomings before conducting the tests on the remaining test persons, since these shortcomings went on the expense of the test's purpose.

6.2 Test Results

We will go through the results for each of the manuals and highlight the most interesting findings, before comparing them.

6.2.1 Manual 1: Manual for Connecting the MP02 Directly to Cabled Internet

After test person 1 tested this manual, we did a lot of changes to the language and in how the steps were described. The figures were changed out with more descriptive ones and placed closer to the respective steps in order to make it more visual for the user.

This manual was considered the easiest by all test persons. There were little confusion regarding the steps described. The test persons expressed that they liked the pictures and felt it worked as an assurance that they were conducting the steps correctly. Test person 3 and test person 4 both expressed some confusion regarding step 3 where the user is asked to write in terminal-commands. Originally, there were no information stating that the user had to open the terminal, or on how to open the terminal. Due to this feedback, information regarding this was added to the manual. The last step also caused some confusion. Originally, the step described that the login information could be found in the "Get started -How to Use the QUICK

Box"-document. This document was also provided to the test persons, but non of them even looked at it or asked for it. The text in this step has also been improved to avoid confusion.

6.2.2 Manual 2: Manual for Connecting the MP02 to the Internet via PC Getting WiFi from Landline or Cellular Network

Test person 1 expressed some confusion while running through this manual. One obstacle test person 1 pointed out was the use of the word octet. Test person 1 is considered a person with high technical knowledge, but were still unsure about the meaning of this word. In the manual we added more information explaining that with "the last octet" we mean the last number of the IP address. Another step that confused test person 1 was step 5. In this step the user is asked to enter some terminal-commands where the user has to change two of the variables. It was unclear to test person 1 what to write and how to find out if the variables were correct or not. We changed this text to include more information about which variables should be changed and on how to find these. Test person 1 stopped up when receiving an "error-message" after entering the command "route del default" in step 6. This command deletes the default route, if one exists. If no default route is set, an "error-message" will be displayed. Test person 1 was unsure if he had done something wrong. We added information stating why this "error-message" appears and that it can be ignored.

Most steps in this manual are executed in the terminal. Two of the test persons had no previous experience with Linux or the use of the terminal. This showed a clear difference between the technical and "non-technical" test persons. The technical test persons had no problem finding the terminal and immediately started entering the commands described in the manual. The "non-technical" test persons expressed hesitation and confusion around where to find the terminal and on how to write commands. Test person 4 started writing a command with the "$". This symbol is used to indicate that the following is a command. Test person 3 started writing a new command before the last one was "finished". This emphasized the lack of Linux knowledge and Linux-terminal experience.

In step 4, the user is asked to open the web browser and type in the MP's IP address in order to make sure that the PC has established contact with the MP. Test person 3 typed in "192.168.1.x", which is exactly what is stated in the manual. Previously in the manual, it is described that x has to be replaced with the last number of the IP address. The same mistake happened in step 6, where test person 3 also forgot to replace the "x"-value with the last number of the IP address. We

have now added this information in the given steps, in addition to in the beginning of the manual.

Even though we made some changes to step 5, after test person 1's feedback, this step still caused a lot of confusion for the remaining test persons. All started typing the command exactly as stated in the manual, even though it was described in the step that some parameters had to be changed. We rewrote this text in order to avoid any more confusion. Only test person 2 understood that the parameter "<WIRELESS INTERFACE>" had to be changed. The correct alteration is "wlan0", but test person 2 typed "<wlan0>", meaning she did not remove the "crocodile symbols".

The last step also caused some confusion. Originally, the step described that login information could be found in the "Get started -How to Use the QUICK Box"-document. This document was also provided to the test persons, but non of them even looked at it or asked for it. The text in this step has also been improved to avoid this confusion.

6.2.3 Manual 3: Script providing Internet access via PC

While testing this manual, test person 1 pointed out that the manual was missing a lot of necessary information. Test person 1 stopped up at step 1, where the manual did not describe which port on the MP the Ethernet cable should be plugged into. Nor did the manual contain any information regarding that the user had to open the terminal and on how to open it. The user was provided with a USB-stick containing the script, but this was not stated in the manual, nor that the USB-stick has to be plugged in before entering the given commands. After the script started, and the first pop-up window appeared, test person 1 immediately looked at the manual for further instructions, although these are provided in the pop-up window. The manual did not contain any information about what to do after the script started running. Test person 1 also expressed that it was difficult to understand what was meant by "wireless interface". Test person 1 was one of the technical people participating in our test and were able to figure out what the wireless interface was on his own. There were no confusion regarding the second pop-up window, but he pointed out that the text could be structured in a different way to better emphasize the important content. Test person 1 also pointed out that it was positive that the commands were written in a separate font, since this made it easier to understand.

We improved the manual based on the feedback from test person 1. Test person 3 were one of the "non-technical" test persons, and got confused when the first pop-up window appeared. Even though we made it very clear in the manual that it is important for the users to carefully read the information given in the script, test person 3 immediately looked at the manual when she saw the first pop-up. The script

asks the user to enter two variables, the last number of the IP address and the name of the wireless interface, in the terminal. Test person 3 entered just one variable before pressing enter, while test person 2 entered the whole IP address. Several test persons expressed confusion regarding the pop-up windows. Originally, the pop-up window appeared before the browser opened, which means that the test persons did not notice it. We have now changed this so that the browser opens first, then the pop-up window.

The last step also caused some confusion. Originally, the step described that login information could be found in the "Get started -How to Use the QUICK Box"-document. This document was also provided to the test persons, but non of them even looked at it or asked for it. The text in this step has also been improved to avoid this confusion.

6.2.4 Summary of the Test Results

Test person 1 was the first person to test our manuals. He found a lot of mistakes and possible improvements. After the manuals were updated and run on the other test persons there were still steps that was considered confusing. The areas of confusion were mainly around the same steps. All test persons had difficulties understanding what they were supposed to do in step 5 of manual 2, concerning changing the port names. All test persons were also confused about the log-in information in all the three manuals. The test persons had most difficulties with manual 2, and the least difficulties with manual 1. Test person 3 and test person 4 preferred manual 1, because it was the easiest and did not involve much writing. Test person 1 and test person 2, on the other hand, preferred manual 3, script.

The testing process went according to plan, and all the test persons were satisfied. We did not encounter any obstacles of significance, and collected a lot of valuable feedback.

Chapter 7
Discussion

Until today the Mesh Potato has mainly been used to create permanent communication infrastructures in villages all over the world. The deployments have mostly been in rural areas where the existing communications systems are expensive and the coverage is unsatisfactory. There is no doubt that mesh networking is an up-and-coming means of communication. One example is Apple implementing the Multipeer Connectivity framework in their newest iOS. The fact that a large company, like Apple, is investing in this type of technology is a major driving force for the technology itself. During the last decade, Apple has pioneered innovation in the technological world. It is clear that other companies have tried to emulate Apple's technological contributes to the market, both in terms of features and design. The iPad is a good example of this, since Apple were the first to introduce a tablet that caught customers' attention. The iPad became extremely popular, and within a short time other big companies, like Samsung, introduced similar products. This indicates that Apple is a trendsetter, and that by introducing the Multipeer Connectivity framework this will help mesh networking become better known and a more prominent means of communication in the future. In a world that is becoming increasingly technological with every passing day, there are still places and people that are not connected, and there are still locations throughout the world without Internet access.

Even though the Mesh Potato deployments today are permanent, this is not a limitation. The question is how could the Mesh Potato be utilized as a mobile installation, and in what situations would there be a need for a communications system like this? When a natural disaster occurs, there are many examples to illustrate that communications become an important issue. Just look at the situation during hurricane Sandy, the typhoon in the Philippines and the tsunami in Japan. Mobile towers were down, Internet access was lost, and there were power outages. People might have to walk long distances in order to find an Internet café or even to receive cell phone signal. The lack of a communications infrastructure makes the coordination process with and for the relief organizations difficult and time consuming. Natural disasters are not the only scenario where a mobile communications system

would be of great importance. We have also looked at the possibility of using this mobile installation at major festivals and in temporary refugee camps.

Village Telco provides people with an extensive Wiki page. Unfortunately this page is not very well structured and can seem very confusing, as well as not being user friendly. In addition to this, the majority of the descriptions provided on the Wiki are directed towards the MP01. We started our research by setting up a network existing of MP01s, and then moved on to the second generation. The second generation of the MP has been improved in many areas, making the MP02 both faster and easier to use, hence the descriptions are outdated and too complicated. A lot of the descriptions for the MP01 requires the use of shell commands, while with the MP02 more configurations can be carried out using the SECN web interface. Shell commands are not well known to the man in the street, and can easily cause misunderstanding or mistakes, and may create much confusion. It may be hard to undo actions conducted using shell commands, especially if one does not have any knowledge of it. We have simplified these descriptions, both in order to make them more understandable for the user and to direct them towards the second generation of the MP. When a Village Telco is set up there are usually some individuals with the necessary technological expertise who are in charge. With the QUICK box we want to make it possible for anyone to set up the network, since the descriptions are as easy and explanatory as possible.

One of Village Telco's volunteers, Keith Williamson, has created and tested the use of a "go box" in disaster relief scenarios. This box was created with the first generation of the Mesh Potato, and tested during a small exercise in Maine, USA. The main difference between the "go box" and the QUICK box is the fact that we have created our box based on the second generation of the MP. At time of writing only the basic version of the MP02 is available. With the basic version it is not possible to connect a phone, but this feature will become available in the next version of the second generation (available for sale summer 2014). Another difference is the fact that the QUICK box includes everything needed for an installation: a solar panel, the necessary cables, and full descriptions on how to use the box and how to connect it to different uplinks. It is no use having all the descriptions available on the web, if you do not have access to the Internet. The QUICK box can be used both to create a local network without Internet access and a network with Internet access. The local network will not be connected to the outside world, but will make it possible for people to talk and send data between each other. The other option is to connect the QUICK box to an uplink, either through landline, cellular network or satellite. We believe that simplification and making information more accessible is a huge step in the direction of gaining users.

One aspect that is of high importance when talking about a mobile way of creating

a mesh network is the aspect of quick roll-out. By using scripts, and maybe in future self-running scripts, the process will be automated to a higher extent and will make it easier for users to employ. Automation will particularly make it easier for the users who are less technically-minded.

Unfortunately, we were not able to travel to one of the Village Telcos that are in operation. This implies that the study we have conducted is theoretical and based on previous work and the experiences arising from these. Our study is also based on the MP02, in terms of easy and descriptive explanations on "how to use". We believe that our study can constitute the basis for future work in making the MP more suitable for use in mobile situations, and further development of the QUICK box.

We tested the different manuals for providing Internet to the MP on four people of different age, gender and technological knowledge. Testing always retrieves valuable information and shed light on issues we had not previously taken into account. Based on the results presented in Chapter 6, many relevant findings and observations were made. We will present the observations while looking at different categories of test persons: "non-technical" versus "technical" individuals, and men versus women.

One thing we observed was that the "non-technical" test persons preferred manual 1, manual for connecting the MP02 directly to cabled Internet. This manual consists mostly of GUI-interaction, and little use of the terminal. We think this is the reason why the "non-technical" test persons preferred this manual. Most everyday interactions carried out with computers are preformed using the Graphical User Interface (GUI) provided by the different operating systems. This is therefore a more well-known type of interaction than the terminal. We observed that the "non-technical" test persons showed some hesitation when they realized that they had to use a different operating system, Linux, than they were used to. Matters did not improve when they were asked to perform terminal commands. This was the first time using the terminal for both of the "non-technical" persons. Using GUI in an unknown operating system might also be less frightening than using the terminal.

The test persons with a technical background, on the other hand, chose manual 3 (script for getting Internet via PC) when they were asked which manual they preferred. They showed confidence when faced with the use of both Linux and the terminal. It was clear from our observation that this was not the first time the test persons with technical knowledge and background made use of Linux and terminal commands. An observation that backs up this assumption is the fact that they used keyboard shortcuts (Ctrl+Alt+t) to open the terminal window. We also observed that one of them used keyboard shortcuts (arrow up to get the latest command used) in the terminal, and one of them knew the commands in order to find the wireless

interface and to toggle between directories (also inside the terminal). None of these actions were described in the manuals.

Another observation we made while comparing the "non-technical" and the technical test persons is that the technical test persons became more caught up in the different commands and their output. They paid more attention to the content of the commands. An example of this is the command "route del default" in manual 2 (manual for connecting the MP02 to Internet via PC getting WiFi from landline or cellular network). This command prints out a short message that could be perceived as an error-message, although it is not. One of the technical persons stopped up after this message appeared, and thought something had gone wrong. The "non-technical" persons did not pay attention to this output. In fact, they did not pay attention to any outputs at all. When a user telnets into the MP, a large welcoming figure appears in the terminal window. The technical test persons were fascinated by this, and commented on it. The "non-technical" test persons, on the other hand, did not show any visible expression or fascination towards this. This could be because they simply did not notice it, or did not care. We found this strange, since we thought that the graphical elements of the set-up would be of more fascination and more conspicuous. While performing manual 3 (script for getting Internet via PC) two pop-up windows appear during the set-up. All the test persons expressed some hesitation when seeing these pop-up windows. One of the "non-technical" test persons immediately closed the first window when it appeared. It seemed as if she got confused when the pop-up window appeared. It could be that she thought it was something unrelated to the script and wanted to close the window so as not mess up what she was doing. The technical test persons were more interested in how the MP and the set-ups work. During the set-up they asked questions and showed curiosity regarding the tests they were performing. This was not the case for the "non-technical" test persons. This might be because they do not have enough knowledge to ask relevant questions. Internet is a commonly used phenomenon, but very few have detailed knowledge about how it works. The observation mentioned (the fact that the "non-technical" does not pay attention to the output) is not necessarily a negative fact. Since they have little knowledge they do not question the commands or get caught-up in insignificant details. In other words, too much technical knowledge can result in unnecessary trouble and hesitation.

When comparing the men with the women, we made some interesting observations. Men are typically more confident in their own ability, while women often tend to be more cautious and to make sure they do the right thing. Our observations verify this assumption. We immediately noticed that the men seemed more confident, and when provided with the different components immediately wanted to plug everything together, before even opening the manual. The women, on the other hand, read the manual thoroughly. Although the women read the manuals with greater care, the

men were the ones who paid most attention to proof-reading the commands in the terminal before executing them. This resulted in fewer misspelt commands for the men, hence fewer redos.

Chapter 8
Conclusion

The Internet is regarded as being a human right. However, more than two thirds of the world's population are without Internet access. With the extreme weather, and climate change, natural disasters are becoming increasingly common. Whenever these disasters occur, existing communications systems often break down, or can not be utilized due to power outages. The above conditions lead to the need for a mobile communications system. We have created a solution which can be deployed all over the world and give voice services and Internet access to a larger area. This solution can be utilized by everyone, from small and large relief organizations to the man in the street. An important factor is that the system has to be affordable and easy to use. Our solutions builds on Keith Williamson's concept, the "go box". We have taken his solution to the next level, utilizing the second generation Mesh Potato, as well as including everything necessary for a quick set-up anywhere in the world, and in any situation. Hence, we named our solution the QUICK box.

QUICK stands for Quick User friendly Internet-providing Communication Kit. The Q stands for Quick, because it is easy to set up. We wrote manuals for all the different set-ups necessary to get started with the box and to provide Internet access for the network. We have also automated some of the set-up processes by making a script. The U stands for User friendly. The manuals we have made have been tested on both technical and "non-technical" persons, in order to make them easy to understand and as user-friendly as possible. I stands for Internet-providing. The focus during our research has been on providing Internet access to the network of Mesh Potatoes. The manuals we have written guide the user through how to get Internet access to the MP by using different types of uplinks, depending on the uplink available. C stands for Communication. In today's society, and especially during emergency situations, it is crucial to have the opportunity to communicate, both within a community, and with the outside world. K stands for Kit, since this solution is delivered in a mobile suitcase ready to go in any situation. The QUICK box includes a pre-configured Mesh Potato version 2, a battery to provide the MP with power, a solar panel to charge the battery, a charge regulator, necessary cables,

a CD with Linux Ubuntu, a USB-stick containing the script and the different set-up manuals. This results in a kit that can act as a stand-alone solution. This solution can be utilized within the context of different scenarios, covering everything from emergency situations and natural disasters, to festivals and temporary refugee camps.

In the process of setting up the Mesh Potatoes, various configurations and installations were conducted. Since Village Telco is a company based on voluntary work, the descriptions found on the wiki have been partially added along the way, resulting in an extensive, but not a user-friendly and a rather confusing page. We found these instructions difficult to use, and spent a lot of time interpreting them. A big part of our work has therefore been to simplify these instructions, and to include them in our solution. We want the descriptions to be universal, meaning that everyone, including "non-technical" people, can run through them. These descriptions have therefore been "dumbed down", and simplified. We looked at different types of uplinks, and created manuals for connecting the MP to each of them.

Ever since Village Telco was founded in 2008, both Village Telco's devices (MPs) and mesh networking in general have been under constant development. It is clear that Village Telco has a burning passion for providing affordable communications in rural areas. A considerable amount of new research has been conducted in this field during a short period of time. There is no doubt that mesh networking is an up-and-coming technology. This is supported by Apple's introduction of the Connectivity framework. Without hesitation, we can conclude that mesh networking is a technology we will see more and more of in the near future.

8.1 Future Work

The research presented in this paper has only touched the surface of the Mesh Potato's potential. There are a great many aspects that need to be taken into consideration for further work in this area. The results we have presented in this paper can lay the basis for improvements of the QUICK box. One possibility is to conduct a more detailed and extensive testing of the QUICK box, including testing in real-world scenarios. One possibility for future work could be to make automated scripts for connecting to each uplink type. Each uplink type could have its own USB-stick. When Internet connection is desirable, the user could then simply plug in the corresponding USB-stick, and the rest of the set-up would proceed automatically. This emphasizes Village Telco's vision of a plug-and-play solution. Another future possibility for the Mesh Potato, is to enable the possibility to communicate with other commercial mesh networks, such as Apple's. The possibilities are virtually infinite, since this is a complex and a very hot topic.

References

[1] S. Cope, "Internet connection and access methods," 2011. http://www.steves-internet-guide.com/connect-methods/, accessed 31.03.2014.

[2] A. Sedghi and S. Rogers, "Unhcr 2011 refugee statistics: full data," June 2011. http://www.theguardian.com/news/datablog/2011/jun/20/refugee-statistics-unhcr-data, accessed 24.03.2014.

[3] A. Sedghi, "Unhcr 2012 refugee statistics: full data," June 2013. http://www.theguardian.com/news/datablog/2013/jun/19/refugees-unhcr-statistics-data, accessed 20.03.2014.

[4] D. Valenzuela and P. Shrivastava, "Interview as a method for qualitative research." http://www.public.asu.edu/~kroel/www500/Interview%20Fri.pdf, accessed 16.05.2014.

[5] J. Dempsey, "The mesh potato network," 2008. http://ictupdate.cta.int/en/Feature-Articles/The-mesh-potato-network, accessed 26.02.2014.

[6] Village Telco, "Village telco workshop," 2008. http://villagetelco.org/2008/07/village-telco-workshop/, accessed 24.02.2014.

[7] Village Telco, "The origin of the mesh potato," Last edited: 2013. http://villagetelco.org/2008/06/the-origin-of-the-mesh-potato/, accessed 21.02.2014.

[8] Village Telco, "Background village telco," Last edited: 2013. http://wiki.villagetelco.org/Background, accessed 20.02.2014.

[9] Village Telco, "Mesh potato," 2013. http://store.villagetelco.com/mesh-potatoes/mesh-potato.html, accessed 20.02.2014.

[10] Wikipedia, "Binary bolb," Last modified December 2013. http://en.wikipedia.org/wiki/Binary_blob, accessed 05.03.2014.

[11] D. Rowe, "The mesh potato part 1," 2008. http://www.rowetel.com/blog/?p=70, accessed 26.02.2014.

[12] "Village telco deployments." http://villagetelco.org/deployments/, accessed 30.04.2014.

[13] Village Telco, "Dili village telco." http://villagetelco.org/deployments/dili/, accessed 30.04.2014.

[14] Quandl, "Timor-leste." http://www.quandl.com/timor-leste, accessed 11.03.2014.

[15] Wikipedia, "Telecommunications in east timor." http://en.wikipedia.org/wiki/Telecommunications_in_East_Timor, accessed: 20.03.2014.

[16] BuddeComm, "East timor (timor leste) - telecoms, mobile and internet." http://www.budde.com.au/Research/East-Timor-Timor-Leste-Telecoms-Mobile-and-Internet.html, accessed: 20.03.2014.

[17] Village Telco, "Jose soto - puerto rico." http://villagetelco.org/deployments/jose-soto-puerto-rico/, accessed 30.04.2014.

[18] ArsTechnica, "How one man is bringing voip, 'net access where telecoms fear to tread," 2012. http://arstechnica.com/business/2012/08/how-one-man-is-bringing-voip-net-access-where-telecoms-fear-to-tread/, accessed: 29.04.2014.

[19] M. Macadamia, "Ict." http://mataffinmacadamia.co.za/ict.html, accessed: 10.04.2014.

[20] International Telecommunication Union, "50 years of excellence," 2006. http://www.itu.int/itudoc/gs/promo/tsb/88192.pdf, accessed: 11.05.2013.

[21] J. Hallock, "A brief history of voip," *Evolution*, 2004.

[22] T. Bruun, "Evaluation of telecom operator enabled internet telephony by creating a proof-of-concept web application," 2013. Master thesis IDI NTNU.

[23] OpenWrt Wiki, "About openwrt." http://wiki.openwrt.org/about/start, accessed 03.03.2014.

[24] Indiana University, "What is telnet?." http://kb.iu.edu/data/aayd.html, accessed 25.04.2014.

[25] Indiana University, "What is telnet/ssh?." https://service.futurequest.net/index.php?/Knowledgebase/Article/View/31, accessed 25.04.2014.

[26] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," 2004.

[27] J. Wang, B. Xie, and D. P. Agrawal, *Journey from Mobile Ad Hoc Networks to Wireless Mesh Networks*, pp. 1–30. Springer London, 2009.

[28] B. D. Shivahare, C. Wahi, and S. Shivhare, "Comparison of proactive and reactive routing protocols in mobile adhoc network using routing protocol property," *International Journal of Emerging Technology and Advanced Engineering*, 2012.

[29] X. Hong, K. Xu, and M. Gerla, "Scalable routing protocols for mobile ad hoc networks," *IEEE*, 2002.

[30] A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better approach to mobile ad-hoc networking (b.a.t.m.a.n.)," 2008. http://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00, accessed 21.02.2014.

[31] Freie Universität Berlin, "Better approach to mobile ad hoc networking (b.a.t.m.a.n.)." http://www.des-testbed.net/content/better-approach-mobile-ad-hoc-networking-batman, accessed 24.02.2014.

[32] Village Telco, "Spud – simple unified dashboard for mesh networks." http://villagetelco.org/2011/06/spud-simple-unified-dashboard-for-mesh-networks/, accessed 26.02.2014.

[33] D. Kravets, "U.n. report declares internet access a human right." http://www.wired.com/threatlevel/2011/06/internet-a-human-right/, accessed 14.03.2014.

[34] B. Mitchell, "What is an uplink(port)?." http://compnetworking.about.com/od/homenetworking/f/uplink-port.htm, accessed 14.03.2014.

[35] Digital Unite, "How to connect to internet." http://digitalunite.com/guides/using-internet-0/connecting-internet/how-connect-internet, accessed 27.03.2014.

[36] J. A. Audestad, *Technologies and Systems for Access and Transport Networks*. Artech House, Inc., 2008.

[37] A. Chianis, "Cable vs. satellite — which internet connection serves your business best?." http://www.businessbee.com/resources/news/technology-buzz/cable-vs-satellite-internet-connection-serves-business-best/, accessed 14.03.2014.

[38] J. J. Parsons and D. Oja, *New Perspectives on Computer Concepts 2010:Comprehensive*, pp. 313–315. Course Technology, 2010.

[39] International Telecommunication Union, "The world in 2013: Ict facts and figures." http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf, accessed 28.03.2014.

[40] International Telecommunication Union, "The world in 2011: Ict facts and figures." http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf, accessed 28.03.2014.

[41] B. Mithcell, "What is mobile broadband?." http://compnetworking.about.com/od/internetaccessbestuses/f/what-is-mobile-broadband.htm, accessed 28.03.2014.

[42] Diffen, "3g vs 4g." http://www.diffen.com/difference/3G_vs_4G, accessed 28.03.2014.

[43] E. S. Cohen, ed., *Broadband Internet: Access, Regulation and Policy*, pp. 80–81. 2007.

[44] Project Loon, "Projet loon: Balloon-powered internt for everyone." http://www.google.com/loon/, accessed 27.03.2014.

[45] R. Ramsdal, "Google fikk ja til å sende internett-ballonger over norge," March 2014. http://www.tu.no/it/2014/03/22/google-fikk-ja-til-a-sende-internett-ballonger-over-norge, accessed 23.03.2014.

[46] Project Loon, "Project loon," 2013-2014. http://www.youtube.com/user/ProjectLoon, accessed 28.03.2014.

[47] A. B. Smedsrud, "Disse ballongene skal gi internett til hele verden," June 2013. http://www.hardware.no/artikler/disse-ballongene-skal-gi-internett-til-hele-verden/134539, accessed 28.03.2014.

[48] Wikipedia, "Iridium satellite constellation." http://en.wikipedia.org/wiki/Iridium_satellite_constellation, accessed 09.04.2014.

[49] M. Elgan, "How an under-appreciated ios 7 feature will change the world," March 2014. http://www.cultofmac.com/271225/appreciated-ios-7-feature-will-change-world/, accessed 25.03.2014.

[50] FireChat, "app store: Firechat." https://itunes.apple.com/us/app/firechat/id719829352?mt=8&ign-mpt=uo%3D8, accessed 27.03.2014.

[51] Apple, "About multipeer connectivity," September 2013. https://developer.apple.com/library/ios/documentation/MultipeerConnectivity/Reference/MultipeerConnectivityFramework/Introduction/Introduction.html, accessed 25.03.2014.

[52] M. Elgan, "Why google is working on home mesh networking," March 2014. http://www.eweek.com/cloud/why-google-is-working-on-home-mesh-networking.html, accessed 27.03.2014.

[53] The UN Refugee Agency, "What is a refugee?." http://www.unrefugees.org/site/c.lfIQKSOwFqG/b.4950731/k.A894/What_is_a_refugee.htm, accessed 20.03.2014.

[54] Refugees International, "Somalia." http://refugeesinternational.org/where-we-work/africa/somalia, accessed 24.03.2014.

[55] Refugees International, "Iraq." http://www.refugeesinternational.org/where-we-work/middle-east/iraq, accessed 24.03.2014.

[56] Inveneo, "How better connectivity can help dadaab, the world's largest refugee camp," 2012. http://www.inveneo.org/2012/06/how-better-connectivity-can-help-dadaab-the-worlds-largest-refugee-camp/, accessed 10.03.2014.

[57] Care, "Dadaab refugee camps, kenya." http://care.org/emergencies/dadaab-refugee-camp-kenya, accessed 11.03.2014.

[58] Wikipedia, "Nethope," Last edited: 13 May 2013. http://en.wikipedia.org/wiki/NetHope, accessed 11.03.2014.

[59] Inveneo, "Dadaabconnect." http://www.inveneo.org/projects/dadaabconnect/, accessed 11.03.2014.

[60] M. Maasilta, "Outsiders or active citizents? the role of oral amd mediated ommunication in african refugee camps," ?

[61] Village Telco, "Choosing a firmware for the mp." http://villagetelco.org/get-started/choosing-a-firmware-for-the-mp/, accessed 09.04.2014.

[62] Village Telco, "Flash your mesh potato." http://villagetelco.org/get-started/flash-your-mesh-potato/, accessed 09.04.2014.

[63] Village Telco, "Installing vt secn firmware." http://wiki.villagetelco.org/Installing_VT_SECN_Firmware#Using_Potato_Flash_software, accessed 09.04.2014.

[64] K. Williamson, "Guest post: Adapting mesh potatoes for emergency work." http://villagetelco.org/2011/11/guest-post-adapting-mps-for-emergency-work/, accessed 02.04.2014.

[65] AfrikaBurn, "What is afrikaburn?." http://www.afrikaburn.com/about/what-is-afrikaburn, accessed 05.05.2014.

[66] S. Song, "Africa burns for a village telco." http://manypossibilities.net/2010/05/africa-burns-for-a-village-telco/, accessed 05.05.2014.

[67] D. Carman, "Afrikaburns again for a village telco." http://villagetelco.org/2011/05/afrikaburns-again-for-a-village-telco/, accessed 05.05.2014.

[68] Dictionary.com, "Natural disaster." http://dictionary.reference.com/browse/natural+disaster, accessed 19.03.2014.

[69] S. Kelly, "What is the best shtf/disaster communication?." http://graywolfsurvival.com/2716/ham-radio-best-shtfdisaster-communication/, accessed 01.04.2014.

[70] D. Smithfield, "Haiti's uphill battle: Developing countries struggle with natural disasters," October 2013. http://www.refugeesinternational.org/blog/haiti%E2%80%99s-uphill-battle-developing-countries-struggle-natural-disasters, accessed 09.04.2014.

[71] Aurecon, "360° natural disaster," 2011. http://issuu.com/aurecon/docs/aurecon_360_issue3?mode=embed&layout=http%3A//skin.issuu.com/v/light/layout.xml&showFlipBtn=true, accessed 09.04.2014.

[72] Wikipedia, "Orkanen sandy." http://no.wikipedia.org/wiki/Orkanen_Sandy, accessed 31.03.2014.

[73] V. Insinna, "Natural disasters uncover ongoing emergency communications problems," June 2013. http://www.nationaldefensemagazine.org/archive/2013/January/Pages/NaturalDisastersUncoverOngoingEmergencyCommunicationsProblems.aspx, accessed 28.03.2014.

[74] Wikipedia, "Typhoon haiyan." http://en.wikipedia.org/wiki/Typhoon_Haiyan, accessed 01.04.2014.

[75] M. Tran, "Typhoon haiyan disaster response: how the relief effort worked," February 2014. http://www.theguardian.com/global-development/poverty-matters/2014/feb/07/typhoon-haiyan-disaster-response-philippines-relief-effort, accessed 01.04.2014.

[76] P. Greenberg, "Philippines disaster relief: How to help victims of typhoon haiyan." http://petergreenberg.com/2013/11/13/philippines-disaster-relief-efforts/, accessed 12.05.2014.

[77] J. Waits, "Amateur radio operators assist during and after typhoon in philippines," November 2013. http://www.radiosurvivor.com/2013/11/11/amateur-radio-operators-assist-during-and-after-typhoon-in-philippines/, accessed 12.05.2014.

[78] Wikipedia, "Liste over nedetid i mobilnettet i norge." http://no.wikipedia.org/wiki/Liste_over_nedetid_i_mobilnettet_i_Norge, accessed 19.03.2014.

[79] Nettavisen.no, "Telenor: Feilen i mobilnettet er rettet." http://www.nettavisen.no/nyheter/3168897.html, accessed 19.03.2014.

Appendix A
Interview with Care

This appendix contains the summary from the interview conducted on Mary Muia (CARE International in Kenya | Program Assistant Refugee Assistance Programme | Dadaab).

1. Approximately how many people are there in the Dadaab refugee camp? And how long have it been in operation?

   The Dadaab complex of refugee camps, considered the world's largest, was created in 1991 by the Government of Kenya and UNHCR to host Somali refugees displaced by civil war. Over the years, the camps have also hosted other nationalities from the Horn of Africa, the Great Lakes and East Africa regions but they constitute less than two percent of the camp population. The original camps were Dagahaley, Ifo and Hagadera and were intended to host 90,000 refugees. However, in 2011, there was an influx of new refugees from Somalia due to severe drought and new camps were created; Ifo 2 and Kambioos, to cater to the over 175,000 new arrivals and at the peak of the influx in 2011, the camps hosted more than 463,000 refugees, including some 10,000 third-generation refugees born in Dadaab to refugee parents who were also born there. However, in 2013, UNHCR and its partners conducted a verification exercise to ascertain the current population since some of those who had arrived in 2011 due to the famine had returned home. As at February, 2014, the current population stands at 369,294.

2. How do you connect and communicate with the outside world?

   CARE as an organization has invested in communication systems in liaison with Internet Service Providers in the capital city of Nairobi who ensure that all staff have access to internet for both official and social usage.

3. How are the communication inside the camp (communication flow)?

Several telecommunication firms in Kenya have put up their machinery in the area thus there is access to both mobile communication and access to internet services. There are also radio station services and access to digital televisions. CARE uses telephone services to reach out to refugee staff (50%) of the refugees have access to mobile phone services - either owned or through a bureau) posters and radio to reach out to its beneficiary population. In addition, there is word of mouth done through loud speakers during major gatherings like food distribution days and also road shows within the camps.

4. How does the refugees receive information?

   As 3 above.

5. Can you exlain what happens when a new person enters the camp?

   Upon arrival, a new refugee would report to a UNHCR reception desk whereby they are given temporary registration pending full registration and location of their relatives is they have any already in the camp. UNHCR fully briefs the new arrival on all the services available and which Agency is handling what service. Immunizations, medical attention, emergency food supply, tarpaulins, sleeping mats, jerrycans for fetching water and kitchen sets are issued to such new arrivals to help them start their new lives in the camps. UNHCR then hands over the new arrivals to the respective Agency doing camp management in the specific camp they are allocated so that they can be shown where to pitch their tents. The camps are well demarcated into numbered sections and blocks thus at any given time, UNHCR would inform you where a particular refugee resides and the family size. Each Agency working in Dadaab has their own mode of communicating the services they provide to their target beneficiaries. However, UNHCR holds regular meetings with the refugee leaders of each respective camp whereby information is shared with them for dissemination to the entire refugee population.

6. What are the biggest challenges in a refugee camp?

   Lack of enough space to accommodate everyone and lack of enough funds to take care of all the needs of the refugees.

7. What is the biggest challenge when it comes to communication/information spreading in the refugee camp?

   Language barrier between the humanitarian staff and the refugees since many of the staff do not speak/understand the Somali language while 95.6% of the refugees are Somali. Internet and telephone service outages are also common in the area and response by the service providers sometime take a while.

8. What means of communication do you use in the refugee camp?

Mobile phones and computers for both telephone and internet access. Radios and television services.

9. We have the impression that there are not many telecom providers offering telecommunication services in Africa, and hence little competition. Which in general makes the prices higher. How does the ones living in the camp afford to have a phone?

   (a) There are two main telecom provides here so yes, little competing thus high rates (b) Many refugees who have been here for over a long period of time have established small scale business (some supported by the NGO's i.e. IGA's (Income Generating Activities) thus make some little profit. Others have established business through the support of their relatives who have been resettled in other countries thus send them some cash while others who may have been businessmen back in Somalia made it to take some of the cash they had at the time of fleeing their country.

10. Is it "Internet cafes" that people have to pay to be able to use?

    Yes some refugees have set up small internet cafes in the markets thus people who need the services have to pay for it. CARE like other NGO's here has Community Development Projects which include ICT training where we train the youth on ICT and upon successful completion, we support then by providing them with start-up kits to establish their own small cafes for both business and training others youth.

11. How long does it take to set up a communication system?

    N/A since I am not a technical person

12. Do you use video surveillance?

    No

13. Have you heard of something called Freedom fone?

    No

14. Have you heard of the company Village Telco?

    No

15. Do you have anything else to add that can be of interest for our master thesis?

    No

Appendix B
Script for Internet via PC

This appendix contains the script (scriptviaPC.sh) we made and tested to get Internet via a PC to the Mesh Potato.

```
#!bin/bash


zenity --info --text 'This script set up the Mesh Potato
with Internet via a PC with wireless Internet connection.
Before running the script, make sure that the MP is
connected to the PC with Ethernet cable. '


echo -n "Enter the last number of the IP address stated
on the MP: "
read var1
echo "ip = $var1"

sudo apt-get install telnetd
sudo /etc/init.d/openbsd-inetd restart
apt-get install dnsmasq
apt-get install iptables

sleep 2

ifconfig eth0 up 192.168.1.2

sleep 2
```

```
iptables --table nat --flush
iptables --flush
iptables --delete-chain

sleep 2

iptables --table nat --append POSTROUTING --out-interface
wlan0 -j MASQUERADE
iptables --append FORWARD --in-interface eth0 -j ACCEPT
echo 1 > /proc/sys/net/ipv4/ip_forward

{
echo route del default
sleep 2
echo route add default gateway 192.168.1.2
sleep 2
echo "exit"
} | telnet 192.168.1.$var1


xdg-open http://192.168.1.$var1  &

sleep 3

zenity --info --text 'The web interface did now open in
the browser. In the interface click on the "Advanced"
tab at the top of the page.
Change the following parameters under "DCHC Server":
(1) Tick the box "Enable DHCP Server"
(2) Remove the tick from "Use device IP"
(3) Change the address in "Gateway Router" to "192.168.1.2"
(4) Press "Save" at the bottom of the page.

After the page is refreshed, there should be
Internet on the Mesh Potato. The login information
can be found in the
"Get Started - How to Use the Box"-document.'
```

Appendix C

SECN-1.1 User Guide

Village Telco
Small Enterprise / Campus Network
SECN-1.1

User Guide

SECN User Guide by T L Gillett is licensed under a
Creative Commons Attribution-ShareAlike 3.0 Unported License.
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-1.1 firmware.

Table of Contents

1. Introduction

The Small Campus Enterprise Network (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 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.

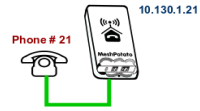
Configuration and management of individual mesh node devices is possible via telephone IVR commands (MP only), browser or terminal sessions with access to the underlying OpenWrt Linux operating system and software.

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.

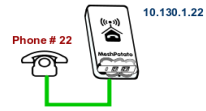
Step 1. Flash the MP devices to the SECN firmware.
(See following section for details of how to flash the devices.)

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 wwhen prompted.

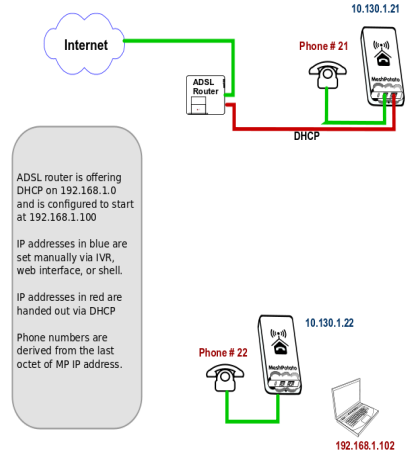


Repeat the process with the second MP, but dial ***22*** and wait for it to reboot.

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

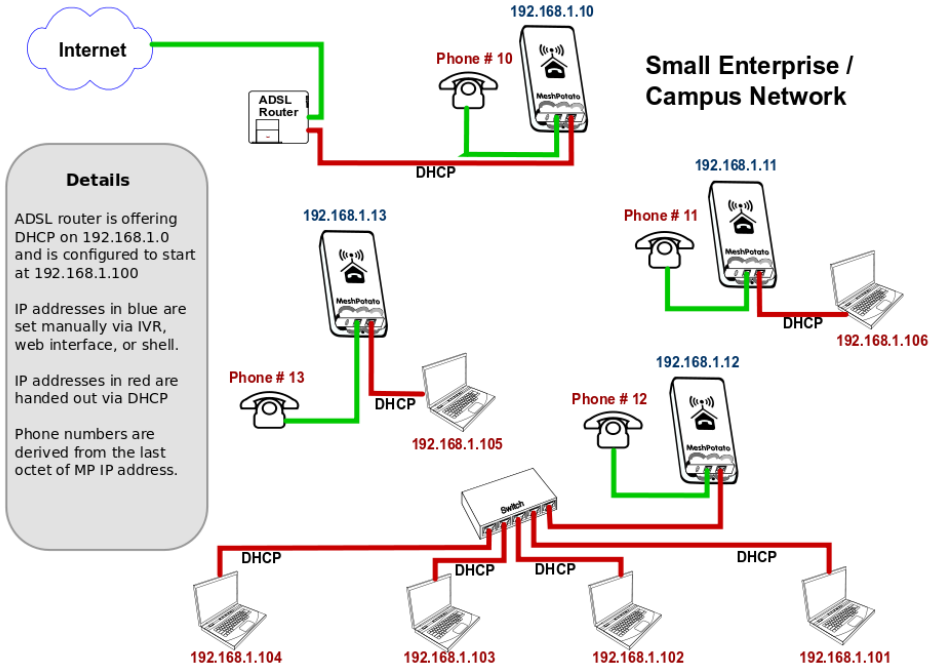
In this network, MP devices have been assigned static IP addresses that are part of the LAN address space, 192.168.1.xxx, and appropriate Gateway and DNS addresses.

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.

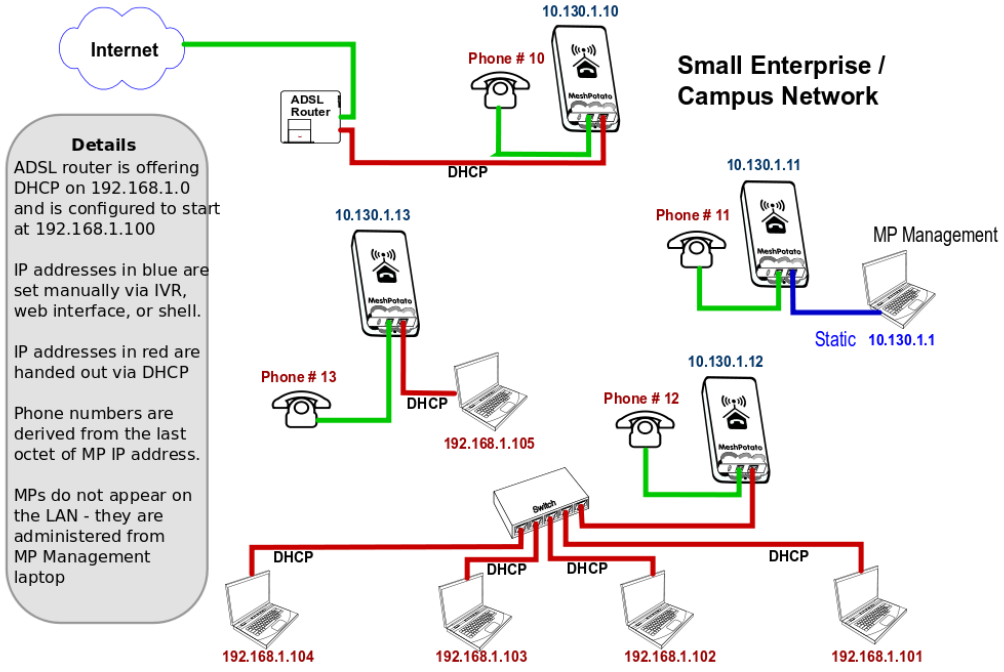
This means that the MP administration interfaces (SECN web interface and ***ssh*** command line) will not be accessible from workstations connected to the LAN with IP addresses assigned in the LAN address space.

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 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 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 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.l7" 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).

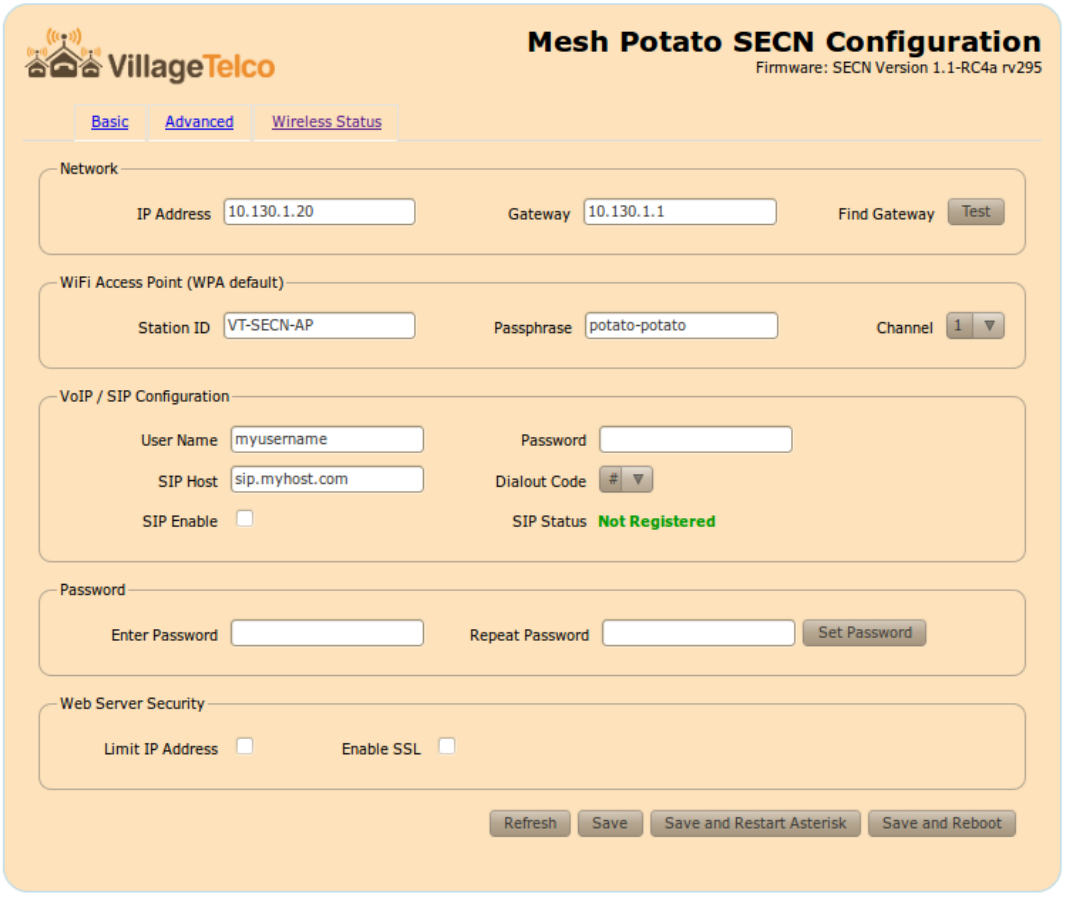
After the device has rebooted, you should be able to make a call to the device using either the full IP number, or abbreviated dialling using just the last octet of the address.

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



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

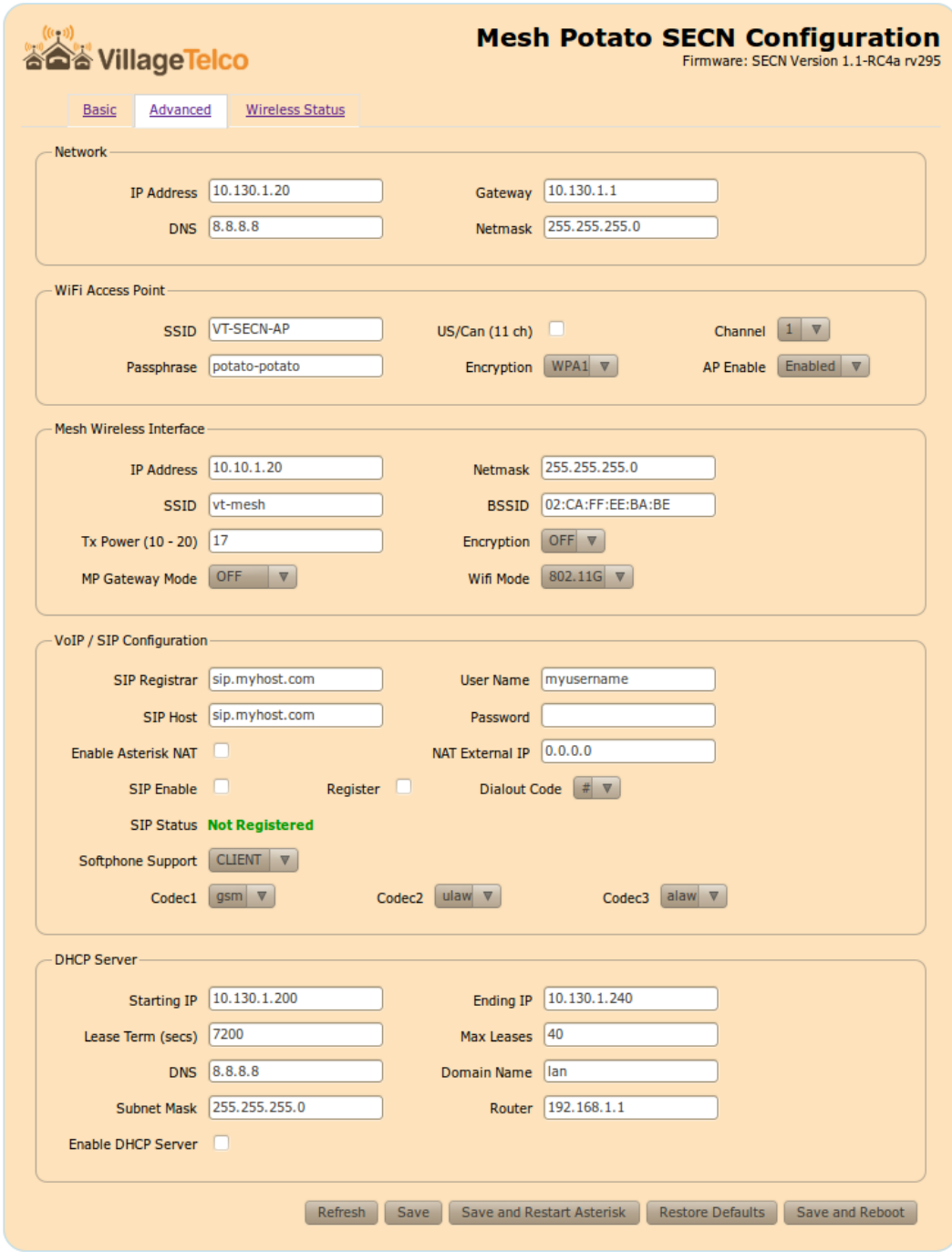
The ***Refresh*** button will simply refresh the field values from saved values in memory and check the registration status of the SIP/VoIP service.

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



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.

WiFi Access Point Configuration

The WiFi configuration allows you to set the ***Station ID*** (SSID), ***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 ***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 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.

Mesh Wireless Interface 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 ***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.

VoIP / SIP 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 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 address 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.

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 255.255.2555.0

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 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, ***ath0*** and ***ath1***, are set up on the wireless interface ***wifi0***.
- Batman-adv is configured to run on the ***ath0*** interface using the ***batctl*** command and generates the ***bat0*** interface.
- The second wireless interface, ***ath1***, is set up to operate as a WiFi access point using the *iwconfig* command.
- The ***bat0***, ***ath1*** 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 range used for the ***br-lan*** interface is 10.130.1.xxx

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 devicess 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 MPs 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), ***ath0*** 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 ***ath0*** 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, Zeroconf (yes, you can run mDNS on ***bat0***!), 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 ***ath1*** and ***eth0***.

eth0 is the LAN port of the MP. ***ath1*** is a access-point interface, operating as a master in WiFi infrastructure mode. (As opposed to a infrastructure client, like laptops or smartphones with a WiFi interface).

Hence **all** ***eth0*** and ***ath1*** 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 ***ath1***, ***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***, ***ath1*** 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 mod-ule 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:

```
uci set batman-adv.bat0.gw_mode=client 1
uci commit
/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 ***ath0*** mesh wireless interface IP address
2664	Read out the ***br-lan, eth0, ath1*** 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 list	Lists signal data for nearby devices on the mesh.
wlanconfig ath1 list	Lists signal data for devices attached to the MP's WiFi Access Point.
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:

***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:

```
# 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.

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:

- Start up Sipdroid and go to the Sipdroid settings.
- Create a SIP account with Authorization Username set to one of the account entries in the file ***softphone.sip.conf*** (e.g. softph300),
- Set the Password to match the account entry e.g. "Pa55uu0rd300"
- 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.

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:

 # 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

Appendix D

SECN-2.0 User Guide

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.
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

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 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

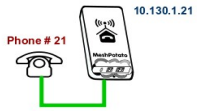
In this simple mesh network we will set up a network of two MP devices so that phone calls can be made between them, then connect one MP to a Local Area Network with Internet access so that a laptop can connect wirelessly to the virtual Access Point and access the LAN and Internet.

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.

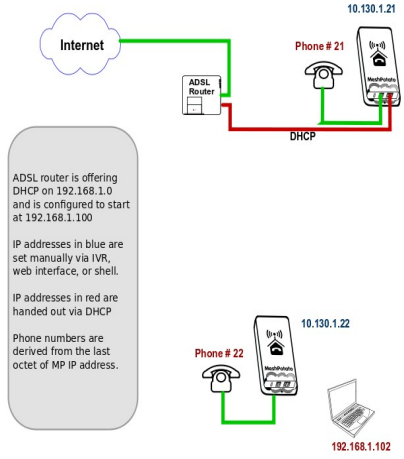
The MP devices are now set to IP addresses 10.130.1.21 and 10.130.1.22 respectively. It may be useful to label the devices as '21' and '22'

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

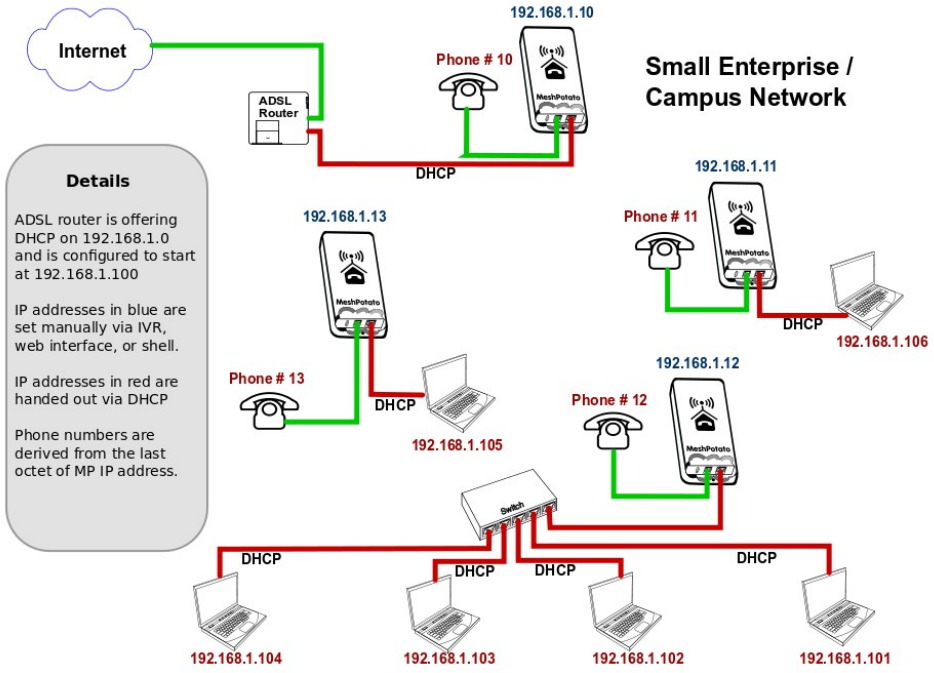
In this network, MP devices have been assigned static IP addresses that are part of the LAN address space, 192.168.1.xxx, and appropriate Gateway and DNS addresses.

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.

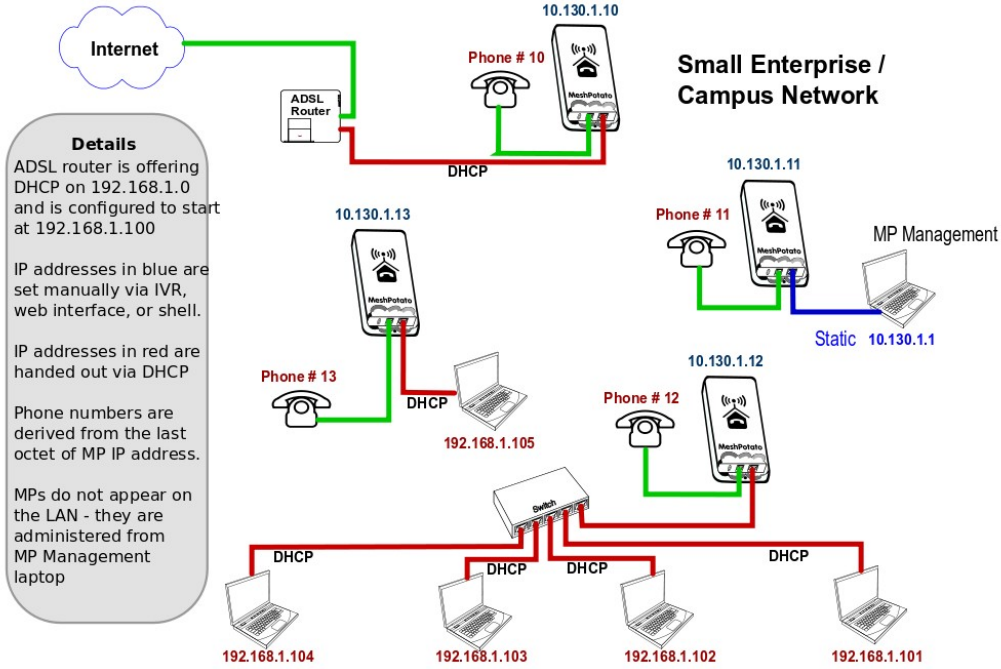
This means that the MP administration interfaces (SECN web interface and ***ssh*** command line) will not be accessible from workstations connected to the LAN with IP addresses assigned in the LAN address space.

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 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 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.l7"  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.

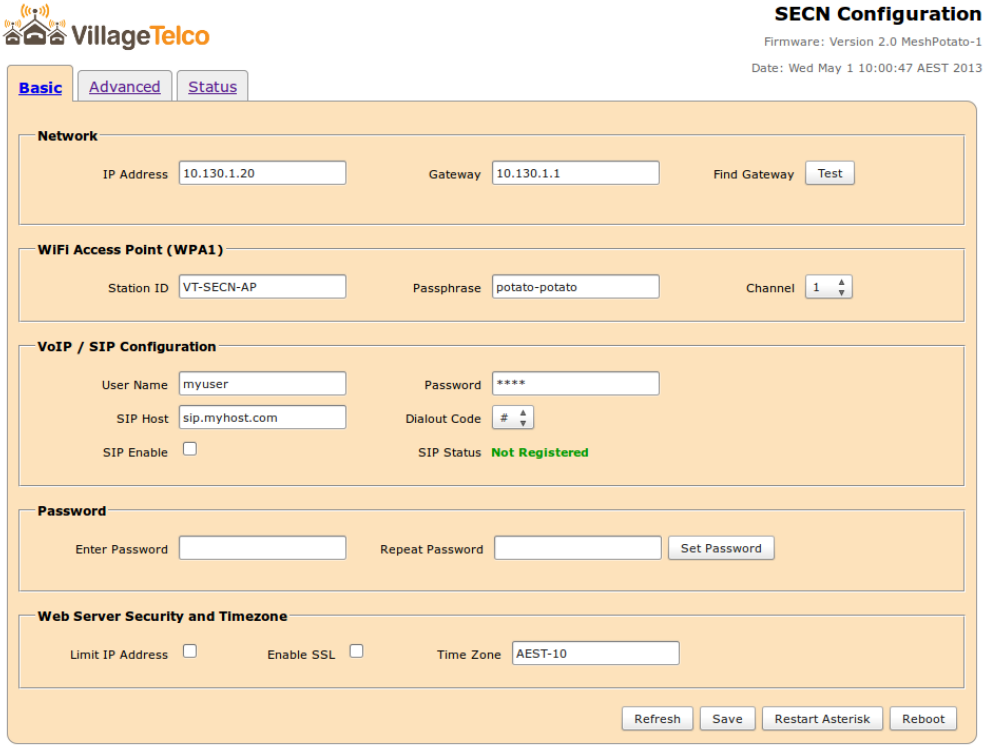
Note: When the ***br-lan*** address is set using IVR, the device's ***gateway*** address will be automatically be set to an address in the same subnet with the last octet set to **1** e.g 10.130.1.1 to ensure correct operation of Asterisk.

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



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

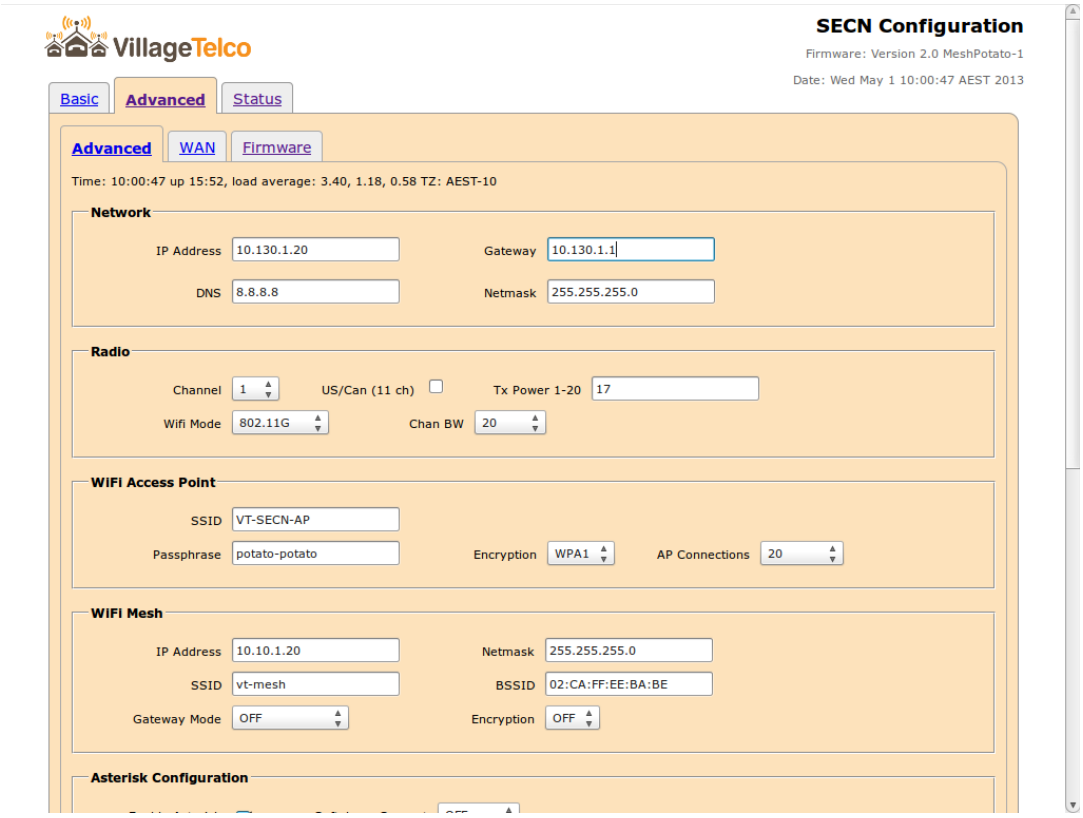
The Refresh button will simply refresh the field values from saved values in memory and check the registration status of the SIP/VoIP service.

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



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 XXXXXXXXXXXXXXXXXXXXXXXXX

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.

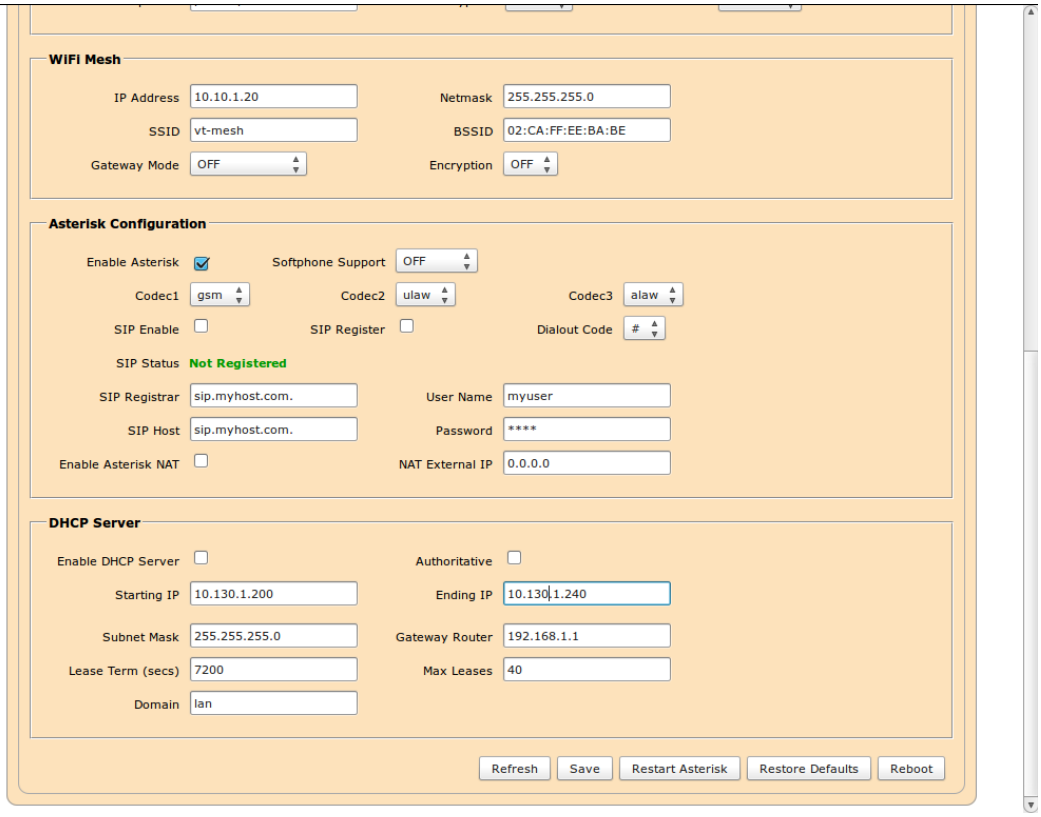
The Tx Power parameter may be used to adjust the power of the device radio transmitter. It is set by default to the maximum value of 17. Normally this should not need to be adjusted but doing so may be useful in certain circumstances such as testing.

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.



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 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.

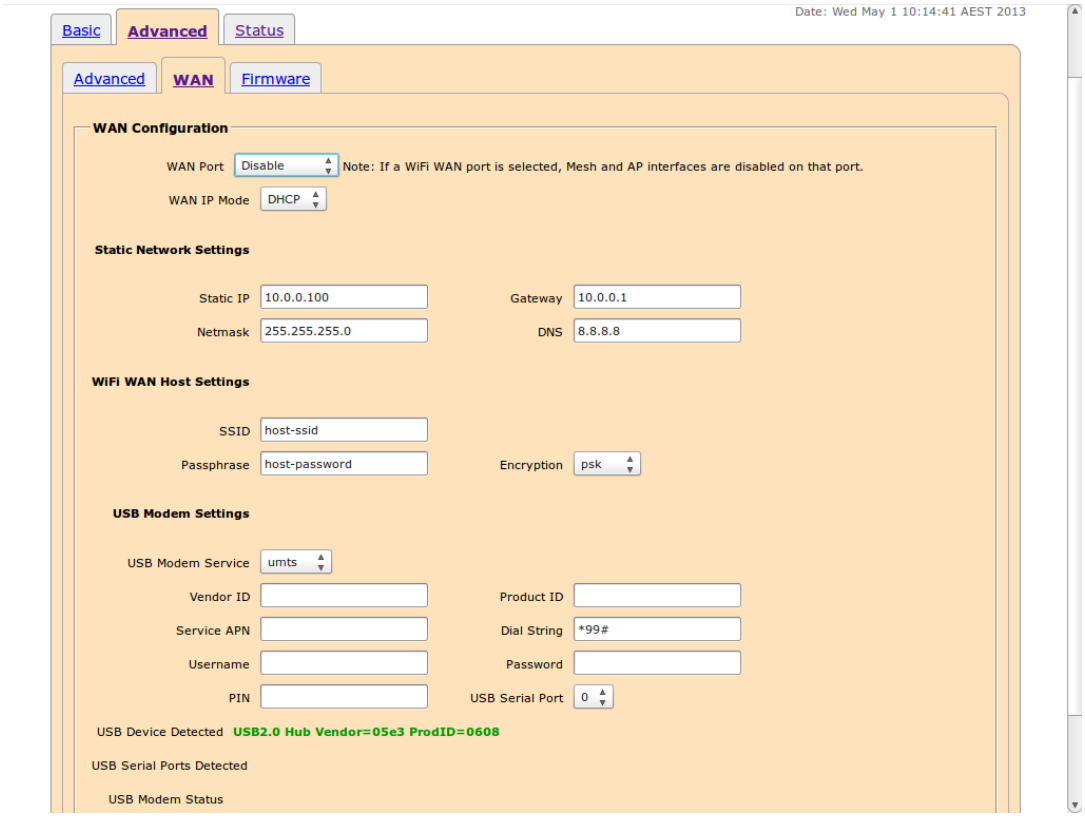
DNS defines the Domain Name Server IP addresses that will be handed out to clients as part of the DHCP protocol.

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.

WAN Configuration



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 ***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.

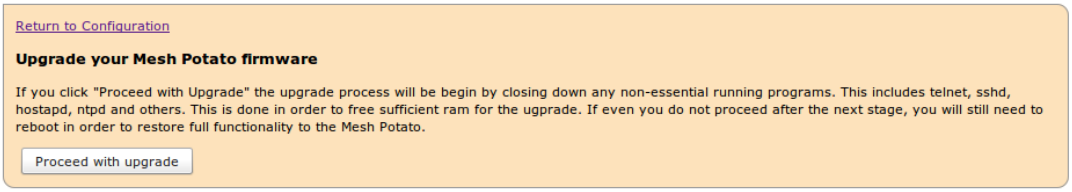
When the USB modem settings have been correctly entered and the device restarted with the modem installed and the Wireless Broadband service is available, the connection status will be displayed in the status line at the bottom of the page.

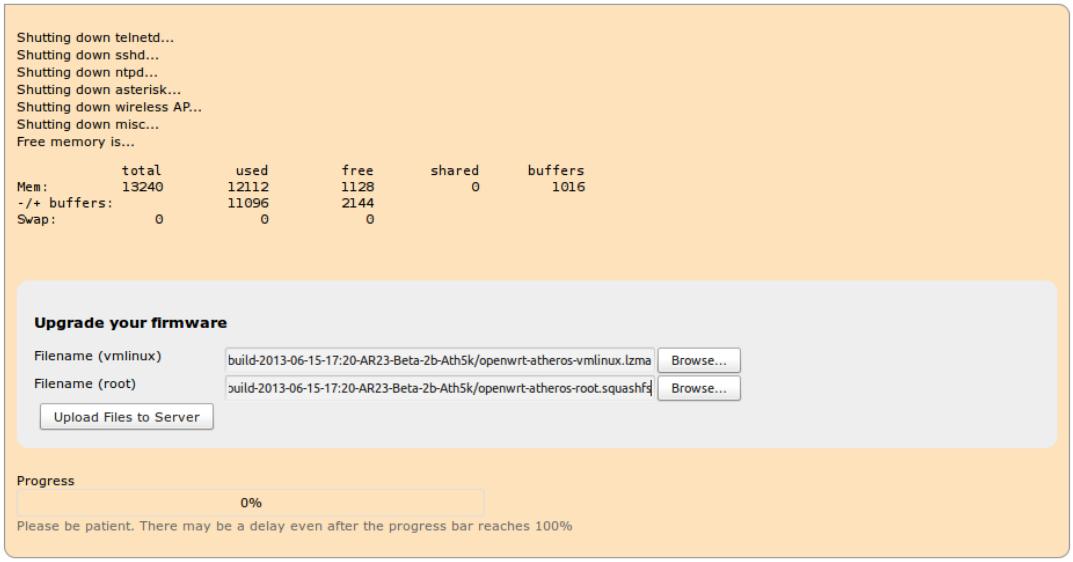
Firmware Upgrade - MP-1 and AR23

For the Mesh Potato 1 and Ubiquity 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.





Firmware Upgrade - TP and AR71 Devices

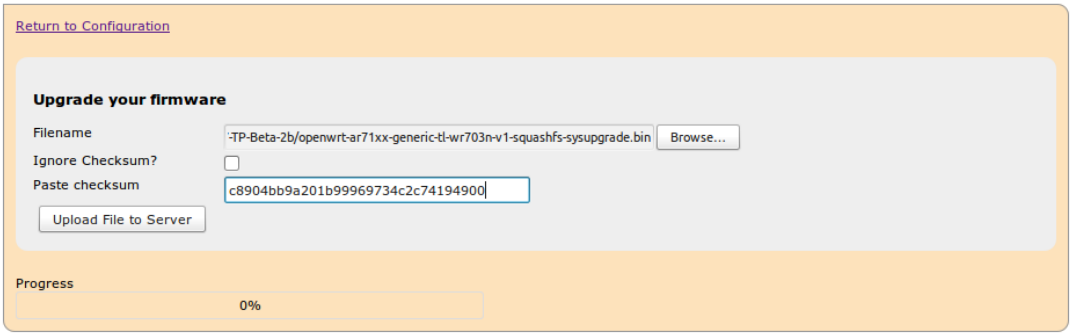
For TP Link, Ubiquity and other and devices based on AR71 and compatible chipsets, this page allows you to upload a 'sysupgrade' firmware file in order to reflash the device.

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.

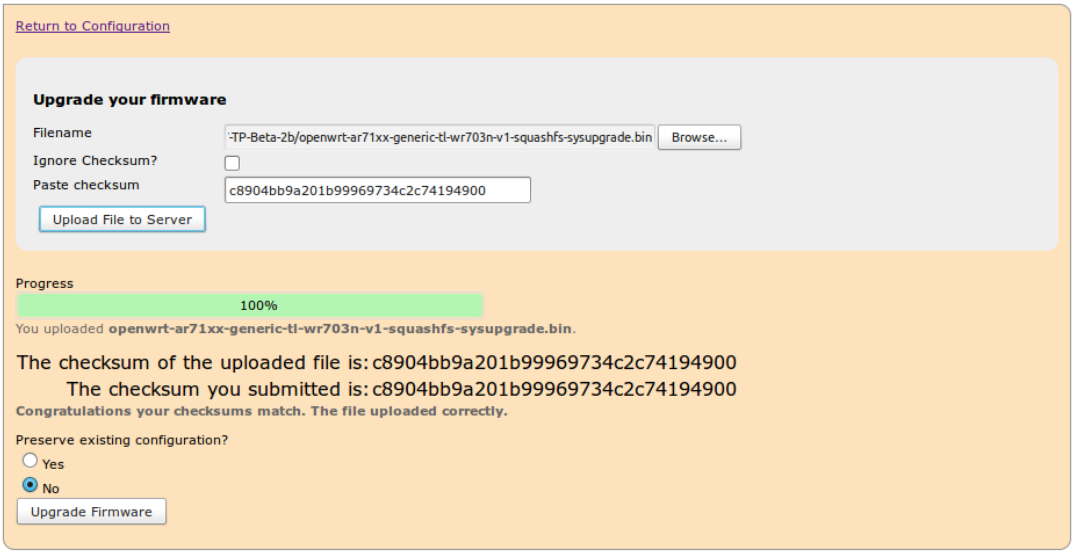
Select ***Upload File to Server*** to transfer the fie and checksum to the device.

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.



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 255.255.2555.0

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 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 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.

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.

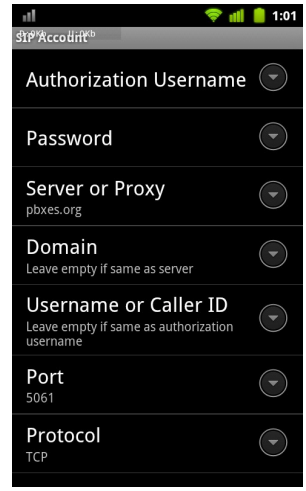
Where a MP network is attached to a LAN, there will usually be some device on the LAN running a DHCP server that will hand out a suitable IP address to an attaching device. As long as the MP static addresses are on the same sub net range as the DHCP addresses, all will be well.

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.

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