

Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

**Web Enabled Embedded Devices using SNMP
Technology for Real-Time Monitoring and Control
Applications**

A thesis presented in fulfilment of the requirements for

Master of Engineering Degree

In

Electronics and Communications Engineering

School of Engineering and Advanced Technology

Massey University at Albany

New Zealand

Saba Taimoori

July 2012

Abstract

Connecting other devices over the internet than just PCs is becoming a common place now. There are web enabled embedded devices almost everywhere. By combining the internet world to the embedded devices, it makes it much easier to be able to achieve the real-time data from across any location. This thesis aims to web - enable an embedded device, a power supply using a web interface. The development will be constituted with a combination of the correct product and the technology. The technology that we consider using for this project is the SNMPv1 protocol.

SNMP (Simple Network Management Protocol) is now a days the key enabling technology, while, with the development of embedded internet, manufacturers are required to “web-enable” the configuration and management of their products. Thus the integration of SNMP and Web in embedded devices will make products competitive.

The main task in achieving the aim was the programming and the communication between the power supply and the Lantronix Xport Pro device. The programming was done on the Linux environment for the Xport Pro device and then the integration for loading the web pages were done using a GUI software through FTP server. The majority of the work involved in this project was developing the correct data and making a stable communication link between the power supply and the Xport Pro device.

During the development process, several issues were encountered with the software as well as the Xport Pro devices. The loading of the software on these devices consumed most of the time as it kept on encountering faults which made the devices dead. However, with the help of the FTP server on the windows machine, it was much easier to connect the power supplies and re-load the software onto the Xport Pro software. Testing was the easiest task and real-time data was displayed on the web pages with no other faults.

Acknowledgements

I would like to thank my supervisor Dr. M A Rashid for his advice, feedback and all his guidance which has helped me reach the standards in completion of this thesis.

I would like to thank all the people who have helped me through this project. The success of this project would not have been possible without the guidance, assistance and dedication of the team involved in this project.

I would also like to thank Matt Jones for offering the opportunity to be a part of this project. I would also like to thank Klaus, Regis, David and Sinclair; their knowledge and experience have helped me move ahead in this project.

I would also like to thank my family, my husband for his ongoing support. I would also thank my daughters who have been my inspiration during my study of Masters of Engineering.

Table of Contents

Abstract.....	ii
Acknowledgements.....	iii
Table of Contents.....	iv
List of Figures.....	vii
List of Abbreviations	ix
1 INTRODUCTION.....	1
1.1 Introduction	1
1.2 Statement of the Problem	3
1.3 Research Methodology.....	4
1.4 Thesis Structure	6
2 AN OVERVIEW OF WEB ENABLED EMBEDDED DEVICES	8
2.1 Web Enabled Devices	8
2.2 Web based Technologies.....	9
2.2.1 TCP/IP Model	10
2.3 Network Management	15
2.4 Protocols	17
2.4.1 Internet Protocols	19
2.4.2 Address Resolution Protocol.....	20
2.4.3 User Datagram Protocol	20
2.4.4 Dynamic Host Configuration Protocol	20
2.4.5 Transmission Control Protocol	21
2.4.6 Hyper Text Transfer Protocol	21
2.5 Architecture	24
2.5.1 OSI Model	24
2.5.2 Client/Server Model	24
2.6 Security	26
2.6.1 SSL: Securing Web GUI Sessions	27
2.6.2 SSH: Secure Remote Terminal Sessions	27
2.7 Summary	28
3 SNMP TECHNOLOGY	29
3.1 Introduction	29
3.2 SNMP Background	30
3.2.1 Client-Server Protocol	31
3.3 SNMP Architecture	32
3.4 SNMP Components	33
3.5 SNMP Commands	36
3.6 SNMP Versions	37
3.6.1 SNMP v1	38

3.7 Operating Systems	39
3.7.1 Linux	39
3.7.2 Windows	39
3.8 Summary	40
4 LITERATURE REVIEW	41
4.1 Introduction	41
4.2 Open Issues and Research Trends	44
4.2.1 Open Issues	44
4.2.2 Research Trends	45
4.2.2.1) The Serial Tunnelling Concept	46
4.2.2.2) Machine to Machine Concept	47
4.2.2.3) Web Server	48
4.3 Analytics drives real-time value	49
4.4 Conclusion	49
5 DESIGN OF WEB ENABLED POWER SUPPLY	51
5.1 Introduction	51
5.2 Key features of Design	52
5.3 User Interface	52
5.3.1 CGI Programming	53
5.3.2 HTTP Interface	54
5.4 Embedded Devices	55
5.4.1 ATMEL Microcontroller	55
5.4.2 Lantronix Xport Pro	56
5.4.2.1 Xport Pro Features	57
5.4.2.2 Xport Pro Block diagrams	58
5.4.2.3 PCB Interface	58
5.4.2.4 Ethernet Interface	59
5.5 Design steps for proposed protocol	59
5.5.1 Creating the web pages	61
5.5.2 Parameters	62
5.5.3 Assigning IP address	66
5.5.4 Creating the .COB files	67
5.6 Summary	68
6 PERFORMANCE SIMULATION OF THE WEB ENABLED DEVICE.....	70
6.1 Introduction	70
6.2 Simulation Environment	71
6.2.1 WinSCP	71
6.2.2 Putty	72

6.2.3 Web Page	75
6.3 Parameters monitored while simulation	76
6.4 Conclusion	78
7 RESULTS & DISCUSSION	79
7.1 Introduction	79
7.2 Results	79
7.2.1 Login Page	79
7.2.2 Monitoring & Control	81
7.2.3 Control – Understanding Control Terms	86
7.2.4 Network Settings	87
7.2.5 PSU Configuration	88
7.2.6 SNMP Configuration	90
7.2.7 Syslog Configuration	93
7.2.8 Firmware Upgrade	94
7.2.9 Change Password	95
7.3 Conclusion	95
8 CONCLUSIONS AND FUTURE STUDY	96
REFERENCES.....	99

List of Figures

Fig 1: Block diagram of the proposed project.....	3
Fig 2 – Comparison of TCP/IP & OSI Model.....	11
Fig 3 – IP Packet Structure	12
Fig 4 – Architectural Model of Network Management System.....	16
Fig 5 – Protocol Stack.....	18
Fig 6 – Encapsulation of IP packets in TCP/IP model.....	19
Fig 7 – HTTP Session Example.....	22
Fig 8 – Client – Server Model.....	25
Fig 9 – Internet Model showing the protocols in each layer with OSI Model.....	30
Fig 10: The model of network management architecture.....	32
Fig 11 – SNMP Architecture.....	36
Fig 12- Scenario of Exposing and Consuming Web service.....	42
Fig 13 - Serial Tunnelling Concept.....	47
Fig 14 – Design of a system to support security communication.....	53
Fig 15 – Lantronix Xport Pro.....	56
Fig 16 – Xport Pro Block Diagram.....	58
Fig 17 – Structure of SNMP data transfer.....	60
Fig 18 – WinSCP window.....	71
Fig 19 – Putty Window.....	72
Fig 20 – Web page for the power supply.....	75
Fig 21 – Login Page.....	79

Fig 22 – Monitoring & Control Page.....	81
Fig 23 – Network Settings.....	87
Fig 24 – PSU Configuration page.....	88
Fig 25 – SNMP Configuration.....	91
Fig 26 – SYSLOG Configuration page.....	93
Fig 27 – Firmware Upgrade page.....	94

List of Abbreviations

ARP – Address Resolution Protocol

BCT – Battery Condition Test

CGI – Common Gateway Interface

COTS - Connection-Oriented Transport Services

CLTS - connectionless-mode Transport Service.

CLI – Common Line Interface

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

ECS- Embedded Computer System

EEPROM - Electrically Erasable Programmable Read-Only Memory

FTP – File Transfer Protocol

HTML – Hyper Text Markup Language

HTTP – Hyper Text Transfer Protocol

IP – Internet Protocol

ISO – International Organisation for Standardization

ICMP – Internet Control Message Protocol

LLC – Link Layer Control

LAN – Local Area Network

MAC – Media Access Control

MIB – Management Information Base

M2M – Machine to Machine

NMS – Network Management System

OID – Object Identifier

OSI – Open Systems Interconnection

PDA – Personal Digital Assistant

PC – Personal Computer

POP – Post Office Protocol

SNMP – Simple Network Management Protocol

SYSLOG – System log

SMTP – Simple Mail Transfer Protocol

SSL – Secure Socket Layer

SSH - Secure Socket Shell

PSU – Power Supply Unit

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

Chapter 1

INTRODUCTION

1.1 Introduction

Embedded devices with web enabled feature are now a common scenario of everyday life. They provide a communication interface between man and machine. Web enabling embedded devices makes the device efficient and allows communication a very easy tool. Embedded web devices are a major development of technology; they tend to combine human work to the world of machines. This comes in a variety of technology such as wireless communication, remote communication using software and other types of media to communicate across the world. The introduction of web enabled devices happened with the release of mobile browser for a PDA called PocketWeb [1] in 1994, which is basically a web browser in a mobile. This is an example of a web enabled device. Mobile browsers are optimized so as to display web content most effectively for small screen on portable devices. Web enabled devices are used in almost every area such as Health sectors, Educational institutions, Government, supermarkets, military applications etc are a few names revolutionised by web enable technologies. There are few great reasons to web enable a device in today's world. An embedded web server can be used for implementing many features and functions in a device. This helps the user to easily navigate their device from a remote location.

Web enabled devices communicate with other devices using various technologies. This involves server, a web browser, HTTP interface and the hardware interface. Web enabled devices makes it easier for the users to communicate with appliances using a remote device

with a built in web browser. With the help of web enabled devices, appliances can be communicated by a web browser.

User-interface hardware (electromechanical) costs can be eliminated and more user friendly interfaces can be designed with low costs. Techniques such as control, monitor and updates can be performed from anywhere in the world. This reduces maintenance costs by updating the new firmware on a regular basis.

This thesis describes the development of a web enabled device using an external device that works as a remote server to a power supply. Working in a remote place, this helps to overcome the problem of maintenance and monitoring of the battery life of the power supply.

The embedded systems usually have limited CPU and memory resources and these resources are mostly used by real-time applications; which causes a delay up to few seconds for the end user for an HTTP response. While making an embedded device web enabled, there is a set of protocols that needs to be followed. These protocols belong to the TCP/IP protocol suite: TCP, UDP, IP, ICMP and ARP.

Users communicate with the embedded device by sending a request to the embedded web server. The request is then processed by the CGI script. The results are sent back to the users as an HTML page. The codes written to web enable the devices stores all the data and can be changed accordingly. In this project, we have chosen a compatible web server called Xport Pro made by Lantronix which is compatible with the microcontroller of the power supply and accommodates the protocols to web enable the device.

1.2 Statement of the Problem

Web enabling a device has its benefits as well as loss. Many times it's difficult to identify the benefits of a web enabling device. With the aid of web enabling technology, it's much easier to make improvements in the areas such as remote access and user interface. For example, we can visualize a vending machine which is web enabled and uses an embedded web server. The web server is linked with internet and has capability to send and receive data signals. In this scenario, the machine acts as a website where the web site address is given to any browser that is connected globally. Web enabling a product requires many applications and technology to be combined together.

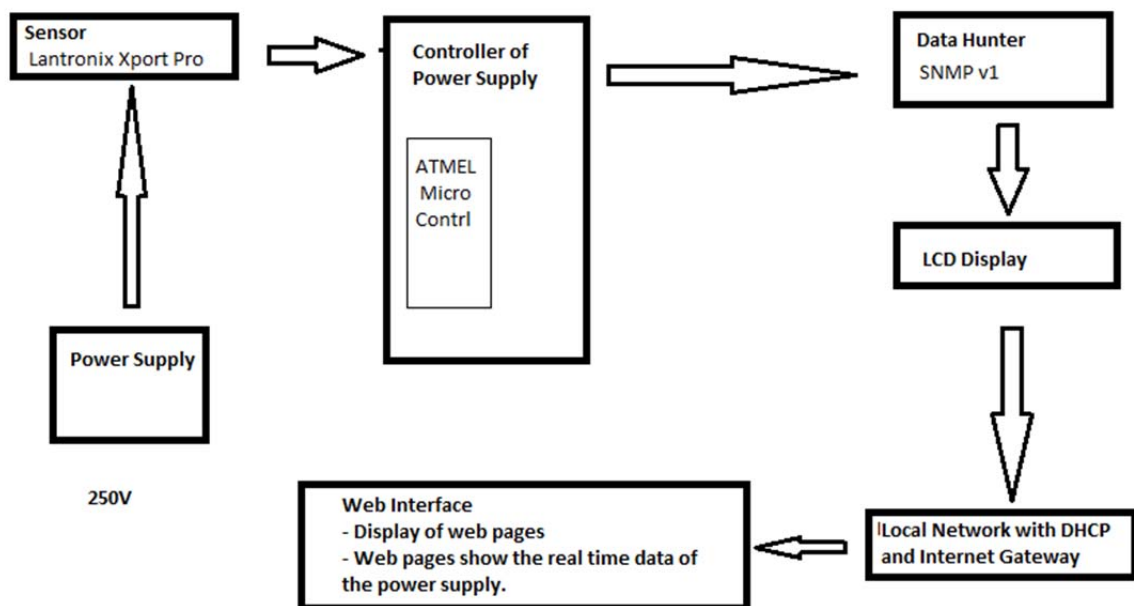


Fig 1 Block diagram of the proposed project

Much research has been carried out on implementing web enable devices using the SNMP technology. The power supplies which are used as an embedded device in this project have the capability to be SNMP enabled as they have a LAN+, Ethernet socket built in to be web enabled. Much less research has been done on making these power supplies web enabled. The problem we want to solve is to find a device that is capable of accepting the SNMP technology and has enough memory that supports the HTTP functionality too.

1.3 Research Methodology

After comparing a lot of devices with built in web servers, we chose the Lantronix Xport Pro device as it matched the requirements of the power supply.

The first couple of months in this project involved lots of research on the previous projects on Web enabled devices. During this period, a detailed study was undertaken in order to study the various types of embedded devices and the technology they have used to web enable their devices.

A study was also done on the most compatible technology that we can use in order to meet the requirements of the embedded device as well as the server specifications. This includes, matching the temperature, memory, and data information etc of the device.

The next task is to implement the research into practice. This involves a thorough review of the research and the literature relating to the SNMP technology used in web enabling embedded devices. This also includes a detail study of the programming of HTML pages along with the TCP/IP structure.

Next, the final product is selected and the development is therefore started in order to implement the research techniques. The Lantronix Xport Pro development kit was studied and developed in order to match the power supplies embedded system.

This also allowed us to identify the weakness and the strengths of the Xport Pro device. The required features are used along with the other parts in order to achieve the desired results.

The simulation tools also play an important role in the research methodology. In this project, there are combinations of simulation tools that we have used to test the web enabled device.

This included simulations tools from the programming side for the microcontroller in the power supply to the HTML pages for the web site to display the web enabled device over the web.

The simulation involves designing and testing. This is covered in detail in the chapters ahead.

After the testing of the web pages is performed, the results are then gathered to check that the firmware has been loaded onto all the required devices. The web pages are closely monitored to check the real-time data that is displayed on the web pages. This denotes that there is a thorough communication between the server and the microcontroller of the power supplies.

However, the final stage involves documenting and comparison of the results. It also includes the future work that can be done in order to continue with this project. This can be choosing a new technology or continuing with the same technology but with a higher version.

1.4 Thesis Structure

Chapter one of this thesis introduces the topic of web enabled devices using the SNMP technology. A comparison and the use of web enabled devices in today's world have been discussed. A brief discussion of choosing the correct embedded device that is capable to work along with the microcontroller of the power supply has been made. Finally, it discusses the simulation tools used in this project to achieve the desired results.

Chapter 2 provides a literature review of previous research and industry work undertaken in the field of embedded devices and wireless communication. This chapter also discusses open issues, research trends and outcomes.

Chapter 3 provides a technical overview of LAN technologies that are used in web enabling embedded devices. This chapter also discusses about SNMP technology and its benefits when used in Web enabling embedded devices.

Chapter 4 discusses the simulation tools used in order to implement SNMP features into the embedded devices. Then, a comparison of simulation tools that are already available is presented. The remaining of this chapter focuses on the HTTP interface and the CGI interface, which is used for this study.

Chapter 5 describes the simulation models involved with the SNMP standards. In recent years, there has been much improvement in technology. This improvement has helped devices to communicate from remote locations using Ethernet network. In order, to make this communication possible, low cost hardware can be used. This includes converting the serial ports such as RD-232, RS422 into an Ethernet interface.

Chapter 6 discusses the results after web enabling the power supplies. Real-time data is analysed in this chapter. Different parameters are compared and analysed in terms of temperature control, Battery condition test, Voltage, Current etc.

Chapter 7 goes through the work done in completion of this project including the research. It draws conclusions from the finding of the study and finally discusses about the future development for SNMP.

Chapter 2

Overview of Web Enabled Embedded Devices using LAN Technology

This chapter provides a technical overview of LAN technologies that are used in web enabling embedded devices. This chapter also discusses about SNMP technology and its benefits when used in Web enabling embedded devices.

2.1 Web Enabled Devices

Web enabled devices are getting very common in today's internet world. They propose an easier solution too many developments that are made in the technical world.

The combination for web enabled systems consists of both hardware and software to control their functionality. Web enabled home appliances include TV sets, washing machines, ovens etc. Embedded devices with a communication feature include mobile phones, laptops, tablets etc. Such devices are known as Embedded Computer System (ECS).

The most important functionality is the "remote monitor & control" function. The modifications within the embedded system are limited. The most important addition is a command interpreter supporting "remote monitor & control" functionality. This interpreter can serve as a protocol gateway to map the proprietary protocols to more standard ones.

The advantages of we enabling a device are not very obvious. Web enabling helps and improves the user interfaces and remote access capabilities. Incorporating an embedded web

server is a useful tool for easily implementing a variety of features and functions in many devices.

An example of a standard interface is a user browsing a web site. A website acts as a web enabled device. It responds to buttons, hot links and the complete array of familiar browser controls. We often associate server as a heavyweight object. Due to the technology, web servers are now as small as a footprint. The web server used in this project is a small device which is very efficient and holds enough memory in order to get a web site up and running. Lantronix Xport Pro adds 30KB of code and 30KB of data to the application. Lantronix Xport Pro has the web client, browser built in the device. It acts as the client/server pair, which accepts the HTML code and outputs the graphics on the website.

Comparatively, there are advantages and disadvantages in web enabling embedded devices that we will discuss further in this chapter.

2.2 Web based Technologies

Web Technologies help in managing network devices. It helps in releasing network managers from the difficult circumstances. Web technologies bring valuable cost improvements, flexibility and security enhancement to configuration management and performance management. It is capable of controlling and monitoring remotely the configuration information of enterprise networks.

SNMP is the chosen web technology for this project. Lots of monitoring systems are SNMP enabled. Due to the demand of the clients, implementation of SNMP in the Innovative Energies Power supplies was a new development as it helps their clients to monitor and control their power supplies remotely.

The Simple Network Management Protocol (SNMP) is a protocol that helps in the exchange of information between network devices. It belongs to application layer and is also a part of TCP/IP protocol structure. Network administrators use SNMP to manage network performance, find network issues and plan ahead for network growth.

2.2.1 TCP/IP model

The TCP/IP protocol structure is significantly different from the OSI model. It is a structure based on four layers.

In comparison, the Application layer of the TCP/IP suite similar to the first three layers of the OSI model. Similarly, the bottom layers of the TCP/IP suite are equivalent to the physical layer and the Data link layer of the OSI model.

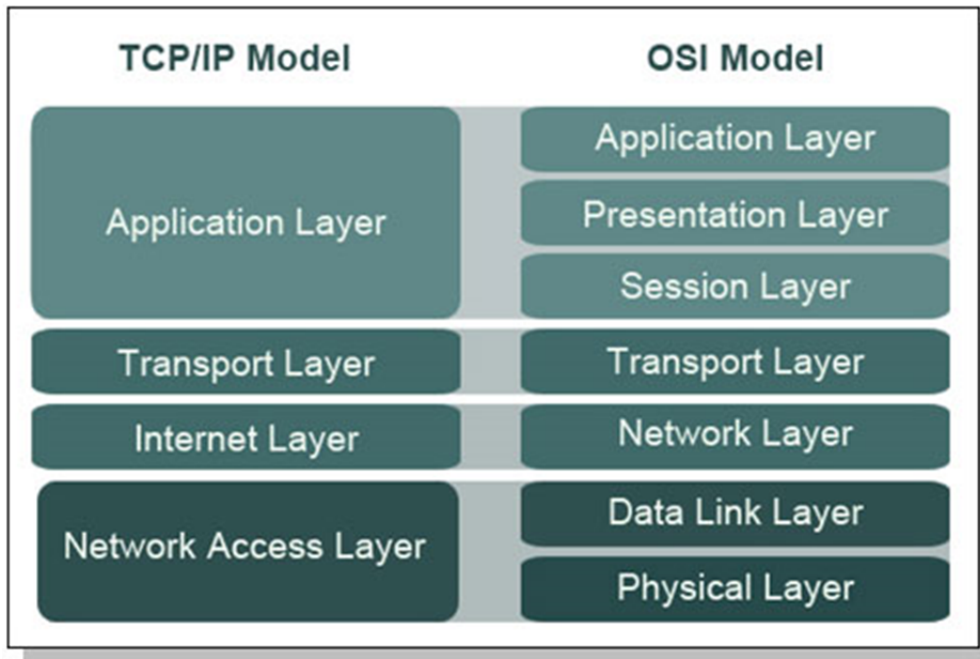


Fig 2 – Comparison of TCP/IP & OSI Model

The layers work along in order to provide services to other layers. They work in such a way that each layer aims to provide an extra thought from other layers. For example, the information or data within the datagram is not known by the link layer; similarly the application layer has no information about the routing of networks.

During the transmission of data, each layers of the ads its header which includes information of the protocol itself. The equivalent protocols use this information of the destination host to decide as to what needs to be done with the packet.

Several changes can be made while implementing TCP/IP stack for any microcontrollers. It depends on each application as to which features can be omitted as they have specific requirements. For a developer, it is essential to maintain the application requirements while keeping the size of the microcontroller very compact. It is necessary for a TCP/IP protocol suite to contain the following protocols: TCP, UDP, IP, ICMP and ARP.

A form is submitted to an embedded web server, so that the users can interact with the appliances. It is processed by a CGI script and the results are sent back to the user in an HTML form. Forms are used for monitoring and controlling the appliances.

Source/Destination Port: In order to allow multiplexing TCP over several different applications, source and destination port combined with remote node's IP address can give many concurrent, persistence and individual connections.

Several ports are well known, for example port 80 is used for HTTP. Web servers will listen to port 80 for incoming TCP connections.

- **Physical Layer**

The Physical layer is bottom layer of the protocol structures of internet. The physical layer sends and receives datagram's on behalf of the upper layers. The source of communication used by physical layer is the physical media.

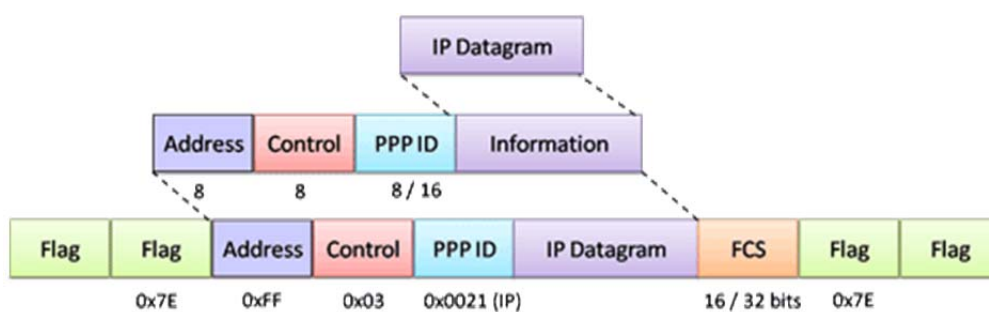


Fig 3 – IP Packet Structure

The data link layer defines the protocol used to maintain the physical link, which may include: data framing, checksum/CRC, and collision detection. The data link layer is divided into two parts media access control (MAC) and link layer control (LLC). MAC controls

access and encodes signals to a valid format. LLC creates a link to the network via low level link negotiation.

- **Network Layer**

Internet Protocol is the main component of the Network Layer. It is responsible for addressing, routing and host-to-host delivery. The hosts situated on the IP network needs to contain one identifiable address. The can accept several other address as an option. It is up to IP to make decision about which packets to accept, route and which to discard. These actions as based on the way its configured and the standard rules.

IP Fragmentation is an important process that is performed by IP. There is a set limit for each link layer protocol on the amount of data to be transmitted in a single datagram. This process is known as the Maximum Transmission Units (MTU). Furthermore, network layer provides address and routing information for the packet. The network protocol primarily used on the internet is IP. Addresses are provided in IP via a byte denomination, for example 192.100.123.1. IP can route incoming and outgoing packets by inspecting the IP address in the protocol and determine the best route for such packets. Another network layer often seen in Ethernet is ARP, which is used to resolve MAC addresses with IP address.

- **Transport Layer**

TCP (Transmission Control Protocol) or User Datagram Protocol (UDP) are the two protocols associated with in the TCP/IP stack. Either one of them provides this service to the Transport Layer.

UDP is not a reliable protocol as it does not provide a connected service. There is no assurance whether the data is received at the provided destination or in which state it gets there. The application layer is not notified when a packet is dropped after it fails an integrity check.

Comparatively, TCP can be trusted and is an active connected service. If there is no confirmation, then it is considered that the packet has dropped or re-transmitted. The transport layer also links the datagrams to applications by the use of port numbers and addresses. The port numbers for both source and destination are carried out by each datagram. The numbers are then used for identification purposes to send and receive their applications.

- **Application Layer**

The Application layer is the top most layers, where the data originates and also ends up. At the application layer, major communications take place. Such as, World Wide Web (HTTP), Emails (SMTP, POP) and File transfer (FTP, TFTP). In most operating systems, protocols below the Application layer are integral features of the operating system itself, implemented as part of the kernel, while Application layer tasks are typically performed by user processes [17].

The application holds less information about the networking process. It only reads and writes to the Transport layers in the same way as if it were a file on the local system [17].

HTTP is a common application layer protocol as it carries WWW traffic. HTTP provides a user interface by using the programming language of HTML. User can send data back by using HTML forms. This communication helps in providing remote control and management facilities.

2.3 Network Management

Network management refers to the methods, procedures and tools that assist in monitoring a system over the network.

The international Organization for Standardization (ISO) defines five major functional areas of network management. As shown in Fig 3, the Network Management System (NMS) consists of three categories a) User Presentation Software, b) Network Management Software, c) Communications and database support software.

Fig 4 – Architectural Model of Network Management System

It consists of the five main elements that make up the Network system. The management systems are Fault management, Account management, Configuration management, Performance management and Security management.

Fault management: The fault management deals with detection, isolation and faults in network components.

Account Management: It charges the use of managed objects.

Configuration Management: It maintains relationship between the network components and parts of entire network.

Performance management: It monitors the performance of the network such as utilization, throughputs and network resources.

Security Management: Manages the security of the network such as network access, encryption keys and data security.

2.4 Protocols

A protocol is the special set of rules that end points in a telecommunication connection use in order to communicate. A communication language is a framework is generally called a protocol. For example, take two people one from India and one from New Zealand. Now that, if they wheeling to have a communication between them, it has to be in one language, which in this could be English. We can say that English language is the name of the protocol, these two people used in order to establish a communication. Two computers may different processors, language, and operating systems, but if they both use a common set of rules (protocols), then they can communicate.

However, protocol doesn't just enable communications, they also restrict them. Neither communicator may stray outside the bounds of protocol without facing incomprehension or rejection to keep the communication going. So a protocol doesn't just define how communication may occur but also provides a framework for the information that is communicated. In order to encompass all the variety of present-day computer communications, one protocol is not enough. Therefore a family of protocols is required, where each of simpler oriented talks at the bottom and the higher user oriented task at the top. Such a structure is often called a protocol stack.

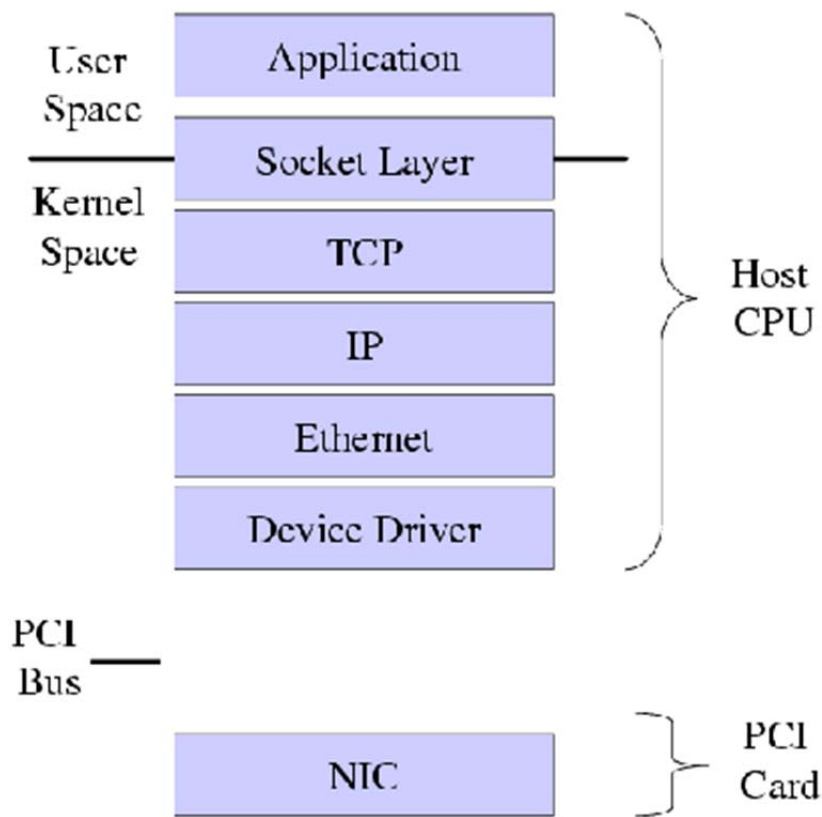


Fig 5 – Protocol Stack

Here, the term stack refers to the way protocol components are stacked on top of each other to give the desired functionality. If we want to transfer a file, we might take a standard file transfer protocol and stack it on the top of a communications protocols. The communications protocol wouldn't understand about files – it simply moves blocks of data around.

Conversely, the file transfer protocol wouldn't understand about networks – it simply converts files into blocks of data. Combine the two and, to provide us network file transfer capability.

2.4.1 Internet Protocols

The information on the internet with binary code is transmitted into packets. This binary code is then grouped into octets (bytes) and the bytes are grouped into packets of data.

The IP protocol enables exchanging of traffic between two computers. It is a network layer protocol. An IP address is allocated to each computer. This helps to identify which computer the packet is addresses to and which address the packet is coming from.

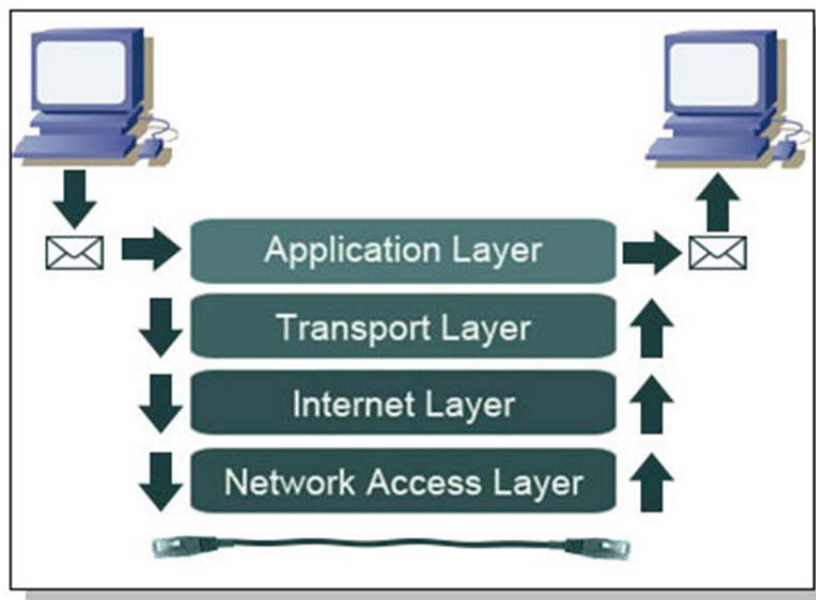


Fig 6 – Encapsulation of IP Packets in TCP/IP model.

The tasks of error checking, reliability and flow control are given to upper layers such as TCP. The protocol number field indicates the type of upper layer service required by the data packet.

2.4.2 ARP (Address Resolution Protocol)

The ARP translates IP address to MAC (the link addresses) and hides all the addresses from the upper layers. The IP addresses are mapped to the following MAC address by the ARP. If a machine recognizes its IP address, it will return an ARP response to the required machine that holds a MAC address within. In order to send the Ethernet packets, it is essential that we know the MAC address of the machine. Thus, ARP is an important protocol required in this project.

2.4.3 UDP (User Datagram Protocol)

UDP is a protocol that sends data and contains limited checksum. With UDP, the start to end traffic data is not taken into consideration. UDP comes into usage only when full TCP service is not required. For the web server in this project, the use of UDP protocol is to send and receive DHCP messages. The datagram's are directed to the specific upper layer application by the port fields.

2.4.4 DHCP (Dynamic Host Configuration Protocol)

DHCP is a bootstrap protocol (BOOTP) based protocol. It is used for the transfer of configuration information to hosts in a TCP/IP network. DHCP obtains an IP address from a designated DHCP server such as a router. Dynamic IP allocation is mainly used in embedded web servers as the server leases the IP address. Dynamic Host Configuration Protocol (DHCP) allows a node of an IP network to automatically allocate an IP address to the unit and learn the network parameters such as gateway and subnet mask. DHCP is found all most on all the networks, and is great for allowing laptops to simply plug into a network without

having a user enter network configuration parameter. In this stack, DHCP is used to get the IP address of the remote PC accessing server.

2.4.5 TCP (Transmission Control Protocol)

Most of the traffic in the internet world is accountable through TCP. It mainly deals with end to end reliability. The socket calls are used for determining the service needed. For this project, the common port 80 is used to identify a HTTP request.

2.4.6 HTTP (Hyper Text Transfer Protocol)

Hyper Text Transfer Protocol (HTTP) is used to serve and request web pages from web-servers. The protocol is fairly simple: requests are made in ASCII strings, where each parameter of the request is the separate line of ASCII. An empty line is used to denote end of parameters. Once client makes its request, then the web server answers with its response.

First the web server responds with its own parameter, where each parameter is a separate line of ASCII code. An empty line is used to denote end of parameters, and then any data following is considered the web page or the content that was requested by the web client.

Most HTTP servers listen to TCP port 80, but in this stack we have assigned the Mini web-server to port 8080. Typically a web browser opens a communication socket to TCP port 8080 and will not close the socket until after a user closes the web browser or goes to a different site. By keeping the TCP port open as long as possible, it can speed up the time it takes to download a page by not having to open/close a socket for each request, especially since webpage may have linked images that need to be downloaded to properly display the page.

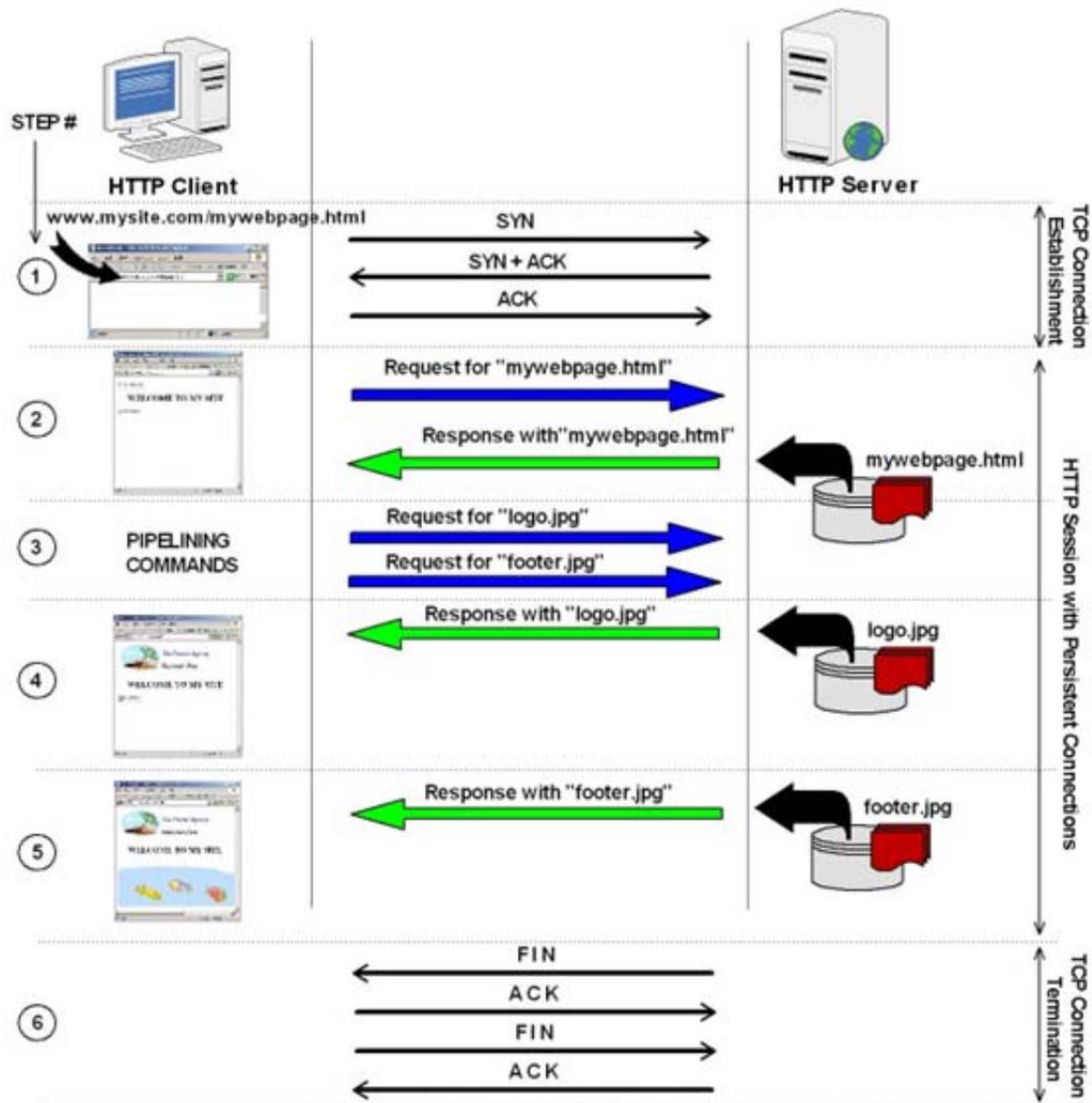


Fig 7 – HTTP Session Example

The Hyper Text Transfer Protocol (HTTP) server is executed as task that co-exists with TCP/IP stack. The server itself is implemented in the main source file **miniwebserver.c**. It supports multiple HTTP connections. Support all the web pages located in the internal memory. Supports HTTP GET method and POST method, but due to the simplicity we used GET method. It also supports, a common Gateway Interface (CGI) to call up on predefined functions from the remote server. Dynamic web page support is also included. This is the

basic example of how protocols are used to code web pages. Due to the code being text-based it is easier to send in TCP packets. Below is the HTTP code of the webpage

```
<html>
<head><title>MENG PROJECT</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<body bgcolor="#FFFFFF">
<h1><strong><font color="#0000FF" face="Arial, Helvetica, sans-serif">WELCOME
TO ATMEL WEBSERVER </font></strong></h1>
<p>&nbsp;</p>
<p><strong><font color="#0000FF" face="Arial, Helvetica, sans-serif"> this web server
is running on a mega32 and using an EDTP packet wacker</font></strong></p>
<p>&nbsp;</p>
<p>ATMEL embedded webserver</p>
<p>TCP/IP is the communications protocol most widely used for accessing the internet
today. The objective of this project is to introduce this protocol to the ATMEL Mega 32
Microcontroller chip such that it can run as a simple webserver which can then be
adapted for useful lab-based applications.</p>
<p> Although the Mega 32 and the development board will only be able to run limited
web functions, it is a relatively inexpensive device compared to high power web servers.
Therefore it can still have many applications for example connecting the microcontroller
to household appliances will allow the user to turn them on and off anywhere using the
internet. <br> \r\n
The current temperature is now "<font color=#FF0000>" temp "</font>" degrees F. </p>
<p>&nbsp;</p>
</body>
</html> [18]
```

2.5 Architecture

2.5.1 OSI Model

Short for **Open System Interconnection**, an ISO standard for worldwide communications that defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

In OSI, there are two services; a connection-oriented transport services (COTS) and a connectionless-mode transport service (CLTS). The deployment of the SNMP is over the connectionless-mode transport service that is provided by the Internet suite of protocols (i.e., the User Datagram Protocol or UDP). It was a design aim for SNMP to be capable of using either a CO-mode or CL-mode transport service.

2.5.2 Client/Server Architecture

A network architecture in which each computer or process on the network is either a *client* or a *server*. Servers are powerful computers or processes dedicated to managing disk drives (*file servers*), printers (*print servers*), or network traffic (*network servers*). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

The client-server model differentiates between applications as well as devices. The requests to the server are made by network clients by sending messages. The servers then respond to their clients by acting on each request and returning results.

One server supports many clients, and multiple servers can be joined together in a pool to handle the processing load as the number of clients grows.

Two separate devices, a client computer and a server computer are customized for their designed purpose. For example, a Web client works best with a large screen display, while a Web server does not need any display at all and can be located anywhere in the world.

In some cases a given device can function both as a client and a server for the same application. Similarly, a device that is a server for one application can simultaneously act as a client to other servers, for different applications.

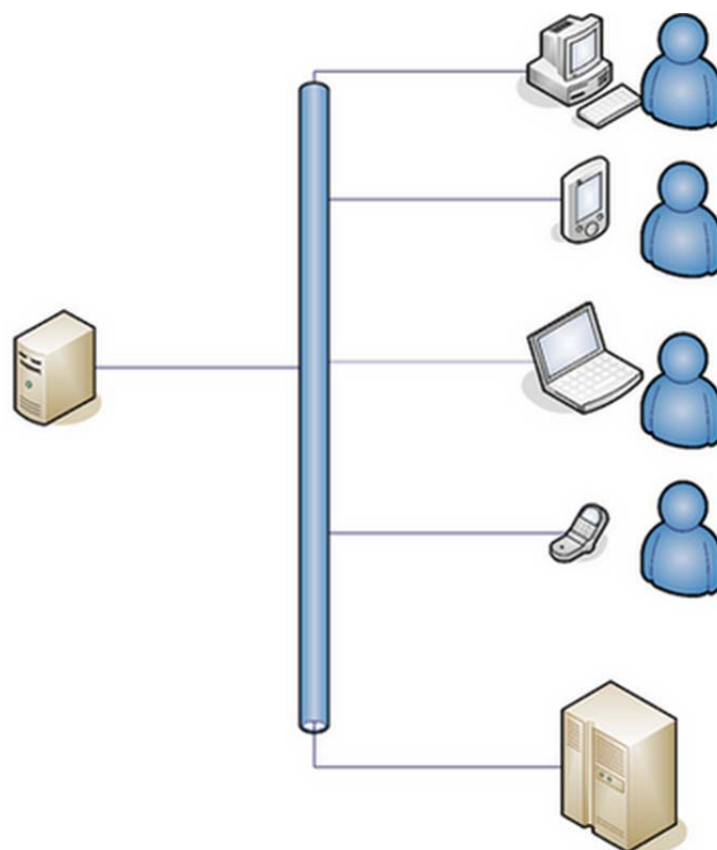


Fig 8 – Client – Server Model

Applications such as Email, FTP and Web services are commonly used in the internet/Web services. These clients feature a user interface and a client application through which a user can connect to the servers.

SNMP network management protocol is mainly used in TCP/IP based network applications and it is based on the client/server model. Each host that is to be managed runs a process called an *agent*. The agent maintains the Management Information Base (MIB) database for the host. Hosts involved in network management decision-making runs a process called a manager. A *manager* is a client application that generates requests for MIB information and processes responses.

2.6 Security

The quickest way to reboot an individual server or router is to directly access the TCP/IP to a Remote Power Management device. This method can also increase security issues within the network. There is a possibility that non-secure network traffic can be involved and information such as login details along with the passwords can be hacked.

It is necessary that the network should be secured. In order to get rid of any attacks, it is essential that the Remote Power Manager should provide security solutions. Two main security protocols that are considered for network securities are SSH & SSL. They communicate using TCP/IP network. These protocols can manage and provide strongest encryption for the entire network.

2.6.1 SSL: Securing Web GUI Sessions

The SSL security service makes sure that no sensitive information is passed anywhere outside the network. Sensitive information can include information such as user accounts and passwords or login details. It helps user to verify how authentic a device is and how securely he can communicate with that device. This procedure secures in private information and protects information from getting hacked or corrupted.

2.6.2 SSH: Secure Remote Terminal Sessions

Secure Socket Shell (SSH) helps a user to access a remote computer in a secure way. It provides strong authentication and data integrity. Due to the sessions being encrypted by SSH, there is no further risk in the sessions of remote management. SSH can also be used instead of telnet if necessary.

Secure Shell protects against:

- IP spoofing
- IP source routing
- DNS spoofing

2.7 Summary

This chapter discussed the various technologies behind web enabling embedded devices.

Web enabling an embedded device requires developer to choose the right technology. In this project, we have used the SNMP (Simple Network Management Protocol) to web enable the power supply.

The network models of OSI and TCP/IP have also been discussed, the SNMP protocol lies in the application layer of these models. Other protocols such as DHCP, ARP etc contribute towards combining the hardware of an embedded device to the internet world.

Network Management System provides a way that helps in monitor the network. It is essential to have a managed network as it helps in monitor the network from any remote location.

Security is one of the main factors in the internet world. It is highly important to have a secured network. In order to make a network secure, technologies such as SSH and SSL can be implemented. These technologies have been discussed in this chapter.

Overall, all the above factors contribute towards making an embedded device available over the web.

Chapter 3

SNMP Technology

3.1 Introduction

This chapter introduces the SNMP technology and describes its architecture and components. SNMP is required to work using two types of programming languages. This chapter also discusses the versions of SNMP and the operating systems that have been used in order to imply this technology.

The Simple Network Management Protocol (SNMP) is a well-established protocol framework that has been in form since 1990. It provides an infrastructure for the exchange of information among network components. SNMP is a key enabling technology in the modern cooperate network.

By integrating SNMP and web into the embedded products, manufacturers make their products more accessible and manageable. The integrated solution provides new access methods by using the SNMP technology. It allows users to employ a browser as an interface to any embedded device connected to a network. It also eliminates the need for customised end-user software and allows users to take advantage of standard, time-saving browser features.

3.2 SNMP Background

The Simple Network Management Protocol (SNMP), a protocol designed to manage a diverse set of networked equipment which is a common feature used in all types of broadcast such as television broadcast studios, energy distribution systems and emergency radio networks.

By the use of SNMP, network administrators can manage network performance, solve network problems, and plan for network growth. SNMP belongs to the application layer. It assists in the exchange of information between network devices. It is a part of the Transmission Control Protocol (TCP/IP).

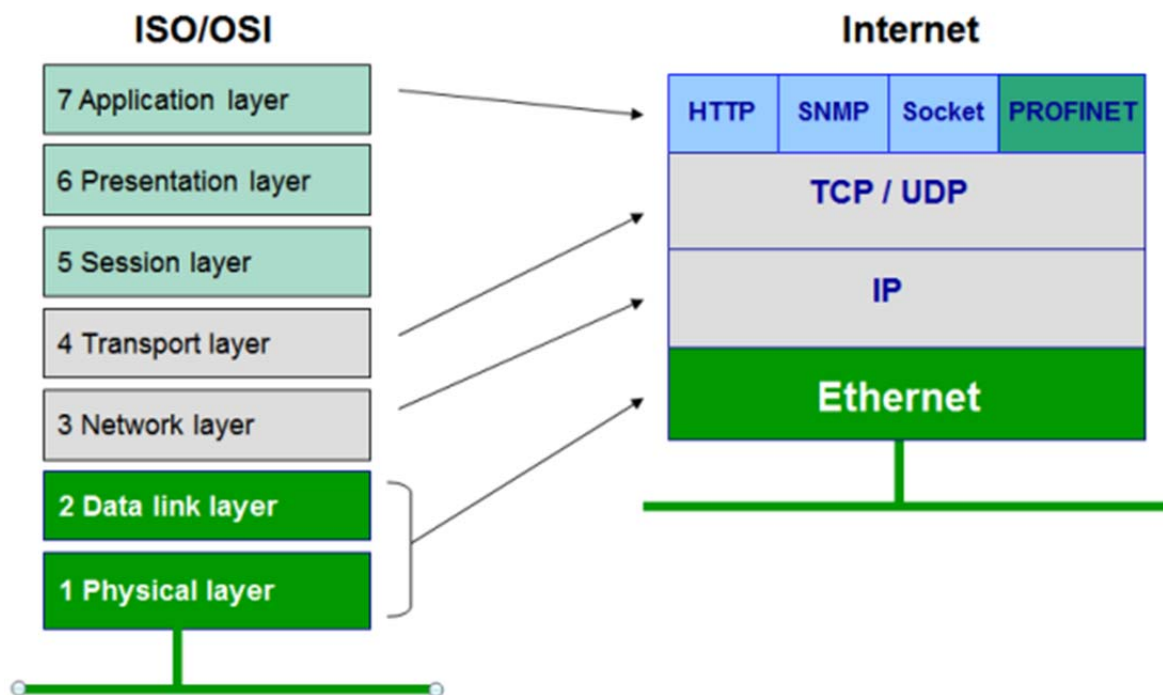


Fig 9 – Internet Model showing the protocols in each layer in comparison with OSI Model.

3.2.1 Client-Server Protocol

❖ Client Server Protocol

The term *client-server* refers to a popular model for computer networking that utilizes client and server devices each designed for specific purposes. The client-server model can be used on the Internet as well as local area networks (LANs). The DNS, FTP, Web Servers and Web browsers are all part of the client-server systems (Macia-Perez Francisco, Marcos-Jorquera Diego & Gilart-Iglesias Virgilio; 2008).

❖ Client-Server Applications

Applications and other devices, they all use the client-server model. By using the client-server model, messages are sent to the server and server returns results by acting on each request. A single server has a capability to support number of clients. Therefore, in order to handle increased processing load, multiple servers can be joined together.

A client computer and a server are two separate devices. They both are used for different purposes. For example, a web server does not need to be displayed and can be located anywhere where as the web client works best with a display. In some cases a given device can function both as a client and a server for the same application. The client-server model is most common application of the internet world. FTP, Emails and web service systems are all part of the Client-Server model. (Macia-Perez Francisco, Marcos-Jorquera Diego & Gilart-Iglesias Virgilio; 2008).

3.3 SNMP Architecture

SNMP consists of a manager and an agent. It is a database of management information, managed objects and the network itself. They all work together, as the manager provides the interface between the human interface and the management system.

The agent provides the interface between the manager and the physical device(s) involved.

Physical devices include systems such as hubs, routers or servers.

These objects are arranged in MIB. MIB is the Management Information Base also known as virtual information database.

SNMP allows managers and agents to communicate so that they can access these objects.

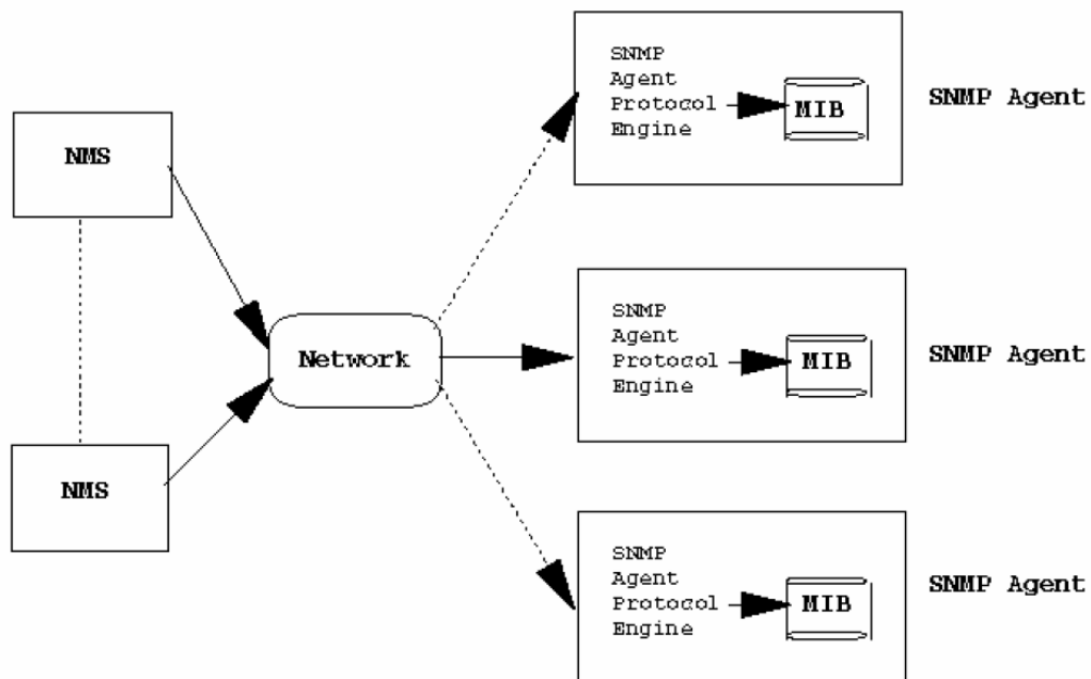


Fig 10: Network management architecture.

There are five important messages used by the SNMP to communicate between the manager and the agent. These messages are Get, GetNext, GetResponse, Set and Trap. The manager requests information for a specific variable using the GET \$ GetNext message.

Once the agent receives a Get or GetNext message, it will issue a GetResponse message to the manager with the requested information. If it encountered an error, it will explain the reason for the error caused in processing.

The trap message allows the agent to inform the manager of an ‘important’ event.

The SNMP manager issues all the messages such as Get, GetNext and Set. Only the Trap message is capable of being initiated by the agent. It is used by RTU’s (Remote Telemetry Units (RTUs) to report alarms. This immediately notifies the SNMP manager when an alarm condition occurs, instead of waiting for a response from SNMP manager.

3.4 SNMP Components

A network management for TCP/IP consists of four basic components.

They are as follows:

- Management agent
- Management Station
- Management Information base (MIB)
- Network Management Protocol

A management station (known as “manager”) is responsible for monitoring, configuring and controlling a number of nodes on a network. Each of them is attached with a management agent (known as “agent”).

A manager can supervise any node on a network through an agent. This can be done by either residing on the node or acting remotely as a proxy. Network devices such as bridges, hosts, routers and hubs are usually equipped with agents.

MIB

A MIB is a collection of objects of the node where the agent is based. A message sent from the manager to the agent results in reading or configuring an object in the MIB. It is not necessary that an MIB should contain the information of interest. It is more likely a logical representation of the information.

A network management protocol is used for communication between the manager and the agent. This enabled the manager to access objects in the agents MIBs. SNMP is a standard protocol used in TCP/IP networks.

As far as the use of SNMP is concerned, it is assumed that it has the combination of these four components described above. The SNMP architecture is very complex when compared with the protocol itself.

The structure itself is hierarchical, where each block is an interest to a manager. Since there is no inheritance from outside, the data structure is not an object-oriented structure. It is rather a logical grouping of objects that are related to each other.

In order to process the concept of network management with MIBs, two things need to be considered:

- The structure of information should be consistent within a system. This is achieved by using standard MIBs on all agents & holding the same type of information. It is important for the manager to be aware of MIB structures.
- The data representation has to be standardized.

OID – Object Identifier

All the objects within the SNMP management framework are equipped with an object identifier (OID). This is a sequence of non-negative integers.

Once an OID of an object is registered, it can never be registered for another object.

This also means that the characters of the object can never be changed or removed.

3.5 SNMP Commands

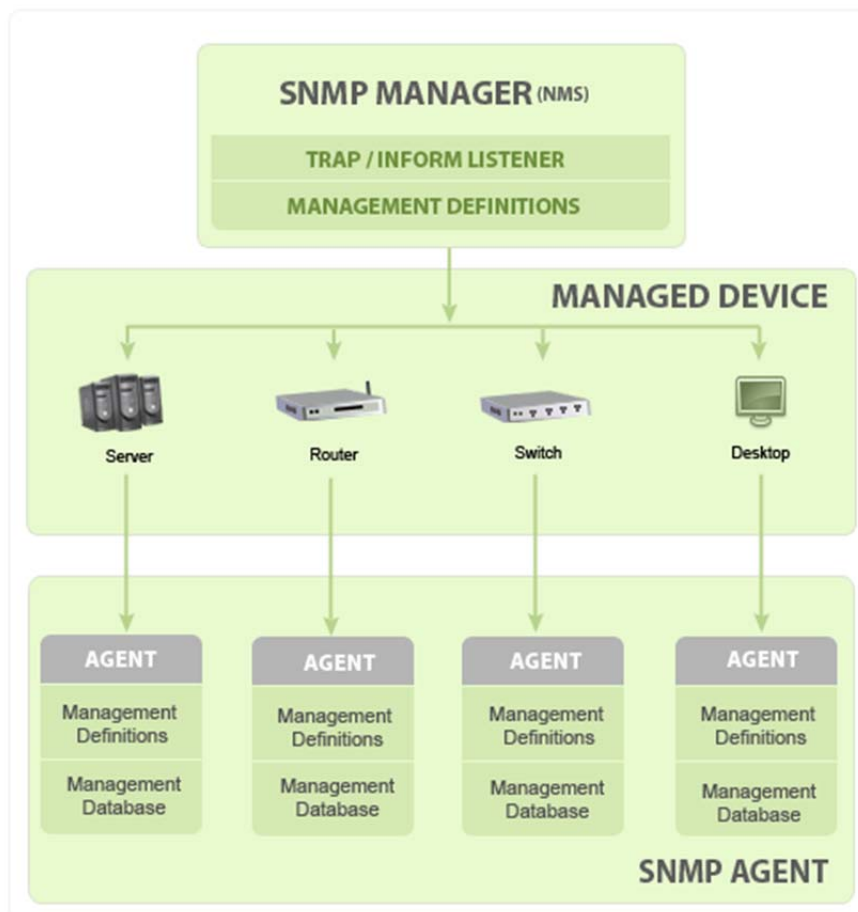


Fig 11 – SNMP Architecture

There are three basic messages being sent between manager and agent:

- **GET** – The GET command retrieves the value of an object in an MIB agent.
- **SET** – The SET command configures the value of an object in an agent MIB.
- **TRAP** – The TRAP command enables the agent to alert a manager of an event.

The SET and GET messages are issued by the manager. They are followed by a responding message from the agent.

The NMS (Network Management System) uses the SET command to configure a managed device. For example, the NMS wants to configure or “set” a threshold on a managed device. Here the SET command becomes a write operation.

The NMS uses the GET command to gain a single piece of information from a managed device. In case the NMS requests the name of the configured device, then the GET command is a read function.

The NMS issues the GetNext operation to gain more information from a managed device.

While using SNMPv1, if the NMS wants to gain information from a managed device, it needs to send commands such as Get and GetNext. The “GetNext” is a read function.

A TRAP message is sent by the agent to the manager. This is the only way an agent can communicate with its manager. A TRAP command is initiated from a managed device. It alerts the NMS once the threshold set by NMS has been reached or if there is any error involved.

3.6 SNMP Versions

There are 3 main versions of SNMP, with each one offering more and more capabilities. The 3 versions are SNMPv1, SNMPv2C, and now SNMP v3. Over time, security enhancements and other features were added to versions of SNMP, and it’s important to understand the differences between them.

3.6.1 SNMP v1

The message format for all versions of SNMP is similar except PDU. The PDU (Protocol Data Unit) for SNMPv1 have five different PDU types: GetRequest, GetNextRequest, GetResponse, SetRequest, and Trap.

The SNMPv1 is very simple and basic when compared with other versions of SNMP. The simplicity of its version can be seen in the message format as it is very straight-forward. The message format is called a “wrapper” in SNMPv1 consisting of a small header and an encapsulated PDU. Header fields are not needed in the SNMPv1 because of their security method.

For this particular project we chose the SNMP v1 due to the authentication schemes involved as well as the security involved.

When using **SNMPv1**, the snmp agent uses a simple authentication scheme to determine which **Simple Network Management Protocol (SNMP)** manager stations can access its Management Information Base (MIB) variables.

This authentication scheme involves the specification of **SNMP** access policies for **SNMPv1**. An **SNMP** access policy is an administrative relationship involving an association among an **SNMP** community, an access mode, and an MIB view.

3.7 Operating System

3.7.1 Linux

With the growing need to provide equipment with network connectivity and the power to manage it remotely, Lantronix uses a reliable embedded Ethernet and wireless network solutions that offer a simple, cost-effective way to seamlessly embed network connectivity into the products.

Lantronix uses the Linux software suite that allows developers to easily create applications for embedded networking modules.

3.7.2 Windows

Windows environment was used in the project for testing purpose. The web pages are displayed in the windows environment.

Due to the Lantronix Xport Pro being compatible with both the operating systems, it was easier to develop in Linux and then test and display results in the windows environment.

3.8 Summary

Web –based management is one of the trends of network management. Industries and other manufacturers are making their devices web enabled to compete in today’s market, while SNMP is nowadays the key enabling technology. The layered architecture of SNMP separates the embedded code from the interface ensuring the interface design won’t affect the embedded code. This helps manufacturers to create different integrations of their products interface without reengineering or recompiling any code. The generic data format and access method makes it possible for various management interface – SNMP, web, Telnet, and others – to uniformly access MIB modules and their associated MIB objects.

With the tremendous development of technology, it is an important factor where the embedded device is web enabled and can be monitored and controlled remotely. Therefore the products with flexible and various access methods are required to remain competitive.

Chapter 4

Literature Review

4.1 Introduction

The rapid development of micro technologies, embedded devices and other related technologies has enabled us to develop various kinds of sensors both wired and wireless and use them in order to web enable embedded devices. Embedded systems have limited resources compared with PCs. Some applications require large memory space and high processing power. Therefore, it is essential to use the most efficient product that acts as a server and has a comparatively good memory.

This chapter introduces the web technology that has been used to web enable the embedded devices. This chapter provides a literature review of research and industry works undertaken in the field of embedded devices and wireless communication. This chapter also discusses open issues, research trends and outcomes.

One of the common computer technologies in today's world is to utilise the web. Web technology is the most common technology used for computer users. By using web browser, user can view web-pages developed or located within any operating systems, whether that is a Windows or Linux environment.

Web services are a standardized way to call a remote procedure over the internet. They allow a distributing computing scheme to work independently from the technology, language and

device. The advantage of this technology is that the web client software (web browser) can communicate with any web-server using the Hyper-text Transfer Protocol (HTTP).

HTTP is used as a transport protocol, to move messages between clients and servers, for secure transmissions, HTTPS can be used. Many industries have developed products with embedded devices over the web interface. Fig 11 shows a typical scenario of web services user in an industry.

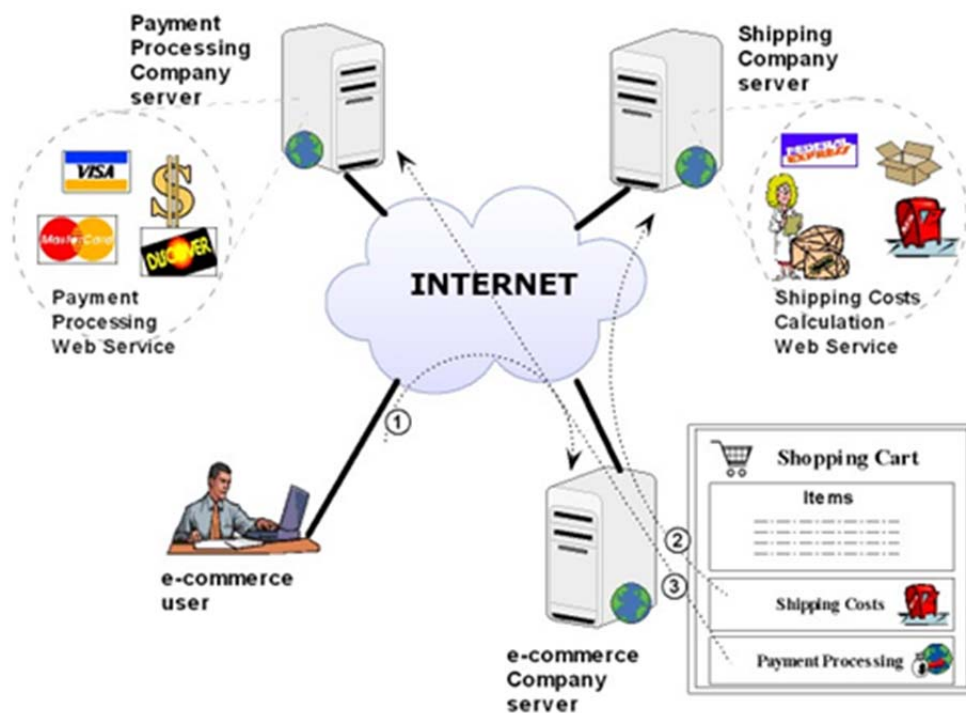


Fig 12- Scenario of Exposing and Consuming Web services.

Projects have been conducted to provide embedded IT management services in physical network devices with simple services, so that in order to deploy those services, it is enough to

select the specific device providing the service, and connect it to the communications network.

Web-servers that are embedded consist of a CPU (Central Processing Unit) and a RTOS (Real-time operating system). In order to communicate with other devices using a serial interface, it has a TCP/IP Stack and an Ethernet connection built in as a source of communication. Companies such as Lantronix, Tibbo, Digi, Moxa etc. provide embedded web servers. {*“Embedded web-servers for remote control in domotics”*, Sandu & Ioln }

From a functional point of view, the services offered by these devices are totally compatible with the traditional network services, and therefore, their integration and interoperability are ensured. The services implemented are compatible with standard web services and with other more traditional client-server protocols within scope of systems management such as telnet, TFTP, HTTP or SNMP. The main aim of a network monitoring service is to check the correct operation of the TCP/IP network applications and services running in manufacturing components.

One of the main architectures used in designing this type of network is the client-server architecture. This brings the server capability to machines – by device-server technology and working out the distance, by device networking technology, “machine to machine” (M2M) (Lantronix Inc, 2009).

Today, technology utilizing the web is one of the most popular used computer technologies. A Web-browser can view web pages developed or located within any operating systems. The beauty of this technology is that the web client software (web Browser) can communicate with any web-server using the Hyper-text Transfer protocol (HTTP). Also the pages displayed by these systems look identical even though generated by a variety of computer systems. This technology is used with embedded systems for control and monitoring purposes. There are few factors which need to be considered while making web-based embedded devices. Once a device is web enabled, it can be accessed from anywhere and it displays real time data.

4.2 Open Issues and Research Trends

Despite the fact that there are many products that have used communication technology in their embedded devices, there exist many open issues. This section attempts to summarize some of the open issues, which may be considered as potential research themes in further study.

4.2.1 Open Issues

There are always risks and controversies associated with web-enabled technologies.

While we try to understand the potential of these technologies, it is important to consider other factors such as its limits and provisions in bigger organisations. Below is a summary of many issues that are considered while using web-enabled devices.

- **Bandwidth restrictions and latency**

Slow transmissions and methods and large number of access to a site in a given time.

- **User Ignorance and Perceptions**

Lack of understanding of web-based applications and its usefulness

- **Maintaining and integrity of data**

Maintaining up-to-date and accurate information on the site for users to use as a user-friendly application

- **Security**

Maintaining secure and safe systems and keeping unauthorized user access out.

- **System Incompatibilities**

Cross-platform incompatibility that prevents a broad system integrations and access.

- **Web Performance Tracking**

Maintaining account of traffic volumes and utilization of the webpage and its content

[19]

4.2.2 Research Trends

In its most basic and practical form, the concept of “systems applications” is based on “managed services integrated with embedded computing.” It requires more than just providing connectivity, data base and HTML language to acquire the real image of internet connected devices. By allowing embedded devices to execute remote applications, it enhances in the growth of network embedded devices.

System applications are fairly generalized and are created by applying generic connectivity functions to a particular venue. The breakdown of System Applications is as follows:

- **Status, Monitoring & Diagnostics:** Status applications capture and report on the operation, performance, and usage of a device, or the environment that the device is monitoring. Diagnostics applications allow for remote monitoring, troubleshooting, repair, and maintenance of networked devices.
- **Upgrades & Configuration Management:** Upgrade applications improve or augment the performance or features of a device. They can prevent problems with version control, technology obsolescence, and device failure. This kind of program makes site visits to upgrade products unnecessary and eliminates the need to keep track of what has been upgraded and when, thus saving time and money.
- **Control & Automation:** Control and automation applications coordinate devices into a sequenced pattern of behaviour. These applications also allow for special-case discrete actions of a device under certain circumstances.
- **Location & Tracking:** Profiling and behaviour-tracking applications are used to monitor variations in geography, culture, performance, usage, and sales of a device. These applications can also be used to create a more customized or predictive response to end-users of a device.
- **Data Management & Analytics:** Business intelligence and specialized analytical software such as data mining and predictive analytics, video image analysis, pattern recognition, and artificial intelligence [3].

4.2.2.1) The Serial Tunnelling Concept

The server which is implemented in the project can serve static and dynamic web pages.

If a user requests any queries on the port 80, it checks whether is it a GET request or not and if it is then, it sends the response of that queries.

Serial Tunnelling is a process of sending serial data over Ethernet. For instance, if a letter is send through a postal service then it becomes analogue. In this case, “letter” becomes the serial data, the “envelope” is the TCP/IP packet and the “postal service” is the infrastructure of the network (Sandu, Florin & Iolu, Daniel, 2007).

If we analyse the serial tunnelling by its design, it seems to be transparent between the application software and the devices connected.

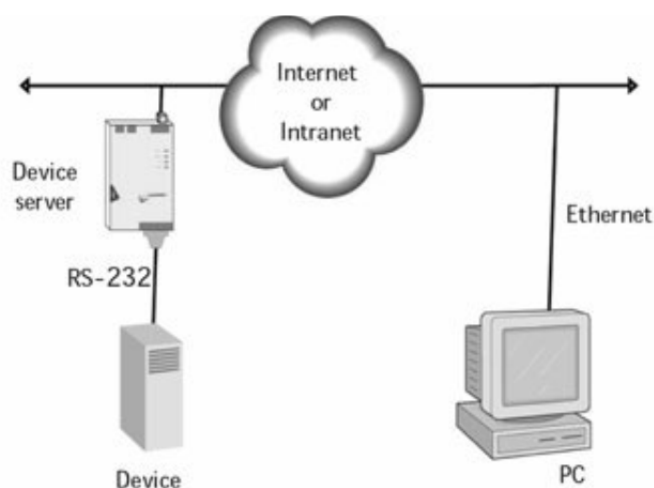


Fig 13: Serial Tunnelling Concept

By using the Serial Tunnelling Concept, it gives us an option to choose the protocols along with an option to use the same infrastructure for new protocols.

4.2.2 b) Machine to Machine Concept

The Machine to Machine communication begins with taking data out of a machine so that it can be analysed and sent over a network. The goal of M2M hardware is to bridge the intelligence in the machine with the communication network (<http://www.m2mcomm.com>).

With an intelligent electronic device, it may be possible to simply connect to the equipments serial port and ask for the data.

Lantronix device servers enable machine-to-machine (M2M) communications between a computer and serial device or from one serial device to another over an Ethernet network or the Internet (Lantronix Inc, 2009).

4.2.2 c) The Web Server

The XPort Pro module can be used to add networking capabilities to your device.

The development board includes an RS-232 serial port and a 10/100Base-TX network connection (RJ45).

Based on the 2.6 Linux kernel, and leveraging existing open source software, the SDK simplifies the process of adding custom applications. Device drivers, GNU Tool chain, pre-defined configuration profiles, and sample applications are all included.

Highly developed networking and safety features allow machine-to-machine (M2M) edge computing with unlimited customisation possibilities and application hosting so that the developer can get their product on the market quicker as well as having countless development options.

The XPort Pro runs on Linux and already supports Ipv6. It is also available with the complete Lantronix operation system and Software development kit Evolution OS™ as well as numerous additional features. In addition this product includes Lantronix's patented VirtualIP (VIP) technology that enables a flawless integration of the remote management platform ManageLinx™ from Lantronix.

The XPort Pro offers five times better processor performance and 32 times more memory capacity than its predecessor. It includes SSH and SSL security and code encryption and supports numerous protocol conversions.

4.3 Analytics drives real-time value

“Real-time awareness” is driving renewed interest and deployment of analytic tools. By using extensible and adaptable systems, it is possible to analyse and store huge amount of data. Technologies such as Rules engines and work flow are used to decide on which alternative courses to use, either automatically through the application of a rule that says “if this happens, do this,” or through human review based on work flow.

With specific components moved towards intelligent devices so they execute actions as commanded, the business scenarios adapt the processed applications. Converting the processed applications to service-oriented architecture will allow these adoptions by the business scenarios. For example, alerting a person about the next bus time on his Smartphone. A doctor is notified about the next patient on his tablet PC.

4.4 Conclusion

There are various approaches to the problem of web enabling embedded devices. Each device has its own protocols and needs to be merged with the web technology. Each proposed scheme has its own benefits and drawbacks. This trade-off between benefits and drawbacks means that each embedded device can be compatible with one technology but unsuitable for another type of device.

The critical issues discussed in this chapter are a part of this emerging technology. These issues are it is important that these issues are handled rapidly without any delay. There are possibilities that new issues are encounters to the user as the web continues to expand.

This chapter emphasised on the technologies involved and the protocols that are used in this process of making an embedded devices accessible with real-time data over the web. In order to build this communication link, all the hardware and software equipment used as clearly discussed in the following chapters ahead.

Chapter 5

Design of the Web Enabled Power Supply

5.1 Introduction

This chapter describes the simulation models involved with the SNMP standards. Due to the increment in technology, it is much easier to interact with devices from a remote location using a web browser over an Ethernet network. There are hardware devices which help in converting the RD-232, RS-422 or RS-485 serial port into an Ethernet interface. These can be accessed by any IP based application (like a web browser) over an IP network from any location in the world. In this project, we use the Lantronix Device Installer application to meet the configuration requirements.

Web browsers, like Microsoft's Internet Explorer requests information from web servers by using a protocol known as Hypertext Transfer Protocol (HTTP).

There are three basic methods such as (GET, HEAD and POST) which are used to interact with the server.

The Lantronix supports an internal web server that may be utilized by the web programmer for storage and retrieval of documents, images and Java Applets.

The Lantronix acts as a device server. It includes UDS and Xport and supports a HTTP server. The HTTP server transfers static documents or files as per web browser's request.

5.2 Key Features of the Design

In order to accomplish this project, it is important that we choose the right tools for integration of embedded devices onto the web.

When this project was started, the appropriate tools that could be used to develop this project were unclear. CGI & HTML programming language is used as a development tools for web applications. Lantronix Xport Pro was the device that supported web interface. It has a built in web server that supports all the programming languages including Java. After realizing its potential (as discussed below), it was selected as the language to be used for this project.

Some of the many critical reasons for its selection are mentioned below.

5.3 User Interface

User Interface is an important factor in this project. This is a way of communication for the user through to the embedded device. There are two types of user interfaces. The operator has control over the individual power modules by using a graphical user interface (GUI).

The script files are constructed and sent directly for execution by the command line interface (CLI).

The HTTP interface represents the GUI and the CGI programming represents the Command Line Interface. An embedded device can only be web enabled with the combination of these two User Interfaces.

5.3.1 CGI Programming

The widest source of communication on the internet is the web. For example, a user downloads an applet from a server to send some data, and the applet directly communicates with a CGI Program [2]. The server agent runs on a system that has CGI programs. In Fig 13, it offers API Libraries to CGI programs to communicate with the Server agent to the jobs related to security. It also maintains security sessions with the Web Proxy.

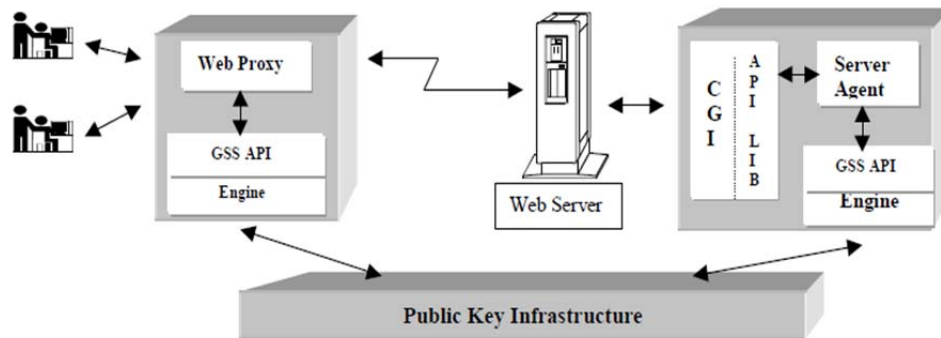


Fig 14 – “Design of a system to support security communication between a Web Proxy and a CGI program.

On a dynamic embedded web server, the CGI program is adopted to complete the required workflow. Due to the resource limitation of embedded systems, the performance of an embedded web server is an important issue. As mentioned by ZhenXing, Wang & Xian Yi, Ren [3], in their study on CGI of Embedded Webserver that it is ideal to combine CGI with Java script and make them collaboratively running to satisfy the requirement of an embedded application. On embedded servers, the CGI processes the parameters submitted by the client

PC and appends results to the end of the html page. On the user interface Internet Explorer, the javascript embedded in the HTML page will parse the results and display on the webpage.

5.3.2 HTTP Interface

HTTP server is the program which is built inside the same file as the mini web-server.

The web interface provides the user with basic status information including system voltage, system current, number of alarms and Battery condition status.

HTTP server passes CGI request and calls the main request with the selected method (GET or POST) CODE and its parameter (ZhenXing, Wang & Yi Xian, Ren 2008).

As this is not the most secure web server this does not perform many operation which other web server would do, such as; it will not perform URL decoding, means if it contains any special characters then it would come as error page.

Mini web-server contains many functions but two being most important are:

`http_format_char()` and `http_exec_cgi()`.

http_formate_char(): This is a call back function application must provide and it is called by the function called `http_taks()` in the same file. This function returns the special formatting information for the web-pages stored in the memory.

Means when, the HTTP server encounters a string in the CGI, which it is serving, it calls this function. This function is executed via main user application and it is used to transfer certain variable status to the HTTP.

http_exec_cgi(): is a callback function the application must provide and returns special formatting information for the web pages stored in the program memory.

When the HTTP server receives a GET method with more than one parameter, it calls this function.

The server which is implemented in the project, can serve static and dynamic web pages.

If a user request any queries on the port 80, it checks whether GET is request or not and if it is then, it sends the response of that queries.

Mentioned above are a few examples taken from projects that have implemented embedded devices over the web. These projects are very helpful while implementing SNMP and making the power supplies web enabled.

5.4 EMBEDDED DEVICES

5.4.1 ATMEL – Microcontroller

The power supplies have an ATMEL AT89LP6440 microcontroller built in that contains all the information and data about the power supply.

AT89LP6440 is from the 8051 microcontroller family. It comes along with a Development Studio which is used for programming and communicating to other devices.

The microcontroller has 3 I/O pins that are programmable and can be used for device configuration.

The AT89LP6440 micro controller is programmed in such a way that it contains all the required information about the power supply including the voltage, current and status of the batteries in the power supplies.

The AT89LP6440 is a low-power, high performance CMOS 8-bit microcontroller with 64K bytes of In-system Programmable Flash program memory and 8K bytes of Flash data memory.

5.4.2 Lantronix Xport Pro

Lots of research was involved until the end of the project, precisely on understanding the Xport Pro device. Xport pro features involved lots of implementation from installing the device software to connecting to the web server of the device.



Fig 15 – Lantronix Xport Pro

The Lantronix Xport pro is a powerful, self-contained embedded networking device. It is with the popular XPort pro and can it can be run on either Linux or Windows operating systems. The XPort Pro allows user to deploy advanced applications without any complexity of designing a network. It has a very manageable size as a hardware product. The unique smaller size of the XPort Pro provides everything inclusive in a single embedded solution. It contains an advanced architecture called the 32-bit processor. By using this processor it handles applications with the pair of a high-speed [21].

It also allows unlimited flexibility for customizations and application enablement.

The xport pro allows mounting of file systems, the ability to run a minimalist web server called Boa, and the telnet access. The main function of this tiny machine is to push data back and forth between LAN connection and the serial port.

The Lantronix Xport Pro kit comes with a Developers kit. The Lantronix Linux Software Developer's Kit (SDK) is an embedded hardware and software suite that enables Linux developers to create applications on Lantronix embedded networking modules.

5.4.2a XPort Pro Features

The XPort Pro contains a 32-bit processor, with 8 Mbytes of SDRAM,

It also contains 16 Mbytes of Flash and an integrated Broadcom 10/100 PHY [21].

Hardware in-built features are as follows:

- 3.3-volt serial interface
- I/O pins are 3.3V tolerant
- Ethernet socket

- Power supply filters
- Reset circuit
- +1.5V regulator [21].

5.4.2b XPort Pro Block Diagram

The Xport Pro block diagram below shows the connections between the components.

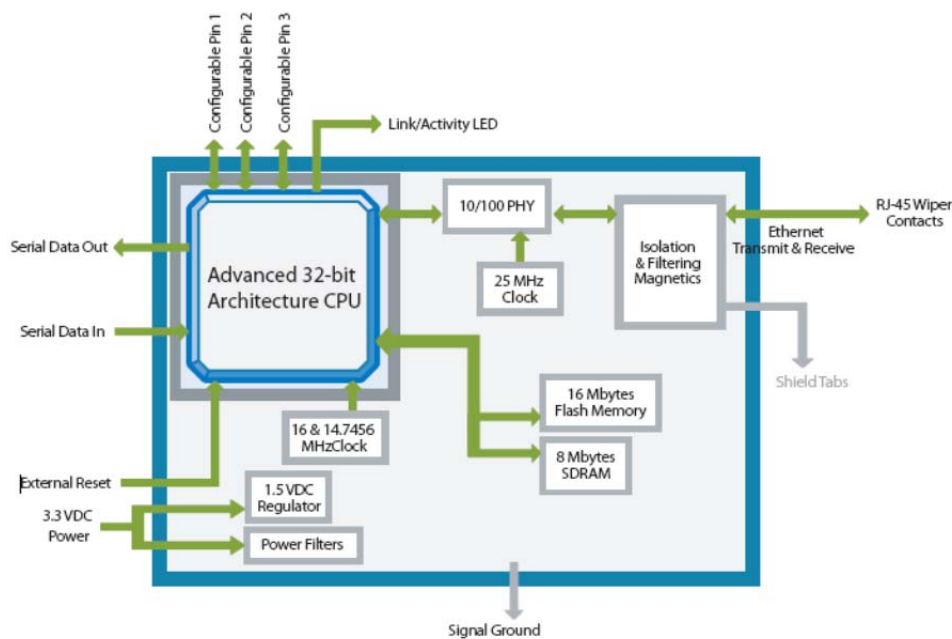


Figure 16 - XPort Pro Block Diagram [21].

5.4.2c PCB Interface

In the PCB interface, the XPort Pro has a serial port. It is compatible with data rates up to 921600 bps.

The serial interface pins (4-8) include +3.3V, ground, and reset. The serial signals connect to an internal UART driven at 3.3V [21].

5.4.2d Ethernet Interface

The Ethernet interface consists of RJ45 connector, Ethernet status LEDs. They are all in the device server shell. The XPort Pro PHY is Auto MDIX capable allowing connection to either straight through or cross over Ethernet cables.

5.5 Design steps for the proposed protocol

The design of the project included many tools and designing of the web pages. The primary system to test was the V series SR500i LAN+ unit's power supplies.

Real-time data is executed and displayed on the web pages, which helps in constant monitoring of the device. SNMP is currently available on the "I" series and the "V" series of power supplies.

SNMP, short for Simple Network Management Protocol, depends on centralized Managers (software) managing Agents (also software) on distributed devices, based on data defined in MIB (Management Information Base) text documents. Managers use the protocol to "get" data from Agents and to "set" read-write data to Agents. Agents are also able to send unsolicited alarms (called "traps") to Managers.

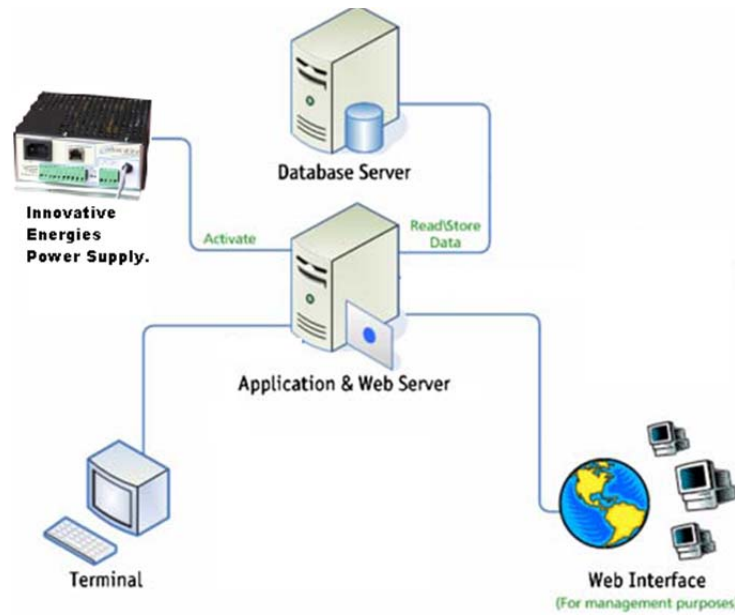


Fig 17 – Structure of SNMP data transfer

The Device Server’s HTTP server supports GET and HEAD methods. This support helps in configuration, and file service. The loading of web pages was first implemented into the I series of the power supplies.

The web pages are added to the Device Server HTTP server using a tool called ‘web2cob’. Device server products that contain 512KB or more flash memory support the HTTP server. The flash memory area is divided into 64KB pages, which are available for “web sites”. These areas are called WEB1 – WEB6 (for 512K flash) [22].

If a request for GET or HEAD is made for a file, the HTTP server will look into the WEB1 slot for the file. If the file is not available in WEB1, it then searches in other slots, i.e, WEB2, WEB 3 until WEB 6 or until it finds the data. Once the file is found, it is sent to the client.

It is essential for the HTTP server process needs to determine if the WEB area contains a valid “web site”. The archive of HTML is created by designing a web2cob.exe design. There

is a storage limit in the embedded device. Therefore, not much data can be stored at a time. Each “web site” or .COB file cannot be larger than 64KB [22].

5.5.1 Creating the Web pages

Creating the web pages for this project was done using the basic coding of HTML. This was done using a simple web editor with no java applets. The web pages contained just plain HTML text. The main purpose was to create web pages with low memory size as it would be easier to load on the web server.

The web pages were created in accordance with the parameters of the power supply that were to be monitored. The parameters consist of real time data such as temperature, voltage, battery condition etc. The labels which are the parameters of the power supply were included in the code in order to display the real-time data on the web pages.

It is essential to check the code that it is in combination with the same parameters that are sent by the CGI programming. Every web page displays different parameters; therefore it is an important factor to be monitored as it displays the real time data.

Further in this chapter, the steps involved in converting the code into a file using the TCP/IP protocol are described. This is the process to display the real time data on the web pages.

5.5.2 Parameters

Parameters or Labels have been created in order to load the commands of power supply into the Lantronix Xport Pro device. These labels are used to read the real time data and then to be displayed on the web pages.

The labels are made in accordance with the power supply parameters. The labels are then inserted into the HTML code as commands. It then reads the data from the power supply and displays it on the web pages.

SRXXX denotes the series of the Innovative Energies power supplies.

```
{ "SRXXX_VER",                srxxx_meta  },
{ "SRXXX_STATUS1",           srxxx_meta  },
{ "SRXXX_STATUS2",           srxxx_meta  },

/* CMDs */

{ "SRXXX_STATUS_BCT",        srxxx_meta  },
{ "SRXXX_CMD_BCTSTART",      srxxx_meta  },
{ "SRXXX_CMD_BCTSTOP",      srxxx_meta  },
{ "SRXXX_CMD_BCTENABLE",     srxxx_meta  },
{ "SRXXX_CMD_BCTDISABLE",    srxxx_meta  },
{ "SRXXX_CMD_RESETTEMPLOG",  srxxx_meta  },
{ "SRXXX_CMD_BATTERYSELECTSTATUS", srxxx_meta  },
```

```

{ "SRXXX_CMD_BATTERYTOGGLE",          srxxx_meta  },
{ "SRXXX_CMD_ACK_BCTSTART",          srxxx_meta  },
{ "SRXXX_CMD_ACK_BCTSTOP",          srxxx_meta  },
{ "SRXXX_CMD_ACK_BCTENABLE",        srxxx_meta  },
{ "SRXXX_CMD_ACK_BCTDISABLE",       srxxx_meta  },
{ "SRXXX_CMD_ACK_RESETTEMPLOG",     srxxx_meta  },
{ "SRXXX_CMD_ACK_BATTERYSELECTSTATUS", srxxx_meta  },
{ "SRXXX_CMD_ACK_BATTERYTOGGLE",    srxxx_meta  },
{ "SRXXX_CMD_CONFIG_REFRESH",       srxxx_meta  },
{ "SRXXX_CMD_STATUS_REFRESH",       srxxx_meta  },

/* STATUS */

{ "SRXXX_DATA_OUTPUTVOLTAGE1",      srxxx_meta  },
{ "SRXXX_DATA_BATTERYCURRENT1",    srxxx_meta  },
{ "SRXXX_DATA_POWERSUPPLYCURRENT1", srxxx_meta  },
{ "SRXXX_DATA_TEMPERATURE1",        srxxx_meta  },
{ "SRXXX_DATA_TIMEINMINUTESBETWEENBATTERYDETECTTESTS1",
srxxx_meta  },

{ "SRXXX_DATA_MINVOLTAGEODETECTBATTERYPRESENCE1",
srxxx_meta  },

```

```

{ "SRXXX_DATA_SHUTDOWNVOLTAGE1",          srxxx_meta  },

{ "SRXXX_DATA_BATTERYLOWALARMVOLTAGELEVEL1",      srxxx_meta  }

{ "SRXXX_DATA_BATTERYDISCONNECTVOLTAGE1",        srxxx_meta  },

{ "SRXXX_DATA_BATTERCHARGECURRENTLIMITPERCENTAGE1",
srxxx_meta  },

{ "SRXXX_DATA_LENTGHOFBATTERYCONDITIONTESTMINS1",
srxxx_meta  },

{ "SRXXX_DATA_TIMEINTERVALBETWEENBCTSINMINS1",    srxxx_meta
},

{ "SRXXX_DATA_TIMEINTERVALBETWEENBCTSINHRS1",     srxxx_meta
},

{ "SRXXX_DATA_TIMEINTERVALBETWEENBCTSINDAYS1",    srxxx_meta
},

{ "SRXXX_DATA_MAINSFAILCHECKINTERVALDURINGBCT1",
srxxx_meta  },

{ "SRXXX_DATA_TEMPERATURELOWTRIGGER",              srxxx_meta  },

{ "SRXXX_DATA_TEMPERATUREHIGHTRIGGER",            srxxx_meta  },

/* SRXXXCONFIG settings */

{ "SRXXX_CFG_SYSLOG_ENABLED",                      srxxx_meta  },

{ "SRXXX_CFG_SYSLOG_SELECTED_ENABLED",            srxxx_meta  },

```

```

{ "SRXXX_CFG_SYSLOG_SELECTED_DISABLED",          srxxx_meta  } ,

{ "SRXXX_CFG_SYSLOG_SERVER_IP_1",              srxxx_meta  } ,

{ "SRXXX_CFG_SYSLOG_SERVER_IP_2",              srxxx_meta  } ,

{ "SRXXX_CFG_SYSLOG_SERVER_IP_3",              srxxx_meta  } ,

{ "SRXXX_CFG_SYSLOG_SERVER_IP_4",              srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_ENABLED",                srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SELECTED_ENABLED",        srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SELECTED_DISABLED",        srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SERVER_IP_1",            srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SERVER_IP_2",            srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SERVER_IP_3",            srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_SERVER_IP_4",            srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_RETRY_COUNT",            srxxx_meta  } ,

{ "SRXXX_CFG_SNMPTRAP_TIMEOUT",                srxxx_meta  } ,

{ "SRXXX_CFG_REBOOT",                          srxxx_meta  }

```

These are all the parameters that have been inserted into the CGI and HTML programming as they read the real time data from the power supply.

The procedure for this project involved liaising with the power supply parameters. In order to that, labels were created for each and every individual parameter of the power supply.

The labels were created in a format which could be included in the CGI based programming as well as the HTML code.

Continuous modifications were made to the code to achieve the end product. If there are any modifications made, then the task has to be run again to check the program. This task takes weeks and weeks just in terms of testing the product.

For example, new traps were implemented into the code in order to create new alarms to the system. MIB browser is used to monitor the traps to make sure they are working in the correct order.

Testing of the project was done on the new set of web pages created. This allowed us to monitor the exact information from the power supply.

5.5.3 Assigning an IP Address

Depending on the compatibility of XPORT PRO, it is only compatible with Linux. Therefore, we had Linux machine setup with a DHCP server built into that.

The Linux machine in the development unit was configured and access was granted with admin rights. The operating system used is the FEDORA 14 with a DHCP server set up in the Linux machine.

The DHCP server is used to assign IP address to the machine depending on the MAC address of the device.

The Xport / Xport pro devices were assigned an IP address from the DHCP server settings.

For eg: XPORT PRO MAC Address: 00-20-4A-BF-FD-AD was assigned with an IP address of 192.168.101.53.

Once the Xport was assigned an IP address, we were able to communicate with the device using the Ping commands. The IP address was associated to each device according to their MAC address entered.

5.5.4 Creating the .COB files

Lantronix provides a utility called “web2cob.exe” to create the required archive file for the archive file for the “web site”. [15]

Syntax: Web2cob.exe/d <directory> /o <output_file_name>

Where: “directory” is the directory that contains the files to be archived

“output_file_name” is the name of the archive to be created. [15]

Example: Web2cob/d source/o lan2.cob

We have created the .COB files first so that we could upload the web pages into the power supply.

Once the .COB files have been created, we then need to download them to the Device Server.

To download the .COB files into the Device Server, we need a tftp client program. A tftp client program was downloaded from the web.

Meanwhile, within the DHCP server, an IP address was associated to the Device using their MAC address.

E.g.: A Xport device of Lantronix containing a MAC address of 00-20-4A-A7-B5-75 is associated with an Ip address of 192.168.101.51.

To load the .COB file into the Device Server, the below process was followed:

1. From a command or DOS prompt on Windows 2000 or NT. [15]
 - a. C: tftp -i 192.168.101.51 PUT /lan1.cob WEB1.

The new web page can now be accessed from any browser using the new URL:

<http://192.168.101.51/home.html> - The IP address denotes the IP address of the Device Server.

The web pages were successfully loaded on the Xport device in the power supply.

5.6 Summary

This chapter discussed the key steps that were taken to design and implement in this project. The user interface is a combination of other interfaces such as CGI programming and HTTP interface, which are used in order to web enable the power supply. The important factor was to choose the right web server which collaborates with the embedded device in the power supply. The Lantronix Xport Pro device has a built in web server that incorporates the required specifications we use for this project.

Other part of designing involved web page designing using basic HTML code so that it uses less memory of the web server and can be easily loaded on the webs server. In order to display the real time data, the process of converting the code into a .cob file and then to the server is involved. The parameters are an important factor as they display the real-time data.

The HTML code includes all the parameters as labels in its code in order to display the real-time data on the web pages. On the other side the Xport Pro devices are to be displayed on the network. This is done by assigning the IP address to each of the devices so that they are shown on the network and can be communicated using the web.

In the next chapter, we shall discuss the simulation methods used to web enable the power supplies.

Chapter 6

Performance Simulation of the Project

6.1 Introduction

This chapter discusses the software's used in order to simulate the required parameters.

Furthermore, it discusses the parameters that are being used for testing purposes while web enabling the power supplies.

Before starting the analysis, it is important to understand the parameters that are associated with this project. It is important that the web server reads the correct data from the power supply and then displays it across on a Graphical User Interface, i.e. web page.

This set of web pages created are very basic and simple to use as they contain just plain text in HTML format.

In the communication side, the DHCP server should read the MAC address of the Lantronix Xport Pro device and assign an IP address to it. Communication portal such as Ipscan reads all the hardware installed through an ethernet connection. It displays the MAC address of all the devices attached and assigns an IP address of the range.

The IP address is then inserted into the web page and the login page is displayed.

6.2 Simulation Environment

Programming was done for the Version 1 of SNMP. CGI programming was implemented so that the web pages could communicate with the actual data in the power supplies.

Once all the programming was done for Xport Pro to be able to communicate with the Power Supply, the programmed files are then converted into a image.bin file.

This file contains all the huge number of data and compresses into a .bin file.

6.2.1 WinSCP

Initially, A Linux SDK 2_0_0_0 Firmware was installed into the Linux Machine. Software called WinSCP was downloaded so that we could see the Linux Machine remotely.

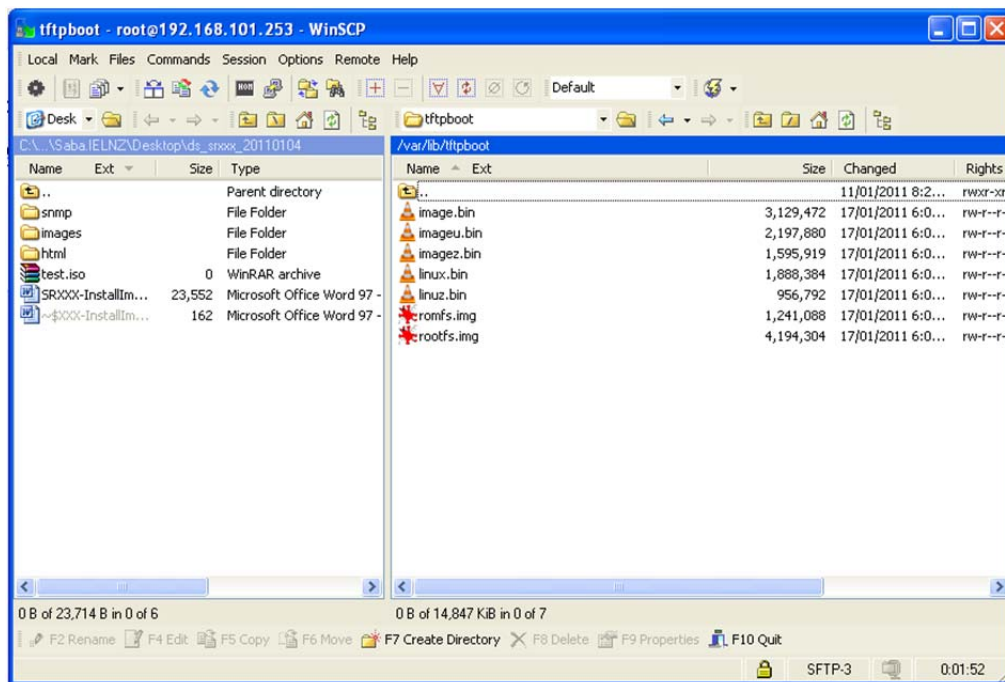


Fig 18– WinSCP window, where the image files are loaded

6.2.2 Putty

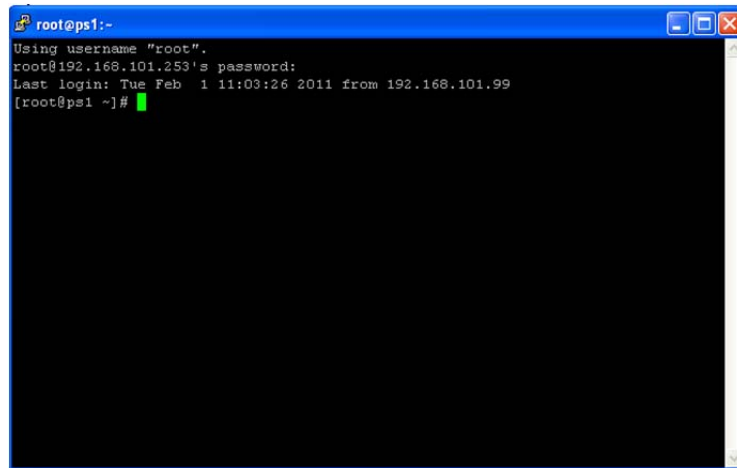


Fig 19 – Putty Window

Fig 19 represents the WinSCP window along with Putty that we use to issue commands to the Xport Pro Device.

Series of commands are issues using the Root login where root login is like an Admin login.

From the Linux SDK programme, a TFTP-Server was installed using the following commands.

1. Install the tftp-server package (rpm)

Yum install tftp-server

2. Edit /etc/xinetd.d/tftp and change the value of disable to “NO:.
3. Restart the xinetd service.

Service xinetd restart.

4. The system was configured and built in order to allow access to the command line function to netcon for later use.

>iexport

5. Image is copied into the release directory and the tftp directory.

```
>cp ds_srxxx_20yymmdd/images/* {IEXPORT_ROOT}/linux/images
```

```
>cp ds_srxxx_20yymmdd/images/*/var/lib/tftpboot
```

6. Determine MAC address for lantronix device.

```
Edit /etc/dhcpd/dhcpd.conf
```

7. Add MAC address to IP address translation to subnet.

```
Host xportpro-dev {
```

```
    Hardware Ethernet 00:20:4A:BF:FD:AD;
```

```
    Fixed-address 192.168.101.50;
```

```
}
```

8. Restart DHCPD

```
>service dhcpd restart
```

9. Configuring method to upload image to Lantronix.

After the IP address has been changed then it's now possible to telnet into the device.

```
>iexport
```

```
>netcon 192.168.101.50
```

```
dBUG>
```

10. Set the image type

```
dBUG>set filename image.bin
```

11. Set tftp server address

```
dBUG>set server 192.168.101.254
```

12. Downlaod imageto flash

```
dBUG>dnfl
```

13. Downloading image 'image.bin' from 192.168.101.50

```
TFTP transfer completed.
```

```
Program successfully flashed.....
```

14. After image flashed , configure the device to autoboot from flash

```
dBUG> set autoboot flash
```

15. Power cycle device

```
dBUG>reset
```

16. After the device has re-powered and acquired its IP address, check the web page.

6.2.3 Web Page

The webpage was successfully loaded with the programmed HTML pages.

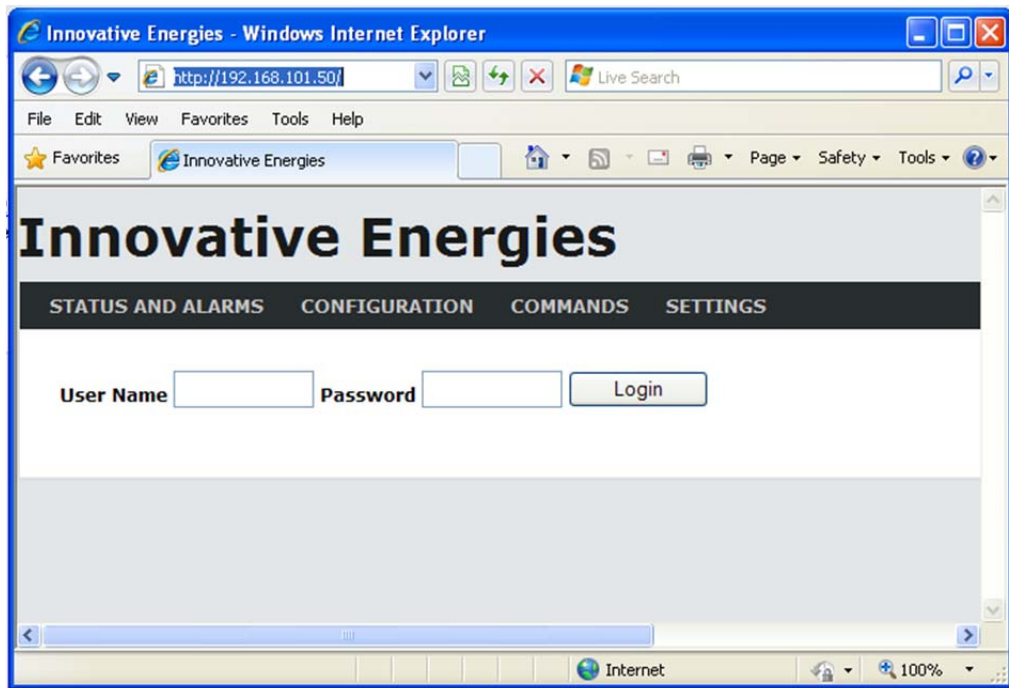


Fig 20 – Web page for the power supply [16]

The HTTP application models web browsing. The user accesses this web site through the web server of the Lantronix Xport Pro device in the power supply. Every page contains text and graphic information that displays real-time data. [16]

The DHCP will show on the connected network list as its IP address is automatically allocated by the LAN, DHCP server is connected to. The Ethernet interface is DHCP enabled by default.

Using a web browser, such as Internet Explorer, Firefox, Google Chrome, type the IP address of the Power Supply Unit or Battery Charger into the url address box of the web browser eg) <http://192.168.100.51>. [16]

6.3 Parameters monitored while simulation

Parameters being the main factor in web enabling the power supply in order to display the real-time data on the web pages.

Once the first set of web pages were made, only few parameters were tested by adding the labels on the html code. It was essential to set a few basic parameters that could be used for testing the real-time data. By testing few basic parameters, we could confirm that the data that the web pages are spitting out is the real-time data. This also ensures that the communication between the web server and the power supply has no errors.

Below, the parameters have been described that are used for the simulation.

Output Voltage: Displays power supply voltage when mains are on
 Displays battery voltage when mains are off or during a battery condition test (BCT)

Battery Current: Displays a positive reading when being charged
 Displays a negative reading when being discharged

PSU Current: Displays the total of the Load and the Battery Current

Load Current: Displays load current calculated by subtracting the PSU current from the Battery Current

Temperature: Temperature reading is taken from the temperature sensor placed near the batteries (note that the reading will be very high if no sensor is connected)

Temperature Log Low: Displays the Lowest temperature recorded

Temperature Log High: Displays the Highest temperature recorded

Estimated Battery Time Remaining: Indicates run time in minutes when there is no input power

Refresh Configuration: This function refreshes all of the variables above, capturing the most current information from your Power Supply or Battery Charger (Note that this does not include temperature logs

BCT Start: Starts a Battery Condition Test

BCT Stop: Stops a Battery Condition Test

BCT Enable: Enables a scheduled Battery Condition Test.

BCT Disable: Disables a scheduled Battery Condition Test.

Reset Temperature Log: Resets the temperature log.

6.4 Conclusion

This chapter has discussed the various aspects of testing and how the software testing was closely bound with the software development. The approach made for the devices to be web enable was through the help of the various softwares. Each software was then combined in order to output the real time data on the web pages.

Using these software and the programming interface, we are now able to see the real time data through a web interface using an advanced technology such as SNMP.

All these paramaters can now be viewed by using a web interface. This helps cut costs and usage of equipment to monitor on site.

This project totally focused on the development of SNMP feature using the web interface. There is considerable amount of work still required to enhance the final product.

Chapter 7

Results & Discussion

7.1 Introduction

This chapter discusses the results after web enabling the power supplies. Real-time data is analysed in this chapter. Different parameters are compared and analysed in terms of temperature control, Battery condition test, Voltage, Current etc. The real-time data is tested by making changes to the hardware of the embedded device. This involves changing of the parameters such as temperature, voltage etc.

7.2 Results

7.2.1 LOGIN Page [16]

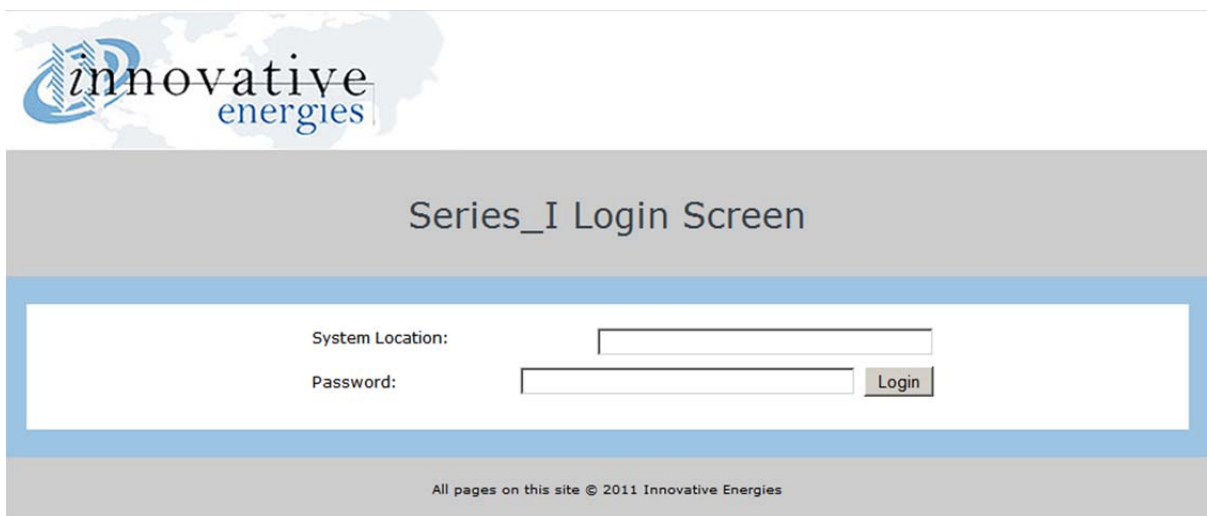


Fig 21 – Login Page

Once the Innovative Energies Power Supply/Battery Charger is connected to the network, you have typed the IP Address into the url address box of the browser and found the long-in webpage, then the user is ready to login.

The default password is: **iepassW1** (Note that the password is case sensitive)

Insert the default password into the 'Password box.

Note: The 'System Location' field can be changed/personalised on the 'SNMP Configuration' web page.

Click on 'Login' with the mouse (Note that in some browsers pushing the 'Enter' key to log-in may not work)

7.2.2 MONITORING & CONTROL

Monitoring & Control
SR250i12T

- **Monitoring & Control**
- Network Settings
- PSU Configuration
- SNMP Configuration
- Syslog Configuration
- Firmware Upgrade
- Contact Details

CONTROL

BCT Start BCT Enable

BCT Stop BCT Disable

Reset Temperature Log

MONITORING

Power Supply Status:	System Down
Battery Status:	Battery Low
Output Voltage:	10.0
Battery Current:	-15.1
PSU Current:	0.3
Load Current:	15.4
Temperature:	21
Temperature Log Low:	18
Temperature Log High:	22
Estimated Battery Time Remaining:	N/A

Refresh Configuration

THRESHOLDS *(Please note that only integer values are accepted)*

Temperature High Threshold (degC):

Temperature Low Threshold (degC):

Over Voltage Threshold(V):

Load Current Threshold(A):

Threshold Update

Fig 22 – Monitoring & Control Page [16]

MONITORING - Understanding Monitored Variables Terms:

Output Voltage: Displays power supply voltage when mains are on
 Displays battery voltage when mains are off or during a battery
 condition test (BCT)

- Battery Current:** Displays a positive reading when being charged
Displays a negative reading when being discharged
- PSU Current:** Displays the total of the Load and the Battery Current
- Load Current:** Displays load current calculated by subtracting the PSU current from the Battery Current
- Temperature:** Temperature reading is taken from the temperature sensor placed near the batteries (note that the reading will be very high if no sensor is connected)
- Temperature Log Low:** Displays the Lowest temperature recorded
- Temperature Log High:** Displays the Highest temperature recorded
- Estimated Battery Time Remaining:** Indicates run time in minutes when there is no input power
- Refresh Configuration:** This function refreshes all of the variables above, capturing the most current information from your Power Supply or Battery Charger (Note that this does not include temperature logs

MONITORING - Typical alerts & displays for Power Supply and Battery Status:

1. Input power present, battery passed BCT and fully charged*¹

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Good (Possible Battery Missing)* ¹

2. Input power present, battery charging and passed previous BCT

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Good

3. Input power present, BCT in progress

Power Supply Status:	Battery Condition Test
Battery Status:	Battery Condition Test

4. Input power present, failed BCT, battery charging

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Battery Bad

5. Input power present, battery charged, failed previous BCT

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Possible Battery Missing (Battery Bad)

6. Input power present, battery missing

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Battery Missing

7. No input power (in the 30 sec period before before power failure confirmed)

Power Supply Status:	Charge Cycle (Normal Operation)
Battery Status:	Possible Mains Fail

8. No input power (in the 30 sec period before before power failure confirmed), $V_{out} < V_{pres}$

Power Supply Status:	Overload
Battery Status:	Possible Mains Fail

9. No input power (for longer than 30sec), battery has passed previous BCT

Power Supply Status:	Mains Failure
Battery Status:	Mains Fail (Battery Good)

10. No input power, battery voltage is below V_{batl} level, battery passed previous BCT

Power Supply Status:	Mains Failure
Battery Status:	Battery Low

11. No input power, battery has reached the low voltage disconnect level, battery passed previous BCT. *Note that this message is only displayed briefly as communications will also be lost shortly after this point is reached.*

Power Supply Status:	System Down
Battery Status:	Battery Low

12. No input power, battery has failed previous BCT

Power Supply Status:	Mains Failure
Battery Status:	Mains Fail (Battery Bad)

13. No input power, battery has failed previous BCT and below Vbatlow

Power Supply Status:	Mains Failure
Battery Status:	Battery Low (Battery Bad)

14. No input power, battery has reached the low voltage disconnect level, battery failed previous BCT. *Note that this message is only displayed briefly as communications will also be lost shortly after this point is reached.*

Power Supply Status:	System Down
Battery Status:	Battery Low (Battery Bad)

15. No data being sent between web page and power supply

Power Supply Status:	Comm's Failure
Battery Status:	Comm's Failure

7.2.3 CONTROL – Understanding Control Terms:

BCT Start: Starts a Battery Condition Test

BCT Stop: Stops a Battery Condition Test

BCT Enable: Enables a scheduled Battery Condition Test.

BCT Disable: Disables a scheduled Battery Condition Test.

Reset Temperature Log: Resets the temperature log.

Note: Once a Battery Condition Test has been started you cannot stop it until it is complete.

[16]

CONTROL – Customizable Thresholds

Threshold values can be set by the user according to their requirements. SNMP trap (alert) messages will be sent when one of the thresholds are exceeded.

CONTROL – Units

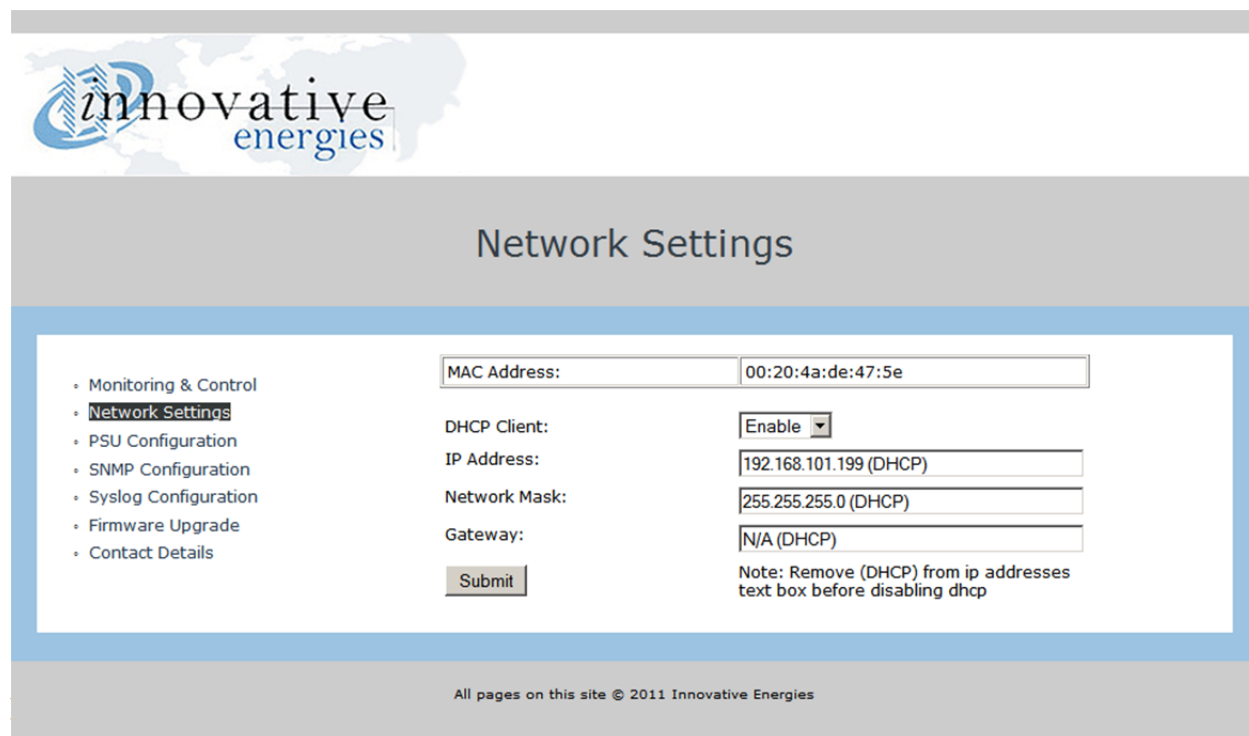
Temperature:degrees C

Voltage: volts

Current: am

7.2.4 Network Settings

This page enables the user to set a **static IP address** for the web page by disabling the DHCP function.



The screenshot displays the 'Network Settings' page. On the left, a sidebar lists navigation options: Monitoring & Control, Network Settings (highlighted), PSU Configuration, SNMP Configuration, Syslog Configuration, Firmware Upgrade, and Contact Details. The main content area contains the following form fields:

MAC Address:	00:20:4a:de:47:5e
DHCP Client:	Enable
IP Address:	192.168.101.199 (DHCP)
Network Mask:	255.255.255.0 (DHCP)
Gateway:	N/A (DHCP)

Below the form fields is a 'Submit' button and a note: 'Note: Remove (DHCP) from ip addresses text box before disabling dhcp'. At the bottom of the page, a footer reads: 'All pages on this site © 2011 Innovative Energies'.

Fig 23 – Network Settings

The factory default setting is DHCP enabled. To disable DHCP (**Allocating a static Ip address**) follow the steps below:

- (a) Set DHCP Client to **'Disable'**
- (b) Type in the desired **IP address** eg.192.168.100.51
- (c) Remove **'DHCP'** and all preceding spaces from the **Network Mask** and **Gateway** fields

- (d) Click on the 'Submit' button

To enable DHCP if your device has a static IP address:

- (a) Set DHCP Client to **'Enable'**
- (b) Leave all other fields blank
- (c) Click on the 'Submit' button

7.2.5 PSU Configuration

This page displays the parameters programmed into the firmware of the power supply. These parameters are programmed in the factory and are not able to be changed by the user.

The screenshot shows the 'PSU Configuration' page for the SR250i12T model. The page features the Innovative Energies logo at the top left. A navigation menu on the left includes: Monitoring & Control, Network Settings, **PSU Configuration**, SNMP Configuration, Syslog Configuration, Firmware Upgrade, and Contact Details. The main content area displays a table of parameters:

BatDetect:	60
Vpres:	12.2
Vbatl:	11.0
Vshutd:	11.5
Vdisco:	10.0
Bccl:	100
BCTim:	20
CC Mins:	40
CC Hrs:	23
CC Days:	27
MfIBCT:	60
Serial Number:	0025
PSU Version:	IEL NB5sys.V13

At the bottom of the page, a copyright notice reads: 'All pages on this site © 2011 Innovative Energies'.

Fig 24 – PSU Configuration page [16]

The basic model number of the power supply unit is shown below the 'PSU Configuration' heading. In the screenshot above you can see that it is displayed as SR250i12T.

Understanding PSU Configuration Terms

BatDetect:	Time between battery detections (minutes) [23]
Vpres:	Displays the threshold of Voltage for battery detection and BCT [23] During this process, if the voltage drops the test is aborted and it displays the BAT LOW alarm [23]
Vshut:	Displays Output Voltage of the power supply during battery detection and battery condition tests [23]
Vbatl:	Displays BAT LOW alarm voltage levels during mains fail [23]
Vdisco:	Displays the Voltage at which the load is disconnected from the battery during mains fail [23]
Bccl:	Displays the Battery Charge Current Limits as percentage of the rated power supply current [23]
BCTim:	Displays the total length of BCT in minutes [23]
CC Mins:	Displays the set time intervals between the automatically scheduled BCTs in minutes [23]

CC Hrs: Displays the set time intervals between the automatically scheduled BCTs in hours [23]

CC Days: Displays the set time intervals between the automatically scheduled BCTs in days [23]

Note: The total time interval between BCTs is the accumulation of the above three settings [23]

MFIBCT: Displays in minutes the time before the mains fail check, during the BCT [23]

TL: Displays the Lowest temperature recorded [23]

TH: Displays the Highest temperature recorded [23]

Serial Number: Displays the Serial Number of the power supply [23]

PSU version: Displays the power supply version number [23]

7.2.6 SNMP Configuration

All fields are customisable and may be specified by the user to suit their specific applications.

SNMP traps (alerts) can be monitored using a SNMP manager of the user's choice.

The user may select which traps are set by changing the 'alarm trap mask code' which is accessed by using a MIB Browser such as 'iReasoning MIB Browser'.

The default code for the 'alarm trap mask' is set at 1048187. A new code may be calculated by using the excel spreadsheet available at <http://www.innovative.co.nz/service/SNMP>, by

clicking on 'ALARM MASK CALCULATOR'. Simply insert '1' into the required yellow column to enable a trap or insert '0' into the required yellow column to disable a trap.

MIB files are available by going to www.innovative.co.nz and clicking on 'Communication Enabled DC' on the side menu bar.

Alarm traps may be resent if a fault continues to persist. The 'resend time' can be set by modifying the SNMP variable 'TrapPeriodicResendTimeInMinutes'. The 'resend time' range for resending traps is between 30minutes and 10079 minutes (7 days). If the user sets the range outside of these parameters, it will default to 1440 (24hours) which is also the factory default for a new device.

Note: The new settings only take effect after performing a 'soft reboot' of the power supply web server.

SNMP Configuration
SR100i12T

- Monitoring & Control
- Network Settings
- PSU Configuration
- **SNMP Configuration**
- Syslog Configuration
- Firmware Upgrade
- Contact Details

SNMP Trap:

Read/Write Community:

System Contact:

System Name:

System Description:

System Location:

Trap Destination IP:

SNMP Trap Port:

SNMP Agent Port:

Fig 25 – SNMP Configuration [16]

Understanding SNMP Configuration Terms:

SNMP Trap:	An alert message that the user can enable or disable.
Read/Write Community:	Identifies groups and their set permission rights. The default setting for this is 'iepublic'
System Contact:	This is user specified and able to display names, phone numbers or email addresses
System Name:	This area is user specified
System Description:	This area is user specified
System Location:	This area is user specified
Trap Destination IP:	Identifies where the alert message is to be sent. The user specifies the IP Address of the PC they want the SNMP traps (alerts) sent to
SNMP Trap Port:	Displays the port number of the SNMP trap (default is 162)
SNMP Agent Port:	Displays the port number of the SNMP agent (default is 161)

7.2.7 SYSLOG Configuration

The Syslog is used for recording SNMP syslog messages.

The screenshot shows the 'SYSLOG Configuration' page for device 'SR250i12T'. On the left is a navigation menu with items: Monitoring & Control, Network Settings, PSU Configuration, SNMP Configuration, Syslog Configuration (highlighted), Firmware Upgrade, and Contact Details. The main configuration area includes: 'SYSLOG:' with a dropdown menu set to 'ENABLED'; 'SYSLOG Server IP:' with a text input field containing '192.168.101.252'; 'SYSLOG Port:' with a text input field containing '514'; and a 'SYSLOG Update' button. At the bottom, a footer reads 'All pages on this site © 2011 Innovative Energies'.

Fig 26 – SYSLOG Configuration page [16]

Understanding Syslog Configuration Terms:

Syslog: The syslog can be enabled or disabled

Syslog Server IP: This displays the user specified IP address that is used for monitoring the Syslog data

Syslog Port: This displays the port number of the PC setup to monitor the Syslog (default is 514)

SYSLOG Update: This function refreshes all of the user specified data above

7.2.8 Firmware Upgrade

Firmware Upgrade
SR250i12T

- Monitoring & Control
- Network Settings
- PSU Configuration
- SNMP Configuration
- Syslog Configuration
- **Firmware Upgrade**
- Contact Details

Current LAN firmware version: RWC_a1

Enter LAN firmware filename:

Change Password

New Password:

New Password: (Confirm)

All pages on this site © 2011 Innovative Energies

Fig 27 – Firmware Upgrade page [16]

This page is used to update the software to the latest version. This is done by using a standard FTP programme such as the Filezilla Client available at: www.filezilla-project.org.

The upgrade file is always named 'firmware.img' and needs to be transferred to the **/mnt/flash** folder in the web server built into the power supply.

Note: After completing the firmware upgrade the power supply will automatically reboot and you will need to log-in again.

7.2.9 Change Password

The default password is **iepassW1** and may be updated by the user. Please contact Innovative Energies to obtain the procedure for recovering lost or forgotten passwords. [16]

7.3 Conclusion

This chapter has discussed the results of the web enabled power supply. This is denoted through the display of real-time data on the web pages. The approach made for the devices to be web enabled was through the help of the various softwares. Each software was then combined in order to output the real time data on the web pages.

Each page displays different parameters of the power supply. The monitoring page contains the parameters that require monitoring through the web, such as battery voltage, current, status etc. These are the most important parameters that denote the priority of the fault in the device.

Similarly, other pages such as communications page and SNMP page display their required parameters. The firmware page is very useful for the consumer as it gives an option to upgrade to the updated version of the web pages via the web. This eliminates the need for an IT Technician to go onsite and upgrade the system for consumers.

The change password option makes the web enabled power supply a secure link for the consumer. This protects their devices to be secured via internet scam.

Web enabling an embedded device is only successful when the results show the real-time data on the web. In this case, it has been successfully displaying the required data.

Chapter 8

Conclusion and Future Study

This chapter goes through the work done in completion of this project including the research. It draws conclusions from the finding of the study and finally discusses about the future development for SNMP.

In the context of web enabling embedded devices, a number of studies have been carried out. There are several projects which compare the security, technology and the design for SNMP. An overview has been provided, investigating some related studies along with some of the web enabled SNMP features.

Web-based Management is one of the trends of network management. Manufacturers are promoted by the surge of web to “web-enable” the configuration and management of products, while SNMP is nowadays the key enabling technology. It is mainly characterized by layered architecture and common data representation. The layered architecture separates embedded code from the interface, ensuring that interface design changes will never impact the underlying embedded code.

Most of the time was spent on selecting the right device for this project which supported the SNMP technology and other specifications. After all the considerations, Lantronix Xport Pro device was chosen for this project because of its compatibility with the SNMP technology. Lantronix Xport pro has a built in web server which can load upto 6 webpages.

The firmware upgrade feature provides user to upgrade the features without reengineering or recompiling any code. The generic data format and access method make it possible for

various management interface - SNMP, web, Telnet, and others - to uniformly access MIB modules and their associated **MIB** objects. In addition, the Web Keywords flexibly link the dynamic data on the embedded device with the HTML pages that constitute the web-based user interface.

The SNMP technology helps clients to monitor and control their power supplies on a site or remotely through a web interface. Real-time data is executed and displayed on the web pages, which helps in constant monitoring of the device. SNMP is currently available on the “T” series and the “V” series of Innovative Energies power supplies.

This project involved research, designing and developing the SNMP feature. Two other contractors were hired to work through developing the SNMP feature in the power supplies. Team work was a key point which helped in completion of this project.

With the tremendous development of network, it is important more and more to administer network efficiently, which calls for effective way to access the network elements. Therefore, the products with flexible and various access methods are required to remain competitive. Moreover, it is feasible. At the present time, the study work is still in progress.

In the beginning of the project it was very difficult to decide, where to start project from. After moving along with the project, the time used for analyzing the product was very long. Most of the time was consumed in getting the team together and working on the same time for this project. The Lantronix Pro device took extremely long to arrive, because of that we were unable to spend more time on practical part of the project.

Loading and testing the power supplies were the major factors that took a reasonable amount of time as one mistake would erase the Xport Pro device MAC address. A manual reset was then required to re-use the Xport Pro web server.

An Xport Pro software was new to us and had different user interface from the software we used which we used earlier, and so understanding of new software took us longer than expected. Making of communication gateway took us very long than expected.

Future Work

In future, this project can be extended in order to make the most developed product.

Due to the lack of time, it was essential for me to complete and deliver the final product by the due date to the client. Because of this reason, we only implemented the basic SNMP v1 into the power supplies. In future, the plan is to implement SNMP feature into all the versions of power supply including the higher versions of SNMP.

For future preference, security can be enhanced by using a mini web-server with POST method rather than GET commands. Also, SMTP feature can be introduced so that the users can be alerted through emails.

This project can be taken to a higher level by introducing a more advanced GUI for the web pages. They also like to increase the security by creating a secure database for all their clients.

References

- [1] M. Can Filibeli, Oznur Ozkasap, M. Reha Civanlar “Embedded web server-based home appliance networks” Department of Computer Engineering, Koc University, Rumeli Feneri Yolu, Sariyer 34450, Istanbul, Turkey, 18 July 2005, pp 52 – 60.
- [2] Lantronix. (2013). Lantronix eDevices [online]. Available: <http://www.lantronix.com>
- [3] Sergio Scaglia *et al* “Enabling Embedded Systems to access Internet Resources” TCP/IP Basics, implementation and applications.2007, pp 63-66.
- [4] Network World. (1994). Network Management Research Center [online]. Available:<http://www.networkworld.com/topics/network-management.html>
- [5] Faqs.org (1990). RFC 1161 – SNMP over OSI [online]. Available:<http://www.faqs.org/rfcs/rfc1161.html>
- [6] Marshall DenHartog “The Fast Track Introduction to SNMP Alarm Monitoring” dps Telecom, USA, 2010, chp 1, pp18-27.
- [7] Mehdi Khosrow-Pour, D.B.A . An Overview of Web-Enabled Technologies Assessment and Management: Critical Issues. Available:http://users.dec.uwi.edu/smarshall/encyclopedia/sample_manuscript.pdf
- [8] Harbor Research. (2010-2014). M2M & Smart Systems. [online]. Available:http://www.windriver.com/m2m/edk/Harbor_Research-M2M_and_Smart_Sys_Report.pdf
- [8] Barranca Parkway “Enabling business Intellegince with M2M”, an introduction to device networking. Lantronix, Inc.15353, 2011.
- [9] Sandu, Florin & Iolu, Daniel, serial tunnelling concept “Embedded web-servers for remote control in Domotics”, 2007.
- [10] B. Kainka. “A universal measurement interface (in dutch)”. (434): chp 5, sec:X2–X6, December 1999.
- [11] Dr. J.J. Lukkien, (2005). Internet-based Monitoring and Control of Embedded Systems. [online]. Available:<http://www.win.tue.nl/~mtjiong/EES5413/>
- [12] Samir Bonho, Valderrama, Carlos, “Embedded-oriented system for real-time tracking and sensing in multimodal transportation”, 2005.
- [13] Junseok Lee, Kisong Yoon “Design of a System to Support Security Communication between a Web Proxy and a CGI Program Based on PKI” 2009.Computer and Software Technology Laboratory; Electronic & Telecommunication Research Institute, Korea, 2009, pp305-310.
- [14] ZhenXing, Wang & Yi Xian, Ren; “CGI Programming with HTTP interface”, 2008.
- [15] Lantronix Xport Pro, “XPort Pro™ Integration Guide”, 2006.

- [16] Communication Enabled UPS & DC power supplies. SNMP Manual [online].
Available: http://innovative.co.nz/uploads/pdf/SNMP_i_usermanual.pdf
- [17] Haslem, Stuart; "Network connectivity for Embedded systems", 2003.
- [18] Tan, Tzeming & Jeremy; "Embedded ATMEL HTTP Server" May 2004.
- [19] Available: <http://genderitencyclopedia.ist.psu.edu/samplemanuscript.doc>
- [20] Research trends on Embedded devices, "The Royal Institute of Technology on 2013-04-02".
- [21] Lantronix Xport Pro Manual 2004; [online]. Available: http://www.hy-line.de/fileadmin/hy-line/computer/connectivity/lantronix/dokumente/XPort-Pro_IG.pdf.
- [22] Lantronix, July 2004; "Web enabling your device server" Lantronix Manual [online]. Available:
http://www.endurance-rc.com/media/Creating_Custom_Web_Pages.pdf.
- [23] Innovative Energies; "SNMP Manual" 2011; [online].
Available: <http://www.innovative.co.nz/pdf/SR250i.pdf>

