Remote Residential Control System

Ming-Shuang Lang

KTH Microelectronics
and Information Technology

Master of Science Thesis
Stockholm, Sweden 2004

IMIT/LCN 2004-03

Remote Residential Control System

M. Sc. Thesis Report

Ming-Shuang Lang

(lms@kth.se)

Department of Microelectronics and Information Technology

Royal Institute of Technology

Stockholm, March 2004

Academic Supervisor and Examiner:

Professor Gerald Q. Maguire Jr.

Department of Microelectronics

and Information Technology

Royal Institute of Technology, Sweden

Industrial Supervisors:

Erik Wallin

SiceIT AB, Stockholm, Sweden

Björn Thelin

Ecton AB, Stockholm, Sweden

Abstract

A remote residential control system enables home users to remotely manage devices at their homes. These devices may include energy management, security surveillance, household appliances, consumer electronics, etc. This system involves technologies in home automation, home networking, and interfacing a home network with external networks. However, lacking a single standard poses a big challenge to the design of such a system. This thesis proposed three methods of turning an IP Set-Top Box into a remote residential control platform. Additionally, future trends are discussed. Various technologies in the fields mentioned above are also examined.

Sammanfattning

Ett system för fjärrstyrning av intelligenta hem (remote residential control system) är ett system som möjliggör för hemanvändare att på distans övervaka och styra utrustning i hemmet. Denna utrustning kan vara energiövervakning, säkerhetsutrustning, hushållsapparater, konsumentelektronik, etc. Det saknas dock en gemensam standard, vilket gör det till en stor utmaning att konstruera ett sådant system. I detta examensarbete föreslås tre sätt att göra en set-top box till en plattform för fjärrstyrning av intelligenta hem. Framtida trender diskuteras också. Olika tekniker inom nämnda områden undersöks

Acknowledgement

This work has been performed as a degree project at Ecton AB during the period October 2003 – March 2004. I would like to express my sincere thanks to:

Prof. Gerald Q. Maguire Jr., my supervisor at KTH, for his guidance, unbelievably rapid responses, his suggestions, and genuine kindness.

Erik Wallin, my supervisor at SiceIT AB, for helping me to understand this project, to make decisions, and his patience during the project.

Ecton AB, especially Johan Ohlsson for giving me the opportunity to perform my thesis project; Björn Thelin and Robert Sahlin for their support and helpfulness.

I also want to thank my friends for their friendship and ideas.

A special thank to my parents and brother, who gave me the opportunity of coming and studying here in Stockholm, and always supporting my decisions.

Table of Contents

1 – Introduction

It has always been a dream of human beings to have an intelligent home and have total control of it from anywhere at anytime. Think that while you are at your office, you get a message saying someone is at your door. You use your computer to instruct the door camera of your house to show an image, it turns out to be a postman delivering a package to you. You then open the front door so that the postman can leave your package inside. Meanwhile you can see that it is only a delivery! For another example, you are driving home after work, as you approach your home, you use your mobile phone to connect to your home network, turn on the light in the hall and adjust the air conditioning to a comfortable temperature. These might sound like a movie, but people have been working on implementing these as products for years!

Conventionally, personal computing devices and consumer electronics were separate categories. With the development of home networking technologies, these two categories began to converge. The growth of Internet content and advances in broadband technologies has resulted in increasing demand for broadband access by consumers. The explosion of portable devices makes consumers' expect to access information from anywhere more than ever before. All these phenomena also stimulate manufacturers and content providers to deliver more services to home consumers. A remote residential control system is part of a larger system attempting to meet these requirements.

Remote residential control involves communication between a home network and an external network, generally the Internet. The major hindrance to the achievement of this is that there are too many standards for home networks and external networks. Because many manufacturers have developed proprietary products, interoperability is a big problem. This has resulted in higher costs and has limited the growth of this market.

This thesis discusses the various technologies and standards involved in a remote residential control system. Usually, each device comes with its own controller, and these controllers do not interoperate with each other. Quite often control is limited to within a home. In this project, an IP based Set-Top Box (STB) is envisioned as a common 'controller' in a home network, which will collect information from those devices being controlled, and it will extend the home network to the Internet, so that remote control can be via the web, a mobile, or a Personal Digital Assistant (PDA) from anywhere and at anytime.

This report discusses general considerations and technologies involved in a remote control system. Developments in home networking, home automation, and remote residential control are also introduced. The STB and its advantages as a control platform for home are also

discussed. Several possible ways of turning a STB into remote residential control platform are proposed. Finally, future trends in home networking that may ease the task of remote residential control are described and future work is suggested.

2 – Background

A remote residential control system can bring a great number of benefits to consumer electronics manufacturers, service providers, network operators, and home users. Manufacturers can deliver new 'intelligent' devices to be attached to the system. Service providers can concentrate on developing value-added services. The system will need 'always on' network support, so Internet Service Providers (ISP) have a new type of traffic and possibly new revenue from it. Home users will benefit of course, the most from it. It will bring them ease-of-mind, besides residential amenities and cost savings.

A scenario of using such a system might be: you are away on vacation, you hear on the news about freezing weather at home and you are not sure if your home is in good condition (i.e., if a pipe has frozen and is now leaking water). You can open a web browser on your PC or PDA, and log into your home control system. You can then access to the surveillance system in your house. You angle the cameras in your house to inspect wherever you want. At night, you can turn on lights in some rooms to scare away burglars. You can adjust the air-conditioning according to the weather to save energy while keeping your plants healthy. The system can also be configured to send you an alert if a specific event occurs, such as fire alert, leakage alert, an appliance malfunction alert, etc., so that you can take appropriate measures.

Although such a system is desirable, it's complicated to design. Some of the reasons have been mentioned in the Introduction (Section 1). Such a system presents some unique requirements because it targets home users and requires facilitating communications between home and external networks. Some of these requirements are:

Easy — It should be easy to install and easy to use. Devices to be controlled are placed in a home, where professionals are not usually found. These devices should begin to work without (much) effort. It would be desirable to have them be simply 'plug-and-play'. Intensive configuration and maintenance should only be done by service providers. Easy to use is also important, and that's why most systems now provide a web based User Interface (UI).

Low cost — Cost is always an important element when considering the residential market. This is also a reason why so many home networking technologies are developing in parallel with industrial technologies. For

instance, LonWork[1] is a suitable technology for the enterprise, but it is a little too expensive for home users. In contrast with LonWork, X10[2] products are less capable, but they are widely accepted in homes because of their affordable low cost, since cost is a deciding element. Previous investments should be protected too. Many remote residential control systems today require replacing devices in the home. However, most people are usually reluctant to do so. Such new investments should be future proof, i.e., it should accommodate new mainstream standards in home automation/electronics.

Interoperable — Users should be able to choose different devices from different vendors. These devices should be easily attached to the control system and work seamlessly. Users should enjoy the flexibility of choosing a product from among several vendors.

Secure — Since such a system may expose private information to insecure public networks, proper mutual authentication, encryption, and other security measures are required.

Experts have been trying to resolve these problems for some time. To properly address these requirements, home networking, home automation, and remote control methods, all elements must be considered. Different technologies were developed, each optimized for different goals. For example, in home networking, UPnP[3] aims to facilitate a PC centered IP network, HAVi[4] is intended for Audio/Video electronics, and Jini[5] leverages Java. The diverse character of technologies and products are advantageous when building separate systems, but it's disadvantageous when systems should converge. Various international organizations have paid attention to this problem, and have been working to come up with a single open standard for home network area.

However, standardization is a long process. Parts of some standards have been approved, but before the complete standards come out and are widely adopted and tested, it's vital for a manufacturer to choose a proper and promising standard and commit to it. To cope with the current and future market, the technologies used should be able to be easily adjusted to be compatible with others. This is a major challenge facing manufacturers.

Ecton AB is currently an IP STB vendor. It plans to equip these STBs with more advanced functions, to act as a remote control platform in a home network. Thus, a STB needs to

[1] LonWork (Local Operation Networks) technology is a solution for control networks developed by Echelon Corporation. It provides a peer-to-peer communication protocol LonTalk. See <http://www.echelon.com>.
[2] X10 is a protocol using a power line to transmit control commands. See Section 4.2.7.
[3] UPnP represents Universal Plug-and-Play. A home networking technology. See Section 4.2.1.
[4] HAVi represents Home Audio/Video interoperability. It is an open standard for intelligent audio and video devices to interoperate with each other regardless of manufacturer, OS, CPU or programming language used for implementation. See Section 4.2.3.
[5] Jini is a Java technology that provides a simple infrastructure for interactions between network services. See Section 4.2.2.

communicate with both external and internal networks, and most often must act as a translator between the two. As a component in the home network, the STB should meet the requirements for home network devices. As it will control many home automation devices, it should include support for as many of these products as possible. As a focal point for remote residential control, it should integrate closely with the whole remote control system. Since it's a high end STB, it should also meet the special requirements for products of this kind. Possible ways of turning an IP STB into a remote control platform were examined in this thesis project.

3 – Technical Overview

In a network, separate devices are interconnected, which raises a lot more considerations than when they work alone. For example, addressing, service discovery, service access, network management, etc., all need to be constructed and cooperate seamlessly. Some general considerations and solutions for a remote control system are discussed in this section.

3.1 – Address Allocation

Upon connection to a network, a device should be assigned a unique address for communicating with other devices in the network. This address can be assigned manually or automatically. To ease the task of home users, this should be done automatically. Different technologies have different addressing methods. For an IP home environment, there are two major ways for allocating addresses automatically.

(1) Dynamic Host Configuration Protocol (DHCP)

DHCP is an Internet protocol for automating the configuration of computers that use TCP/IP. It can automatically assign IP addresses and deliver TCP/IP configuration parameters (such as the subnet mask and default router) and provide other configuration information (such as the addresses for printer, time and news servers) [1].

DHCP works in a client-server pattern. It consists of two components: a mechanism for allocation of network addresses to hosts and a protocol for delivering host-specific configuration parameters from a server to a host. For the later, the client sends a message to request configuration parameters and the server responds with a message carrying the desired parameters.

This DHCP server can be in a Firewall or Network Address Translation (NAT) device in the home network. A STB can easily be used for this purpose, since it frequently has all the functions of a generic PC. Servers such like DHCP could be enabled before they are delivered to a home user. A device with DHCP client software can then get an address automatically.

(2) Zero Configuration Networking (Zeroconf)
If devices are connected to the same physical (or logical) link, Zeroconf [2] can be used to assign link-local addresses automatically. Zeroconf is intended for use in small wired or wireless local-area networks. It offers a solution in which address configuration is managed by individual devices when they are connected to a network. A device will first try to find a DHCP server, if not successful, the device will randomly choose an IP address from the range 169.254.1.0 – 169.254.254.255. Then the device sends messages to other devices already connected to the network, asking whether this address is already used. If no reply is received within a reasonable period, the device starts using this IP address.

Besides address auto-configuration, Zeroconf also provides name-to-address translation (Domain Naming Service – DNS), service discovery (Service Location Protocol - SLP), and multicast address allocation [3].

Using IPv6 compatible devices can also solve automatic address allocation easily since IPv6 inherently offers auto-configuration. IPv6 provides bigger address space (128 bits), support for mobile devices (Mobile IP), and has build-in security (IPSec). In IPv6, the address of a device is derived from the Media Access Control (MAC) address of the underlying network interface and a network address prefix. With a globally unique IPv6 address, a device can be accessed anywhere. So remote control will be easier. However, full migration to IPv6 is still a long way off.

3.2 – Service Discovery

The next step to achieve remote control is to find the intended services. There are various kinds of solutions to both advertising and locating services. They are usually designed to facilitate a specific type of networking environment. This section introduces some popular protocols for service discovery.

3.2.1 – Service Location Protocol (SLP)

The Internet Engineering Task Force (IETF) has standardized two mechanisms for service discovery over IP networks. One of them is SLP (see SLPv2 RFC2608 [4]).

SLP provides service discovery both based on service type and attribute, so a client can find a specific service by specifying required characteristics. SLP allows networking applications to discover the existence, location, and configuration of networked services in enterprise networks. Thus a user does not need to know the host name where a service resides. The user only needs to know the description (service name and attributes) of the service. Because SLP binds a service description to the network address of the host, SLP is then able to return the Uniform Resource Locater (URL) of the desired service. However, it was designed primarily for a local area network. Although SLP can be configured to use 'scopes' and Directory Agents so that it can scale well in very large networks.

Components:

User Agent (UA)	A process working on the user's behalf to establish contact with a useful service.
Service Agent (SA)	A process working on the behalf of one or more services to advertise the services.
Directory Agent (DA)	Collects and caches service advertisements from SAs.

The basic operation in SLP is that a client attempts to discover the location of a service. In smaller installations, each service will be configured to respond individually to each client. In larger installations, services will register their services with one or more DAs, and clients will contact the DA to fulfill requests for service location information. Clients may discover the whereabouts of a DA by pre-configuration, DHCP, or by issuing queries to the well-known DA discovery multicast address.

3.2.2 – DNS Service (SRV)

The other IETF service discovery mechanism is the DNS SRV [5] Resource Record (RR), which allows clients to look up services via DNS. This RR specifies the location of the server for a specific protocol and domain. It allows moving services from host to host. Clients specify the type of service, the transport protocol, and the domain name to look up. The reply to this query supplies a list of hosts that match the request.

3.2.3 – Salutation

Salutation [6] is a solution for service discovery and utilization especially for wireless environments. It provides a mechanism to describe the capabilities of an application, service, or device. It also allows searching for all products within a class or a product with a specific set of capabilities. The Salutation architecture provides mechanisms to determine if what you want to find is available and how to set up inter-operable sessions with it.

Salutation is designed as middleware isolating the developer from the specifics of the network protocol and the capabilities-matching function necessary to perform discovery. It is specified as a reference implementation called the Salutation Manager. This process manages the resources for the upper levels, performing the discovery functions and brokering interactions with other networked entities.

Components:

Salutation Manager	It manages Functional Units.
Service Functional unit	It provides some form of service to others on the network. It registers itself with the local Salutation Manager by defining its capabilities there.
Client Functional Unit	It uses the services of others on the network. It makes a request to the local Salutation Manager to search for the Service Functional Units it needs. The Client Salutation Manager communicates with other Salutation Managers to locate the desired service and report back to the Client Functional Unit.

Advantages:

- Interoperates with SLPv2, so it can support both peer-to-peer and directory-centric configurations. The Salutation Manager searches for SLPv2 directory agents through multicast, broadcast, or manual configuration. If it finds any, the Salutation Manager will use the SLP protocol instead of Salutation Manager Protocol to register and deregister Functional Units with the SLP directory. Furthermore, the Salutation Manager will use SLP to search for services requested by client applications.
- Designed for heterogeneous networks. Unlike Jini and UPnP which are targeted only for IP networks.
- Non-proprietary solution.
- Language neutral. Unlike Jini that only uses Java.

Salutation cooperates closely with other technologies. For example, the salutation architecture APIs can be mapped to Bluetooth's service discovery layer.

The Salutation API and Salutation Manager provide a single application interface to three protocols: Salutation, SLP, and Lightweight Directory Access Protocol (LDAP [7]). They are complementary with Salutation and each provides a single API.

3.3 – Network Management

Management is very important to keep a network healthy. The best-known management protocol is Simple Network Management Protocol (SNMP) [8]. Nearly all network devices

use SNMP. It is a set of IETF standards (RFC 3414-3416, for version 3). The need for administrative tools for TCP/IP networks, particularly for the Internet made these protocols come into being. Now with them, we can get information about TCP/IP and also other protocols like IPX/SPX and AppleTalk. SNMP standards define a framework including useful information (such as interface configuration type and operational status), how to present this information (Protocol Data Units – PDU, use ASN.1 – Abstract Syntax Notation 1 – to describe the data types), how to address them (global name tree architecture), and how to get or change values (SNMP protocol).

SNMP has three versions. SNMPv1 defined the structure and identification of management information for TCP/IP-based Internets, Management Information Base (MIB) for network management of TCP/IP-based Internets, and a simple Network Management Protocol. SNMPv2 adds security and authentication lacking in version1, but was criticized for adding complexity to it and being incompatible with version1. SNMPv3 adds more security and administration capabilities based on both versions 1 and 2.

SNMP consists of three components: management station (manager – management software), managed entity (agent – agent software module), and MIB (resources and activities. SNMP uses User Data Protocol (UDP) to carry messages). This standard management model enables a manager to examine agent data and update configuration and status information.

Problems with SNMPv1:

- If one of a list of requested variables fails, the whole get-request will fail.
- No effective authentication of the message source, messages are not confidential, and there is no access control.
- Traps have a different format from other PDUs, which adds complexity.

SNMPv2 solves the problems in version 1, yet introduced many changes of PDU format. It adds bulk transfer. It supports the use of authentication (Digest Authentication) protocols, encryption (Data Encryption Standard – DES), but the security features it adds are not very strong. Usually, it is used for network monitoring, but not for network control.

SNMPv3 further enhances administration and security features. In this version, encryption without authentication is not allowed. For authentication, it uses Hash Message Authentication Codes (HMAC), which is an authentication mechanism based on a secret key. For privacy, it uses DES and Cipher Block Chaining (CBC) modes. For access control, it adopts View-based Access Control Model (VACM). Authentication is done for each user while access control done based on a group.

SNMP provide a mechanism for monitoring. In this protocol, a monitor (a device) listens to all traffic on a Local Area Network (LAN) or on a wide area link, gathering statistics, and

capturing traffic that matches some specific criteria. The Remote Monitoring (RMON) MIB contains the tools needed by a network management station to configure and control a monitor. A control table configures information to be monitored.

Advantages of SNMP:

- Simple – Easy to implement and does not stress the network.
- Popular – Almost all major vendors of network products support SNMP.
- Expandable – Can be updated to the users needs.

Disadvantages of SNMP:

- Three versions coexist, which can cause compatible problems.
- The simplicity of SNMP sometimes is inefficient.
- In the manager/agent model of SNMP, messages are usually sent from a manager (only the trap message is initiated by an agent). This may cause inefficient management, as a manager needs to keep track of the status of a network.

3.4 – Remote Control Protocols

The devices in the network contain information about themselves (such as parameters and statistics). This information can help when managing these devices. To control these devices, the drivers of these devices should allow read/set values and receive/send of events. For centralized control, a common Application Programming Interface (API) to different devices will be needed. A software management system may be used to achieve this, since it's usually built to be able to inter-operate with other software and has a centralized server. There are also other methods specially developed for remote control. This section introduces some of these methods.

3.4.1 – Simple Device Control Protocol (SDCP)

SDCP [9] is a lightweight protocol for the exchange of information between two devices. It works in a client-server style. It is an eXtended Mark-up Language (XML) based protocol that encapsulates device information and modifiable data into a compact format. SDCP can potentially be used in conjunction with many transport mechanisms. The motivation behind SDCP is the desire for a universal client application on a hand-held or portable device to connect to a server contained in an embedded system.

An SDCP transaction between two devices can be thought of as having two types of interaction: negotiation and modification. During negotiation, the client knows nothing of the server. During modification, the client already knows the existence of the server and makes changes to its configuration. In both types, the server assumes no knowledge of the client.

Negotiation allows the client and server to 'chat' harmlessly without the client making any configuration changes to the server. It is during this type of interaction that the client learns about the server's current configuration and presents the information to the user.

Negotiation begins when the client attempts to initiate an SDCP transaction. Using the appropriate hardware protocol layer, the SDCP client polls for SDCP servers. Once connected, the SDCP client sends the first inquiry to the server, and the server returns a list of available SDCP devices and their data items. At any time during the connection, the SDCP client may send more inquiries to the server to check for changes. When the hardware connection layer is interrupted or terminated, or the SDCP transaction is complete, both devices should return to their normal state. To avoid potential conflicts, SDCP clients refresh information from the server frequently to maintain consistency.

Modification allows the client to make changes to the server's configuration. Client messages now assume prior knowledge about the server, what variables are named, what types they are, etc. This level of interaction should not take place unless some negotiation has taken place earlier.

All SDCP messages are encoded using American Standard Code for Information Interchange (ASCII) in XML, and encapsulated within an SDCP markup block.

3.4.2 – Remote Device Control (RDC)

RDC is an International Telecommunication Union (ITU) T standard specified in H.282 [10]. It is designed for multimedia conferencing devices. Services that RDC provides are categorized as follows:

- To obtain attributes of devices (DeviceAttribute: control attributes and event attributes).
- To inquire of the status of a specific remote device (DeviceStatus).
- Device control (DeviceControl).
- To be notified of event changes occurring on a remote device (DeviceEvent).
- Source selection service, which allows a node to request that a particular source to be connected to a specific output stream (DeviceSource).

It works like this:

(1) On a controlling node.

RDC application issues a control request primitive to the service provider. Upon receiving the request, the service provider will check the correctness of the request. If correct, a PDU will be sent to the controlled node.

(2) On the controlled node.

After the service provider receives and verifies the request PDU from the controlling node, it will send the request as an indication locally to the user application. The user application handles it, composes a response, and sends it back to its service provider. The service provider then formats the response into a PDU and sends it to the node where the request originated.

(3) On the controlling node.

The service provider receives the PDU and forwards it to the user application as a request confirmation.

Standard device classes in H.282 include camera, microphone, streaming player recorder, slide projector, light source, and source combiner.

3.4.3 – Microsoft's Simple Control Protocol (SCP)

SCP [11] is a non-IP based home networking protocol enabling peer-to-peer communications. Power Line Communications (PLC) is used as the physical layer. It is a complementary technology to UPnP. It targets a class of devices with limited processing resource, low bandwidth requirements, and a relatively low price. It will be further explained in Section 4.2.1.

3.5 – Network Security

To access a device and get its status or change its activities, proper security mechanism should be devised. Some security challenges in a residential control system include:

(1) For a remote residential system to work, the connection between the home network and Internet should be always up, which makes the home network more vulnerable. Without a proper security mechanism, a remote residential control system can give an intruder access.

(2) For those networks that use a power line, because this power line might be shared with neighboring houses, commands on one network might appear in the neighbors' house!

(3) Wireless connections introduce new security issues. An intruder no longer needs access to physical media, which makes eavesdropping, data tempering, etc. easier.

(4) Highly heterogeneous network architectures and applications require different levels of security.

For an outsider to attack a home network successfully, the attacker must find and connect to a vulnerable server process on the home system. A Firewall or a NAT router may effectively block these kinds of attacks.

(1) Firewall

A firewall enforces an access control policy between two networks. A firewall typically takes one of two forms:

- Software firewall. Specialized software running on an individual computer.
- Hardware firewall. A dedicated device designed to protect devices on a network.

Both inbound and outbound access can be protected.

(2) NAT

A NAT provides a way to hide the IP addresses of a private network from the Internet while still allowing computers on that network to access the Internet. It is often used for masquerading. This way, different devices on a LAN can appear to the outside world as having a single IP address. Most network firewalls support this function of NAT.

Corporate and government networks are typically protected by many layers of security, which range from network firewalls to encryption. In addition, they usually have a support team that maintains the security and availability of these network connections. But these methods are not applicable to a home network, thus protecting a home network brings greater challenges.

In a remote residential control context, the home network will be connected to the Internet, which introduces more potential attack paths. Authentication and authorization must be done before a controller and a service perform further actions.

(1) Authentication

Authentication is a process for validating an identity. From the view of object being authenticated, it can be subdivided into:

(a) User authentication. Check if a user is whom he claims. Three means to verify a user's identity:

- What a user knows, for example a password.
- What a user possess, for example a smart card.
- Properties of a user, for example fingerprint.

This authentication should be bi-directional, especially in a wireless network where rogue user/server can access more easily than in a wired network.

(b) Data authentication. Checks that data is from an authorized sender and no alteration occurred during transmission. Various cryptographic solutions can be used; Symmetric/asymmetric encryptions and digital signature are common methods.

(2) Authorization

After authentication, the authorization process will grant a user/device rights to access or manipulate a service. There are three predominant ways to do authorization:

Access Control List (ACL)	A file residing on a device that provides a certain service, contains a list of user name and rights associated with the user, or maybe other data.
Authorization server	This provides a central point for authorization. If an ACL file becomes too big, this method can relieve the burden on those devices providing a service. It's a solution for relatively large networks, like enterprise range, but is not suitable for home network.
Authorization Certificate	A certificate is issued to those who can control a service. The certificate states the rights granted. In this scenario, servers issuing certificates are required. But these certificate servers should also be authenticated before a device accepting a certificate from them. In this case an ACL on a device is also needed to grant control to a certificate server.

There are myriads of solutions to authentication/authorization for the remote residential control. Some protocols have defined the security mechanisms inherently. Some examples of solutions are listed below.

(1) SNMPv3

Since SNMPv3 adds administration and security features, a software management system compliant with it may solve many security problems.

(2) UPnP Security

UPnP Security defines a service to be added to each secured device that allows its security to be managed [12]. It also defines a service and control point behavior for an application called a Security Console, which edits the ACL of a secured UPnP device and controls other security functions of that Device.

(3) Jini Security

Jini makes use of a service by downloading code from the service provider (see Section 4.2.3). This gives special security concerns. Mutual authorization must be realized. Jini should implement Java Authentication and Authorization Service (JAAS [13]). It specifies:

- An authentication framework. It's policy-based, can be plugged and stacked.
- Enhanced authorization. Principal-based.
- Low level binding between authentication and authorization.

(4) By utilizing widely available systems that address security at the network layer (IPSec) and the session layer (Secure Socket Layer – SSL/Transport Layer Security – TLS), and combined with firewall technology, we can address security issues in an IP-based network.

3.6 – User Interface

A user interface (UI) is needed for applications to control devices, this could be a web based Graphical User Interface (GUI) or a Short Message Service (SMS) application. Designing a good UI is very hard, as this involves quite a lot of very complex UI issues.

The UI should provide:
(1) Access to data from different sources, of different types.
(2) A unified view of different data sources in order to facilitate harmonized aggregation.
(3) A man/machine communication model for control purposes.

More and more UI applications today are web based. Thus the user needs only open a web browser. A device can transmit its web address, from where the (central) controller can automatically download the required software. This avoids the need to install software on every device that a user may want to use.

4 – Home Networking Technologies

"*Home networking is the collection of elements that process, manage, transport, and store information, enabling the connection and integration of multiple computing, control, monitoring, and communication devices in the home.*"[6]

The reasons for the flourishing of home networking lies in increasing numbers of telecommuters, multiple PCs at home, and more and more networking devices in a home. This section will give an introduction to these technologies.

4.1 – Home Networking Media

Based on the media used to carry data, home networking technologies can be subdivided into two major categories: wired and wireless. This section will address these two categories separately.

4.1.1 – Wired Home Networks

[6] International Engineering Consortium (IEC) online tutorials of Home Networking. See <http://www.iec.org/online/tutorials/home_net>.

(1) Twisted Copper-Pair or Coaxial-Based Transport Systems (Ethernet)
Based on the Institute of Electrical and Electronic Engineers (IEEE) 802.3 standard [14]. These networks are usually bi-directional and reliable. Transmission rate is high (up to 100Mbps). They are widely adopted by industry. Ethernet requires Category 5 (CAT5) cabling. Although it's a low cost solution, connecting by cables can be difficult depending on devices' locations.

(2) Twisted Copper-Pair-Based Systems (Phone Line)
Uses existing phone wiring. The Home Phone Network Alliance (HomePNA [15]) is one organization dedicated to this. It supports data transmission speed of 1 Mbps and works simultaneously with regular phone service. Although the phone wires are already there, there are a limited number of RJ-11 jacks in a home. Interference with and to traditional phone services is also a problem when using phone lines as the communications medium.

(3) Two-Way Coaxial Cable-Based Transport Systems (Broadband)
The same type of coaxial cable as used by cable TV is used. It provides a reliable medium for data transport and has long distance capability. This kind of network needs to be well planned, i.e., planning jack locations. This solution is more expensive then either of the twisted pair solutions described above.

(4) Power line-Based Transportation
Alternating current (AC) power lines are used. This is a very appealing technology, because power lines are available throughout a home. There are already smart devices that manage lighting and environmental systems (like turning on/off lights) using this technology. Interference and low data rate are the two main problems. Security can be also a problem, because control messages might be seen on a neighbor's power line network. X.10 is a popular standard for controlling over power lines. HomePlug [16] [17] is a LAN specification for high-speed networking of computers and other intelligent devices using home power lines.

Table 1 summarizes the characteristics of these wired media.

Medium	Standard	Speed	Distance between devices	Connected via	Connector	Max. number of devices	Advantages	Disadvantages
Twisted pair or cable	IEEE 802.3 Ethernet	10/100 Mbps	100 m (device to hub)	Cat. 5 UTP cable	RJ-45	No rated	Low cost; Fast; Reliable; Proven Tech.; secure	Difficult to connect by cables; Increased cable mass; available cable slots
Phone line	HomePNA	10 Mbps	300 m	Standard phone cable	RJ-11	50 for full 10 Mbps performance	Easy connectivity Relatively inexpensive	Moderate speed; phone jacks not ubiquitous
Power line	HomePlug	14 Mbps (future estimated at 100 Mbps)	300 m	Power line	Power outlet	256 (as in X10)	Availability of power outlets in every room; easy to install; inexpensive	Noise on power line limits speed and affects performance; minimum security level provided; data attenuation; Higher costs of residential appliances than phone line

Table 1 – Comparison of Wired Networking Technologies

4.1.2 – Wireless Home Networks

Wireless connections provide more mobility and offer greater convenience. Radio Frequency (RF) links are commonly used for this reason. Popular technologies include IEEE 802.11 and Bluetooth. These technologies usually offer high bandwidth. The range is often affected by various elements, such as the materials of the building.

(1) IEEE 802.11 wireless LAN [18]
Two types of networks: ad hoc and infrastructure networks are defined. An ad hoc network does not have an access point present. In a wireless infrastructure network, access points are used to route data between wireless stations or to and from the network server.

(2) Bluetooth [19]
It provides a mechanism to form small private ad hoc groups. It is designed to operate in a noisy RF environment. The Bluetooth radio uses a fast-acknowledgment and frequency-hopping scheme to make the link robust. Its normal speed is 1Mbps and range is 10 m.

(3) Zigbee [20]
Zigbee was approved by the IEEE (802.15.4) early in 2003 and addresses the need for home automation, machine-to-machine communication, etc. at a very low cost and with greater range than technologies like Bluetooth. It specifies three topologies of networks: master-slave, peer-to-peer, and mesh mode. Some Zigbee applications might be served by technologies like Bluetooth, cell phone systems, or proprietary radios. However, no effort has been made to provide Zigbee-enabled combination radios/devices and interconnectivity with other wireless networks.

(4) Ultra Wide Band (UWB)
IEEE 802.15.3a [21] committee is developing an open standard for UWB. UWB aims at transmitting digital data over a wide spectrum of frequency bands with very low power. It will have the potential to provide high data rates and good quality of transmissions at low cost. Initially, it is expected that the IEEE version of UWB will be limited in range to about ten meters and will be applied to wireless connection of entertainment system components (e.g., supporting isochronous data streams from a 1394 or USB connection in a STB to a television display).

Table 2 shows a comparison of technical features of wireless media.

Standard		Speed	Range	Frequency Spectrum	Max. number of devices	Advantages	Disadvantages
IEEE 802.11	a	54 Mbps	20 m	5 GHz	128	Free from noisy 2.4 GHz; high performance	Higher cost; 802.11a is incompatible with b & g
	b	11 Mbps	100 m	2.4 GHz		Better range than a; mature tech	
	g	54 Mbps	100 m	2.4 GHz		Same range with b Compatible with b	
HomeRF[7]		1.6-10 Mbps	50 m	2.4 GHz	127	Better price; built in support for voice communications; wideband frequency hopping is less susceptible	Limited range; Moderately high cost
Bluetooth		1 Mbps	10-1000 m	2.4 GHz	8 active devices in one piconet; totally 256 devices	Low cost; will be used in multiple devices	Not robust enough to be a full home network; lack of products; power consumption is not low enough
Zigbee		28/250 Kbps	13-134 m	2.4 GHz (also 915 MHz in US, 868 MHz in Europe	254	Low power; simple	Low rate; lack of products
UWB [44]		10 Gbps	10 m	3-6 GHz (sends out short, fast low power pulses)	No rated	High speed; high density; low complexity & cost	Short range; no products available

Table 2 – Comparison of Wireless Networking Technologies

[7] It has disbanded at the beginning of year 2003. This represents its commercial end.

Summarization: whether in new buildings or old buildings, less new wire introduced is always preferred. In this sense, wireless technologies and power line networking have advantages. In most houses, you can at least find one power outlet in a room, which makes using power line possible. While to be truly wireless, the power supply should be wireless too. In most cases, battery is used. This makes power consumption a critical issue in wireless networking. Zigbee seems very suitable for home environment since home automation is considered while it's designed. Because it is a low power solution, it will be more suitable to mobile devices. But no commercial products ready yet. At present, 802.11 and Bluetooth compete. They are still a bit expensive for use in homes. If the price of Bluetooth chipsets will reduce to its expected low price (less than $5), it will probably become a popular choice to home wireless networks. For home networks other than IP based, a STB should be able to translate between the home networks and the external IP networks.

4.2 – Home Network Communication Protocols

With the development of home networks, various technologies are introduces to promote home networking. At first, some industrial technologies were utilized. Later on, technologies particularly designed for home networks emerged. This section only provides an introduction to some of them.

4.2.1 – UPnP

UPnP [22] aims to facilitate automatic networking for ordinary people. It's designed as a Personal Computer (PC) centered system, although a PC may not present.

We are familiar with the Plug-and-Play technology used to ease communication between a PC and its peripherals. That is to automatically map a physical device to its driver and also establish communication channels between the device and its driver. Universal Plug-and-play is targeted at a "*distributed, open networking architecture that leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and everywhere in between.*"[8] This architecture is based on peer-to-peer technology.

It's called *universal* Plug-and-Play because of several features:

- Media independent. Designed to run on any media, such as phone line, power line, Ethernet, RF, and IEEE 1394.
- Platform independent. Any operating system (OS) and programming language can be used.

[8] UPnP motivation. See <http://www.upnp.org>.

- Internet-based technologies. It is built upon Internet Protocol (IP), Transport Control Protocol (TCP), UDP, Hyper Text Transport Protocol (HTTP), XML, and others.
- UI Control. Control over device UI and interaction using the browser.
- Expendable. Value-added services can be add-ons. It supports zero-configuration networking and automatic discovery.

Note that UPnP only defines a means to invoke actions and poll for values. It does not specify the design of an API for those applications running on control points and devices.

Basic components of UPnP:

Device	Contains services and nested services.
Service	Includes state table, control server, and event server. It's where the service functions lie.
Control point	Discover and control devices or services.

When a device or control point is attached to a network, it configures itself in order to work in the network (such as automatically getting an address). Each device is required to be a DHCP client. It will then first try to get an address from a DHCP server. If no DHCP server presents, the device then use Auto IP [22] to get a link local address.

A control point will then send a Simple Service Discovery Protocol (SSDP) (over UDP) containing a search request to discover devices and services. This request can be tailored to search for certain types of devices/services. For a device, it will send out multiple SSDP presence announcements to advertise its services. These service advertisements and responds to requests have a service/device description location pointer associated with them, so that control points can learn more about devices/services capabilities.

A control point can then send commands to control these devices/services. Here, Simple Object Access Protocol (SOAP) [22] (over TCP) is employed, using XML and HTTP to execute Remote Procedure Calls (RPC). SOAP is a standard for RPC based communication over the Internet. The control point can subscribe to a device/service for events like state changes in the device. Events are formatted according to General Event Notification Algorithm (GENA) [22] (over TCP), which defines how to send/receive notifications using HTTP over TCP/IP and multicast UDP.

Finally, information about the service/device and control are presented to a user via a user-friendly interface. XML is used through out the UPnP for carrying device descriptions, control messages, and events.

To sum up, UPnP defines a set of HTTP servers that use open standard Internet based protocols to handle discovery, description, control, events, and presentation.

Advantages:

- It leverages existing standard protocols, so devices can be built upon existing networks.
- Using SOAP for control, secures communication by using SSL, and ease access by using HTTP connection management facilities (i.e., accessing web pages).
- Both control points and devices use SSDP, which reduces the overhead on the network.

Disadvantages:

- An UPnP device needs heavier resources in order to support GENA and SOAP web servers.
- All the event variables are sent to a subscriber, so data filtering is needed.
- Device-interaction only through API or XML pages.
- Its pure peer-to-peer architecture increase network traffic due to extensive use of multicast messaging.

4.2.2 – Jini

Designed for use in java-centered systems, Jini [23] [24] technology is a Java technology that provides a simple infrastructure for interactions between network services. It has distributed system architecture, and in fact it is a specification of a set of middleware components, which include APIs, implementations, and a set of Java packages. When one service wants to interact with another, it downloads a Java object from another service. It can then talk to the service even though it has never seen that kind of service before. The downloaded object plays an important role here since it knows how to interact with the service providing it. The goal of Jini is similar to UPnP's in that both provide plug-and-play on a network level. But Jini leverages Java wherever applicable. However, it requires any device providing a service to have a Java Virtual Machine installed. Jini defines a generic way to deploy a service no matter it is implemented in hardware, software, or a combination of the two.

In a Jini environment, there are three kinds of participants:

Service	That's who really provides a kind of service.
Client	That's who wants to use the service.
One or more 'lookup' services	A lookup service must be present, it acts as a broker between services and clients.

When a service is booted on the network, it uses a discovery process to find the local lookup service. This is usually done by sending UDP multicast requests. If a lookup service exists, it will send a response to the service. The service will register (making a copy of the service object and storing it on the lookup service) the service object with each lookup service it

finds. The object will take the responsibility of providing the service. A client who wants to use this service can get a copy of the service object from the lookup service. The service object is really a proxy, which communicates back to other objects in the service, probably using Remote Method Invocation (RMI). This proxy has the service location specified so that it can communicate with the service.

However the RMI gives rise to a serious system software problem because of its size. It is very difficult to fit a native Jini/Java/Linux stack onto a typical embedded system board, not to mention extra applications required to run on top of the system stack. However current implementations of Jini depends on having a complete Java VM. While RMI offers elaborate remote execution support, it is really more than is necessary for communication by Jini, which can be rather primitive [25].

Disadvantages:

- In order to use Jini, a royalty fee is charged.
- Jini depends on Java being implemented.
- It's targeted only for IP networks.
- RMI which is not light-weighted, is used for device interaction,

In fact, Jini does not eliminate the need for device drivers. It merely provides a mechanism for locating Java-based device drivers.

4.2.3 – HAVi

HAVi [26][27][28] is a software specification used in some media centered systems, and enables interoperability of home entertainment devices. It is independent of platform and language, and was especially designed for digital audio and video devices. IEEE 1394[9] was chosen as the networking media. The HAVi specification contains a number of distinct software elements that each provides certain functionality. The main reason for such a dedicated network for the audio and video devices is that high quality digital video and audio signals need much higher bandwidth than other home network devices.

The main HAVi software components:

Control Model (CM)	Devices exchange control information and data in a peer-to-peer fashion. A controller hosts a Device CM for the controlled device.
Function Control Protocol (FCP)	For the transport of command requests and responses.
Connection Management Protocol (CMP)	For managing isochronous connections.

[9] IEEE 1394 is a very fast external bus standard. It supports data rate of up to 400 Mbps in 1394a, and 800 Mbps in 1394b. FireWire, i.link, and Lynx are all 1394 product brands.

Data Driven Interaction (DDI)	Provides a mechanism for commanding a device remotely.

HAVi devices:

Full AV devices (FAV)	Full featured controlling devices. They contain a java runtime environment.
Intermediate AV devices (IAV)	Controlling devices usually without java environment, thus providing limited control capabilities.
Base AV devices (BAV)	Controlled devices contain uploadable java byte code so that a FAV device can control them. An IAV device using native code can also control them.
Legacy AV devices (LAV)	This category is for non-HAVi compliant device. To enable them communicate with other HAVi devices, a FAV or IAV device needs to act as a gateway.

IEEE 1394 was chosen as the transport media in order to meet the requirements for real-time transfer, high data rate streams (400 Mbps, 800 Mbps, 1600 Mbps), self-management, auto-configuration, and low-cost cabling and interfaces.

The HAVi protection scheme has only two levels: trusted and untrusted. Digital signatures are used for verification. All HAVi software elements communicate via message passing.

Advantages:

- Devices from different vendors can interoperate.
- Devices can be controlled by one remote commander.
- Upgradeable. Most HAVi compliant devices come with their own dynamic device control modules.
- Supports legacy devices.
- Allows devices to present multiple user interfaces, adapting to both the user's needs and the manufacturer's needs for brand differentiation.

Disadvantages:

- Implementation of IEEE 1394 is not easy.
- Leaves most device protection implementation to device manufacturers.
- In a Linux environment, there are still some problems to be solved, such as real-time resource management and making the memory footprint small enough.

Efforts have made to build a bridge between HAVi and Jini [29], which complement each other in providing an open interoperability between audio-video devices and services.

4.2.4 – VESA Home Network (VHN)

VHN [30] is an open industry architecture standard for digital home networks developed by Video Electronics Standards Association (VESA). It is intended for use for data, Audio/Video, telephony, and automation in the home. It spans from physical layer to the application layer for total interoperability. It uses 1394b (a long distance variant of IEEE 1394) as its backbone. It focuses on providing access to VHN from external networks.

Components:

Backbone network	Enables connections to different networks using IEEE 1394b.
Component network	Different network technologies are involved.
Backbone component interface	Connects component network to the backbone network.
Access backbone	Connects the home network to external networks.

VHN is based on IP and aims at Audio/Video and other entertainment devices. Device descriptions are written in XML. Devices can be controlled via a web browser (as in UPnP, which eases remote access). It provides a flexible method of networking, since devices in component networks do not need to support IEEE 1394. Adapters can be developed to connect a component network into the backbone. It's also chosen for home network architecture in HES (see Section 5.4).

4.2.5 – Home API

Home API [31] is designed for a PC environment. It's an open industry specification that defines application programming interfaces. These APIs are protocol and network media independent, enabling software developers to more quickly build applications that operate these devices.

There are currently no standard APIs for home devices, so application developers are faced with the prospect of writing all aspects of a home device control system from scratch, including the handling of network interface hardware and device control protocols. With Home API, the application developer can ignore these low-level details and focus instead on adding features that provide direct benefits to the user.

Home API is based on a centralized control model. In this model, a few general-purpose intelligent nodes control numerous other devices across multiple home network protocols. This feature provides a way to integrate simpler devices that use different protocols into a unified control environment. Home API devices are able to communicate with Jini devices, but the reverse appears not to be the case. This requires the use of a bridge between the two. HomeAPI has merged with the UPnP effort.

4.2.6 – Home Network Control Protocol (HNCP)

Home Network Control Protocol (HNCP) [32] was designed for controlling and monitoring home appliances. It targets a low-speed control network based on Power Line Communications in a home network.

HNCP has a four-layer protocol architecture: physical layer, data link layer, network layer, and application layer. The first two layers are **not** specified in order to guarantee the flexibility; HNCP provides only guidelines for these layers. For those simple devices that do not have micro-controllers, a standard interface between a modem and a device is defined. This way, services can be ported in modems.

Advantages:

- At the data link layer, the data frame contains a Home Address, which avoids interference from neighboring.
- At the network layer, data frames can be prioritized.
- At the application layer, standard message sets are defined. There are three message sets: general message set, device specific message set, and a vendor-specific message set.

Disadvantages:

- Use broadcasting for monitoring of the device's status to keep consistency with multiple masters.
- Only a draft version, real implementations and evaluations are needed.

4.2.7 – X10

X10 [33] is a technology that allows remote control of devices plugged into the electrical network in a house. What makes X10 appealing is that control messages can be sent through the existing power wiring in a house. The X10 system consists of: a remote, a transceiver, and an X10 module. A command is sent from the remote and received by the receiver of the transceiver. The transceiver then decodes the command and transmits it on the house wiring in a particular format. The X10 module receives the command and performs the remote control operation on the device.

In X10, in order to control specific devices, all modules are assigned an address, which consists of a House and Unit code. Any command sent must be preceded by an address matching the specific device module's address. A command can be for a specific device, or for a group of devices. In total 256 devices can be connected into an X10 device network.

The disadvantages are:

- A separate control module is needed for every individual device that is going to be controlled separately, because X10 works by matching the House and Unit code.
- Transmission speed is low on the electrical network (a second or two for a command to be sent), range is limited, and signals are easily attenuated.
- Communication is unidirectional, so there is no acknowledgment. There is also no collision detection. So it is difficult to know if a command was executed properly.

Although the main market for X10 is still the United States, X10 products are also present in Europe, Asia, Africa, Latin America and Oceania.

4.3 – Devices in Home Network

Home network devices can be roughly divided into three categories [34]. This section will give some scenarios of these categories.

4.3.1 – Audio Visual

Audio Visual devices include: TV, Audio, Video, and Camera.

(1) Whole House Audio/Video
Lets you control these devices anywhere in a house. Speakers can be muted automatically when a phone rings or a doorbell chimes. You can download a movie from a PC hard disk and play it on a TV.
(2) Surveillance Cameras
Surveillance cameras enable you to monitor your home with, so that you can view different parts of your house simply by opening a web browser. Emergency events can be sent to you (instantly) as required.

4.3.2 – Amenity

Amenity control includes: air-conditioning, security, and health fitness sensors.

(1) Environmental Control
Thermostat control by a home automation system effects range from comfort to cost. Control can be remote control or manual. For example, you can set your drapes to automatically close when the sun shines directly in, and then open again later, tilt your blinds by remote control, open or close your windows, or automatically close your window(s) when it starts to rain.
(2) Security Alarms and Systems

Security systems may be simple or totally integrated into your home automation plan. Security systems include control panels, keypads, sensors, sirens, locks, lights, monitoring, access control, and more. Example of uses include: controlling your locks by remote control, using sirens to scare away intruders, and notify neighbors and authorities of burglary or fire, protect your family and home from fire with advanced smoke detectors that talk to your automation system, or turn outdoor lights on when someone approaches.

4.3.3 – Information

Information applications includes: Telephone, Fax, and email.

Phones & Intercoms
Transform your regular phone into a high-tech telecommunications system for your home. Add personal extensions to your phone with advanced phones or phone distribution panels; Answer the door from any phone, even cellular phones; Implement an intercom system, direct Caller ID information to be displayed on your TV,….

4.4 – Centralized Control vs. Distributed Control

Centralized control poses a problem of single point of failure. The control point also needs to carry much more burden. But on the other hand, it makes updates easier instead of updating possibly a large number of small devices. For remote control, it's also beneficial in that it easily enables connections outside the home. Controlling home devices via Internet only requires the central point to have an IP address and Internet connectivity. Other devices can utilize different standards than IP. We only need to make sure the central point is accessible via Internet and provides an appropriate (web) UI [35].

Another method is distributed control. This method has become possible due to increased numbers of microprocessors throughout the home and their low price. Each device is controlled separately by its own UI. But with the development of home networking, all of these devices can be connected together, and new functionalities can be built upon their collective capabilities. Distributed control may provide greater flexibility to the control system.

Having a central point does not necessarily mean centralized control. The control pattern can be a mix of the two. However, because of the ease of management, centralized control is likely to be more desirable in a home.

5 – Home Automation Standards

Home automation has developed for over twenty years. Many home bus systems were developed and introduced in the market. In Europe, these caused standardization efforts such as: European Home System (EHS), BatiBUS, and European Installation Bus (EIB). These three efforts are now joined to form Konnex. In America, Electronic Industries Association (EIA) Consumer Electronics Bus (CEBus) for control networks was derived from the LonTalk protocol. In Japan, Home Bus System (HBS) is the dominant home networking protocol standard. Home Electronic System (HES) is under development to be an international standard.

All these standards were motivated by the desire to provide a universal low cost solution for devices in the home to interconnect and interoperate, allowing new products and services to be introduced to homes easily, and to meet the requirements for home management and control. These standards are each introduced in depth in this section.

5.1 – Konnex Association

Konnex [36] is a convergence of three bodies: BatiBUS, EIB, and EHS. It was founded in 1999. It aims to promote a single standard KNX for home and building electronic systems. The CENELEC[10] Technical Committee signed on December 4th, 2003 the final documents to declare the KNX standard as a Norm for Home and Building Control (registered under the following EN numbers 50090-3-1, 50090-4-1,50090-4-2, 50090-5-2 & 50090-7-1). The standardization bodies like European Committee for Standardization and International Organization for Standardization (ISO) will endorse this approval as part of their standardization process. So, the KNX standard is expected to become a worldwide legal standard for Home and Building Control at the end of 2004. KNX technology is the world's first approved standard in this area, and it's an open standard. KNX provides runtime characteristics, an enhanced toolkit of services and mechanisms for network management. The architecture maps to Open Systems Interconnection (OSI) layer 1, 2, 3, 4, and 7. It's independent of any hardware platform.

It includes three configuration modes:
(1) System mode (S-mode). For well trained installers to implement sophisticated functions, typically with the help of PC-based Engineering Tool Software (ETS).
(2) Easy mode (E-mode). For installers with less training and also limited functions without the need for a PC tool.
(3) Automatic mode (A-mode). For end users without special training. The configuration has been pre-set.

[10] European Committee for Electrotechnical Standardization. It is the European Standardization Authority for all electrical equipments. It governs the standardization committees of each member state of the European Community.

It supports several communication media, as showed in Table 3.

Type	Description	Bit rates (bits/s)	Source	Compatible with source
TP-0	Twisted pair type 0	4800	BatiBUS	No
TP-1	Twisted pair type 1	9600	EIB	Yes
PL-110	Power line 110 kHz	1200	EIB	Yes
PL-132	Power line 132 kHz	2400	EHS	No
RF	Radio frequency 868 MHz	38400	KNX	Yes

Table 3 – KNX Communication Media

Apart from these, KNX has been working toward unifying the KNX device network with IP-based media, such like Ethernet, Wireless LAN, IEEE 1394, and Bluetooth. Manufacturers can choose any combination of the configuration mode and media to best deliver their products' functions. To address the integration with IP networks, KNX defines the “Advanced Network for Unified Building Integration and Services” (ANubis). By this effort, KNX will extend KNX devices to wider environment.

5.2 – CEBus

CEBus [37] is an open standard for communications in home networks. It's developed by Electronic Industries Alliance (EIA) and Consumer Electronics Manufacturers Association (CEMA), and it covers three areas: the physical design and topology of the network media, a protocol for message generation, and a common command language. The layers defined by CEBus relate to OSI layer 1, 2, 3, and 7. It also includes a Layer System Management element that resides beside all four layers.

It accommodates communication media such as: power line, twisted-pair, coaxial cable, infrared signaling, radio frequency signaling, fiber optics, and audio-video bus. Power line is the most used CEBus medium.

CEBus uses a peer-to-peer communication model. For larger networks, a central controller can also be used. A large part of the protocol is devoted to the control mechanism. It supports SCP for the UPnP.

For the power line physical layer, it implements carrier sensed multiple access with collision resolution and collision detection (CSMA/CRCD) to avoid collision. The protocol is based on spread spectrum technology. The CEBus power line carrier sweeps through a range of frequencies as it is transmitted. A single sweep covers the frequency band from 100-400

KHz. The frequencies used by this technology restricts its use to only the North American market.

5.3 – HBS

HBS [38] was developed by several individual Japanese manufacturers. It was released in 1986. It consists of the external network connection system and internal system such as speech communication control function. It specifies transmission over twisted pair wires or coaxial cable. Work has also been done to add power line and radio media. The intended application is communications among appliances for demand-side management to control usage of energy. But it has failed to gain a mass market. In 1997, Energy Conservation & Homecare Network (Echonet) developed Echonet[11] specifications based on HBS, which resulted in more powerful solution for different typology of media. Echonet is also open to European collaborations.

5.4 – HES

HES [39] is a joint standardization effort of IEC and ISO. A working group, SC25/WG1, is producing standards for a 'Home Electronic System'. This working group is a working group of ISO/IEC Joint Technical Committee 1 (JTC 1), Sub Committee 25 (SC 25). HES aims to control communication within homes, which includes the control of equipment for heating, lighting, audio/video, telecommunications, security, etc. It also includes residential gateways between the internal HES network and external wide-area networks such as the Internet.

This standard intended to promote interoperability among home system applications is still under development. The first part of the three-part interoperability standard describing the methodology for accomplishing interoperability is complete and approved. HES models of popular home systems, already written and published, will be incorporated into this standard. These systems include lighting control, security, energy management, and others. Models of these systems will be incorporated into the interoperability standard using a common classification (called a taxonomy) and dictionary (called a lexicon). Key functions will be classified and described with XML schema (software tools for managing World Wide Web data).

The technical work on standards is focused on the following areas:

- The residential gateway.
- Application interoperability.
- Broadband home network.
- Structured cabling

Summarization: there are many field bus systems available, either open standards or proprietary technologies. It is hard for a manufacturer to make a decision. Many manufacturers simply choose to wait-and-see, which hinders development within the home automation area. This phenomenon is obvious in European countries, where no standard has gained dominance. Although three major standard organizations (EIB, EHS, and BatiBus) have existed for years, their acceptance is mostly limited to the countries that developed them. Standardization is a strenuous process. Before a single standard prevails, it's better for a manufacturer to rely on open standards rather than develop proprietary solutions.

6 – IP based STB

This thesis considers improvement of a STB. This section will give an introduction to STBs, especially IP based STBs, and why an IP based STB would be a viable alternative as a remote control platform in a home.

6.1 – General Introduction

STBs came with the advent of Television (TV) programs that were not free (to watch). A STB was needed to receive TV program signals and to decrypt them. In the scenario that TV operators transmit digital signals and viewers use analog TVs, a STB is also required to convert the incoming digital signal into an analog format. Today, STBs provide additional features. Most interesting of them are interactive services, such as a Personal Video Recorder (PVR).

Definition: "*a STB is designed to receive the television signal, run the interactive applications and pass them to the TV. Its hardware and software depend on the nature of those signals and applications*" [40]. Any component in a STB has a corresponding part in the network's head end. They need to meet the same requirements in order to function properly. On head end, the scheduling system provides the data, the multiplexer creates a data stream, and the subscriber management system sets viewer permissions. On the STB, the demultiplexer processes the data stream, the conditional access software records permissions to viewers and uses them to decide whether a viewer can watch a program, and then displays the content to a TV screen or other display.

6.2 – STB architecture

[11] Echonet Consortium. See <http://www.echonet.gr.jp/english/>.

Basically, a STB is a specialized computer designed for television. The architecture of it depends on several elements, such as the nature of the TV signals, the services it's going to provide, and manufacturer's cost.

6.2.1 – STB Hardware Components

Hardware components can be divided into three categories [40].
(1) Computing Subsystem.
It's the part of a STB that handles basic computing functions. This part includes standard computer components like CPU, memory, and modem. It determines the performance of a STB. For example, a small amount of non-volatile memory is required to store viewer preferences. Flash memory is now widely adopted so that a STB's software can be updated over the air, and a high-speed port allows a STB to function as the portal for other devices in the home.

(2) TV Subsystem.
This part processes TV signals. It includes Moving Picture Experts Group-2 (MPEG-2) processing capability and video/audio output to TV or video recorder.

(3) Conditional Access Subsystem.
This part decides if a viewer can watch a specific program. The permissions are based on viewer entitlements. A smart card can be used here.

6.2.2 – STB Software Components

Software Components include:
(1) Hardware Drivers.
They are interfaces between the software and the hardware. They are provided by STB vendors.

(2) Core Software.
They provide the software platform for the applications running on the STB. This category includes the OS, boot loader, TV Core, middleware, and conditional access.

(3) Applications.
They provide the services viewers need, such like Electronic Program Guide (EPG), PVR, and interactive applications. The STB platform should be capable of downloading new software, so that new applications can be added later.

6.3 – STB Standards

There are many standards to help defining STBs. Vendors may choose to comply with a standard according to their business models. Sometimes they have no choice except the standard ordained by a government.

6.3.1 – Digital Video Broadcasting (DVB)

The DVB organization was initially set up as a European initiative between TV operators and product/component manufacturers to support interoperability between their various products [41]. Its standards are based on MPEG-2 compression and system specifications. These standards are widely adopted in European countries.

One major area covered by the DVB standards is the format of the information (metadata) used by the STB for program selection, event descriptions, and conditional access. DVB specifies a standard way to handle proprietary information, so that any vendor can add information without affecting the interoperability requirements. DVB specifies a common scrambling algorithm. Any DVB compliant STB can de-scramble a broadcast stream scrambled using this algorithm, if it has the appropriate conditional access. The DVB Simulcrypt standard defines the head end architecture necessary to support multiple conditional access systems by broadcasting conditional access entitlements simultaneously to STBs with different conditional access systems.

6.3.2 – Advanced Television System Committee (ATSC)

ATSC [41] was founded in North America. Its standards are for digital terrestrial broadcasting. Its two main features are the adoption of the 8-VSB transmission system and High Definition TV formats. They are mainly accepted by North American countries and some other countries. ATSC is similar to DVB in many ways.

6.3.3 – Association of Radio Industries and Businesses (ARIB)

ARIB [41] is a Japanese association and its standards have been adopted in Japan. The standards ARIB issued are quite similar to DVB. But they have some local variants, such as the scrambling algorithm and smart card protocol.

There are other standards or consortia defining different aspects of technologies apply to STBs, such as MPEG [42], Multimedia Home Platform (MHP) [43], and OpenCable [44].

6.4 – Types of STB

Based on the functions STBs can provide, they can be categorized into three types.

(1) Low-end STB
They provide only very basic functions like analog-digital signal conversion. They have minimal conditional access services, including ordering subscriptions and pay-per-view through a (personal) phone call, with no STB purchase interactions and no return path. So they are cheap.

(2) Mid-range STB
They offer more functionalities. They usually provide a return-path.

(3) High-end STB
They offer advanced functionalities. They are the platform for enhanced and interactive TV, personal TV, output to a home network, and many other features.

Often thought as a TV ancillary, a STB is expected to last a long time. Therefore, when designing a STB, future proof features should be anticipated. For example, adding a slot for a standard hardware card makes upgrades more flexible. A STB itself should be able to be upgraded for major changes. Application software can be downloaded and run at a later time.

6.5 – IP STB

IP enabled STBs are flourishing in recent years. IP STB, as high-end STB, is emerging as a home delivery platform for a wide and growing range of interactive digital content services. With its single television interface, users can consume videos and music, browse the Internet, play games, and use e-mail services. In the following paragraphs, an IP STB design from Microsoft is introduced.

The embedded IP STB design [45] from Microsoft provides two kinds of embedded OSs, which can be used to deliver complete and scalable client platforms for a wide range of IP STBs. These OSs are Windows CE .NET and Windows XP Embedded respectively. The design principles are to provide rich multimedia experiences, Web browser functionality that is fully customizable, extensive applications and services, including home networking and gateway functionality, VoIP communication, and instant messaging. These services and applications should be easy to update or replace over time. To facilitate further development, Windows CE .NET Platform Builder and Windows XP Embedded Target Designer development tools offer a sample Windows Embedded IP set-top box configuration. Figure 1 shows the Windows CE .NET 4.2 and Windows XP Embedded IP Set-Top Box Architecture. Both of them provide a set of features that give manufacturers' flexibility to build STBs.

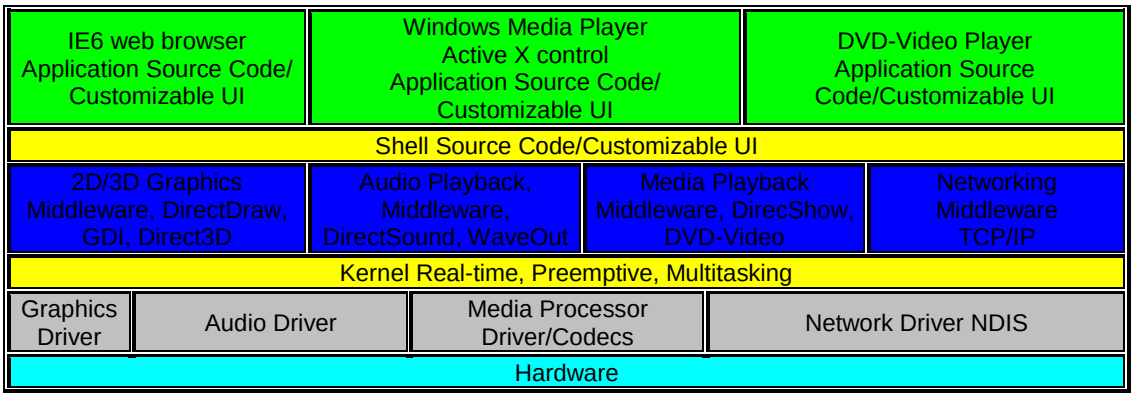

Figure 1 – IP STB Architecture

Windows CE .NET is more flexible in terms of the hardware it supports. Its 350 KB minimum operating system footprint allows the development of extremely cost efficient IP STB. For example, the minimum IP set-top box configuration in Platform Builder for an x86 processor is 6.4 MB RAM.

Windows XP Embedded is designed for more advanced, multi-purpose devices such as IP STBs that include advanced gaming capabilities and home media center features. Building

on its inherent desktop compatibility, STB vendors can easily extend IP set-top box functionality by using the very large application portfolio available for Windows XP.

Most of the features of the two OSs are similar. Some of them are:

(1) Include both IPv4 and IPv6 stacks and provide interoperability. This is not only useful for a STB to communicate with IPv4/v6 compatible devices, but also makes it a possible gateway between incompatible devices.

(2) Support Remote Desktop Protocol (RDP) 5.1. It's a service that allows a device to display and interact with the UI of a remote terminal server or personal computer across a Local Area Network (LAN), Wide Area Network (WAN), or by means of a dial-up, Integrated Services Digital Network (ISDN), Digital Subscriber Line (DSL), or Virtual Private Networking (VPN) connection.

(3) A complete set of advanced home networking and gateway functionality including firewall, Network Address Translation (NAT), modem, and wireless support.

(4) Internet Connection Sharing (ICS). Together with functionalities described in (3), a STB is a good candidate for a Residential Gateway (RG).

Some major differences are:

(1) XP provides full .NET framework support, which provides a hardware-independent program execution environment for secured, downloadable applications. While CE only provides a compact framework support, which is tailored for resource-constrained computing devices.

(2) XP has full win32 API support, while CE only supports a subset.

(3) In CE, Internet Explorer 6 includes: TV-Style 5 key navigation and directional tabbing, which enables a spatial navigation system. CE also support DTV broadcast services and Voice over IP, but XP does not support these.

When choosing which embedded OS to use, decision should be based on target market and applications. For mass market Windows CE .NET 4.2 is a better choice, because it offers full features for the majority of IP STB with a small footprint. While to provide advanced features and high performance applications, such as network gaming, Windows XP Embedded is better, because it provides an easier way of porting existing desktop applications to an IP STB and extensive support for latest multimedia technologies.

A recent press release[12] pointed out that if the price is set competitively, manufacturers tend to consider Microsoft's CE .NET platform. A move towards Linux based advanced STB has begun. Because Linux is capable of supporting advanced functions required by IP STB, such as video recording and IP delivery. The advantage of a Linux OS includes also no licensing fees. So, Microsoft will need a more competitive licensing scheme in order to compete with Linux in the future.

6.6 – Business Opportunities for STB

A STB changes the way people watching TV. With new technologies and applications coming, STBs will play an even more important role in a home. For example, interactive applications may range from games to t-commerce[13] support.

Digital TVs will replace analog TVs in the near future, which will definitely accelerate the deployment of STBs. The emergence of IP based STBs extends STB from an entertainment device to an information platform. For example, by integrating low-cost, interoperable 1394 technology available today, manufacturers of digital STBs can transform the STB from a fixed-function device to a whole-house entertainment server and remote control [46]. Up to 63 devices may be connected to one bus, and up to 1023 buses can be interconnected to create a very large network with over 64,000 devices.

There is a lack of applications interfacing value-added services and motivating end-users to subscribe to these services. Particularly, the mobility aspects (roaming of users, location awareness, varying bandwidth requirements) and the resulting demands concerning convenient personalization need to be addressed for implementing these applications. These next-generation services will bring new revenue to STB operators, service providers, and network operators. For example, new services will attract new customers as well as increase customer retention. These will increase network traffic, thus bring in new revenue to network operators.

Various organizations were working hard to promote this trend. The Plug N Play (PNP) initiative in the United States, uses basic digital cable and basic ATSC decoding and tuning in one STB was proposed. If accepted, PNP should help spur High Definition-set and Digital Terrestrial (DTT) usage. By late 2004, low cost PNP STBs should be on the market. In Europe, similar initiatives like DTT are being tested in Germany and the United Kingdom [47].

[12] 'Linux poised to dominate set-top box market', Mar. 09, 2004. <http://www.linuxdevices.com/news/NS6622794212.html> (Mar. 15, 2004).
[13] Similar to e-commerce, t-commerce enables viewers to purchase goods and services through a TV using a remote control instead of a keyboard.

A STB can be viewed as a generic PC, yet with a different design purpose. Its functionalities make it superb choice for a control platform so that home users can monitor/control devices in a home from anywhere. There are myriad solutions for this purpose. The solution chosen should meet the business model requirements. And the solution should also enable a STB to evolve as the market demands.

7 – Remote Residential Control System

A remote control system (control from web, mobile, PDA, etc.) is usually built like this: in a home, a 'controller' connects all the other devices being controlled, and this controller is connected to the Internet (directly or via a gateway); in the back end, the service provider provides a website for controlling from anywhere. The website maintains address of each controller, and a personalized web page for users to do remote control. The users usually need to subscribe to a service provider. Each time they login to their web page to do control. Events can be also sent to a user's pager, mobile, or as an email.

7.1 – An Example

Shell's HomeGenie is a new integrated home management solution released at the beginning of 2004. It's developed by the joint-effort of Shell[14] and Sun[15]. It's based on Java Enterprise System technologies and compliant with Open Services Gateway Initiative[16] (OSGi). The system provides web-based remote access of household systems and devices through an OSGi-based Residential Gateway (RG) using a broadband connection to the Internet. Table 4 shows its basic components.

Device	Service
Residential Gateway	Broadband connection and service delivery
Digital Programmable Thermostat	Household heating and cooling
Wireless Camera with built in motion sensors	Home area monitoring
Power Switch	Control of lighting

Table – 4 HomeGenie Components

Users can control these devices remotely through most web-enabled personal computers, cellular phones or personal digital assistants (PDAs). In the home, the system uses wireless technology, so few changes are necessary. The system is now only available in North

[14] An energy company. See <http://www.shell.com>.
[15] A leading IT company that developed Java technology. See <http://www.sun.com>.

America. The basic devices cost about $1000. Customers need to pay a monthly fee of about $30 for a personalized web site for viewing security camera images and other services. New devices and sensors are expected in the near future [48]. Up to 256 devices can be plugged into the system.

However, some things need to improve:

- Professional installers are needed for initial set-up.
- Existing thermostats must be replaced by the HomeGenie Programmable Thermostats.
- The system is a separate system from other home network systems.

7.2 – Turning a STB to a Remote Residential Control Platform

The long-term goal of Ecton AB is to grow into a managed service provider in the connected home field. It is now taking steps to build up the infrastructure and develop a basic service portfolio. It chose the STB as their service platform in a home. According to its business model, three methods of turning a STB into a remote residential control platform are proposed. They are explained in depth in this section, in descending order of functions and difficulty of implementation.

7.2.1 – Solution One: Residential Gateway

A residential gateway (RG) functions as a bridge between a home network and external networks. It is also known as a home gateway or home portal. For the home network, it enables the devices interconnected via the home network to be both centrally controlled and remotely controlled. For the external networks, it is a path for service providers to deliver value-added services to devices in the home, and to remotely manage these services and devices at a customer's premise.

It can be a standalone device or embedded into other devices (Digital Subscriber Line – DSL modem, Cable modem, STB, etc.). Home networks enable users, easily and inexpensively, to set up a high-speed data network that allows them to share resources such as files, scanners, and printers. It may also provide a user interface that can support voice and data connections and an interface to the Internet via a high-speed transmission medium such as a DSL, Cable, Integrated Services Digital Network (ISDN), or a Satellite link.

[16] An alliance promotes an open service platform for the delivery and management of multiple applications and services. It's an open industry effort. See <http://www.osgi.org>.

7.2.1.1 – Overview of Residential Gateway (RG)

Based on the functions, RG can be subdivided into three types.

Whole House RG	This is the closest to the original RG concept. It includes entertainment (video and audio), communications (telephony), high-speed data access, and control and monitoring (HVAC, security, lighting, etc.) functions.
Internet RG	This is intended to address the use of multiple computers and multiple high-speed access connection in the home.
Set-Top RG	It's the digital CATV based solution. It is a descendant of the analog TV STB, but with full digital capabilities and many new features.

A substantial market is illustrated in Table 5 (estimated by Clifford Holliday in 2001 [49]).

Year	Whole house	Internet	Set-Top	All types
2001	12,500	190,000	125,000	327,500
2002	30,000	510,000	190,000	730,000
2003	90,000	1,700,000	244,400	2,034,400
2004	140,000	2,850,000	322,600	3,312,600
2005	214,500	4,650,000	475,400	5,339,900

Table 5 – Estimated Home Gateway Units Total [33]

This table shows that users need time to accept the concept of a RG and for it to penetrate into homes. This is mainly due to consideration of price. Also it is because there are relatively small numbers of services available. But whole house RG will play an important role in a smart house in the future. From the description of a whole house RG, we can see that it meets all the functions of a remote residential control system. More and more families have a STB in their house. With the digitalization of TV, this number will surely increase. Turning a STB into a RG is an economical way to acquire advanced features. A software enabled RG is an available product, which solves the problem of replacing old STBs. In Section 7.2.1.2, an example of software RG product is given.

7.2.1.2 – RG Software – An Example

The example given below is taken from Wipro Technologies [50]. The software building blocks of a RG device are shown in Figure 2. The software for RG devices can be classified into three levels: firmware, OS, and application software stacks. The firmware level software includes the diagnostics, boot loader, debug interface drivers, and operating system board support package. A RG device needs an embedded OS, with the device drivers for all the

on-board and on-chip physical interfaces like the cable, DSL, Wireless LAN, Ethernet, Universal Serial Bus (USB), 1394, Bluetooth, HomePNA, Home Plug, etc. Popular embedded operating systems include Embedded Linux, VxWorks, Nucleous, and Windows. The RG application software stacks, shown in Figure 3, and explained in Table 6, provide the core functionality of the RG. The RG application stacks are comprised of the following software components:

- Communication protocol stacks for Routing, Bridging, Address Management (DNS, DHCP, NAT), quality of service (class based queuing, RSVP[17]), security (VPN, IPSec, Firewall), Remote and System Management (SNMP, Software Upgrades, HTML[18] UI, UPnP Internet Gateway Device)
- Voice Over Cable (Cablelabs PacketCable) and Voice Over DSL (DSL Forum BLES Specification) and Voice Over IP (H.323[19], SIP[20], MGCP[21]) infrastructure software stacks.
- Audio/video streaming (RTP[22], RTCP[23], SDP[24], RTSP[25]) and application service delivery (UPnP, OSGi) software stacks.
- All the software components for RG devices are based on the open standards such as IEEE specifications, IETF RFCs, ITU specifications, and industry specific forums like CableLabs, DSL/ATM Forum, UPNP Forum, OSGi Consortium, etc. The RG software should have well defined interfaces to integrate with the underlying hardware and should follow carefully defined and documented APIs to facilitate the application development.

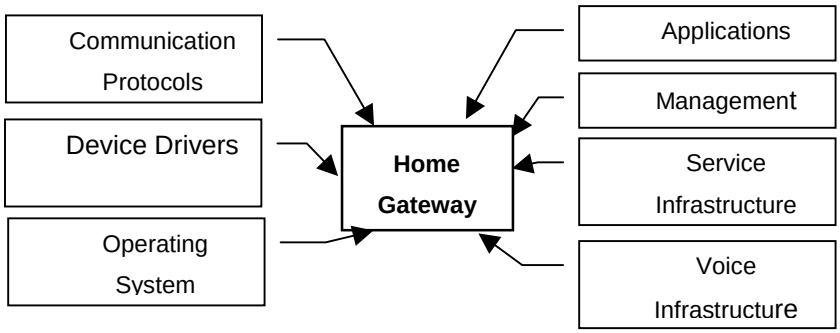

Figure 2 – RG Software Building Block

[17] Resource Reservation Setup Protocol: an Internet protocol developed to enable the Internet to support specified Quality of Service. With it, an application is able to reserve resources along a route from source to destination.
[18] Hyper Text Markup Language. It is used to create documents on the World Wide Web.
[19] A standard defines how audiovisual conferencing data is transmitted across networks.
[20] Session Initiation Protocol: a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. It initiates call setup, routing, authentication and other feature messages to endpoints within an IP domain.
[21] Media Gateway Control Protocol. A control and signal standard developed by Telcordia and Level 3 Communications. It defines how to convert audio signal carried on telephone circuits to data packets.
[22] Real-Time Protocol: an Internet protocol for transmitting real-time data.
[23] Real Time Control Protocol.
[24] Session Description Protocol: defines a text-based format for describing streaming media sessions and multicast transmissions.
[25] Real Time Streaming Protocol: a standard for controlling streaming data over the World Wide Web.

<table>
<tr><td rowspan="8">Log & Debug</td><td rowspan="8">Virtual OS</td><td rowspan="8">Management</td><td>Streaming</td><td colspan="2">HTML User Interface</td><td colspan="3">OSGi Framework</td><td colspan="2">Home Desktop</td></tr>
<tr><td>VoDSL</td><td colspan="2">VoCable</td><td colspan="2">VoIP</td><td>UPNP</td><td>SNMP</td><td>HTTPS</td></tr>
<tr><td colspan="2">VPN</td><td colspan="2">Addressing</td><td colspan="2">Routing</td><td colspan="2">QoS</td></tr>
<tr><td>Bridge</td><td colspan="2">Packet Filter</td><td>MPOA</td><td>CLIP</td><td>PPP</td><td>PPPoE</td><td>PPPoA</td></tr>
<tr><td colspan="3">Broadband Interfaces</td><td colspan="5">In-Home Interfaces</td></tr>
<tr><td>Cable</td><td>DSL</td><td>Ethernet</td><td>IEEE1394</td><td>USB</td><td>HPNA</td><td>Bluetooth</td><td>IEEE802.11</td></tr>
</table>

Figure 3 – RG Software Stack

Interfaces	Broadband: Cable, ADSL, Fixed wireless In-home: IEEE802.11b, USB, IEEE1394, HomePNA, Bluetooth, Ethernet
Protocol Bridging	Spanning tree (IEEE802.1d) and Transparent Bridging, Media Translation
Routing	RIP(RFC1058), Multicast Routing (through IGMP Proxy)
Addressing	NAT/NAPT (RFC1631, 2993), DHCP client, server (RFC2131, 2132), Dynamic DNS (RFC1034-35, 2136, 2535)
QoS	RSVP (RFC2205, 2210) and Traffic Control Module implementing the Class Based Queuing
Security	Layer 2 Stateful and dynamic IP Packet Filtering, URL Filter, HTTPS
VPN	IPSec (RFC 2401, 06), IKE, PPTP (RFC2637), L2TP (RFC2661), PPPoE (RFC2516). Easy integration with third party HW and SW crypto libraries: SHA-1, MD5, 3DES, AES
Data over DSL	ILMI, Classical IP and ARP Over ATM, MPOA (RFC1483), PPPoATM (RFC2364), OAM
Voice Over DSL	BLES (DSL Forum TR-036)
Voice Over Cable	PacketCable NCS (MGCP), PacketCable MTA
VoIP	H323, SIP and MGCP protocols
Streaming Stack	RTP, RTCP, SDP, RTSP, MEP Over RTP
Remote Management	SNMPV3 (RFC1157, 2271-227) with MIBs, Remote Software Upgrades, Logging and System Trace Features
Service Discovery	UPNP Application Framework, OSGi Application Framework, Application Bridging
Home Desktop	Application framework for easy and quicker deployment of Web Based Portal Applications to Discover, Operate, Control, Monitor and Administer the home devices and services

Table 6 – RG Software Specification

7.2.1.3 – Pros and Cons

Benefits:

- As the solution gives a STB many advanced features, the STB will have much wider market opportunities, as it is more than just a remote control platform.
- RG covers most widely adopted technologies for home networking, thus more products can be controlled.
- RG software is already available and tested. The development period is short. For example, Wipro promises to help customers roll out their products in about 6 months time.

Considerations:

- Comprehensive functions come with a cost tradeoff.
- There are many manufacturers in the RG market. To compete with them, price and functionalities are major deciding elements.
- With many devices connected to the STB, available slots on it might be insufficient.

According to the company's business strategy, it wants to add new features gradually so that the cost of a STB won't increase sharply. Based on this strategy, software updates are much preferred to hardware updates. Although there are soft solutions for turning a STB into a RG; from the role of a RG, we can see that the STB needs changes in hardware, such as adding more interfaces to interconnect other devices in a home. This will definitely increase the cost. If the target market is not the mass market, this solution works fine. At present, Ecton AB can choose to utilize only some protocol stacks, those that it needs most in the near future to implement first, and then add on new features from time to time.

7.2.2 – Solution Two: A controller on Home Bus

Home bus systems will enter more homes, especially new buildings. Home automation products run on these home buses. Those products on the home bus networks will comprise most of the devices we want to control. If a STB can be a controller on the home bus, this STB should have a position in future homes.

Before an international standard addressing home automation network comes out, KNX might be a leading standard in European market. Already, connection to the IP world is addressed in the standard. For a remote residential control system, as described in Section 7.1, one critical decision must be made before developing the system, that is to choose the devices that you want to control. A STB can sit between the IP network and a Konnex device network, serving as a gateway.

Konnex Association provides a suite of PC software tools, ETS, for design and configuration of KNX installations. To facilitate access to KNX installations via IP links, it has an internet ETS (iETS). Apart from system interventions through the local LAN, iETS also caters for remote maintenance functionality. ETS is built on top of a framework of Distributed Component Object Model (DCOM), software-engineering components for PC/Windows platforms, called the eTool Environment – Component Architecture (eteC). The later provides an abstract API and object model for on-line and off-line access to KNX resources.

eteC consists of two basic components that are now commercially available. One is Falcon, which provides an abstract frame API for live access to KNX/EIB embedded control networks. It is a DCOM-based 32bit access library for Windows 95/98/NT4. It can be seen as a KNX/EIB protocol stack for PC-implementations. It offers a comfortable API for languages like VC++, Delphi, VB, etc. Scripting languages like Visual Basic for Applications (VBA) can be used in order to access KNX networks from office applications. Falcon completely adapts to the standard PC/EIB gateway and the local communication protocols it uses. Another component is Eagle, which maps the relevant physical database structure of the ETS repository to an abstract object model API [51]. As we mentioned before, KNX specifies ANubis that integrate a KNX Device Network installation into a LAN or WAN environment, ETS will gradually grow into a universal configuration platform.

7.2.3 – Solution Three: Bluetooth Enabler

7.2.3.1 – General Analysis

To introduce a network into a house, less wiring is a big advantage. No wiring pre-planning is needed and device set up is relatively easy. From the comparison in Section 3.2, we can see Bluetooth is a good choice among wireless home networking technologies now available. Although at the first sight, its 10 meters' normal range may limit its usage to short range cable replacement, longer range has been achieved. For example, Bluetooth products from the company Blue2Net[26] achieved 1300 meters' range by the use of a Class-2 Bluetooth radio module and its high-gain Blue2space™ antennas without exceeding the allowed output power. Another concern of using Bluetooth is will the power output be dangerous to a family. The average output power level for Bluetooth is very low, only 1mW for most units and 100 mW for Class-1 modules. Compared with common cellular phone systems (typical output power of 1-2 Watts), it is much safer. With the dropping cost of Bluetooth chips, more and more products are expected to be Bluetooth enabled.

However one big problem in leveraging Bluetooth in this residential control system is that not many home automation products, such as lighting control, remote reading of meters, safety control, etc., are enabled with Bluetooth. Bluetooth products today are still limited to mobile,

[26] See <http://www.blue2net.com>.

automotive, and multimedia products. Of course there are companies like Toshiba working on a Bluetooth enabled refrigerator and micro oven, but that will limit the usage of this control system. Waiting for new products with Bluetooth, or plugging a Bluetooth enabler into the devices available only to be controlled by the control system is not such a good idea. So if we want to address most home devices, we should not limit ourselves to a pure Bluetooth connection, especially as most home automation devices communicate via power lines. But if the STB itself is a Bluetooth enabler, that's to say devices connected to it can communicate with other devices via Bluetooth, it will help promoting Bluetooth technology in a home.

Today, we can find more and more portable devices, such as mobile phones, PDAs, and laptops, are equipped with Bluetooth. These devices usually provide friendly UIs. People have become used to carrying them everyday. This makes them more suitable controllers than traditional controllers, like a TV remote controller. Their portable character makes true remote control from 'anywhere' reality. Since most of these devices support Wireless Application Protocol (WAP[27]), if we can make these devices communicate with a STB via WAP, then further control of devices connected to the STB is possible. The STB acts as a WAP web server. It can provide a unified web based UI for all the devices being controlled. Controllers such as PDAs and mobile phones all have a web browser and thus control can be as easy as browsing a web page. When within the range of Bluetooth, the controller can connect to the STB via a Bluetooth connection. When out of the range, Internet or GSM/GPRS[28] can be used for accessing the STB at home. The most appealing aspect of this method is no specialized remote control is needed. For example, a mobile phone might be enough both inside and outside of a home.

7.2.3.2 – An example Bluetooth Enabler Product

In this section, a product called Bluetooth Web Enabler from ConnectBlue AB[29] is introduced. Its core functionality is to provide a web based UI to existing devices. It also enables Bluetooth connection to controllers [52]. Figure 4 shows a simple set up. Existing devices can be connected to the Enabler via an RS232/422/485 interface. The product complies with Bluetooth Specification 1.1. It supports LAN access, serial port access, and Dial-up networking. Radio signal ranges up to 50 meters (power consumption[30] about 50-100 mA). It has 1 M Byte data storage. For communication, it supports many field buses, and customized protocols can also be developed.

[27] WAP: a secure specification that allows users to access information instantly via handheld wireless devices. It supports most wireless networks, and it is supported by all OSs.
[28] Global System for Mobile Communications/General Packet Radio Service: leading digital cellular systems.
[29] A company in Sweden that provides Bluetooth products and services.
See <http://www.connectblue.se>.
[30] Power consumption depends on different modes. To most devices, generally about 60 mA for Receiving or Transmitting and 20-30 μA in Standby mode.

The Bluetooth Web Enabler provides the UI via a built-in web server. The UI is stored as normal web pages. When a user wants to control a device, the controller (e.g. mobile phone) downloads the UI to their browser. The Enabler converts user commands into control data for the device. Locally, you can control a device via Bluetooth connection; remotely, via Ethernet, Internet, or GSM/GPRS (depending on which you choose among those available).

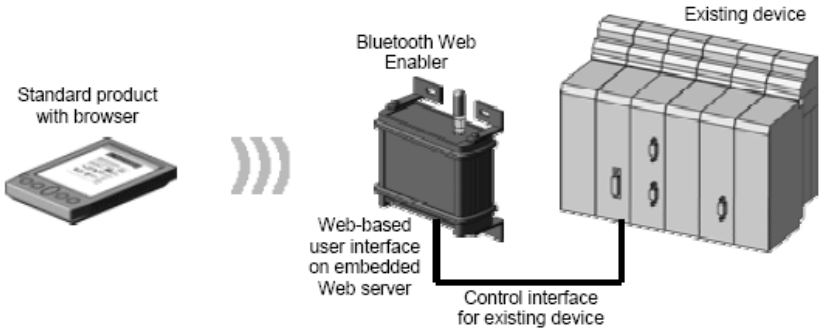

Figure 4 – Simple Bluetooth Web Enabler Working Scenario [52]

7.2.3.3 – Pros and Cons

This solution meets the needs for accessing device networks, user-friendly interface, and a single remote control. Various devices can be used as a controller. It is easy for user to use this system. Turning a STB into a web Bluetooth Enabler, is less costly than creating a RG. A development software kit and Original Equipment Manufacturer (OEM) module exist, which will facilitate this transformation. Extra interfaces will be needed to connect different existing devices.

7.2.4 – Comparison

From the above, we believe that the RG solution is the most comprehensive one. Yet it is the most costly and difficult one. We see it as a long-term goal. Remote control should focus on interfacing to devices that are already on the market, and do so at a reasonable price. We should implement one particular standard to begin with. The choice should be based on the number of available products and their price. Later on we can expand it to different standards. The protocols should ideally be based on the same standard, but we might not include physical layer interfaces for all protocols in the standard product. In this sense, enabling the STB to interact with Konnex products seems a good first step.

For wireless technologies at home, we do not know which solution will win. More and more products will support Bluetooth, but it's not a mature technology for home networking, and not many commercial products exist for home. The controlled devices should ideally be hard wired to reduce power consumption and increase reliability. However, Bluetooth could be used to interface the actual remote control terminal. We will consider including a physical layer interface for Bluetooth, so that when a Bluetooth device can easily access the STB in

the future, such like a Bluetooth keyboard. We can always do a software upgrade of the STB later, as long as there is a physical Bluetooth interface.

Because many portable devices (mobile phones, pagers, two-way radios, smartphones, communicators, etc.) use WAP for communication, WAP can be enabled in the STB. Together with a web based UI, it may provide a 'ubiquitous' controller. This may enable other functions from the remote control as well, such as what viewing channel to use for the TV, etc.

To combine systems with different requirements without compromising too much is hard. The significance of standardization is emphasized in home networks. We chose to control Konnex products as the first step. The remote residential control system should provide a high degree of plug-and-play functionality and provide compatible communications between devices. A good approach to a UI is critical in attracting potential users. Solution 2 with some features from Solution 3 should enable some kind of intelligence in a house.

.

8 – Conclusion

At the beginning of this project, the title of the project was "home gateway service platform". However, after some research concerning RG and discussions with the company, I found out that there was misunderstanding about the concept of a home gateway (or RG) in the company. What the company really wanted was a remote control platform in a STB. So we focused on remote control function later in the project and thus changed the title to remote residential control system. This change did not reduce the amount of work. On the contrary, because of the lack of a single standard in this area, I had to read more in order to get a clearer picture of how to design a remote control system. The company only had a vague idea of the system, which also added to the difficulty. For example, the company did not know the pattern of remote control they wanted and what kinds of devices they wanted to control. In this project, most of the work in the early days was to help the company realize what their real needs are and what technologies can address these needs.

In any case, my knowledge in home networking, home/building automation, and STB has increased a lot. I did not expect to see so many technologies in the home network field, which gave me a lot of trouble in collecting and digesting them. Once I figured out how a general remote residential control system works, the next step was to settle on what kinds of devices will be controlled by the system and which technology to use. There are already many mature products for home networks and home automation. Therefore, it is not wise to build a remote residential control system from start. Choosing products or technologies that will facilitate turning a STB into a platform for such a system will be a cost-effective strategy. It will also help to reduce a product's time-to-market.

Due to limits of time and resources, no actual remote residential control system was set up during this project. The company is talking to KNX device vendors in order to get some devices for testing. A demo will be set up in the near future.

The home network market is still young, but it's growing fast. No one can ignore this large potential market. However, the business opportunities still need to be explored. It always takes more time than expected to actually get things done. I hope that when Ecton AB incorporates remote residential control function for KNX devices into their IP STBs, KNX will have gained more strength both in Europe and world wide, and more KNX devices will be ready to be controlled by these STBs.

A few trials of the solution should be done in order to show how to really integrate remote control function into a STB, how user uses it, and how it benefits users. Some future work is listed in the next section. Trends that will help the development of remote control are also discussed briefly in this section. These trends will also help advance the whole home networking field.

8.1 – Future Work

An actual testbed is needed to test the proposed solutions. First, we need to choose some simple and affordable Konnex products for testing. Then we must buy or implement the relevant protocols in a STB to enable user interactions. This will require development of a web UI. Additional programming might be needed to provide the desired control results. Finally we need to test the whole system.

8.2 – Trends Facilitating Remote Control

Much effort has been put into interoperation. Some of these that may help residential control are introduced below.

8.2.1 – Expanding a Home Device Network to an IP Network

Legacy intelligent home devices are not aware of IP. They usually run on a home bus system and can only cooperate with devices on the same device network. The consumers are always driving forces of home automation market. They demand services that may facilitate everyday life or even change users' lifestyles, so manufacturers are now beginning to give their products the ability to access service networks (usually IP based). This trend can be seen as many standard organizations (in this field) have begun to include IP network connectivity in their standards. For instance, Konnex has ANubis in its KNX standard, which

integrates a KNX device network installation into a LAN or Wide Area Network (WAN) environment.

8.2.2 – Transition to IPv6

One issue that must be addressed in order to enable communication between a home network and an external network is address translation. Due to the limited address space in IPv4, it's not possible for every device in a private network to get a globally unique IP address. This hinders accessing a device freely. IPv6 has been in development for many years. Its main aim is to solve the address availability problem (of IPv4). Additionally, while designing IPv6, better mobility and security were also included.

All the remote residential control systems mentioned earlier in this report involve some kind of address mapping. For example, a STB's IP address may change due to power down or reboot, so that a service provider must learn the new address. Also a device in a home network with a private address needs to utilize a public address to communicate outside. With IPv6, all the devices can then get a local IPv6 address, so mutual communication will be easier to realize. A gateway will not be needed any longer, be it a PC, a phone, or any other.

However, the transition from IPv4 to IPv6 is not easy and it takes time. The two types of IP addresses may coexist for a while before a full transition. The full transition requires:

- Every single device that connects to the Internet to support IPv6 at every layer.
- Both the home network and the provider network need to support IPv6.
- The core backbone of the Internet connected to the provider network must support IPv6.

Some people expect the transition to evolve and emerge initially in the home network where IPv6 deployment is relatively simple. This may create islands of IPv6 enabled homes. Tunneling may be used for connecting these homes to the Internet [53].

8.2.3 – A Common Language/Protocol

A myriad of protocols is the main obstacle to interoperation. At present, this is usually overcome by gateways. The gateways will contain multiple protocol stacks and must translate between them. While true interoperability can only be achieved without requiring the presence of a gateway. That is to say all the devices should speak the same language. XML may help different systems to communicate with each other in a similar manner.

XML can deliver structured content over the Web, and it's becoming the IT industry standard for data exchange. XML will ultimately replace HTML [54], which is well suited for displaying

information but does not provide the structure necessary to organize and exchange data. However, XML was not especially designed for exchange home/building data, such as temperatures. The format of the data traveling between systems should be defined before XML becomes a prevailing protocol in home/building management field. Throughout the IT industry, committees such as OASIS (the Organization for the Advancement of Structured Information Standards), W3C (World Wide Web Consortium), and XML.org have been formed to develop guidelines for machine-to-machine interaction. Again it's a huge amount of work, but once the time comes, control tasks, as discussed in this report will be easier.

References

[1] <http://www.dhcp.org> (11 November 2003)

[2] <http://www.zeroconf.org> (11 November 2003)

[3] Erik Guttman, 'Autoconfiguration for IP Networking: Enabling Local Communication', June 2001. <http://www.zeroconf.org/w3onwire-zeroconf.pdf>

[4] RFC2608, 'Service Location Protocol, version 2', June 1999. <ftp://ftp.rfc-editor.org/in-notes/rfc2608.txt> (13 November 2003)

[5] RFC2782, 'A DNS RR for specifying the location of services (DNS SRV)', Feb 2000. <ftp://ftp.rfc-editor.org/in-notes/rfc2782.txt> (13 November 2003)

[6] Salutation Organization Website. <http://www.salutation.org> (20 November 2003)

[7] <http://www.openldap.org> (21 November 2003)

[8] SNMP Introduction. < http://www.et.put.poznan.pl/snmp/intro/iovervi4.html> (15 December 2003)

[9] SDCP 1.0, 2001. < http://users.cafwap.net/~sdcp/spec/20010208> (23 November 2003)

[10] <http://www.itu.int/ITU-T/asn1/database/itu-t/h/h282/1999/> (10 January 2004)

[11] SCP, Mitsubishi Electric Research Laboratories, Sep 2003. <http://www.merl.com/projects/SCP/> (12 December 2003)

[12] Mauri Kangas, “Authentication and Authorization in Universal Plug and Play Home Networks”, Ad Hoc Mobile Wireless Networks – Research Seminar on Telecommunications Software, Autumn 2002. < http://www.tml.hut.fi/Studies/T-110.557/2002/papers/mauri_kangas.pdf > (8 January 2004)

[13] JAAS. <http://www.javaolympus.com/J2SE/SECURITY/JAAS/JAAS.jsp> (8 January 2004)

[14] < http://grouper.ieee.org/groups/802/3/ > (3 January 2004)

[15] <http://www.homepna.org> (3 January 2004)

[16] <http://www.homeplug.org> (3 January 2004)

[17] ‘IOGEAR HomePlug Powerline Network Guide, Introduction to HomePlug Power line Networking’, IOGEAR. <http://www.iogear.com/products/homeplug_guide.pdf> (4 January 2004)

[18] <http://standards.ieee.org/getieee802/802.11.html> (5 January 2004)

[19] <http://www.bluetooth.org> (5 January 2004)

[20] <http://www.zigbee.org> (6 January 2004)

[21] <http://www.multispectral.com/UWBFAQ.html#UWBFAQ20> (6 januari 2004)

[22] <http://www.upnp.org/ > (21 November 2003)

[23] ‘Why Jini’, Faculty of Applied Sciences at University of Freiburg, Germany, 2001. <http://tele.informatik.uni-freiburg.de/Teaching/ss01/smok/Introduction/Jini-Introduction.htm> (22 November 2003)

[24] Jan Newmarch, ‘Jan Newmarch’s Guide to Jini Technologies’, Version 3.02, Sept. 2003. <http://pandonia.canberra.edu.au/java/jini/tutorial/Jini.xml> (22 November 2003)

[25] Vincent Lenders, Polly Huang, and Men Muheim, ‘Hybrid Jini For Limited Devices’, ETH Zürich, Dec. 2001. < http://www.tik.ee.ethz.ch/~huang/publication/hybrid-jini-icwlhn01.pdf > (23 November 2003)

[26] Santosh Kumar, ‘Hardware Audio/Video Interoperability (HAVi)’, CIS, OSU, 2001. <http://www.cis.ohio-state.edu/siefast/presentations/havi-kumar-2001/havi.ppt> (24 November 2003)

[27] Jussi Teirikangas, ‘HAVi: Home Audio Video Interoperability’, Helsinki University of Technology, 2001. <http://www.tml.hut.fi/Studies/Tik-111.590/2001s/papers/

jussi_teirikangas.pdf> (24 November 2003)

[28] ‘HAVi Home Audio Video Interoperability’, XiLinx. <http://www.xilinx.com/

esp/consumer/home_networking/pdf_files/havi/complete.pdf> (25 November 2003)

[29] Henrik Hedlund, 'A gateway between Jini and Universal Plug and Play', Master Thesis Project at the Department of Teleinformatics, KTH, July 1999.

[30] 'VHN (Vesa Home Network)', DMN Software-Entwicklung GmbH. <http://www.dmn.at/Info/VHN/vhn-en.html > (27 November 2003)

[31] Home API Working Group. <http://www.htc.honeywell.com/projects/homeapi/> (28 November 2003)

[32] Jae-Min Lee, Kwan-Joo Myoung, Kam-Rok Lee, Dong-Sung Kim, and Wook-Hyun Kwon, 'A New Home Network Protocol For Controlling and Monitoring Home Appliances-HNCP', CISL, School of Electrical Engr. and Computer Sci. Seoul National University, Korea, 2002. <http://icat.snu.ac.kr:3333/papers/pdf /c2002e.pdf> (5 January 2004)

[33] 'X10 Protocol'. <http://www.x10.com/support/basicx10.htm#introduction> (12 November 2003)

[34] <http://gawain.membrane.com/alarm_systems/smart_homes.html> (5 February 2004)

[35] Arto Ylisaukko-oja and Marko Suojanen, 'Low Capacity Wireless Home Networks – Cheap and Simple Interconnections between Devices', Version 1.0, Wireless Wellness Monitor II Project, May 2002. < http://www.vtt.fi/tte/samba/projects/wwm/ reports/Wireless_Solutions_for_Home.pdf > (12 February 2004)

[36] 'System Architecture – KNX The one-Single-Standard for the integration of Home and Building applications', Konnex Association, 2003. <http://www.knx.org> (3 January 2004)

[37] <http://www.cebus.org> (8 January 2004)

[38] 'Report on Home Automation', IGU – WOC 6 SG 6.1, Oct. 2002. <http://igu_woc6_1.dgc.dk/WORK_BY_TOPIC/topics_documents/homautoma/SG_61%20Report%20Home_A_Oct%2002.htm> (8 January 2004)

[39] ISO/IEC JTC1 SC25 WG1 Home Page. <http://hes-standards.org> (9 January 2004)

[40] Xiaoyan Ren and Willy Hu, 'The Digital Set-Top-Box Decision and Your Interactive Business', NDS White Paper, May 2002. <http://videosystems.com/ar/ video_digital_settopbox_decision/> (10 January 2004)

[41] 'The NDS Guide To Digital Set-Top Boxes', third edition, NDS Ltd, 2002. <http://www.broadcastpapers.com/data/NDSGuideSetTopBox101.htm> (11 January 2004)

[42] <http://www.mpeg.org> (8 March 2004)

[43] <http://www.mhp.org> (8 March 2004)

[44] <http://www.opencable.com> (8 March 2004)

[45] Bill Wittress, 'Internet Protocol (IP) Set-Top Boxes, Windows CE .NET 4.2 and Windows XP Embedded – Scalable Software Platforms for Building Flexible, IP Set-Top Boxes' Windows Embedded Devices Group, Microsoft Corporation, Sep. 2003. < http://download.microsoft.com/download/8/2/0/820203f2-f092-4e2e-9ffc-c6e2c650adbd/IP_SetTop_Boxes_Whitepaper.doc> (10 January 2004)

[46] Greg Bartlett, 'The role of the digital STB in home entertainment system', May 2000. <http://www.eetasia.com/ARTICLES/2000MAY

/2000MAY03_NTEK_ID_MSD_PD_TAC.PDF> (10 January 2004)

[47] 'Home Gateway Report: Worldwide Multi-Carrier Digital Settop & Services Analysis & Forecast – 2003-2006', Executive Overview, Published by Multimedia Research Group, Inc., April 2003.

[48] <http://www.shellenergy.com/HomeGenie/mkt/ExperienceHomeGenie/> (30 December 2003)

[49] Clifford Holliday, 'Residential Gateway', volume 2, IGI Consulting Inc., April 2001. <http://www.igigroup.com/st/pages/bringlightv2.html> (15 October 2003)

[50] Satish Gupta, 'Home Gateway', Wipro Technologies, 2002. <http://www.wipro.com/insights/homegateway.htm> (16 October 2003)

[51] 'Structure of the eteC Framework', November 2000. <http://www.eiba.com/

technology.nsf/software%2FeteC%2FFramework%20structure?OpenPage> (04 February 2004)

[52] 'Bluetooth Web Enabler, Use Cases and Features 1.0', ConnectBlue AB, 2003.

<http://www.connectblue.se/files/Bluetooth%20Web%20Enabler%20Appl.%20Scenarios%201.0.pdf>

[53] Venkat R Gokulrangan, 'Internetworking Using Ipv6 Technology Inside and Outside the Home', Desktop Products Group, Intel Corporation. Intel Technology Journal, Vol. 6, Issue 4, 2002.

[54] Rachel Reiss, 'The Future of Building Controls', CABA Home & Building Automation Quarterly, Winter 2003.

Appendix I – Acronyms and Abbreviations

AC	Alternating Current
ACL	Access Control List
AGP	Advanced Graphics Port
API	Application Programming Interface
ARIB	Association of Radio Industries and Businesses
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
ATSC	Advanced Television Systems Committee
CAT5	Category 5
CATV	Cable Television
CBC	Cipher Block Chaining
CEMA	Consumer Electronics Manufacturers Association
CM	Control Module
CMP	Connection Management Protocol
CPU	Central Processing Unit
CSMA/CRCD	Carrier Sensed Multiple Access with Collision Resolution and Collision Detection
DA	Directory Agent
DCOM	Distributed Component Object Module
DDI	Data Driven Interaction
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
DNS	Domain Naming Service
DRM	Digital Rights Management
DSL	Digital Subscriber Line
DTT	Digital Terrestrial
DTV	Digital Television
DVB	Digital Video Broadcasting
EIA	Electronic Industries Alliance
ETS	Engineering Tool Software
EPG	Electronic Program Guide
FCP	Function Control Protocol
GENA	General Event Notification Algorithm
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
H.323	Signaling Standard for Voice Over IP

HAVi	Home Audio/Video interoperability
HMAC	Hash Message Authentication Codes
HNCP	Home Network Control Protocol
HomePlug	Home
HomePNA	Home Phone Network Alliance
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HVAC	Heating Ventilation and Air-Conditioning
ICS	Internet Connection Sharing
IEC	International Engineering Consortium
IEEE	International Electronic and Engineering
IEEE 1394	A standard defining a high speed serial bus
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
IPX/SPX	Internetwork Packet Exchange/Sequence Packet Exchange
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
Jini	A home networking technology from Sun
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MGCP	Media Gateway Control Protocol
MHP	Multimedia Home Platform
MIB	Management Information Base
MPEG	Moving Pictures Experts Group
NAT	Network Address Translation
OASIS	Organization for the Advancement of Structured Information Standards
OEM	Original Equipment Manufacturer
OS	Operating System
OSI	Open Systems Interconnection
OSGI	Open Services Gateway Initiative
PC	Personal Computer
PDA	Personal Digital Assistant
PDU	Protocol Data Units
PLC	Power Line Communication
PNP	Plug N Play
PPTP	Point-to-Point Tunneling Protocol

PVR	Personal Video Recorder
RDC	Remote Device Control
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request For Comments
RG	Residential Gateway
RMI	Remote Method Invocation
RMON	Remote Monitoring
RPC	Remote Procedure Call
RR	Resource Record
RSVP	Resource Reservation Setup Protocol
RTCP	Real Time Control Protocol
RTP	Real-Time Protocol
RTSP	Real Time Streaming Protocol
SA	Service Agent
SCP	Simple Control Protocol
SDP	Session Description Protocol
SDCP	Simple Device Control Protocol
SIP	Session Initiation Protocol
SLP	Service Location Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSDP	Simple Service Discovery Protocol
SSL	Secure Socket Layer
STB	Set-Top-Box
TCP	Transport Control Protocol
TSL	Transport Layer Security
TV	Television
UA	User Agent
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
URL	Uniform Resource Locater
USB	Universal Serial Bus
UWB	Ultra Wide Band
VACM	View-based Access Control Model
VESA	Video Electronics Standards Association
VHN	VESA Home Network
VPN	Virtual Private Networking
W3C	World Wide Web Consortium
WAN	Wide Area Network

WAP	Wireless Application Protocol
XML	eXtended Mark-up Language
Zeroconf	Zero Configuration Networking
8-VSB	8-level Vestigial Sideband, a kind of Radio Frequency modulation format

IMIT/LCN 2004-03

www.kth.se