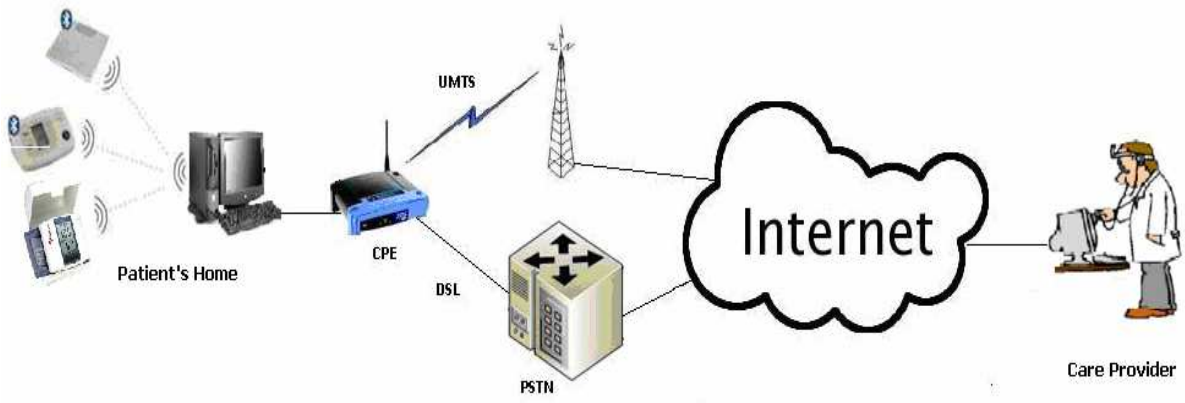
Technical Report, IDE0944, May 2009

Robust Home Care Access Network

Master's Thesis in Computer Systems Engineering

Sajid Sohail, Tariq Javid



School of Information Science, Computer and Electrical Engineering
Halmstad University

Robust Home Care Access Network

Master's Thesis in Computer Systems Engineering

School of Information Science, Computer and Electrical Engineering
Halmstad University
Box 823, S-301 18 Halmstad, Sweden

May 2009

Description of cover page picture: Remote patient monitoring communication model.

Preface

The work would have not been possible without the help and interest from several people those contributed immensely to the success on the thesis, morally and financially.

This Master's thesis is the final step of the Master of Science Degree at the School of Information Science, Computer and Electrical Engineering (IDE-section) at Halmstad University, Sweden. We would like to express our gratitude to our supervisor, Prof. Nicholas Wickström, for his enormously keen support and helpful suggestions throughout the whole interval of the project. Finally, we would like to thank our friends and families for their moral support during our thesis.

Sajid Sohail & Tariq Javid,
Halmstad University, May 2009.

Abstract

Critical networks e.g. telecare services, telemonitoring, are implemented to provide the information security and reliability that the end user desires, especially during an emergency. Unlike business carrier systems that are planned for the general public's use, critical communication systems are designed particularly for public protection and other serious communication situations. Availability and reliability of such networks is highly desirable. The following thesis works to compare and analyze a variety of communication access technologies to find out the best primary means of data transportation for health critical services and model reliable communication link by using redundancy. This study also provides an efficient failover mechanism to implement redundant links. This strategy is intended to provide the reliable communication and to protect the established communication link.

List of Figures

List of Tables

Table of Contents

1 Introduction

It is estimated that in 2051, 40% of the European population will be 65 years or older. It means keeping on this way, the percentage of people functioning in care services would need to be doubled, or even more, in the near future. The dilemma is that there is not that number of people in care and, even if there were it would not be easy to afford**.** To resolve this unsettling situation, there is a need to embrace and drive new ways of thinking and working to provide care for old and vulnerable people to assist them so that they could live independently and comfortably in their home environment much longer. The difficulties of transport in the big cities, the scarcity of hospital beds, and the increasing pressure on intensive care or emergency units, turn the telecare into an attractive solution. In telecare, the communication technology is used in conjunction with sensing technologies (for example, fall detector, movement detector, bed/chair occupancy sensor, gas detector, extreme temperature detector, infra red sensor, flood detector, smoke detector etc.) to provide a means of manually or automatically signalling a call of care/emergency to a remote base service centre, which can then send or arrange a suitable care response to the intended telecare service consumer. Telemedicine is the use of telecommunication technologies to provide medical information (ECG, heat beat, blood pressure, etc) and services (diagnostics, surgery, video conferencing, etc) remotely [1].

These life saving critical technologies are one of the fastest growing fields because of their swift, economic and effective service in the domain of remote health care services. The use of such applications is increasing rapidly and getting attention to be widely deployed in the field of medical and home care services. Often we encounter several instances of the remote monitoring of patients in hospitals or in homes. These services are also being used in very critical and life saving activities like diagnostics and surgery. In such highly critical medical routines, it is essential that networking applications must perform with the real time surgical precision otherwise the consequences could be fatal, both for patients and for the future of telecommunication technologies in the field of tele-health systems. For this, it is obligatory that the information signals must reach the end location with a high degree of reliability and predictability.

Such decisive applications require round-the-clock availability of services – this is one of the key parameters in determining the quality of a service. The supreme values of availability required or expected for such vital responses are very high - a typical domestic user in Western Europe would expect an availability of 99.98 %, while a commercial user, or mission critical application like Tele-care, which cannot tolerate any sort of inconvenience may require even better than 99.996%, and even up to 99.999% [2]. Such high levels of availability do not happen as you would expect, or by chance: they come as a result of an excellent system design and efficient maintenance procedures because no network, however robust, is 100% fail-proofs. Even systems designed with highly reliable hardware and software still have a chance of failure. Therefore, to achieve continuous availability of such critical communication networks, there must be in place some fall back strategies to make the system fault tolerant. This thesis work provides a comparative study of currently available access technologies, from which the best one can be chosen for such critical applications. The availability chapter suggests utilizing redundant

communication architecture to remove single point failure remedy from the system by ensuring alternate paths in the event of failure. This work also provides a design of CPE (Customer Premises Equipment), which gives an efficient failover mechanism without losing any data packet in the event of link failure detection.

1.1 Motivation

The number of the people suffering from chronic diseases who need constant care is increasing. This increase puts more pressure on medical facilities in the hospitals [3] [4]. Now, the hospitals are trying to discharge such patient earlier. Some surveillance systems are used to provide care afterwards. On the other side elderly people living in their homes that need personal monitoring system for their safety are also increasing. The major reason why this sort of work is interesting at all is that, nowadays the people are switching from PSTN to IP telephony services and IP networks, while there are no more PSTN solutions. PSTN networks have very good reliability and higher uptime as compare to IP networks. So in this transition to bridge the gap of uptime between PSTN an IP networks need to be cater in some way. Using the technical means in doing this is what about that his report is addressing.

1.2 Goal

As telecare services deals with life saving situations and will become more widely available in the future. That is why there is a corresponding need that these services should be as good, and as safe, as they are expected to be. The main intension is to maintain a reasonably high uptime for such critical services that require round-the-clock availability. However, here the problem is that communication may go down due to communication link failure, poor performance of the link or power outage of the system. Thus, the main objective of the thesis is to investigate what are the available technologies and how they can be used to resolve these challenges.

1.3 Limitations

In order to just focus the work some limitations are made that are given below:

1- The backbone network is considered fixed. This work only view from end user's perspective. So this is a solution for last mile. Therefore the only thing that can be done is to maximize the last mile working.
2- Bandwidth issue of the connections/links is not a matter of subject that is dealt in this report. It is assumed that the links have sufficient bandwidth to meet the requirements of the services.
3- It is obvious that the cost of any system as itself is a limitation. The cost of the system should not be high. So this work can not add more than a certain amount of extra cost on this sort of system.

1.4 Methodology

The approaches adopted in order to accomplish the objective of the projected thesis are as follows:

- A review of today's broadband access technologies e.g. wired broad band, terrestrial wireless broad band and satellite, is conducted. Then a comparative analysis of these broadband technologies was made to pick the two best technologies to implement the backup-mode mechanism, to propose a reliable, survivable and failsafe communication system for home care solutions.

- Based on the comparative analysis architecture is proposed where the reliability of the ongoing communication and the customer premises environment is emphasized.

2 Related Work

Telecommunication comprises infrastructure of telephone lines, data lines and cellular, which provide services like video audio and data. Infrastructures play an important role in the functioning of our society. This infrastructure facilitates us, and has a serious impact on the security, safety, health, economic well-being of citizens, and the effective functioning of governments. Failure of telecommunication infrastructure will cause coordination capabilities to be disabled, security problems and it would be hard to conduct the repair and recovery of other critical infrastructures (banking transactions, remote medical operations) which may malfunction due to accidents.

Telecommunication is considered a new and emerging area in telecare systems and telemedicine systems that have an important role in remotely caring for patients at home or in hospitals. In the last decade, engineers have not done enough work on telecare systems which gives survivable, reliable, scalable, and ubiquitous services. There was a telecare system based on GSM technology [5] which collected the data of patient and transferred it to the service provider via wireless GSM link. This system was not able to provide real time services (video audio) due to limited service of GSM. There is also another telecare system [6] based on 2G cellular system which cannot play a versatile role in remotely live video monitoring due to the limitation of 2G services.

A system named as “A mobile-phone based telecare system for the elderly” [7] does not provide live monitoring of patient. It only reads patient’s data (blood pressure, blood test, and static health picture) and stores in hard disk and then sends to control room via wireless system. These limitations are because of the lack of network infrastructure. This telecommunication system does not provide high quality connection, reliability of system and does not cope with failure.

The GPRS based system “Mobile Telemedicine System for Home Care and Patient monitoring” [8] relies on TCP protocol for reliability of communication. TCP communication is very slow because it uses an acknowledgment for every packet, which results in high latency. Consequently, this telecommunication system does not provide the real time service for home care, and can not cope with critical applications.

“High-quality mobile telemedicine system” [9] uses four lines of connection, 2 lines for CDMA 2000 and 2 lines from GPRS channels are aggregated in a single channel, and used for critical applications, especially in ambulances. If one channel is down, then 3 channels will work, but throughput will decrease. This telecommunication system is a very costly solution and used in emergency cases. This system can not be used for regular bases, like in the home for regular caring. 3G based telecare systems [10] [11] provide the real time (audio, video conferencing) services for patients; it is easy to monitor the patient remotely, but can not reliably support communication between patients and service providers.

3 Overview of Broadband Access Technologies

This chapter proposes a number of possible candidate access technologies that can be used as means of communication. A survey of these access technologies gives an overview of their strengths and weaknesses. This information helps to analyze them to find out the best technology.

3.1 DSL (Digital subscriber line)

DSL is one of several popular broadband internet connectivity options. DSL transmits over ordinary existing infrastructure of PSTN copper pair from the central office to the customer's house. Normal PSTN network communication uses the frequency range of 0-4 KHz, but DSL modem utilizes higher frequencies up to several MHz [12] in the copper wire, thus increases the utilization of caper channel by providing both data and voice services simultaneously, and without interfering each with other. The digital subscriber line family constitutes a number of different flavours of symmetric and asymmetric technologies:

- **SDSL** (Symmetrical Digital Subscriber Line)
- **ADSL** (Asymmetrical Digital Subscriber Line)
- **IDSL** (ISDN DSL)
- **HDSL** (High bit rate Digital Subscriber Line)
- **VDSL** (Very high bit-rate DSL)

These flavours have their own specifications (data rate, distance, etc) as shown in the Table 1 [13].

Technology	Down stream	Upstream	Distance in feet	Application
HDSL	1.544 - 2.048 Mbps	1.544 - 2.048 Mbps	12,000 (1 to 3 pairs)	Alike T1/E1
IDSL	144 kbps	144 kbps	18,000	Data Transmission
SDSL	144 kbps – 2 Mbps	144 kbps – 2 Mbps	15,000 to 22,000	Multiple Data transmission
ADSL	1.5 – 8 Mbps	32 – 800 kbps	9,000 - 18,000	Internet, video multimedia
VDSL	2.3 - 52 Mbps	1.6 – 26 Mbps	1000 to 4,500	Same as ADSL but more of it.

Table 1. Data rate of different DSL technologies

These are the maximum theoretical speed limitations of xDSL technologies which can only be achieved under the most ideal or sympathetic conditions.

3.1.1 Ideal conditions for DSL

Conditions are most encouraging with:

- Very short lines (typically <1km) in case of ADSL,
- The cables are in an excellent state of repair,
- Heavier gauge copper has been used in the cables,
- The absence of interference from other DSL services in the same cable,
- The absence of other interference sources.

DSL is a very clean, stable and effective way of getting bandwidth. Unlike cable that can clog up due to mass volumes of traffic DSL offers a sturdy, consistent stream of bandwidth. The closer you are to the so-called central office, the faster your DSL will run. Despite all of its benefits, broadband service performance over the DSL is influenced by a number of impairments [14] from which each must be addressed to improve the quality of service and manage the cross-impact between service types.

3.1.2 Performance limiting factors of DSL

These factors can be summarized as:

- Substandard loop plant such as bridged taps,
- Crosstalk from a nearby cable binder,
- Environmental factors like temperature changes and moisture,
- Poor premises wiring structure and interference from common noise sources such as AM radio, light dimmers, hair dryers, and fluorescent lights,
- Long loops (efficiency and reliability decrease as distance increases),
- The DSL services are not available everywhere,
- If online traffic is too heavy, then you may experience cut out from your internet connectivity.

The important issue is that there are always tradeoffs among performance, price and reliability. However, DSL is a low price choice for an internet “access and transport" method with a sufficiently acceptable reliability.

3.1.3 DSL services

DSL traffic is classified into a service flow, and each service flow has its own set of QoS parameters:

- Best effort flow
- Non-real-time polling service (NRTPS) flow
- Real-time polling service (RTPS) flow
- Unsolicited grant service (UGS) flow

- Unsolicited grant service with activity detection (UGS-AD) flow
- Downstream flow

A person who really needs high data rates can subscribe to it on a promising basis by paying extra money while those, mainly the home users, who do not have a need of high speeds can pay a lower cost.

3.2 Cable Technology

An alternative to ISDN and ADSL network for a fast Internet connection and data transfer is the use of a cable modem technology [15]. Cable modem network offers, relatively, a much higher bandwidth than tradition lines (PSTN). It could be a prevailing substitute to telephone lines. Speed of cable modem depends on its network architecture and traffic load. Most commonly, cable networks provide 27Mbps in the downstream direction that is shared by all users in the network. Only a few users can enjoy such high speeds, while most of the users receive only 1 to 3 Mbps. In the upstream direction speed can be up to 10 Mbps. An asymmetric cable modem scheme is the most common. The downstream channel has a much higher data rate than the upstream channel, because Internet applications are asymmetric in nature.

In current times, cable technology is delivering multiple services over a solo network [16] [17]. Internet access, high speed data transfer, video on demand, games and video conferencing are some of the applications motivating this tendency. Extremely fast internet access can be achieved at much longer distances (can be up to 100km in ideal environment) by using a cable modem. The range of higher data rates depends upon the conditions of the cable modem loop plant. A cable modem provides a permanent connection (i.e. always on) to browse the internet without the need to dial up every time because of its packet switched nature. As soon as the subscriber turns on his system, it detects its presence and start a new session by obtaining a dynamic IP [18].

3.2.1 Upstream downstream traffic

Upstream traffic (from the subscriber) and downstream traffic (to the subscriber) share the same coaxial cables. Downstream transmission from the head end is a typical broadcast. The same signal is sent to all users in the network. In upstream transmission, each subscriber is placing a different signal onto the network. The cable network is shared by all subscribers connected to it. This makes cable plant fundamentally different from a telephone network that dedicates a twisted pair line to each subscriber. Sharing access among multiple users gives rise to privacy and security problems. Being always on means it has a stable online presence that makes it trouble-free for hackers, crackers to breach into the system and cause devastation.

3.2.2 Cable standards

Two international standards [16] [19], as shown in Table 2, have emerged for cable modems and interactive set-top boxes as a result of battle between the USA and Europe for supporting the transmission of packets over cable networks.

1- **DOCSIS** (Data over Cable Service Interface Specification) was built-up in USA for cable modems.

2- **DVB/DAVIC** (Digital Video Broadcasting Project /Digital Audio Visual Council) was developed for set-top boxes and cable modems in Europe.

The major difference [20] between DVB/DAVIC and the DOCSIS standard is that the former standard uses fixed-length ATM cells for transport, instead of variable-length IP packets in case of DOCSIS. There is also a one more, called Euro DOCSIS, the only difference in this and the American one is of physical layer.

Feature	**Euro DOCSIS1.0/1.1**	**DVB-RCC**
Downstream Rates	Set-Top Box & Cable Modem In-Band: 38 Mbps to 52 Mbps (8MHz canalization)	Cable Modem In-band: 38 Mbps to 52 Mbps (8MHz channelization) Set-Top Box OOB: 1.544 Mbps to 3.088Mbps
Upstream Rates	QPSK: .320, .640, 1.280, 2.560 and 5.120 Mbps 16-QAM: .640, 1.280, 2.560, 5.120, 10.24 Mbps (5-65MHz)	Differential QPSK 256Kbps; 1.544 Mbps; 3.088 Mbps and 6.176Mbps (3.088Mbps is mandatory) (5-65MHz)
Performance	>80%bandwidth efficiency over mixed voice, data services at up to 10.24 Mbps in 3.2 MHz	>50-72% bandwidth efficiency at 3.088 Mbps in 2 MHz
Services	Internet access, high speed interactive Set-Top Box, voice over IP,SNMP	Internet access, low-speed interactive Set-Top Box, voice over IP,SNMP
Security	Good and strong hardware based baseline privacy and security	Encryption included as an option.

Table 2. DOCSIS vs DVB-RCC technical comparison

3.2.3 Disadvantages

Having considered all of its benefits, the main disadvantages of coax are as follows.

Problems with the deployment architecture: the bus topology, in which coax is deployed, is susceptible to congestion, noise, and security risks.

Bidirectional upgrade required: cable systems were designed for broadcasting, not for interactive communications. Before they can offer to the subscriber any form of two-way services, those networks have to be upgraded to bidirectional systems.

Line noise: the return path has some noise problems, and the end equipment requires added intelligence to take care of error control.

High installation costs: installation costs in the local environment are high.

Susceptible to damage from lightning strikes: coax may be damaged by lightning strikes. People who live in an area with a lot of lightning strikes must be wary because if that lightning is conducted by a coax, it could very well burn out the equipment at the end of it.

3.3 Broadband Satellite

If you are running a business or living in an area where you do not have fast DSL and cable, or have lack of access to such conventional broadband in that area. Then you have to look to the skies to receive broadband Internet, through satellite.

Satellite broadband employs a satellite in geostationary orbit [21] to provide internet service from the satellite to end user. Satellite Internet is a most expensive solution to obtain broadband Internet access, but in rural areas, it is only viable option in the absence of other access networks. The satellite industry's primary business was the delivery of television and concentrating on downlinks. Broadband, on the other hand, requires the use of bidirectional communication. Satellite broadband systems offer a flexible means with very wide geographical coverage to provide broadband access to all parts of a country, including the most inaccessible rural districts. Satellites are providing two types of services:

- One-way systems that provide broadband capability for downloads only
- Two-way systems provide broadband services in both upstream and downstream

One-way systems are more cost effective solutions, but consumers must have to use terrestrial access lines (modem) for uploading data and the satellite link just for downloading. However, there is an extra cost attached to using the modem cable for uploads. More expensive, but closer to the terrestrial broadband, offers 2 ways systems are increasingly becoming the norm, and their capability varies depending on the quality of the offer. Finally, in some cases, satellite is used in combination with fixed wireless access technology to deliver broadband to communities. The major European satellite does not provide broadband over satellite. In fact, satellite providers are still not seeing broadband as a mainstream market for them, and they prefer to concentrate on their traditional markets.

Satellite broadband speed clearly does not come close to DSL or cable, but satellites give facility to isolated areas to have almost the same level of service as heavily populated areas. Satellite service is primarily complementary to DSL and cable by serving areas that are underserved, or

not served at all, by these technologies. Broadband satellite is primarily serving consumers in rural, and other hard-to-reach areas, that do not have terrestrial broadband services, although the data rates are lower than that of DSL and cable. One of the main advantages of satellite broadband is that it can be installed at very short notice to individual homes located in remote areas, or areas where the typology does not allow terrestrial access. Satellite can be a solution when used in combination with fixed wireless access to bring broadband to small communities and the business environment.

The European Commission's broadband penetration figures indicate that satellite broadband represents 1%, or less, of the overall broadband market. Another down side is that satellite is more expensive, particularly when getting started. Installation fees and monthly rates vary widely. Just like cable broadband customers, satellite users compete with each other for limited bandwidth. As more people logon to, and use, the system, everyone's overall performance slows down. To address this problem, satellite providers have fair-access policies that can cut consumer off if he uses more than allocated portion of bandwidth. A good design of traffic and resource management schemes, it is possible to guarantee the target QoS to different multimedia traffic classes, while optimally utilizing the satellite signalling bandwidth.

3.3.1 Weather and distance

For the better delivery of services, satellite dishes need clear views of the skies. Connection outages are more often in case of heavy rainstorms and other severe weather. Also, because the Internet signal has to travel from the client's dish to a satellite, there is a built-in latency or delay — typically a quarter of a second. This latency can be reduced by using LEO orbit satellites and different QoS provisioning protocols [22]. Usually, latency is not a problem when you are surfing Web pages, but can affect real time applications, such as VoIP and real-time interactive gaming.

3.3.2 Market trend

From a marketing point of view, satellite does not have the support and/or commitment from the major operators and ISPs like DSL and cable. Only in some cases satellite is provided by major operators but it is only targeted in areas where they do not have DSL or cable coverage. Continuous, rapid mass acceptance of DSL and cable technologies will further limit the potential markets for broadband satellite. However, if you are running a small business in an area where these technologies are not an option, then satellite may give you an improved speed, to some extent.

3.4 UMTS (Universal mobile telephone service)

UMTS is a 3rd generation cellular technology, which provides data speeds up to 2 Mbps and installation penetration rate is 80% [23]**.** UMTS was developed and standardized by the European Telecommunications Standard Institute within the ITU's IMT-2000 framework. This technology provides very high-speed multimedia services, such as full motion video, Internet access and videoconferencing.

UMTS gives high data rates and has a comparatively low cost for data transmission. Due to these improved technology features, UMTS is estimated to revolutionize the current state of the art in mobile services and applications. This is even more so because the handsets equipped with large-size, high resolution displays are currently being developed.

A key challenge for the UMTS infrastructure is to carry different types of applications on the same medium, when meeting the QoS objectives. To fulfill the requirements of the user, UMTS provides a variety of QoS service classes [24].

3.4.1 UMTS service classes

UMTS provides four service classes. The classification is based on individual delay, bit rate, bit error rate, and traffic handling priority requirements. The four different classes are defined as

1- **Conversational class:** this class supports conversational real-time applications such as video telephony. Conversational class services can be supported by fixed resource allocation in the network.

2- **Streaming class:** this class is meant for streaming media applications e.g. video downloading. In this class, due to application level buffering, a certain amount of delay variation is tolerable. Streaming class service is a variant of the constant bit rate and real-time variable bit rate services of ATM.

3- **Interactive class:** is appropriate for services requiring assured throughput. To get better response times for this class, a higher scheduling priority should be applied as compared to the background class, and traffic flow prioritization is considered important within this service class. Some examples are e-commerce, ERP, and interactive Web.

4-**Background class:** this class used for traditional best-effort services such as background download of emails and files, calendar applications etc. This type of traffic has the lowest priority between all the classes [25] [26].

3.4.2 Market trend and threats

According to market analysis UMTS can be used for e-mail applications, mobile payment systems, mobile shopping, mobile online banking and health care systems. Many mobile operators and banks have begun collaborating to develop these mobile banking, payment and shopping applications for their future UMTS customers. These applications are security-critical, particularly with respect to the confidentiality and integrity protection authenticity of the data traffic, as well as authenticity of the user. The security of different applications depends on the security of the mobile communication system. UMTS suffers from many security weaknesses; UMTS was designed to be secure against the known GSM attacks but UMTS faces some threats e.g. man-in-the-middle attack, eavesdropping, de-registration spoofing and location update spoofing. Passive identity catching and active identity catching have solution of these threats [27].

3.5 WiMax (Worldwide interoperability for microwave access)

WiMax aims to provide consumer and business wireless broadband services on the scale of Metropolitan Area Network (MAN). This standard was approved in jun.2005 for the latest 802.16 standard for fixed wireless access, known as IEEE 802.16-2004 using frequency ranges between 10 GHz and 66 GHz. In December 2005 another flavour of WiMax was introduced as IEEE 802.16e-2005, using frequency ranges between 2 GHz and 11 GHz. WiMax is used for moving devices such as mobile, lap top etc.

WiMax technology provides wide variety of applications, such as serving as a backbone for 802.11 hotspots for connecting to the Internet**.** Users can also connect mobile devices and handsets directly to WiMax base stations without using 802.11, and can get a range of 5 to 6 miles.

In rural areas and unwired countries, this technology can also provide fast and cheap broadband access to markets that lack infrastructure. Currently, numerous companies offer proprietary solutions for wireless broadband access, many of which are costly because they use chipsets from contiguous technologies, such as 802.11.

3.5.1 WiMax service classes

WiMax supports multimedia applications, such as voice over IP, video conference, online gaming and critical applications. To support different kind of traffic, quality of service provides different traffic classes [28]. Unsolicited grant service (UGS): This type of service supports the real time traffic, like voice, video and real time transmission. Real time polling service (rtPS): this type of service supports the video on demand, MPEG video and voice over IP. Non real time polling service (nrtPS): this supports a standard internet traffic that requires high throughput, and traffic that requires variable-size data grants on a regular basis, such as high-bandwidth FTP. Best effort (BE): this supports standard internet traffic, such as instant messaging, e-mails, web browsing.

3.5.2 Threats to WiMax

WiMax has to face some threats [29] [30] like:

Passive threats: in this type of attack, an unauthorized party gains access to an asset and observes a message and sees the pattern of communication at network level between two communication parties. Passive threats attack may be eavesdropping, traffic analysis etc.

Active threats: An intruder performs modifications of traffic (message, data stream, or a file). The intruders access the network and behave like authorized users and thereby achieve certain unauthorized privileges**.** Active threats comprise: denial of-service (DoS) message modification, replay and masquerading.

3.6 Comparison of WiMax and UMTS

3G system is a universal digital system which provides different types of services. It integrates diversiform technology functions in mobile communication networks which include cordless, and

cellular. 3G system provides voice and data services through mobile phones. UMTS infrastructure is mostly available in all Europe and rest of world because the operators of GSM are the operators of UMTS. For this reason, the coverage area of UMTS is greater than WiMax. UMTS operators have also using a profitable business model and longer term practice about cellular communication business.

WiMax is a new technology, a replacement of DSL technology, but does not replace UMTS directly in high density traffic areas especially in big cities [31] [32]. WiMax is focusing on high-speed data transmission, and supports a wide range of terminal equipment like laptops and PDA. WiMax has some advantages to 3G, like high data rate and transmission range. The penetration rate of UMTS is greater than WiMax. Currently, WiMax has no widely spread infrastructures. There is only one country, Pakistan, where WiMax is deployed widely and it is commercially available in more than 20 cities. So, UMTS is a more dominant technology than WiMax from the market perspective, and the service's availability. In the future, if the WiMax gets the acceptance from the market, then WiMax will surely master the all-wireless technologies and take over the market due its higher data services potential.

4 Analysis of Access Technologies

The comparative study, given in Table 3, of broadband technologies provides a good insight into the technical considerations of high speed home and small business networks. It is now well known that the fixed land line broad band access technologies (DSL, Cable) have much faster speed and capability to transmit a much larger amounts of data over the network than wireless broadband technologies(UMTS, WiMax, Satellite) and with greater reliability. Within the domain of wired broadband, DSL has the upper hand over cable in terms of the dedicated nature of its link, rather than a shared link as in cable, that makes it possible to better implement QoS and Security services. The other advantage is that DSL shares almost 70% of broadband subscribers all around the world while cable has only about 20% of the share which DSL the primary choice for broadband connectivity.

Compare to wired, wireless broadband access networks (UMTS, WiMax, and Satellite) have lower capability to transmit data, but they have an edge of delivering the broadband services at much greater distances than wired. Among the wireless technologies, WiMax is the one that has the highest proficiency to carry data much faster and at longer distances. But its infrastructure is emerging and is not widely available, unlike 3G. UMTS is evolving to be widely available, according to forecast and news. By the end of 2010, around 60-70 percent people of Europe will have the access of UMTS. Sweden has the best 3G system, and has almost 85% geographical coverage. Satellite broadband provides the services everywhere even in those locations which are hard to reach for the terrestrial broadband networks.

But the major problem with it is the long propagation delays, which make it less attractive for the delivery of real-time services, especially the voice conferencing, which does not tolerate long delays. As a result of comparative studies of these broadband technologies, there are the following interesting areas to pursue further studies:

- Continue this comparative analysis of these broadband offering technologies.
- To increase the availability and reliability, UMTS and DSL networks can be used by exploiting the redundancy of access links. One line (DSL) as a primary connection and other (UMTS) as a backup link. These can be used together only in those areas where they live together. Mostly, they co-exist in residential and suburban locations. It is hard to find them in rural areas because of long local loop, worse geographical surroundings and distance limiting factors of DSL.
- The other option is to use satellite and UMTS. These together provide a solo solution as hole for both metropolitan and widely dispersed rural areas, which are difficult to reach with traditional wire line broadband access networks, in order to achieve the ubiquitous, fail safe connectivity of the communication link.

Technology	Data Speed	Distance	Qos Level	Cost (California statistics, February 1, 2005)	Services Availability	Reliability	Limitations	Advantages
EDGE	473 kbps	35km	Very Low		Available	High	Limited data rate	
UMTS	7.2 Mbps	35km	High	71$ P.M	Available	High	Little bit Costly	Low deployment costs and widespread access
WiMAx	10 - 70 Mbps	2 - 4 Km NLOS 5 -30 Km LOS	Medium	71$ P.M	Under deploy	Medium	NLOS 1km-2km, spectrum availability, higher bandwidth and long range standards under experiment, expensive dedicated services licensed.	Give high data rate
DSL	8 - 50 Mbps	5 - 5 Km	Very High	15$ - 80$ P. M	Available	Very High	Distance sensitive transmission	Broadly available and reasonably affordable; leading platform for broadband
Cable	30 Mbps	2 Km	Medium	20$ - 50$ P.M	Available	Medium	Shared medium and securities problems. Limited future bandwidth; not widely deployed to business customers	urban availability and relatively affordable
Satellite	155 Mbps down	Every where	Very Low	50$ - 100$ P.M	Available	Very Low		Cover all areas

Table 3. Comparison of access technologies

Although these two (UMTS and satellite) provide the broadband services at much larger areas, this combination has its own pros and cons. Both networks use the wireless link to transmit data that have its own strengths and weaknesses. Both are vulnerable to the bad weather conditions like heavy rain, thunder storms and lightning storms etc. It means that if any application is caught in these conditions, then it is obviously going to face poor services, or lose connectivity. The idea of achieving reliability by using two unreliable technologies is not sustainable for the implementation of mission critical, or life saving, applications.

The combination of DSL and UMTS is more robust against the failures due to the diverse nature of its alternate paths. They can cope better with the critical situations than other access networks. It will be a better choice to select DSL and UMTS closure to pursue further studies because it provides much better reliability and is less vulnerable to failures.

4.1 UMTS in Support to ADSL

For a long time, ADSL broadband technology has been serving as the root means for data transmission. ADSL broadband connection provides a mature technology. Its dominance in the data communication market was due to the lack of competitive alternatives, but the inventions brought new conventional and unconventional communication means, which can be used as an alternate to ADSL

From technological perspectives, wireless technology UMTS has gained a strong enough prevalence and stands as a possible choice, or an alternative to, ADSL broadband with respect to high data transfer, encouraging costs and widespread accessibility. Now it is no more a matter of "either/or" for the companies who want to use these access technologies. Consequently, UMTS is proving to be more of a complement to ADSL broadband. It can be employed to meet new, challenging scenarios in data transfer.

4.1.1 UMTS as a complement to ADSL broadband

In many fields of health care, and other conventional businesses of today, connecting locations to each other through the internet has become very important and, in the coming years, there will be a progressive expansion in connectivity. The objective of connectivity is not just restricted to accessing shared data from different sites. Health services, community services and security services are going to be digitalized. Also the trade is heading towards worldwide e-payment. The basis for all of this is internet technology. This type of life saving and financially critical applications can be leveraged, without interruption, by providing UMTS backup. Thus, significant data losses and critical services failures can be avoided due to possible disruptions.

In case of backup solutions, it is very easy and rapid to setup and deploy a connection via UMTS as a secondary access link. When the primary connection fails, an alternative connection to the network is automatically set up via UMTS, making the network access uninterrupted. UMTS has the capability to provide IP based services, at data rates of up to 7.2 Mbps. It is greatly faster than the widespread ISDN backup. UMTS services have a modest disparity in speed compared to the ADSL broadband connection.

The backup feature becomes particularly appealing when taking into account the separation of voice and data services. If an organization uses an IP bit stream access, then it can not use an ISDN line as a backup connection in case of primary data-connection failure.

As an option of backup connection for site coupling, UMTS is a better choice than the conventional alternative, ISDN, in terms of significantly high data rates and low prices. Moreover, it is considerably less prone to breakdown as there are no cables, which are at danger from construction works because, even if a site has both DSL and ISDN connection, both links can be affected if the wire is damaged. To repair underground cables is a matter of days rather than hours; this kind of situation is a serious danger to the survival of the mission critical applications. To avoid such threats, UMTS access links can be employed for absolute independence from the physical medium of the cable.

A backup solution via UMTS will use a suitable data package that only charges money when the UMTS link will actually be exercised. The mounting fame of UMTS communication is expected to make further price cutbacks in future.

4.1.2 UMTS an alternate to DSL broadband

As the time passes, the prices of wireless services are going down. Various mobile service providers have cut down UMTS data tariffs dramatically. Some UMTS packages have very reasonable rates that compare well with traditional DSL broadband packages as shown in Figure 1 [33]. UMTS offerings can generate significant investments, depending on the application.

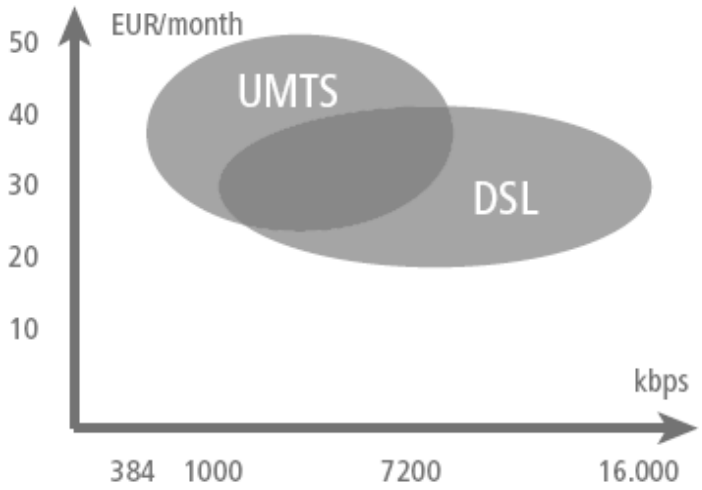


Figure 1. DSL, UMTS cost evaluation

In emergency and disaster situations, portable control capability of UMTS allows moving from vulnerable to safe environment without the loss of service availability.

5 Link Availability and Redundancy

This chapter gives an insight to the concept of availability and its importance .Further it delineates different redundant schemes and their implementation to improve the availability of networked services.

5.1 Why availability is desirable?

The IP packet based communication systems are getting more and more attentions as being a mission-critical application for the provision of e-health services and other tele-businesses in today's global infrastructure. Such critical systems are produced to supply the information security and reliability that an end user requires, particularly during an emergency. Unlike business-related systems, which are planned for the common public's use, critical communication systems are designed especially for public safety and other critical communication circumstances. Loss of connection connectivity in such life-saving applications cannot be tolerated very much because it may result in loss of life. The loss of access to real-time information on a patient's medical diagnostics, connectivity to remote patient monitoring applications and other crisis management services further adds to losses by decreasing efficiency and medical worker's productivity. Serious applications require around-the-clock network reliability and availability.

5.2 How availability is determined?

Availability, as given in Table 4, typically measures the percentage of time that a system is operational and not failing. An objective for critical communication systems is to attain 99.999 percent availability. This is the uptime during which a system, or a part of system, will always work. How much downtime is tolerable depends on the nature of applications and revenue potential.

Availability	Yearly DownTime
90%	**876 Hours**
99%	**87 Hours, 36 Minutes**
99.9%	**8 Hours, 45 Minutes**
99.99%	**52 minutes, 33 Seconds**
99.999%	**5 Minutes, 15 Seconds**

Table 4. Availability evaluation and expected downtime

Availability of a system is the most demanding requirement from the perspectives of end users. Particularly in crisis management systems, if a user calls to ask for emergency services, how probable that call will be successful is the main concern of the end user. However, reliability is a key requirement in ensuring system availability. Two different measures are used to quantify reliability:

• **MTBF (**Mean Time between Failure), it is the average time span from an initial fault free working state to a failure.

• **MTTR** (Mean Time to Repair), it is the average time span taken to identify a malfunction and fix it. Availability is then defined as [34]:

Availability = MTBF / (MTBF + MTTR)

This illustrates that availability can be enhanced by either increasing MTBF, or by decreasing MTTR. Mean time between failure of the components can be improved by employing the reliability engineering techniques [35] [36] [37] [38] during their design and manufacturing process. Thus, using components with enhanced reliability can ensure the overall system availability and as well as minimize the chance of a system failure. It is impossible to design a system that never fails. Therefore another significant factor is maintainability or how swiftly a component can be restored or repaired once it has gone down. So reducing MTTR will boost availability.

5.3 Redundancy

Redundancy means an efficient duplication of critical parts or resources of the system to reduce the single point failure. Alternative circuits, equipment or components, are installed so that this methodology builds up a resilient system that has the adequate capability of immunity to failure events. The level and type of redundancy employed determines the level of functionality preserved, and the number and type of the failures likely to happen.

5.3.1 Why redundancy is needed?

It is very much clear from the studies that no network or technology, however robust, is 100% fail proof. Even after carefully designing a system with highly reliable components, there is still an inevitable chance of failure. This demands that there should be an in-built fault tolerance capability of the system to ensure maximum availability for critical communication systems. This capability of fault tolerance makes the system able to offer services continuously, even in the presence of faults. Fault tolerance of a communication link can be achieved by a combination of software and redundant elements of the link. A redundant link to the services insures a system against its downtimes and the consequent losses. As the life protecting health industry is going to be increasingly dependent on to the digital IP access networks for remote monitoring, diagnostics and other mission-critical applications, there is a corresponding need for a backup strategy to ensure full time connectivity against the event of a failure. This backup mechanism needs redundancy.

5.3.2 How redundant links effects availability?

In the past times, IP-based network services were suffering to achieve the high reliability standards associated with real-time network applications. However developments in network hardware, software and inbuilt redundant architecture have made it possible to achieve high network availability goals such like 99.999% uptime in the core of IP networks. But the last mile is still at the 99.9 % uptime that puts a limit on the end to end availability [39] [40]. This last mile availability factor can be improved by employing redundant links as it is elaborated below along with Figure 2 and 3. The calculations made below based on the following assumptions:

1- Availability of core networked is assumed to be 99.999%

2- Availability of last mile link is assumed to be 99.9%

3- Both the last mile links in case 2 are completely independent from each other i.e. the causes of failures to one link will not affect the connectivity of other link.

Case- 1 IP network availability without redundancy

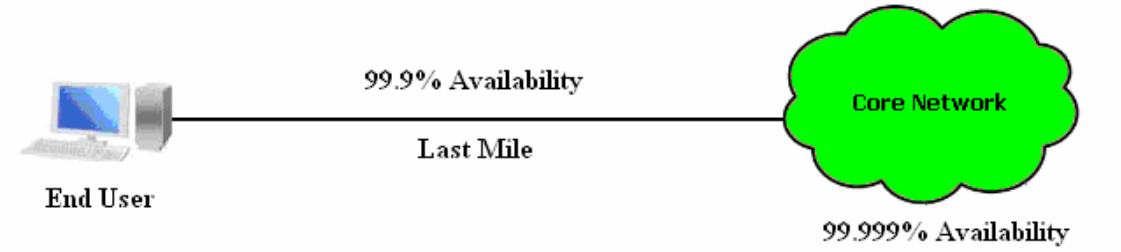


Figure 2. Single Link Last Mile, network infrastructure

The total infrastructure availability percentage can be calculated as:
Availability = Last Mile * Core Network
Calculation = 0.999 * 0.99999 = 0.99899
Total Infrastructure Availability = 99.899%

The total infrastructure down time can be calculated as:
Down Time= Number of Hours in a year - [(Number Hours in a year) * Total Availability]
Calculation = 8760 – [8760 * 0.99899]
Total infrastructure Down Time = 8 hours 50 minutes 51 seconds/ year

Case- 2 IP network availability using last mile link redundancy

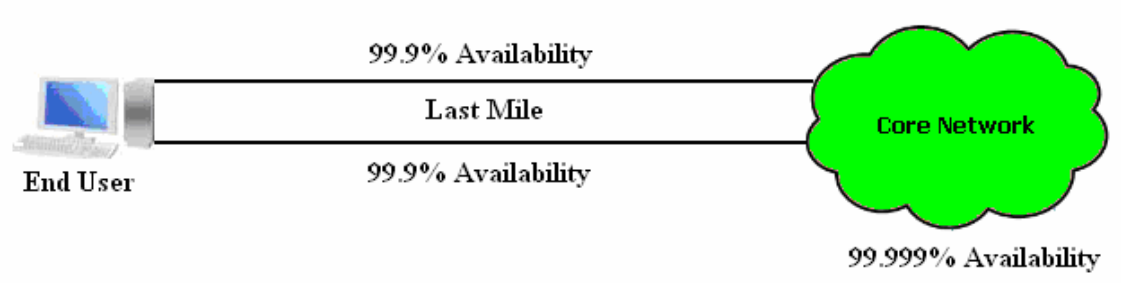


Figure 3. Redundant Dual Link Last Mile network infrastructure

The last mile availability percentage is calculated as:

Last Mile Availability = 1 - ((1-0.999)*(1-0.999)) = 0.999999
Last Mile Availability = 99.999%

With the extra link availability provided for the last mile, the total infrastructure availability percentage can be calculated as:

Availability = Last Mile * Core Network
Calculation = 0.99999 * 0.99999 = 0.99998
Total Infrastructure Availability = 99.998%

Down Time = Number of Hours in a year - [(Number Hours in a year) * Total Availability]
Calculation = 8760 – [8760 * 0.99998]
Total infrastructure Down Time = 10 minutes 30 seconds / year

So by setting up an additional path in the last mile, the over all availability of the system has improved from 99.899% to 99.998% by a factor of 0.099% availability. While the Down Time of system decreases by 8 hours, 40 minutes and 31 seconds. It means 98% Down Time is decreased by using redundancy.

5.4 Implementation of redundancy

There are two ways to implement the redundancy: Active-Active redundancy and Active-Standby redundancy [41].

5.4.1 Active-Standby redundancy

In Active-Standby redundancy as shown in Figure 2, a substitute means is supplied to perform the function but remains out-of-action until required. Standby components are only switched to be operational upon the failure of the primary operating components. Active-Standby redundancy suffers from a shortcoming that there is an inevitable period of disruption, during the switch over

between the failure occurring and the redundant standby unit becoming operational. Such schemes suffer from the lack of confidence building measures for today's decisive systems in modern commercial and industrial environments.

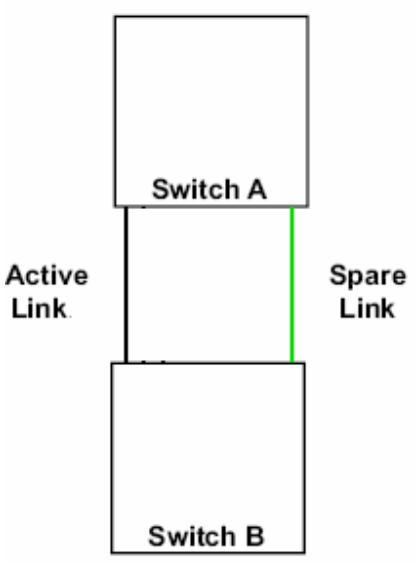


Figure 4. Active-Standby redundancy

5.4.2 Active-Active or parallel redundancy

Contrary to Active-Standby redundancy mechanisms, all redundant links are in the operational state in Active-Active redundancy as in Figure 3, and work simultaneously instead of being switched in the failure event. A Variety of approaches can be taken up to implement Active-active redundancy. Commonly, the most apparent approach is to use two matching links, each having the ability to carry the accumulated load. So, that if one link fails then the other link will take the responsibility to serve. This is known as 1+1 redundancy. The other possible way that can be adopted is to distribute the load among a number of identical links. Each link is able to carry only a part of the load. This is called N+1 redundancy. Active-Active redundancy best fits to the real-time applications because it does not have any interruption.

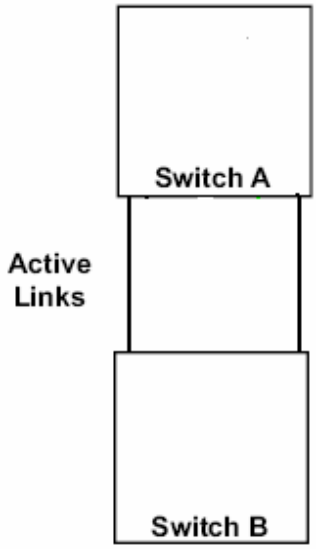


Figure 5. Active-Active redundancy

5.4.3 Architectural redundancy

In the analysis of different access technologies, it has been concluded that, relatively, there are two best reliable communication access technologies: UMTS and DSL. Keeping these technologies, there are the following three ways to secure a communication path by exploiting the redundant link methodology. All these flavors of redundancy have their own pros and cons.

1- Two identical links can be leased from an ISP, i.e. two DSL connections from ISPs.

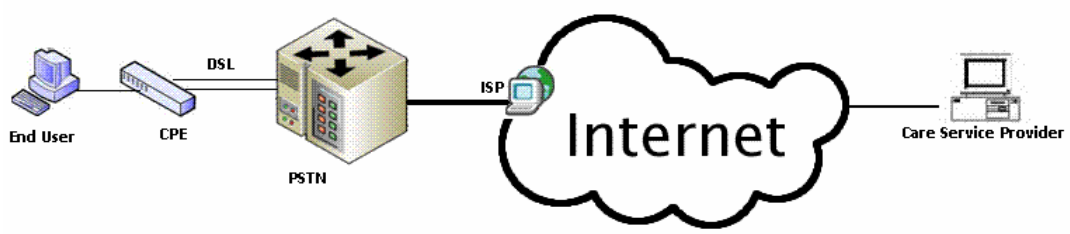


Figure 6. Redundant links from same ISPs

This scenario provides two identical DSL connections from the same service provider. One connection acts as a primary connection and other as a backup connection. This sort of redundant connections has its own limits and edges which are given below:

- PSTN exchanges have limited number of lines. If there are a large number of potential users, then it is not possible to provide multiple DSL connections for every client.
- In case of active-standby backup, one connection will be active while the other will remain idle until the primary connection failure. This is the wastage of resources instead of efficient utilization of communication means.
- As DSL lines are underground, they may be affected by construction work. If that happens, then our both connections will fail, resulting in the total system outage.
- PSTN network is designed to be robust against failure, but still there is a chance of failure. If the PSTN exchange goes down, then both connections will have failed and our system will not work.
- Demand for multiple lines increases the volume of public network PSTN, which raises its cost.
- Due to the identical nature, both lines can be configured into on active-active setup, in which the spare line could actually be set into functional, as opposed to just being idle. Traffic is shared between the two lines via the load balancing mechanism [42]. In the situation when one line goes down, then the entire traffic is diverted to the remaining active line.
- Combining both lines can benefit from higher data capacity and speedy data transfer.

2- Two links can be leased from two different ISPs i.e. two DSL connections from Two Different ISPs.

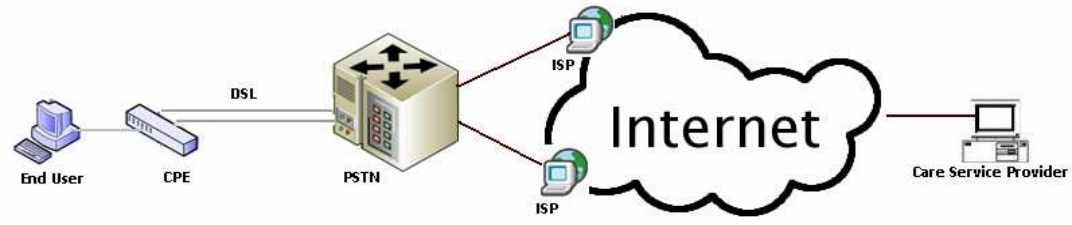


Figure 7. Identical redundant links from different ISPs

This scenario experiences almost the same bounds and advantages as these were examined in the above case. The only advantage to this scheme is that it provides us with an additional redundancy at ISP level. It eliminates the chance of communication failure due to the breach of ISP, but is still vulnerable to total failure if the local PSTN central office goes down. Redundancy can also be achieved at the level of PSTN central office, but only those clients may use this facility that will be at the border of the local loop.

Such a design cannot get the advantage of bonding both lines, because both are diverse connections from two different ISPs.

3- Two different links can be used from two different carriers, i.e. DSL and UMTS, which uses PSTN and terrestrial wireless networks respectively.

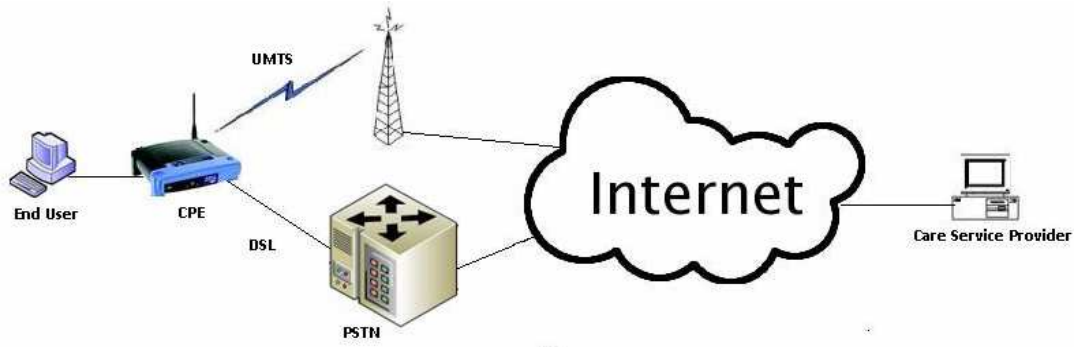


Figure 8. Redundant links from heterogeneous networks

This communication strategy provides us almost a complete redundant communication link, because it makes use of two connections from two diverse networks which have their own communication patterns, policies and infrastructure, completely independent of each other. One is a 3G wireless communication link, while other will be the traditional DSL connection. Using these diverse connections as alternatives to each other to provide backup communication path has its own propositions, which are stated below:

- It provides absolute complete redundant communication paths, and removes the single pint of failure on PSTN central office and ISP. It provides two complete independent links which significantly improves the fault tolerance capability of our communication scheme.
- It removes the need for extra cables.
- It could not be possible to implement active-active backup methodology because of the diverse nature of both links. The only possible backup strategy is the active-standby scheme, where one link operates as an active link while the other remains idle till the one link is failed.
- It maximizes the utilization of resources because the wireless link only consumes the resources when it will be actually in the operational state. So configuring DSL as active and wireless link as standby recourses can be better utilized. This scheme provides another key advantage of minimising the cost of system.
- This scheme also reduces the risk of cable damage by using the backup wireless link.
- It also reduces the time to restore the link because wireless links are easy to deploy, repair and configure. The land line communication links take more time to be functional, even days or weeks, if underground cable has damaged.

So for the studies have given much knowledge about the reliability of different access networks, which architectural redundancy is best and what implementations are. Therefore, in this thesis, to enhance the reliability and availability of communication services, two links of diverse nature will be deployed: DSL access link and the other is wireless (UMTS) access link. To implement it, the best choice is to use the Active-Standby redundancy approach instead of Active-Active redundancy. Active-Active redundancy is not achievable for a reason such as that both links are not identical and use different nature of transmission mediums for data carriage. For example, both links have different sizes of the packet and transmission delay. This diverse behaviour does not allow them to operate simultaneously, but they can work well with Active-Standby approach.

It is known that the Active-Standby technique has an inevitable interruption time during switching from the failed primary link to the back-up link. This deficiency heightens the idea to use an intelligent, and fast, switchover scheme to make the switchover delay as minimal as possible to reduce packet loss, so that it could become acceptable to employ it for real-time critical services. The next chapter talks about switchover mechanism in detail.

6 Proposed Design

So for the studies have figured out that, to make the communication system acceptably reliable, it is necessary to employ redundant communication links. Preferably, these links should belong to two complementary nature technologies e.g. UMTS and DSL. Due to their diverse nature and different characteristics both links follow absolutely different network infrastructures, as shown in Figure 7. This makes it ensure that the failure to any link will not affect the connectivity of other links. Currently, the equipments [43] are available that supports diverse links redundancy with the functionality of failover from primary link to backup link. Also, the commercially available Cisco routers can be equipped with both the wired and wireless links, e.g. ADSL and UMTS (3G Wireless WAN HWICs), to provide diverse redundant links. The study of Cisco routers equipped with wireless 3G card further discloses that these routers can only use the following failover mechanisms [44]:

1- Dialer Watch,

2- Static Floating Route,

3- Backup Interface.

All these mechanisms have the problem that they offer failover when the total link failure is reported and they have no capability to switch the link when its performance is being deteriorated. The analysis of such off-the-shelf solutions reveals that they are basically designed for general purpose high availability and they does not feasibly fit in the solution for specific home telecare applications. Because the existing equipment has no capability of automatically notifying the care service provider that which link is currently being used whether it is wired or wireless, and also does not provide the monitoring of backup power. Another key disadvantage of using existing systems is that they are very expensive. All these factors motivate the drive for a new system which constitutes only those components which are particularly necessary to resolve all these problems as shown in the Figure 7.

6.1 Customer Premises Equipment

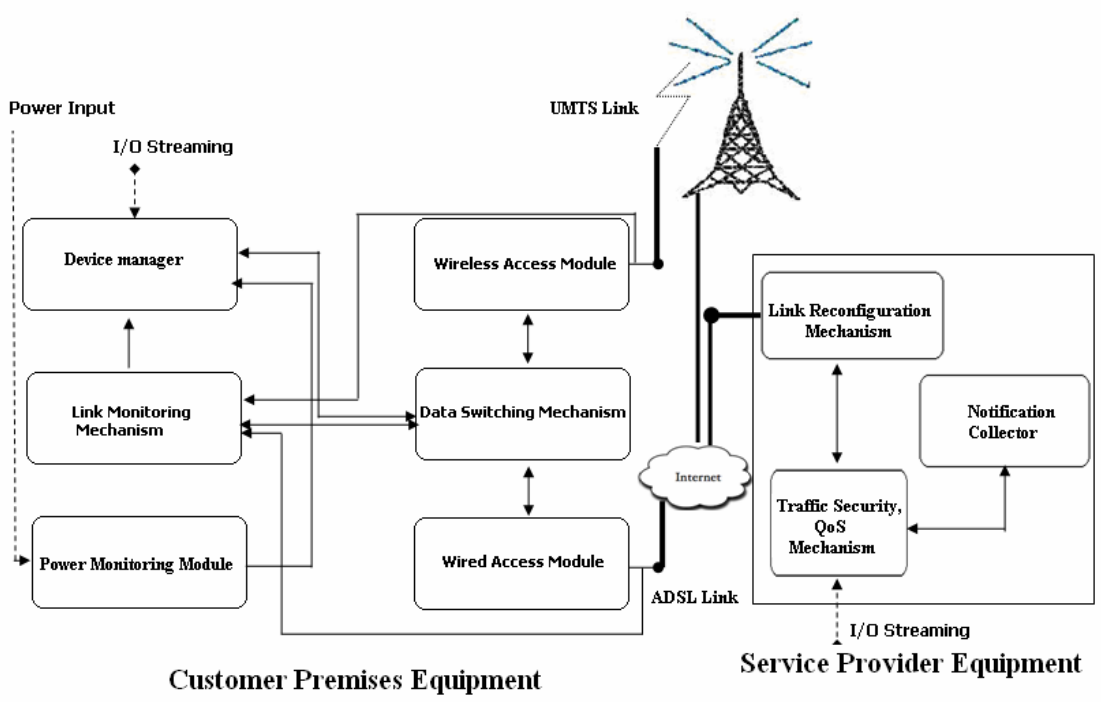


Figure 9. Customer's premises equipment design

The Figure 7 depicts the blue print of our proposed system to achieve a reliable and highly available broadband access link. This model is designed by having inspiration from the architecture of ALCATEL equipment that was also aiming to improve the availability of broadband connections [45]. Although both the designs look very similar to each other but they are different in their functionality. The ALCATEL system design provides a more general solution to improve availability. It has no capability to send the critical messages about the system status that helps to mitigate the risks.

The customers' premises equipment is connected with the service provider through two different access networks as wired access network and a wireless access network. Wired access network uses ADSL services to carry out the traffic, and wireless access network uses UMTS services to build a reliable connection between the home customer and the care provider. As claimed earlier, ADSL is more reliable and robust than the UMTS, because it has very power full and superior characteristics, such as high throughput, low cost per bit, low packet loss, low latency (packet delay) and small jitter value as compared to the UMTS. In accordance with these highly valued features, normally the wired link is given the priority over wireless link and selected as the default link to establish a connection between two parties.

The availability of the two access links, one as a primary link and the other as secondary link (backup link), enables the customer's premises equipment to restore the communication path in

case of ADSL link failure, by setting up a connection through UMTS. In this way, the system makes sure of the preservation of the connection in the event of any single point failure.

The availability of the two access links, one as a primary link and the other as secondary link (backup link), enables the customer's premises equipment to restore the communication path in case of ADSL link failure, by setting up a connection through UMTS. In this way, the system makes sure of the preservation of the connection in the event of any single point failure.

During the normal operation, the traffic will pass through the default ADSL link. Under the conditions of failure, the customer's premises equipment automatically redirects data flow to the backup UMTS link. The switch over of traffic to wireless back up link is very swift because the wireless connection is already established through signaling, the same as our mobile cells. The following Figure 8 illustrates the flow of above system.

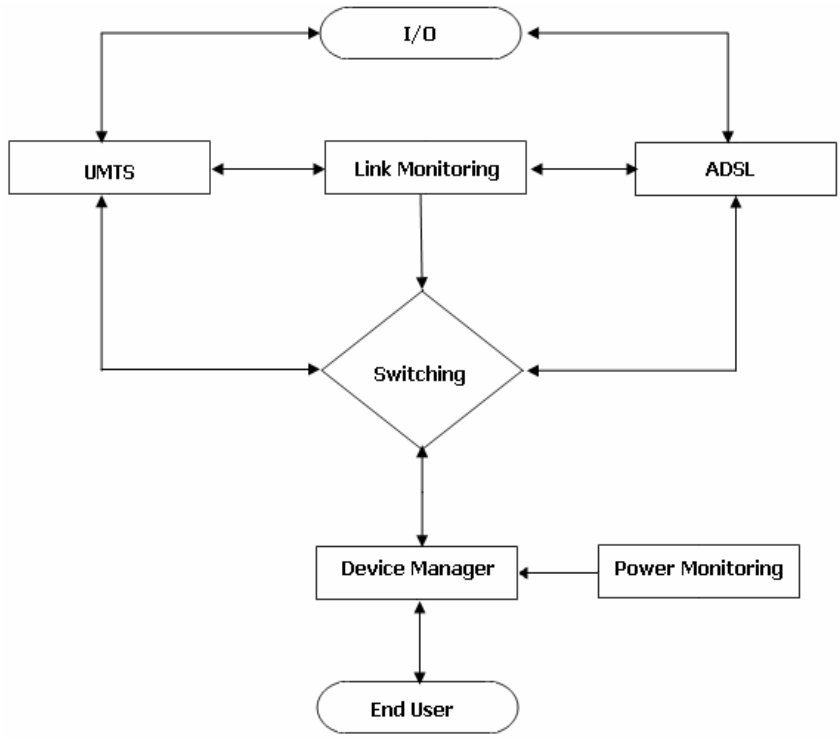


Figure 10. Flow diagram of CPE

6.1.1 Failover mechanism

The failover mechanism comprises of the following mechanisms:

- Link Monitoring,
- Switching Mechanism.

Link monitoring mechanism

The link monitoring mechanism is the heart of failover mechanism. It keeps its eyes on both the wired and wireless link. If it detects something wrong on links, like link failure, or link degradation, then it generates a fault signal to the switching mechanism to switchover to the alternative link. The fault signal is a signal that is used to initiate the data switching operation to switch traffic to the alternative path.

Another feature of the link monitoring mechanism is that it also sends link status notification to the care provider through the “remote notification mechanism”.

The monitoring mechanism can be employed at different levels of the OSI model. There is a variety of protocols to monitor the link and to diagnose the quality of the link i.e. link degradation, link failure, etc. Mostly, link quality monitoring protocols work at higher layers of OSI model. For example, SNMP [46] is of application layer. This protocol suffers from the higher failure detection time that makes their use disappointing for critical, real-time applications. It is obvious that, as the protocol belongs to a higher layer, it has slower failure detection because they have to wait for the lower layers to receive data. Therefore, we can make our failure detection much faster by using a mechanism which could work at the lowest level of the OSI model. There is a point-to-point protocol (PPP) which operates at the data link layer. PPP uses its sub module link control protocol (LCP) [47], which monitors the link status by incorporating with the physical layer of the system. This is the only protocol that can provide earlier failure indication

Data switching mechanism

The data switching mechanism is used to switch data traffic from the primary link to the backup link in the event of fault detection that is detected by the monitoring mechanism in the link. It also again switches data traffic from the backup link to primary when the primary link has recovered. The data switching mechanism activates in two situations: link failure and link degradation due to insufficient throughput of channel, unwanted packet losses, or too much packet delay. The data switching mechanism triggering the switching process depends on the monitoring mechanism because the characteristics and threshold values of these link performances is configured in the link monitoring mechanism.

One important thing is that, in the case of primary link failure or link degradation, “Device Manager” prioritizes the highly sensitive delay traffic over the less sensitive delay because the wireless link suffers from the lower channel capacity than the wired link, and the wired link is

more consistent than the wireless link. With regard to physical implementations, the “data swathing mechanism” can be employed at different layers of OSI Model.

- The first approach can employed at the physical layer of the OSI model. In this approach, the link monitoring mechanism examines link. If a fault signal is detected, then the switching mechanism will be triggered and switch traffic to the alternative link. This mechanism is very spontaneous and extremely inexpensive to implement. The problem with this technique is that it will fail all the sessions in progress during the switchover. As a result, re-authentication is required for the re-establishment of services after the switchover.

- The second possible scheme of switching can be employed at OSI layer 2 switching by using 802.3ad Ethernet standard [48]. This approach allows data switching from the wired link to the wireless link without loss of any ongoing IP session. This technique requires that both the primary and backup links must be equipped with an Ethernet interface while the proposed model has two different kinds of links: ADSL and UMTS. The switching of layer2 will not be applicable for the proposed model.
- The limitation of the second scheme for the proposed model can be coped at OSI layer 3. There are a number of techniques for layer 3 switching that can be used for switching, such as: ML-PPP (multi-link point to point protocol), automatic protection switching mechanism [49], interface backup technology [50] [51] and etc. After making an observation of layer3 switching techniques, it comes out that, except for the interface backup technology, the rest of the techniques do not efficiently suit to the system model because of their own pros and cons. For example, the ML-PPP mechanism binds the multiple links into a single virtual link, and distributes the traffic on both links. This technique operates just like a load balancing, and does not support the backup mode, where one link acts as a primary link while the other as backup, and while the automatic protection switching technique operates between two devices instead of two interfaces, to employ the backup mode strategy.

Switching mechanism can be employed at a higher layer level, but the problem is that it suffers from higher switching delay and that is not reasonable for critical application. It is concluded that monitoring mechanism is employed at the data link layer and the switching mechanism is employed at network layer of the OSI model, as shown in following Figure 9.

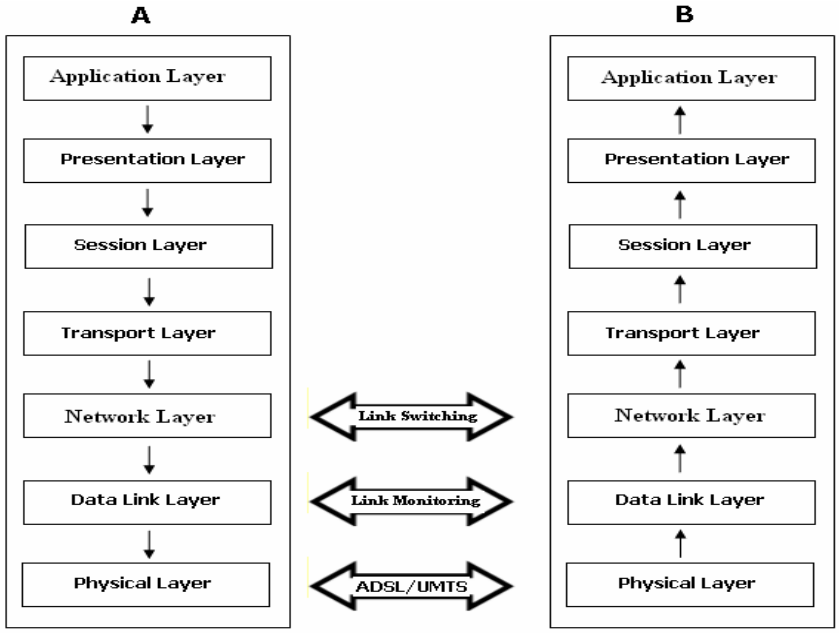


Figure 11. Layered view of link monitoring and link switching mechanism

SCTPfx [52] is a fast and transparent failover mechanism which switches traffic softly from primary to backup path within 40ms.SCTPfx failover mechanism based on cross-layer architecture uses primitives [53] to communicate with other layers of the OSI Model. Link monitoring and traffic switching is employed at different layers of OSI Model. Cross-layer architecture is used to inform SCTPfx of link failure. This mechanism can be used for the proposed model.

6.1.2 Wireless access module

To set up communication over the backup wireless link in case of primary link failure, wireless module is used [54]. During the forward communication, this module performs the formatting and signaling of the customer data to make it traversable, according to the wireless link principles. Some of the possible wireless broadband access technologies which can be used for a wireless back up connection are UMTS, GSM, 802.11 network (Wi-Fi), 802.16 or WiMax network , or satellite broadband access networks.

6.1.3 Wired access module

In Figure 7, wired access module is simply an ADSL modem that performs the data formatting and signaling, according to the protocol used on wired link during the forward traffic flow, while

in the backward direction it reassembles the received packet, according to the system requirements.

6.1.4 Device manager

This mechanism controls the incoming and outgoing traffic from, and to, the user end. Security features are added in to this mechanism that keeps an eye on incoming and outgoing traffic. The QoS mechanism plays an important role from the end user coming traffic. Incoming traffic is divided into classes [55] such as conversational class, streaming class, interactive class, and background class services. The main difference between these classes is how delay sensitive the traffic is, conversational class, streaming class carry real time flows, like voice and video. Interactive class, background includes traditional internet applications like traditional internet applications WWW, Email, Telnet, FTP and news. Delay sensitive traffic serve first and less delay sensitive traffic serve later. After dividing the traffic into classes, QoS mechanism passes the traffic to the switching mechanism for further process. This mechanism is also used in "Remote Notification Mechanism" as relay to forward notification to the care provider but it will be discussed under "remote notification mechanism" section.

6.1.5 Power monitoring module

Power management is a fundamental element in the telecommunication environment in the sense of reliability of the system. In emergency cases, it is necessary to provide continuous power to equipment that is being used in tele-operations. "DC Power backup system" is provided for tele-operations when the main AC supply has failed. In the event of main power supply failure, it is necessary to monitor the backup power supply by taking pre-emptive measures before the complete outage of the system due to power failure. UPS is connected to CPE via RS-232 serial cable. The power monitoring module [56] monitors AC power as well as battery readings when AC power has failed. This module is used as for means of early notification of power failure to the care provider. Battery backup time depends on the consumption of power and the size of strings of batteries.

6.1.6 Remote notification mechanism

The remote event notification method is a mechanism that automatically sends the information about certain events that occurred in customer premises equipment i.e. link failure, link status changed or power outage indications. Syslog protocol [57] [58] is designed for general purpose application for means of remote notification. It does not support the power monitoring notification remotely. "Remote notification mechanism" supports the link status as well as power status notification. This mechanism provides the instant information about the occurrence of critical events at the client side that helps the server side to take preemptive measures before the total failure of the system. Thus, the remote event notification method plays a significant role in providing the high availability of the services by minimizing the down time probability of the system. In "Robust Home Care Access Network", this method will send the following information of customer premises equipment to care provider in the notification messages:

1- Care provider receives the notification of the traffic path that which link is currently being active at the customer end, either it is wired or wireless.

2- It notifies the service provider end, either the system is currently powered by primary AC power supply or it is working at the backup power DC supply.

If the system is running on primary AC supply, the notification will only inform that the system is on direct AC supply. If however the primary power supply goes off, the system will switch on to the backup power supply provided by the batteries (12v+ or 24V+) installed within the UPS. During the backup power mode, the notification mechanism also sends the remaining battery voltage numbers along with the power source.

Architecture of remote notification

The architecture of the remote notification mechanism constitutes the following logical components as shown in diagram:

Figure 12. Remote notification system logical components

- **Inventor:** This is a mechanism that generates event critical messages and is called 'inventor'. Both the power monitoring and link monitoring mechanisms serve as inventors.
- **Device manager:** This receives the messages generated by inventors in raw format. The device manager further rearranges raw messages into a format that is able to be traversed through the network to the notification collector at the server side. The device manager serves as a proxy, or surrogate relay, for the notification collector.
- **Notification collector:** This is a service provider's end mechanism that receives the notifications relayed from the device manager. It further analyzes these notifications and, according to the significance of these messages, it generates alerts to warn the service provider. These early alerts help to secure the system before the occurrence of failure.

IPC (inter-process communication) [59] is used between running processes on local machine or remote machine over the network to make them communicate with one another. Process can be identified by device IP and name of process. If the process gets packed information sent from the same destination and source IP address, then it is local communication on the same machine. If the source and destination IP addresses are different, then it is remote communication (communication between CPE and SPE). Message passing uses primitives to exchange data between different processes. IPC can be achieved in three different ways: mailbox, direct naming and ports [60]. Alert or notification is exchanged between CPE and SPE by means of ports. When a process wants to communicate with the processes running on a remote machine, notification data encapsulated into data package according to the communication protocol (UDP/TCP) is exchanged.

The power monitoring module sends information to device manger about the system whether it is running on backup power or primary power. The device manager also receives information about the links. Raw information is provided to the device manager from both the power monitoring module and the link monitoring mechanism. The device manger formats raw information and encapsulates notification information in UDP [61] datagram and sends it to the notification collector at the server side. The notification collector receives this information. It de-capsulate the datagram and processes it to generate corresponding alerts.

The notification collector at SPE defines UDP port. This port is only in listen mode. The notification collector can only receive the notification messages from the device manager and can not send responses back to the device manager because it is UDP based communication. UDP is an unreliable protocol and some packets will be lost during congestion in the path. To resolve this problem, the device manager prioritizes these massages over user traffic.

The packet of the device manager consists of priority field, header field and message fields. The priority field is used just to set the priority of notification packet. The notification packet has higher priority than the user's data because it has control information for the system. The header field has information of source IP address, destination IP address and time stamp. Time stamp is the local time of CPE that is used to order packets. The message field has just the notification for the care provider.

6.2 Service Provider Equipment

On the other end of the communication system, is the service provider's equipment, the following logical components are needed:

- Link reconfiguration mechanism,
- Notification collector,
- Traffic security and QoS mechanism.

6.2.1 Link reconfiguring mechanism

This mechanism provides reconfigurations, synchronization and authentications of the links, when the currently operating link becomes unavailable because of link failure or underperformance. When the ongoing communication link fails and, at the CPE end, the failover mechanism switches traffic control to the alternate link, then the destination address for SPE upstream traffic changes. To deal with this problem, reconfiguration of the link is essential for the SPE upstream intended to CPE. This mechanism does not play any role in the switchover mechanism.

6.2.2 Notification collector

This mechanism is a process that only receives critical data information (backup power readings, link status information) and passes them on to higher layers to generate alerts. The CPE device

manger collects this information from the link monitoring module and the battery monitoring module and relays it to the remote notification agent at the SPE end.

6.2.3 Traffic security and QoS mechanism

This mechanism controls upstream and down stream from, and to, the care provider. Security features are added in this mechanism that keeps an eye on incoming and outgoing traffic. QoS of service is also implemented in this mechanism.

7 Conclusion

In aiming to protect communication link and to provide a high availability of broadband services, this report investigates a variety of broadband access technologies to scrutinize their viability against the failure threats. This work also looks at different ways, how to utilize these technologies for better services. This report can be concluded in the following findings:

- It is better to use redundant communication links, of diverse nature access networks, between both the ends to get improved reliability. This diversity of redundant links removes the single point failure bottle necks of an access network by providing completely independent alternate paths. Thus, provide better reliability and uptime of the system. This report suggests UMTS and DSL together to achieve such diversity of redundant communication links.
- Employing SCTPfx failover mechanism in conjunction with LCP provides a fast switching to alternate backup links, without the loss of packets, when a link fails or its performance goes down.
- Power monitoring and remote notification mechanism provides the capability to make early diagnostics of link status and power source monitoring that helps to make counter measures before the total failure of the system due to power outage.

8 References

[1]. S.Mejia, O.Cardona, “Antioquia’s Telemedicine Network informatics and telecommunication technologies to service of health”, Proceedings of the 25' Annual International Conference of the IEEE EMBS Cancun, Mexico, Sep.2003.

[2]. Gary Marshall, “Resilience, Reliability and Redundancy” Communications Ltd & David Chapman, May 2002.

[3]. “International Activities in Tele-homecare”, Office of Health and the information Highway Health Canada, September, Sep.1998.

[4]. R. S. H. Istepanian, "Telemedicine in the United Kingdom: Current Status and Future Prospects", IEEE Transactions on Information Technology in Biomedicine, vol. 3, no. 2, Jun.1999.

[5]. Robert S.Habib Istepanian,” Modelling of GSM-based Mobile Telemedical System”, Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Vol. 20, No 3, Nov.1998.

[6]. Sathish Chandran, ”Enhanced Telemedicine Applications with Next Generation Telecommunication Systems”, proceedings of the first Joint IEEE EMBS conference Serving Humanity, Advancing Technology, GA, USA, Oct.1999.

[7]. Tamura, Masuda, “A mobile-phone based telecare system for the elderly”, Proceedings of the 26th Annual International Conference of the IEEE EMBS San Francisco, CA, USA, Sep.2004.

[8]. M. V. M. Figueredo1, J. S. Dias, ”Mobile Telemedicine System for Home Care and patient monitoring”, Proceedings of the 26th Annual International conference of the IEEE EMBS San Francisco, CA, USA, Sep.2004.

[9]. Asfandyar, Shoeb, ”Building a high, quality mobile Telemedicine System using networks striping over dissimilar wireless wide area”, proceedings of the IEEE Engineering in Medicine and Biology 27th Annual Conference Shanghai, China, Sep.2005.

[10]. Miaou, CY Huang, ”A next generation mobile telemedicine test bed based on 3G cellular standard”, Proceedings of the Annual International conference of the IEEE Netherlands, 2001.

[11]. E.A.Viruete Navarro,” Performance of a 3G-Based Mobile Telemedicine System”, proceedings of IEEE CCNC Communications Society subject matter experts for publication, Jan.2006.

[12]. Kenneth J. Kerpez, “Advanced DSL Management”, IEEE Communications Magazine, Sep.2003.

[13]. “Understating XDSL”,Teledata Networks,Jul.2004.

[14]. T. Starr et al, “DSL Advances”, Prentice Hall, 2003.

[15]. Amitava Dutta-Roy, “An Overview of Cable Modem Technology and Market Perspectives”, IEEE communication Magazine, Jun.2001.

[16]. Tomislav, Nikola,” Comparison of Broadband Network Technologies”, University of Zagreb facility of electrical engineering and computing, Osaka, Sep.2003.

[17]. Low, R. “An Over View”, IEEE Communications Engineer, 2004.

[18]. Amative Dutta-Roy, “An Overview of Cable Modem Technology and Market Perspectives”, IEEE communication Magazine, June.2001.

[19]. “Deploying European Data, Voice, and Video Services over Cable”, Cisco System, Inc.2000.
[20]. Jewell, Matmore,” Cable TV technology for local access”, BT Technologies journal, Oct.1998.
[21]. Antonio, Salvatore, “Dimensioning and Effective Handling of Signalling Channels in a Multimedia GEO Satellite Platform”, IEEE Transactions on vehicular technology, VOL. 54, Mar.2005.
[22]. Mahnoosh, Victor C. M. Leung, “Bandwidth Assignment for VBR Traffic in Broadband Satellite Networks”, Department of Electrical and Computer Engineering, the University of British Columbia, IEEE, 2000.
[23]. Jarmo Harno, “3G Business Prospects – Analysis of Western European UMTS Markets”, EEE Communications Magazine, Sep.2004.
[24]. S. Baudet, C. Besset-Bathias, “QoS implementations in UMTS networks”, Alcatel Telecommunications, 2001.
[25]. Rajeev Koodli, Mikko Puuskari, “Supporting Packet-Data QoS in Next Generation Cellular Networks”, IEEE Communications Magazine, Feb. 2001.
[26]. Sotiris I. Maniatis, “QoS Issues in the Converged 3G Wireless and Wired Networks”, IEEE Communications Magazine, Aug.2002.
[27]. Abdul Bais, “Evaluation of UMTS security architecture and services”, IEEE Communications Magazine, Aug.2006.
[28]. Enrico Angori1, “Extending WiMaX technology to support end to end QoS guarantees”, University POLITEHNICA Bucharest, 2004.
[29]. Adrian Leunga, ”The security challenges for mobile ubiquitous services”, information Security Group, Royal Holloway, University of London, Surrey, TW20 0EX, UK, 2007.
[30]. Jamshed Hasan, “Security Issues of IEEE 802.16 (WiMaX)”, School of Computer and Information Science Edith Cowan University, Australia”, 2006.
[31]. Aktul Kavas, “Comparative Analysis of WLAN, WiMaX and UMTS Technologies”, Department of Electronics & Communication Engineering, PIERS Proceedings, Czech Republic, Aug.2007.
[32]. Ricardo Preguica ,“Comparison between UMTS/HSPA+ and WiMAX 802.16e in Mobility”, Instituto de Telecomunicações/Instituto Superior Técnico, Av.Rovisco Pais 1, 1049-001 Lisboa, Portugal,2005.
[33]. “Internet Access via UMTS for Enterprises”, LANCOM Systems, 2008.
[34]. Mohammad Modarres, Mark Kaminskiy,” Reliability engineering and risk analysis” ISBN-0-8247-2000-8 Page (331).
[35]. Siani, “Probability Theory”, ISBN 3-540-53348-6, page (1-9).
[36]. Marvin Rausand, Arnljot Høyland, “system reliability theory”, second Edition, ISBN 0-71-47133-x, page (28).
[37]. Marvin Rausand, Arnljot Høyland, “system reliability theory”, second Edition, ISBN 0-471-47133-x, page (37).
[38]. Marvin Rausand, Arnljot Høyland, “system reliability theory”, second Edition, ISBN 0-471-47133-x, page (525-535).
[39]. “Seven reasons to use end-to-end thinking when building all-IP networks”, Ericsson, 284 23-3123 Uen Rev A, jan.2009.

[40]. “Managed Wireless Internet”, NIRIX Technology.
[41]. Marvin Rausand, Arnljot Høyland, “system reliability theory”, second Edition, ISBN 0-471-47133-x, page [12-13].
[42]. Faizan.J,El-Rewini.H, “Introducing Reliability and load balancing in home link of mobile IPv6 based networks”, IEEE Communications Magazine, Jun. 2006.
[43]. “Bipac 7402GX”, Billion Electric Co.Ltd, available from: http://au.billion.com/product/3g/bipac7402x.php accessed 2009-06-10.
[44]. “Evaluating Backup Interfaces, Floating Static Routes, and Dialer Watch for DDR Backup”, Cisco Systems, 2007.
[45]. Segel Jonathan Dean, “High availability broadband connections through witching from wire line to diverse wireless networks”, Patent No.P20050300089, ALCATEL, Aug.2004.
[46]. Kwang Sik Shin, Jin Ha Jung, “Real-time network monitoring scheme based on SNMP for dynamic information”, Department of Electronic Engineering, Inha University, Jul. 2005.
[47]. W. Simpson, “PPP Link Quality Monitoring”, RFC, May 1992.
[48]. Tomoya Hatano, Yasunobu Kasahara, "Dynamic L2 Distribution based on Connection Priority for Enhanced Bandwidth Utilization”, IEEE Communications Magazine, Jun.2006.
[49]. Andre N,Fredette,Groton, “Automatic protection switching using link-level redundancy supporting multi-protocol label switching”, United States, Patent No. 6987727,2006.
[50]. Kim-Joan Chen, Ying Cheng, “An intermodal switching technique for high speed packet networks”, IEEE Communications Magazine, Jun.2006.
[51]. “Technical White Paper for Interface Backup”, Huawei Technologies Co. Ltd, 2007.
[52]. Yunsop HAN, Fumio TERAOKA, “A Fast Failover Mechanism Based on Cross-Layer Architecture in SCTP Multihoming”, November 2008.
[53]. F. Teraoka, K. Gogo,”L2 Abstractions for L3-Driven Fast Handover”, RFC, May.2008.
[54]. “3G Wireless WAN HWIC”, Cisco Systems, Inc.
[55]. Karlsson, G. Mas, “A critical review of End-to-end arguments in system design”, IEEE Communications Magazine, 2004.
[56]. Charles F. Blair, Mark Gabel,” Modular uninterruptible power supply battery management”, US Liberty Corporation, 2001.
[57]. C. Lonvick,” The BSD Syslog Protocol”, RFC 3164, August 2001.
[58]. Dario V. Forte, “SecSyslog: an Approach to Secure Logging Based on Covert Channels”, proceedings of the IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, 2005.
[59]. Patrick,”Message-oriented and workflow-based inter-process communication distributed manufacturing”, IEEE international conference, Sep.2008.
[60]. Bao Yanru, “CommMgr: A new inter-process communication management software”, Department of Computer Science and Technology, Tianjin University, Tianjin 300072, China, Feb.2005
[61]. Yunhong Gu,” UDP based data transfer for high speed wide area Networks”, National enter for Data Mining, University of Illinois at Chicago, Dec.2006.