大学校园网架构

重庆大学硕士学位论文

学生姓名: Águeda Sofia Monteiro Tavares

指导教师: 胡致远　副教授

专　　业：电子与通信工程

学科门类：工　学

重庆大学通信工程学院

二 O 一一年四

Network Architecture for University Campus Network

A Thesis Submitted to Chongqing University in

Partial Fulfillment of the Requirement for the

Degree of Master of Engineering

By

Águeda Sofia Tavares

Supervised by Ass.Prof. Zhi-Yuan Hu

Major: Electronics and Communication Engineering

College of Communication Engineering of Chongqing University,

Chongqing, China

May 2011

摘　　要

今天，信息化技术已成为公司企业、政府部门以及高等学府等机构非常重要的目标与愿望。

随着全球新兴信息技术的发展，现代通信能够提供快速通信服务并提高个人通信效率，因此现代大学校园通信面对新的挑战，比如：需要提供一个信息网络能够支持个人需求并适应多元化的校园环境。一个新的网络架构成为校园网的骨干基础之一，它能够使教师，研究者，学生，管理者和员工组成一个社会群体更方便的进行教学、科研、学习并相互沟通。

本文重点在于对校园网架构的定义以及校园网的基本组成部分的介绍。三个最重要的高质量的架构特征为：开放的网络架构、服务导向的特征以及基于包交换的 IP 网络。架构中四个重要的组成部分为：服务和网络管理、网络控制、中心交换单元和边缘接入。

本文的理论贡献是提出大学校园网的参考模型架构，这个参考模型架构可以适用于建立一个健壮的灵活的网络能够满足下一代需求。结果的建立可以为建立现代校园网提供一个重要的参考指导。研究的校园网模型是可靠的、健壮的并且具有扩展性。

关键字：校园网架构，接入技术，网络管理，移动代理

ABSTRACT

Today, information technology is strategically important to the goals and aspirations of the business enterprises, government and high-level education institutions – university.

Universities are facing new challenges with the emerging global economy characterized by the importance of providing faster communication services and improving the productivity and effectiveness of individuals. New challenges such as provides an information network that supports the demands and diversification of university issues. A new network architecture, which is a set of design principles for build a network, is one of the pillar bases. It is the cornerstone that enables the university's faculty, researchers, students, administrators, and staff to discover, learn, reach out, and serve society.

This thesis focuses on the network architecture definitions and fundamental components. Three most important characteristics of high-quality architecture are that: it's open network architecture; it's service-oriented characteristics and is an IP network based on packets. There are four important components in the architecture, which are: Services and Network Management, Network Control, Core Switching and Edge Access.

The theoretical contribution of this study is a reference model Architecture of University Campus Network that can be followed or adapted to build a robust yet flexible network that respond next generation requirements. The results found are relevant to provide an important complete reference guide to the process of building campus network which nowadays play a very important role. Respectively, the research gives university networks a structured modular model that is reliable, robust and can easily grow.

Keywords: University campus network architecture, access technologies, network management, mobile agents

TABLE OF CONTENTS

LIST OF FIGURE

LIST OF TABLES

1 INTRODUCTION

In today's modern and global world, the importance and added values provided by Network infrastructure is evident whether it is for business enterprises, government entities or educational institutions particularly universities. It contributes to achieve important goals such as more productivity, collaboration, efficiency and acquire knowledge. Increased use of Information technologies in the university requires a robust technical infrastructure and adequate network architecture.

Network architecture is a fundamental pillar above where the network will be built. Kaufmann [12] defines Network architecture "as guide of the technical design of the network, through the application of high-level design principles". When planning a network if the right network architecture is followed, performance and reliability can easily be achieved. It is an essential and common practice to follow a hierarchical model when design a campus network. This model provides a modular topology of building blocks that allow the network to scale easily.

The hierarchical model is comprised of three main blocks that are: access layer, the distribution or convergence layer, and the core or backbone layer. Each layer has distinctive functions, though in small networks convergence between layers may occur. The core network provides the backbone for the network. The distribution layer aggregates multiple technologies from the access layer. These technologies include ISDN, DSL, cable, Ethernet, and Wireless. The access layer is the first point of entrance into the network as so it provides the required interfaces for edge devices and stations.

A university campus network is an important instrument for communication and facilitating collaborative research which are key factor to build a strong knowledge culture and efficiently support academic mission. The implementation of Campus University Network help universities becomes more a collaborative center, which helps achieve their goals and provide development of higher level of knowledge for the students. When planning and design a network it is very important to "build it for the future".

This thesis proposes a model for "Network Architecture for University Campus Network" based on subsystems and focuses on open and integrated interfaces and on a network which is service oriented. Three most important characteristics are: it's open and subsystem-based network architecture; it has service-oriented characteristics and is

an IP network based on packets. There are five components in the architecture, which are: Services, Network Management, Network Control, Core Switching and Edge Access.

This chapter outlines research problem statement, significance and motivation. It also presents an overview of the following chapters of the research.

1.1 PROBLEM STATEMENT AND SIGNIFICANCE OF THE RESEARCH

1.1.1 Problem Statement

In the search for greater competitiveness, universities are investing massively in the constant advances of the Information Technology (IT). Universities leaders are facing a significant number of challenges to maintain the competition, respond to a rapidly changing environment, and enhance academic strengths. To respond to present and future new challenges and demands, network architecture designed according to new principles including an open and integrated system constitute a starting point. The term architecture implies a model that can be followed for university campus when building their next generation network (NGN) with integrated services such as voice, data, video and multimedia, even supports internet of things (IoT) layout. Aware of the importance of network and all sorts of advantages that it brings to university, therefore it becomes important to choose an architecture that fits the specific characteristics and needs of campus network.

The goal of this research is to propose an architecture model suitable for university campus network with meet and adapt to the specific requirements of such kind of network environment and provides characteristics like flexibility, scalability and manageability. The main advantage and importance of this architecture is that it adapts the specifics requirements of campus network.

The campus architecture proposed in this thesis defines five modular components which cooperate to provide a network that can respond to current and future university technology demands. To achieve the above purposes we focused first on the definition of architecture, second on the access network services or layout and third in the management system. To verify, this paper layout an experiment campus network is carried out.

1.1.2 Significance of the research

In the information age providing a high-quality information technology infrastructure has become fundamental to accomplish strategic objectives. A robust network is the basic starting point for these achievements. At the campus level, institutions are investing financial and human resources to enhance campus network to support new technologies and services. However without a well defined and clear architecture model that can be followed during the network design process it make difficult to achieve their goals. They lack a standard architecture model.

Over the past two decades, colleges and universities have recognized the importance of network as essential to their research and teaching mission. Universities are making efforts to ensure that their network infrastructure is reliable, secure, adaptable, flexible, scalable, and fault tolerant.

A networking survey followed by a study conducted by EDUCAUSE Center for Applied Research (ECAR)[25], to 517 higher education institutions in United States and Canada, found out that respondents overwhelmingly agree that their leadership perceives the campus network to be:

- More important than it was ten years ago (2000) - (94 %),
- A critical infrastructure - (89 %), and
- A strategic resource - (81 %).

Due to the demands for new types of services, universities campus are facing new challenges related to network infrastructure and without a clear and well-defined architecture it becomes very hard to upgrade and provides network growth[3]. The architecture is the essential foundation of network's success. It is a technical plan that guides the decision making and the process of identify network components. The architecture model should transcend specific technologies, vendors and physical design and wiring, and instead is a guide for choosing those parameters during the process of network design.

Several architecture models for enterprises exist. However they are not the most suitable for universities requirements. The simplest starting point for many universities is to follow one of those enterprise models and try to adapt to campus necessity which usually does not fulfill all the campus network requirements. At the time this thesis project began, there was no standard architecture model for campus network. This project aimed to explore university campus network architecture designing criteria and concentrate on access network and network management system.

The main advantage of this research is to propose a model that can be a standard architecture model for campus network. A model that is flexible, robust and supports a multitude of services demands currently faced by the university campus environment. However, since many universities campuses are already being deployed and to rebuild it again from scratch can be financial unfeasible, since the proposed architecture is built in a modular way, this make possible to be adapted for existing network.

Another problem faced by campus universities is related with centralized network management model based on client-server model which is no longer suitable for currently heterogeneous and complex technological environment [13]. Therefore a management system with distributed management architecture that supports Mobile Agents is proposed to solve the problem of centralized management architecture.

This thesis proposes network architecture and entities suitable for university campus specific requirements. It is built in modular and flexible way which makes it easy for future-growth. It provides ways to respond to actual challenges faced by university campus network.

1.2 RESEARCH MOTIVATION AND CONTENTS

1.2.1 Research motivations

In this global world, higher education is becoming more and more competitive and international. In this particular, campus network can provide its users new technologies with numberless possibilities for networking and also for share knowledge and information about the challenges and prospects they daily face.

Intensive research have been done for network architecture model, however most of them are in big enterprises or government networks, for the best effort of this research there is no standard model for campus network, special one that focus on Next Generation Network. Therefore it constitutes an important topic and interesting challenge to develop a model specific for campus network oriented for Next Generation Network.

Network architecture provides the foundation to achieve business strategy, since it is the technical network plan based on a set of network components, functions and services.

Design campus network architecture following multilayered model provides several advantages. It permits defines distinct layers which provides modularity; group device

with similar function per layer, thereby making the configuration simpler on a modular design. The multilayered design also makes it easier to troubleshoot network problems.
The motivation behind this thesis is to propose network architecture that can be a foundation for supporting diversity communication services and respond to present and future challenge faced by university campus. The architecture serves as a reference guide for universities in the network planning and design process, to help them meet the campus network requirements for next generation network.

1.2.2 Research contents

The term architecture implies a model that can be adopted for university campus when building their next generation network (NGN) with integrated services such as voice, video and data to achieve their goal
The overall thesis is divided into six chapters, with each chapter having the following scope:

Chapter One provides a detailed introduction. It highlights the background and motivation for the work conducted in this thesis. Firstly, the topic is stated and the significance of the research presented. Also, the research contents and motivations are highlighted.

Chapter Two presents the work state of art of campus network. It defines specific requirements and identifies the most important services for campus area network (CAN). First is presented the definition of requirements and identification of campus characteristics and required services. Then, a structure of the architecture according to those requirements and services is proposed. That is the focus point of this thesis, a standard university campus network architecture model that can serve as a reference and be adapted to build the next generation network.

Chapter Three describes key access technologies available, present their characteristics and summarizes their advantages and disadvantages. It also analyzes according to certain criteria's which case they are more suitable for campus network.

Chapter Four explores fundamental about network management and Mobile Agents (MA) paradigm, enlightening the advantages and limitations of MA uses. Furthermore, a simple prototype about network management with mobile agents is implemented using Java programming language to demonstrate the effectiveness of that paradigm.

Chapter Five discusses and builds an experimental campus network that aims to demonstrate the fundamentals concepts described in the previous chapters and our

researching practicability proof. Asterisk will provide multimedia control functions based NGN platform and BRAS provide access to users, authentication and quality of services. Network management with mobile agents is used to proof the advantages of this paradigm over network management traditional and centralized model.

Chapter Six, this chapter concludes the thesis by providing a summary of the work undertaken as well as highlighting its results and contribution to the area of campus network architecture. Suggestions for future work are also noted.

Appendix presents several screenshots and shows general steps to configure VLAN and PPPoE services in Broadband Access Server and SIPp stress calls over Asterisk Server results.

2 CAMPUS NETWORK

This chapter presents an overview about the Campus Network, which includes specific characteristics and requirements. It also outlines the differences between campus network and other's types of network such as government network. Then, it focuses on the fundamental point of this thesis, the network architecture definition and fundamental components.

2.1 Review of the State of the Art of Campus Network

According to Standford and Marsha [11], campus area network (CAN) interconnects networks in a limited geographical area such as university campus or organizational campuses. CAN is a computer network interconnecting a few to several local area networks (LANs) within a university campus or corporate campus. Campus area network may link a variety of campus buildings including colleges departments, the university library and student halls of residence.

Design a network is a very complex and time consuming process. Characteristics such as scalability, flexibility, quality of service (QoS), topology, etc are very important requirements in the design process of network. Therefore many design model, such as hierarchical model, exists that can be followed to simplify the design process. Hierarchical model simplifies the design through the methodology of break the network in three main components that are: access network, distribution network (convergence/aggregation network) and core network (backbone network) which simplify, make it smaller and more manageable.

Core Layer Functions

The core layer provides a high-speed backbone to forwards all traffic in the network. It also provides very strong routing and forwarding capability and wide bandwidth. Functions and attributes of the core layer include the following [34]:

- Providing a high speed and highly reliable and available backbone. This is accomplished by implementing redundancy in both, devices and links, so that no single point of failure exists;
- It provides quickly adaptation to network changes by implementing quick-converging routing protocols. The routing protocol is already

designed with fault tolerance. Only physical route should implement redundant link so that the extra capacity can be used when failures exist.

Distribution/Aggregation Layer Functions

The distribution layer interfaces between the core and access layers. Its functions include:

- Implements policies by filtering, prioritizing and queuing traffic through broadband equipments, such as Broadband Remote Access Server (BRAS);
- Routes traffic between the access and core layers;
- Provides redundant connections, both to access devices and to core devices.

Access Layer Functions

Access layer is the point of entrance of the users to the network. Users can be local or remote. Local users typically access the network through connections to a LAN switch. Remote users might access the network through the Internet, Remote Access Server (RAS) using VPN connections. Access layer functions include:

- Authentication of the users - the access layer must ensure that only users who are authorized to access the network are admitted (Security-Network Access Server);
- Accounting – access network guarantee that users are charged according to accounting policies implemented;
- Implements Quality of Services mechanism.

Using structure based on layers has the main advantage of modularity, this means design a network based on modules. Modularity is a very important characteristic in network since it allow easy scalability and it allows devices that have similar and well-defined functions to be grouped at each layer, which makes easy to add, replace/remove individual device.

The connectivity can be achieved using wired and/or wireless network connections. According to a study conduct by ECAR① （Figure 2.1）the prevalence of wired network in higher education campus is significant. Almost all faculty and staff offices are wired and that most libraries, residence halls, classrooms, and research laboratories are wired.

Wireless network is especially prevalent in areas that were not physically wired early, due to either structural issues or cost and priority. Example area is indoor campus public spaces.

① http://net.educause.edu/ir/library/pdf/ecar_so/ers/ERS0502/ekf0502.pdf

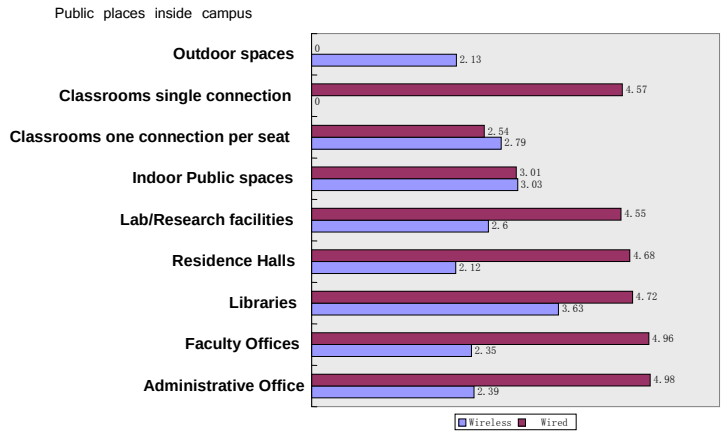

Fig 2.1 Comparison of Wired and Wireless Installations

Note: Mean Value Scale = 1 (none) to 5 (almost all) ①

Both of them have set of advantages and disadvantages. Wired connections offered faster and higher bandwidth capacity with Gigabit Ethernet technology, another advantage is reliability which means that fixed wired connections are less prone to interference and some kind of attack such as eavesdropping which can happen only if security mechanism is not implemented. Some disadvantages of wired connections covers issues that include costs, deployment and adaptability to changes or upgrade – wired networks are more expensive and time consuming to deploy, and they are more difficult to modify when network conditions change.

On the other hand, wireless connections offer attractive advantages such as mobility and flexibility, as they enable the use of a laptop computer, handhelds or other mobile devices with Internet support capability, to access the network or Internet anywhere in the campus covered area. Another advantage is cost effective, setting up a wireless network is less expensive then other structures such as Ethernet and there is no need to run cable across all building and throughout the campus network [7]. Wireless networks disadvantages includes lower bandwidth and variation in throughput due to the share of the medium by users, wireless connections have not offered comparable bandwidth available for wired network. Achieving wireless access at such high rates is difficult and wireless networks also face technical problems similar to those encountered in outdoor wide-area radio-based systems, such as limited available bandwidth and fading due to multipath interference and blockage due to obstacles. The goal in wireless campus area network (WCAN) system design is to transmit at the maximum information rate with an

① http://net.educause.edu/ir/library/pdf/ecar_so/ers/ERS0502/ekf0502.pdf

acceptable probability of error and minimum equipment complexity, power and cost. There are security vulnerabilities problems due to potential data interception and analyzing by malicious user.

The best solution for connectivity is to take the benefits of a hybrid wired/wireless network, which is a combination of both networks. Hybrid networks provide campus university excellent advantages in terms of speed, mobility, and security. Wireless network can be used as an extension of wired network.

2.2 Differences between Campus Network and others Networks

Campus Networks characteristics are different from other types of networks, such as governmental or enterprises networks. The government networks have very high security and high-availability requirements. Preserve facilities and information confidentiality and network equipment from natural disasters, destruction of entities, device interruption which can be caused by misoperation and/or error are of extreme importance [8] as well as network security threats. Enterprise network has several criteria's that determine different network requirements according to specific case. It depends on the business field, such as financial/bank institutions, business sales, service provision, and the size of the enterprise - small, medium or large branch. Regarding to those criteria's demands for high-availability and scalability, security services such as intrusion detection/prevention and manageability can be important requirements to be met by the network. In summary, for government and financial institutions data security and network reliability are of vital concern.

University Campus network core mission is research and build knowledge through teaching goals. As so it has its own specific requirements to support them. The most important characteristics are the following [1]:

- Large-scale networks with active and different user groups
- Multiple and Integrated access network system
- Complex network system management
- Open and flexible network environment and in continuous development
- Multitude of network activities, including researches, laboratories experiments and simulations, electronic learning (e-learning), etc
- Security limitations

- Need for availability and high-performance network design to improve collaboration among researchers, faculty, staff, and students, and to support the deployment of new applications and services.

2.3 Campus Network Design Requirements

Network design follows a set of principles and comprises a set of mechanism that implements network functions. An appropriate design of a campus network is very important to achieve those characteristics stated in the previous section and build a network that meets future requirements. Campus Network design best principles include but are not limited to the following characteristics [34]:

- **Modular**: because of its continuous development and evolutionary nature, campus network designs that are modular easily support growth and change. By using building blocks, scaling the network is simplified by the addition of new modules instead of complete redesigns.
- **Resilient:** is the ability of the network to respond and resist to failure. With most of the services and materials online and in some campus even online classes, resilience is important in backbone or core network to provide high-availability (HA). However for converged and access layer high-availability it's not a critical requirement.
- **Flexibility:** university campus tends to continually evolve; for that reason campus network requires flexibility to quickly adapt. A network must always be built as a flexible long-term entity that adapts to inevitable changes in both equipment and technology.
- **Robust:** to offer security infrastructure that guarantees integrity of information, restrict access to network resource based on authentication and authorization and also prevent security threats and provides infrastructure for multimedia-rich communications environment.
- **Network with QoS**: traditional IP network quality of service is based on best-effort model. This model is no longer suitable for current demands and network multimedia services based on a single IP network infrastructure with a variety kind of traffic included voice and video traffic which are delay-sensitive. Therefore, network design shall be deployed with QoS as critical network requirement and provide classification and prioritization of multimedia traffic.

- **A Network for Research:** within the campus network the requirements among departments and school (even users) are different. Some colleges and departments may have specific needs. University campus network architecture shall be designed to allow segmentation and separation between the main production network and a network on which research can be conducted. A network for research can tolerate outages, it's open and access restrictions is less, and it tolerate on-demand configurations to aid research and will not in any manner affect the production network.

Suffice is to say that network architecture should be carefully planned ahead to avoid having to re-build the network to accommodate new applications or technologies. A multilayer campus design has many advantages such as highly deterministic, easy to scale by adding new block building, easy to troubleshoot as it scales [3].

2.4 Campus Network Architecture

Network architecture deploys many functions. Each function of a network represents a major capability of the network. The components are defined according to main functions of the network and they interface with each other. Based on the requirements, functions and goals for the network, a set of component can be defined.

Networks are evolving from two separate networks – one from International Telecommunication Union's (ITU) that is voice oriented network and another one from Internet Engineering Task Force's (IETF) that's data oriented network – to a converged one – Next Generation Network – with a set of new emerging services, where both data and multimedia traffic are sent using the single IP network with the advantages of offering integrated multi-services to the users. These two different kinds of traffic have different characteristics and Quality of Service requirements. An important challenge for today's network is to properly design an infrastructure that can meet the requirements of different types of traffic, such as provide different quality of service (QoS) to a wide variety of applications and traffic types.

NGN based on converged networks and supported by a single IP network infrastructure is a service-oriented network based on the concept of decomposes network architecture according to main functions. The process of adapt this network architecture and operations is very important and assumes a big challenge for Campus University Network. Thus it must be careful planned and implemented, since it encompasses a multi-service delivery platform based on user demands, scalability to accommodate future needs and necessity of grow, flexibility to quickly adapt as changes

occur, and security measures to prevent attack such as DoS, information diffusion, unauthorized access to services etc [13].

A network architecture model provides a framework and technology foundation for designing, building and managing a communication network [35]. With a layered model which divides the communication tasks into a number of components, each components providing a set of functions and interacting with each other. In developing component architecture, one needs to consider the evolution nature of the network. As stated previous in this thesis, layer structure offers several advantages like scalability and keep the design relatively simple.

A very important characteristic for architecture is to be open, this means it's not vendor dependent and as so no single vendor owns the technology and controls its definition and development. This make possible that the architecture be adopted as a standard and be widely deployed.

Network architecture is a set of functions and abstract design principles. Each of these functions becomes an important component above what network is built. Fig 2.2 depicts the proposed campus network architecture. Three most important characteristics are: it's open network architecture; it's service-oriented characteristics and is a network based on packets. There are five components in the architecture, which are: Services, Network Management, Network Control, Core Switching and Edge Access. The model makes possible the addition of new subsystems over the time to cover new demands and services.

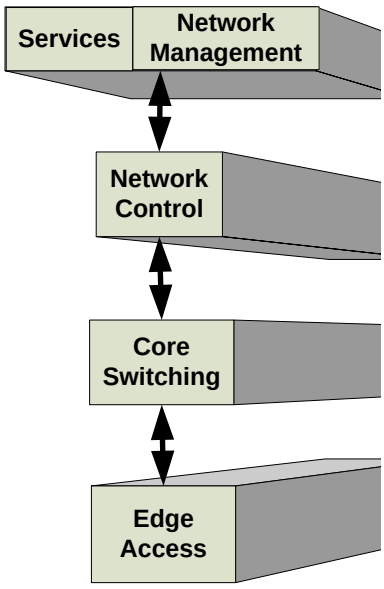

Fig 2.2 Campus Network Architecture

The campus network architecture proposed has the aim of supporting a variety of services running over IP, and supported on multiple accesses network's technologies.

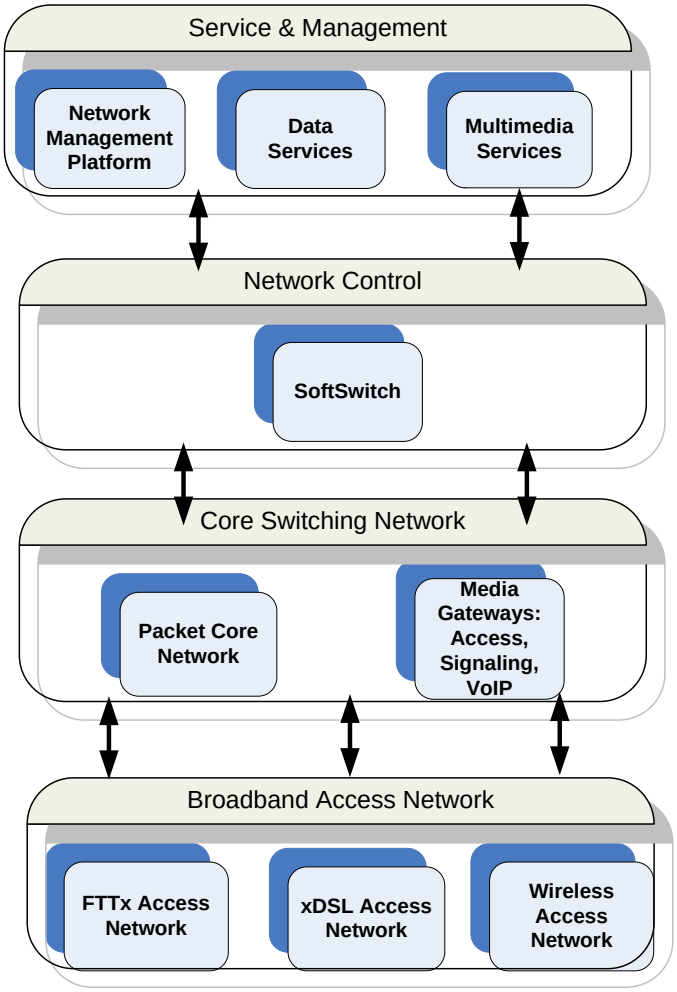

Fig 2.3 Network Functional Areas and Components

2.4.1 Networking overview

New emerging services are driving the quickly network evolution in a way never predicted before. Network is evolving to a service-driven network, with independent service system supported by separated layer from Service, Network Management, Network Control, Core Switching and Edge access, thus enabling service independent of network. One important characteristic that this architecture meets is open system, which gives the possibility to easily incorporate new applications. An example of a network that lack open characteristic is PSTN network, which offers very little flexibility to add new functions. The architecture proposed is constituted of four important layers plus the edge access composed of customer premises equipments.

The campus network architecture proposed meets campus connectivity, flexibility and performance requirements while providing scalability and offer operational simplicity to adapt new technology trends without many alterations in the original structure and design.

The proposed architecture follows the Next Generation Network architecture principles:

- It's a layered approach with clear defined layers according to network main functions;
- Its consist of set of sub-system which make easy to add new subsystem to cover new demands services;
- It's based in IP core technology;
- It allows multi access network technologies.

Access network equipment based on ATM technology is not suitable to deliver multimedia services, therefore this constitute an advantage of IP over ATM and make it a technology of choice for present and for the future broadband network. In case of network where ATM is already deployed and there is no plan for migration in the near future, it can co-exist with IP network while upgrading existing ATM DSLAM to IP DSLAM to provide mapping service between PVC (Private Virtual Circuit) and VLAN (Virtual LAN). Using multi PVC to carry multiple services and maintaining the core ATM. The ATM DSLAM provides access for simple internet user, while the IP DSLAM provides access for multimedia services.

2.4.2 Service and Management Layer

Provide multimedia services in a university environment is important since it facilitate faculty, staff and students researches, work collaboration and communication and also improve the quality of distance learning (e-learning) based on a broad range of converged communications infrastructure access.

The IP infrastructure will offer data services plus multimedia services on the same infrastructure. Video and voice services, whether interactive or on-demand services are becoming a reality present in almost all campus network. An important service implemented is Authentication, Authorization and Accounting service so called AAA services. Authentication verify whether the user has the permission to access the network sever; authorization which services the user is authorized to access and accounting involves tracking the network resources occupied by users and providing the right charging of the user.

Services are not access technology dependent, therefore they are available to users across any access network. This means that hybrid solution can be available comprised of wireless and broadband connection and user roams transparently among them. The possibility to offer many services over IP infrastructure can significantly reduce costs for the university.

Nowadays network management plays a very important and critical role due to proliferation of services. It also has been one of the most challenging areas in networks systems. Managing networks deals with monitor the network in a way to detect and prevents failure, analyze and improves networks performance and respond to demands of services in a shorter time. Network management ensures monitoring and management services and a variety of components of the entire network infrastructure of campus network. The network management system (NMS) component has the function to manage two separate subsystems: call control core technology – next generation device, softswitch and also manage diverse edge access devices such as broadband access devices, IP-DSLAM, access gateways, etc.

Network management system carries out fault management, configuration management, accounting management, performance management and security management for all devices.

A Hybrid management system is proposed for this architecture, it consist of a junction of centralized and distributed management system. It concentrates main functions in a single network manager system while it distributes tasks across the network among multiple platforms

2.4.3 Network Control

Networks are evolving towards the convergence of voice, video, data and mobile network technology over an IP-based infrastructure. However, Multimedia stream have different characteristics and quality of services requirements from data stream and hence it needs different protocols from the original TCP/IP protocols. Thus, news protocols are emerging like the Real-Time Protocol (RTP) and Resource ReSerVation Protocol (RSVP) for improving support to applications like video, audio and interactive multimedia conferencing. Therefore, network control provides critical functions to integrate all those services and support these different protocols. The core technology is based on softswitch and it is also the fundamental component used to support multimedia architecture and provides the interoperability between fixed and mobile convergence.

In the Public Switched Telephone Network, switches used to be predominantly hardware-based switches. With the emerging next generation network, softswitches are replacing those original switches. A softswitch provides similar functionality, but is implemented on a computer system by software. It typically has to support various signaling protocols (such as SIP, H.323, Media Gateway Control Protocol (MGCP), and others) to make call connections for multimedia sessions, often on the boundary point between the circuit and packet network [50].

There are a number of protocols used to provide VoIP services, protocols like SIP (Session Initiation Protocol), H.323 (Gateway Control Protocol), H.248, MGCP (Media Gateway Control Protocol), SGCP (Simple Gateway Control Protocol). VoIP generally uses two types of protocols: Signaling and media transfer. Signaling Protocols are used for setting up a conversation and Media transfer protocols for the actual transfer of data (stream), once the connection has been set up. Session Initiation Protocol (SIP) is an Open System Interconnection (OSI) Session-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls and multimedia distribution [5].

Softswitch is the core technology of network control layer. It provides interoperability between PSTN and IP networks and it also controls heterogeneous traffic consisted of voice, data and video. Softswitch functions include provides call control intelligence for establishing, maintaining, routing, and terminating voice calls through the IP network via media gateways, while seamlessly operating with PSTN. It can be based on session initiation protocol and use other multimedia protocols such as media gateway control protocol to communicate with media gateway. It exchanges IP telephony messages with customer Gateways, IP phones, signaling gateways, trunk gateways, and other softswitches.

Softswitch main functions include:

- Perform call control establishment and termination.
- Provide support for the multitude of edges access equipments, different types of gateways, PBX, DSLAM equipments.
- Support multitude types of protocols from the traditional PSTN, VOIP and signaling protocols as well as preventing future evolution.
- Supports multimedia communication protocols including SIP and H.323 to provide multimedia services.

Asterisk System an open source system can be used as a softswitch because it offers a wide range of features, such as supports many different communications protocols from both the modern world of VoIP and from the traditional PSTN. It is portable and scalable and usable with appliances and gateways and it's facility to interface most of the telephony hardware or software with a wide variety of telephony application.

Asterisk is an open source free software implementation originally created to be a telephone Private Branch Exchange (PBX) created by Mark Spencer of Digium. It was developed to runs over Linux platform, however it actually compatible with BSD and MacOSX operating system. Open source solutions are good options for universities due to the fact that they are not vendor-specific and so can be improved to adapt to university environment. It also helps with budget limitation and so, it helps decrease the cost of enterprise system solution and will enable university to participate and collaborate in beneficial multi-university projects.

Asterisk is a powerful system that can be used in next generation network softswitches, to provide all the services offered by Private Branch eXchange (PBX) and also provides multimedia services facilities. Asterisk's modular architecture allows it to convert between a wide range of communications protocols and media codec's. It includes support for a number of protocols like SIP, IAX, H.323, MGCP and its architecture uses channels like SIP, IAX, MGCP, and DAHDI (evolution of former ZAPTEL channel) to connect with traditional PSTN. Asterisk features facilities support services capabilities of both PSTN and multimedia control protocol, its suitable to work as voice end office as well as multimedia end office.

For connecting Asterisk to mobile network one can choose between adding a standard wireless access point to the Ethernet network or giving Asterisk a direct connection to a wireless networks. For giving Asterisk a direct connection to a wireless network some options are available now. These options include GSM or CDMA gateways box, and also available are GSM cards that are installed in the PC/Server where Asterisk is running.

Asterisk offers among others advanced features:

- Multiple Technology Dialing Application, which makes it possible to make calls through the PBX system using either soft phones or hardware phones;
- Voicemail, which allows user to have personal mail boxes which could be accessed either through the phone or via the web;

- Call Transfer and Call Conferencing, which allows users the freedom of who to include in a conversation. With the conferencing feature, users can talk to multiple callers at the same time;
- Enterprise-wide directory lookup feature, based on LDAP (Lightweight Directory Access Protocol) databases, or ENUM (global Telephone Number Mapping);
- Access to global VoIP services, for affordable international communications;
- Call Detail Recording (CDR), which logs and reports all incoming and outgoing calls for proper accountability;
- Interactive Voice Response (IVR) system, which allows voice, prompts for selecting various options.

For a large university campus with hundreds or thousands of users supported by Asterisk a set of shared Asterisks servers (Asterisk Clusters) can be used to improve the Asterisk capabilities to handle multimedia session, scale the network in a way that if one fails another can takes over.

The interfaces to the Ethernet LAN and the TDM/PSTN and PBX networks enable the Asterisk server to perform its duties as a SoftSwitch and route voice/video calls between the SIP, H.323, PSTN and PBX networks [8].

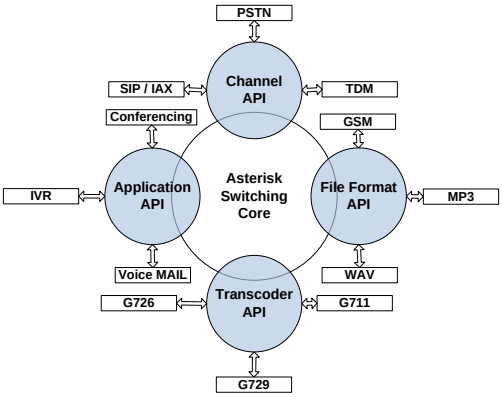

Fig 2.4 Asterisk Switching Core Architecture

Asterisk provides a switching core, with four APIs for modular loading of multimedia applications, hardware interfaces, file format handling, and codec's. Asterisk provides transparent switching between all supported interfaces. This is how Asterisk ties together diverse telephony systems into single switching network [6].

Asterisk Switching Core – is the essential component that allow interconnection of calls between different users and tasks. The switching core connects in a transparent way all calls between different hardware and software.

Channel API – manipulate the type of connection call, such as VoIP, ISDN, PRI or others technology. Dynamic modules are loaded to manipulate the details of interface over a channel.

Application API – it's responsible to launch applications that run services, such as voicemail and parking calls, etc.

Codec Translator – it uses the codec module to code and decode different compressed format that pass through the PBX, such as G711 or G729.

File Format API – interfaces with various file-formats used by different parts of the PBX. In this way, if a developer wants to use a new type of file format for some purpose, he can just create a new module for the File Format API.

Rash [46] has done a very intensive research about SIPexchange and Asterisk. He concluded that Asterisk is a lot more than a private branch exchange. It also takes on the functions of a media server, a protocol gateway and a conference bridge. It goes beyond voice over internet protocol, too, supporting other types of digital communication.

2.4.4 Core Switching

The next generation network is characterized by the convergence of infrastructure and services with IP being the new fundamental technology. The core switching is based on the IP network infrastructure already implemented special because of financial limitation and cost saving. Composed of packet core network, it's usually constituted of Layer2 and Layer 3 switch and routers. Ethernet is widely adopted at campus networks due to its excellent cost/performance ratio and its configuration convenience.

The core technology for the campus network can be hybrid technology consist of fiber optical and wireless technologies because of it advantages, such as high bandwidth facilities and mobility.

2.4.5 Edge Access

Edges access is the part of network responsible to connect subscribers and equipments through different access technologies and provides information conversion to a format suitable to be transported over the network.

According to the total number of users, a centralized broadband remote access server (BRAS) device can connect to multiple L2/L3 switches, as well as DSLAMs,

HFCs, and WLANs equipments according to the access technology deployed in the access layer.

Media gateways are located at the edge access layer, and they have the functions of connecting the circuit-switch (PSTN) and packet-based network. They implement conversion between different types of network.

There are a multitude of customer's premise equipments (CPE) ranging from Wi-Fi (only) phones, Sip desk phones with a wireless link, Dual-mode (GSM and SIP) phones, PDA/smart phones, IP phone and the traditional POTS or Analog Telephones and Fax machine. These equipments have many advantages such as mobility inside the office and in areas covered by wireless networks (hotspots), high speech quality, interoperability between PSTN and VoIP networks and facility to use IP networks to make calls instead of PSTN.

①Media Gateway

A media gateway (MG) is a network element that provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks [10]. A gateway is a network device that acts as an entrance to another network and connects the two different networks. One of its functions is to convert media provided in one type of network to the format required in another type of network. For example, a gateway could terminate bearer channels from a switched circuit network (e.g., DS0s) and media streams from a packet network (e.g., RTP streams in an IP datagrams).

The Media Gateway Controller (MGC) control media gateways. It has the function of establish and disconnect end-to-end devices connection. MGC provides call routing, control of the connection, and the control of network resources. Media gateway architecture and main components are depicted in figure 2.5.

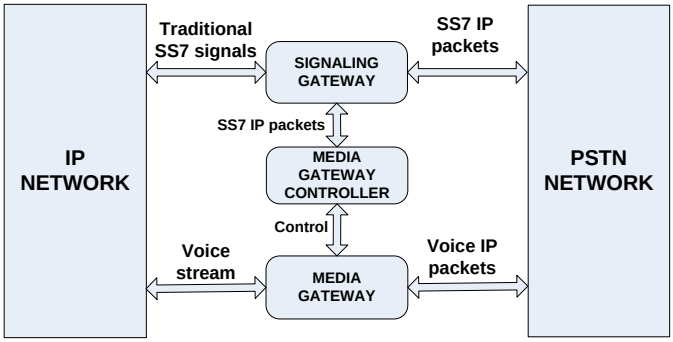

Fig 2.5 Decomposed Media Gateway Architecture

Session Initiation Protocol - Signaling Protocol

SIP is a session protocol standardized by Internet Engineering Task Force (IETF) through a set of (RFC) 2543, 3261, 3515, etc. Because of its simplicity it has been adopted as the VoIP protocol of choice. SIP is an application layer protocol whose functions is to establish, modify and terminate multimedia sessions, such as phone calls and conferencing meeting with one or several participants through the IP network [28]. It makes possible for users to initiate and receive communications and services from any location, and for networks to identify users wherever they are. SIP is a signaling protocol and so it does not transport media between endpoints. It establishes the sessions and then other real-time transfer protocols such as RTP are used for media transmission. SIP uses the Session Description Protocol (SDP) which describes the media content (the codec being used, IP address and port, etc).

SIP implements client/server architecture, but SIP endpoints contain both User Agent Client (UAC) and User Agent Servers (UAS). Every SIP transaction takes the form of a request from a SIP client (UAC), and one or more replies from a server (UAS). SIP comprises set SIP entities that are the following [28]:

- User agents - are the devices that initiates request. Some examples are IP phones and softphones.
- Proxy servers - are application-layer entities that forward SIP requests and responses.
- Redirect servers - provide the alternative location of user agents or proxy servers when the original destination cannot be reached.
- Registrars - keep track of their assigned network domain. They are in charge of authenticating users, and they maintain information about the subscribers SIP address and their actual location (i.e. the IP address at which they can be contacted).

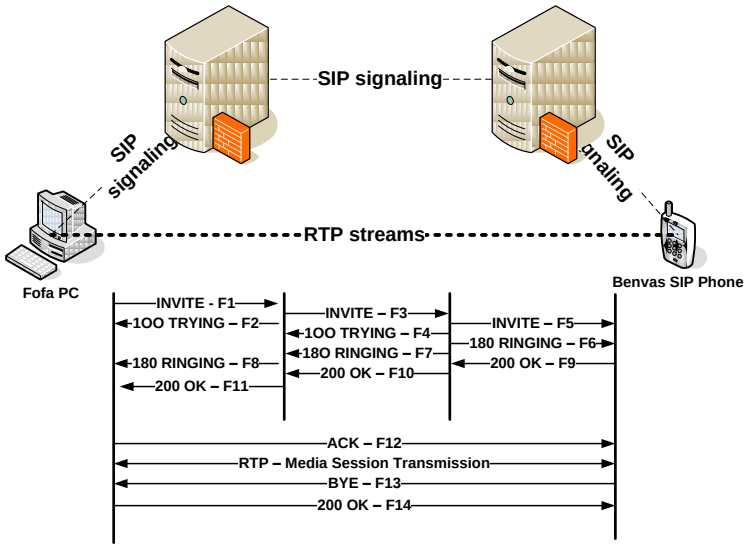

Fig 2.6 - SIP Typical Session Example between Fofa and Benvas

Figure 2.6 depicts the procedure and message flows during the process of establishing a SIP session between two users: Fofa and Benvas.

The Real-time Transport Protocol

The Real-time Transport Protocol (RTP) is one of the most commonly used protocols for carrying audio and video stream. It is often used in conjunction with the Real Time Control Protocol (RTCP) [47], which allows the receiver to control the flow of the data by issuing commands such as pause and rewind. However, for VoIP systems, it needs to be used in conjunction with a signaling protocol such as SIP or H.323. The signaling protocol is used to establish and maintain the session and RTP connection additionally carry the streams and defined the aspects such as codec (the compression/decompression algorithm used to encode the multimedia data contained in the stream).

2.5 Quality of Services (QoS)

As we move toward converged networks, a network that use a single network protocol to send all kind of traffic, be it voice/audio, video and data, a new network model is gradually substituting those traditional separates network of voice and data switched network. Because multimedia streams and data have different requirements therefore different quality of services mechanism should be provided.

The concept of Quality of Service refers “to the ability of a network to provide improved service to selected network traffic over various underlying technologies [36]”.

With the emerging of new multimedia service, such as voice over IP (VoIP), videoconferencing and other real-time applications with different level of sensitivity, assure the appropriate QoS is become more and more important and challenging. Initially IP network was not created to be QoS-aware, and it could only delivery best-effort services, so the IP technology has to be modified to meet the needs of new emerging services.

When congestion occur in the network, traditional procedures such as caching are not suitable for real-time voice data or for videoconferencing application. In case of packet losses, the packet retransmission method cannot be applied because the delay would be unacceptable resulting in a bad quality of services to the user.

Therefore when design a network, QoS policies and rules to classify, prioritize, and schedule sensitivity traffic is a crucial task. Another alternative is to apply congestion management and congestion avoidance in overloaded points in the network. There are several schemes that can be applied to improve the QoS. Schemes such as Weighted Random Early Detection (WRED) and Weighted Fair Queuing (WFQ) are two examples.

WRED is a congestion avoidance queue management algorithm that takes advantages of TCP's congestion control mechanism. In Weighted Random Early Detection selected packets are randomly dropped based on IP precedence. Thus the higher priority traffic is delivered with a higher probability than lower priority traffic. WRED can be useful on core routers interface where congestion are likely to occur.

Weighted Fair Queuing is congestion management strategy. WFQ classifies packets based on flows and each type of packet is isolated and stored in its own queue and given a different priority level and bandwidth reservation for them [28].

2.5.1 Parameters for Measure QoS

Three important parameters are used to measures QoS: Delay, Jitter and packet loss. **Delay** is the time taken by a packet from point-to-point in a network. Delay can be measured in either one-way or round-trip delay. VoIP typically tolerates delays up to 150 ms before the quality of the call become unacceptable.

Jitter is the variation in delay over time from point-to-point. If the delay of transmissions varies too widely in a VoIP call, the call quality is greatly degraded. One mechanism used in VoIP Network to compensate for this is by having jitter buffers.

Packet loss is loosing packets along the data path, which means that it does not arrive at its destination, which severely degrades the voice quality.

Voice traffic is sensitive to delays, variation in delays (jitter), and packet loss. The guidelines for ensuring acceptable quality of service for different traffic type are displayed in table 2.1 [28]:

Table2.1 QoS Requirements for Different Applications

Traffic type	Bandwidth	Packet loss (max)	Delay (max)	Jitter (max)
Interactive voice (G.711)	12-106 kbit/s	1%	150 ms	30 ms
Streamed video (MPEG-4)	0.005-10 Mbit/s	2%	5000 ms	Insensitive
Streamed audio (MP3)	32-320 kbit/s	2%	5000 ms	Insensitive
Data	Variable	Sensitive	Insensitive	Insensitive

2.5.2 Methods of Implementing QoS

①Best Effort (BE)

Best Effort is the standard quality of service provided for traffic transportation. It's a network policy for which no special QoS model is implemented; therefore all kind of traffic is treated equally. As the name imply, "best efforts" are made to delivery all the packet to the destination but with no guarantees of delay, packet loss, etc. There is no differentiation between the kinds of traffic; all packets receive the same treatment independent of its content, there is no classification or prioritization.

BE is the treatment that packets get when no predetermined treatment is specified for them. If there is congestion on the medium, function as caching can be used to store temporarily the packets and when the situation is solved packets will be forwarded. In the event of extreme congestion, when the network device cannot handle the situation no more, packets can be dropped indiscriminately.

For Packet loss the retransmission methods is one of the alternatives method used. This model is well suitable for services such as web mail, file sharing, IM, etc. However for real-time services different models that can guarantee quality of service must be used.

As has been showed, best-effort service is not suitable to guarantee end-to-end QoS for all kind of traffic. To provide end-to-end QoS two models have been deployed: IntServ and DiffServ. End-to-end QoS means that the network provides the level of service required by traffic throughout the entire network, from one end to the other.

②Integrated Services (IntServ)

The basic concept behind IntServ is that an application request specific treatment

from the network device that makes decision in forwarding traffic (such as router or Layer 3 switch), and the network device confirm that it can provide the required resources, and they come to an agreement before any data is sent. Integrated Services QoS is achieved through an agreement of specific treatment for a given type of traffic before it is sent.

IntServ uses an explicit signaling mechanism from applications to network devices. Signaling is used to reserve and release resources in the network. QoS signaling allows network node to communicate with its neighbors to request specific treatment for a given traffic type. The application requests a specific service level, including, for example, its bandwidth and delay requirements. After the network devices have confirmed that it can meet these requirements, the application is assumed to only send data that requires that level of service.

Applications in an IntServ environment use the Resource Reservation Protocol (RSVP) to indicate their requirements to the network devices. The network devices keep information about the flow of packets, and ensure that the flow gets the resources it needs by using appropriate queuing (prioritizing traffic) and policing (selectively dropping other packets) methods. Two types of services provided in an IntServ environment are as follows:

- **Guaranteed Rate Service** - This service allows applications to reserve bandwidth to meet their requirements. The network uses weighted fair queuing (WFQ) with RSVP to provide this service.
- **Controlled Load Service** - This service allows applications to request low delay and high throughput, even during times of congestion. The network uses RSVP with weighted random early detection (WRED) to provide this kind of service.

InterServ is a very networking consuming resources, because it requires RSVP on all network devices. This characteristic make it currently not used as much as DiffServ.

③Differentiated Service (DiffServ)

Differentiated Services mechanism technique is to treat packets with different level of requirements depending on their source, destination and/or the kind of traffic they are carrying. It does not make use of the network signaling techniques. The network tries to provide level of service based on the quality of service defined in the header of each packet. Packets is usually classified or marked by edge network devices according to previous defined criteria such as source, destination and kind of traffic.

Classification and Marking is the fundamental base of DiffServ as it helps implement priority in the network. At first packet is identified, therefore depending on that identification it is given priority over other packets or different treatment from them. The process of classification of packet is the process of analyze and sort packets according to its content between different categories. It means that each packet is assigned as belonging to voice category, data category or multimedia category, etc.

Each category has different level of quality requirements. Marking process will check the category that the packet belong to and therefore put a mark or level of priority within the head of packet. Packets belonging to voice category are marked as high priority.

The place within the network where markings are accepted is known as the trust boundary so any markings made by devices outside the trust boundary can be overwritten at the trust boundary. Establishing a trust boundary means that the classification and marking processes can be done once, at the boundary and the rest of the network then does not have to repeat the analysis.

3 ACCESS NETWORK KEY TECHNOLOGIES

3.1 Introduction

Broadband access to the Internet has evolved rapidly to become essential infrastructure for our global information economy. European Commission concluded that: "widespread and affordable broadband access is essential to realize the potential of the Information Society"[①]. The access network features a number of alternative implementations and several technologies.

Access networks are the most expensive part for operators. The access network connects subscribers to the core network transport facilities, enabling end-to-end service provision. More specific, the access network connects the customer premises equipment and a set of service nodes, either directly connected or remotely connected via a transport network. It provides the link for transportation of the user traffic and control signals to the backbone network. This is the part of the network known as subscriber network, “last mile”/”first mile” or the local loop.

The Telecommunications Act of 1996, which triggered deregulation of telecommunications industry and encourage the rapid deployment of new telecommunications technologies in United States and many others countries around the world, led to the development of several last-mile solutions to relieve the PSTN switches of the data traffic. These solutions include the digital subscriber line group of technologies that are generally referred to as xDSL, hybrid fiber coaxial (HFC) network, fiber-to-the-home (FTTH), and broadband wireless access network. These solutions have one thing in common: they are broadband solutions, which mean that they have the potential to provide data rates of at least 1 Mbps to the user. Also, they are always-on Internet access technologies. Thus, they have the potential to meet the growing demand for multimedia and voice applications [37].

According to ITU-T, the Next Generation Network is defined as a packet-based network able to make use of multiple broadband accesses, with QoS-enabled transport technologies and service-related functions are independent from underlying transport-related technologies. It enables unfettered access for users to networks and to competing service providers and/or services of their choice [38].

① http://www.c-c-g.com/Broadband%20and%20Employment.pdf

Access network is the part of network that provides access capabilities for a wide variety of types of user equipment to access service providers; it connects subscribers to the central office (C.O.). It has been traditionally simple twisted copper pair based and point-to-point, however access network is now becoming increasingly complex.

Given the limitation of the traditional C.O. switches (64k per line), current access infrastructure cannot be the right basis for the Internet emerging services. To meet the requirements of the next generation access network, a convergence between optical and wireless access infrastructure network is required, contrary than the traditional access network when such technology (broadband wireless and optical access network) are deployed separately, which increase network complexity and capital and operational expenditures (CapEx and OpEx)

Access network is evolving towards broadband IP, fixed/mobile convergence and service convergence. For fixed (wired) access network services, FTTx technology is promising to delivery high bandwidth capacity, and recently fiber-to-the-home (FTTH) is gaining wide interests for its high capacity. Among all the FTTx solutions, Passive Optical Network (PON) is considered the most promising technology. The wide deployment of both G(Gigabit)-PON and GE(Gigabit-Ethernet)-PON are increasing rapidly. For wireless services, broadband wireless access such as WiFi and WiMAX are expected to be widely deployed as a complement for 3G and beyond 3G cellular mobile accesses in order to provide portable/mobile multimedia services.

Access network faces several technical challenges, such as poor user management capability, poor service control capability, and unreliable network security. Facing the diversity deployments, especially for campuses, one of the biggest challenges is to build a heterogenic network, that is, different types of access networks are inter-connected and interoperable, allowing users seamless roaming between different network types.
For campus network, the basic technical is mostly same to counterpart in telecom-carriers.

3.1.1 Problems with the Current Access Solutions

A set of problems has driven the evolution of access network [26]:

- Traditional TDM access technologies are very expensive to add additional or new services
- No true integration of services into a single subscriber access line yet
- Multiple bills from the same service provider

- Infrastructure product are all provided from different vendor and there is a need for interoperability
- Scaling and installing subscriber services to the masses has been very difficult
- Not all access technologies will support broadband value added services.

3.1.2 Challenges for Access Network

Challenges of next generation network are to figure out solutions for the problems of current access network. It can be grouped as:

- Proper user management through generating, processing and terminating the user access services (such as VLAN and PPPoE), and also user identification, authentication and authorization, and management.
- Rapid delivery of services, since it should provide bandwidth on demand and flexible response to residential and business demands for services such as VoD.
- A wide range of new services and value added services, to guarantee the provision of services, quality of service and security is very important and the ever –increasing bandwidth demands for them.
- Mobility and ubiquitous demands, always on, anytime and anywhere.

Broadband Access Server is the core and fundamental device of broadband access network, the key component to realize the operable, manageable and profitable broadband network.

User management is a function whereby telecommunication carriers manage the users of their networks. In this particular requirement, Broadband Access Server plays an important role. It is suitable for access networks of Ethernet, Digital Subscriber Line (xDSL), Hybrid Fiber Coaxial (HFC) and Wireless Network, providing subscriber management, accounting control, address management, service control and security management functions.

The network structure of a campus network is similar to that of an enterprise network. The operation mode of a campus network, however, approaches to that of a carrier’s network, because both of the two kinds of networks need to provide functions such as access control and charge policy like by duration or flow. The users can access the campus network directly. If they want to access the Internet, they must first pass the authentication and will be charged according to radius policy implemented. In a campus network, the BAS are usually positioned at the access layer or connected to the convergent switch, providing access authentication, charge management and security control.

3.1.3 Broadband Access Server

Broadband Access Server (BAS) provides the ability to control what each subscriber is doing based on the service they have signed up for, as well as simplifying overall network operations. BAS concatenates network access by providing a central point for change control. When there is a need for network changes, it is simpler to make the change at a single BAS than at many devices. BAS aggregates a very wide range of services, what reduce the necessity to deploy different equipments, perhaps from different vendors preventing problems with interoperability issues.

Another important added value of the broadband network is the ability to effectively manage traffic in the access network. One approach can be per-service QoS or another one prioritization of traffic based strictly on the priority bit settings within the packet.

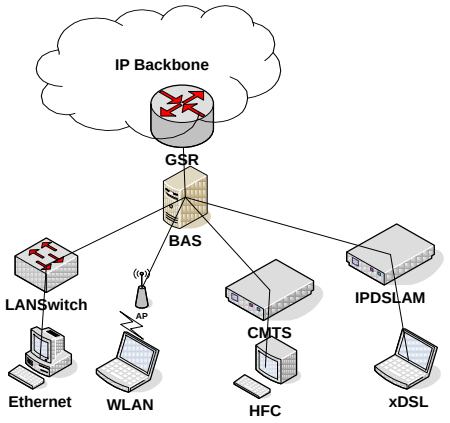

Fig 3.1 - BAS Function in Network

Basic functions for BRAS include aggregation and termination capabilities between the access and aggregation or core network, IP routing, Policy management QoS and CoS, supply connection to RADIUS (Remote Authentication Dial In User Service) therefore provides Authentication, Authorization and Accounting.

An increasing number of services are required to be relayed over the broadband access network, in this particular, one problematic issue is the bottleneck affecting broadband access server equipment given that all traffic originating from a multitude of services passes through it. This culminates in the following problems: forwarding capability, consistent reliability, complex QoS demands and guarantees for real-time services such as VoIP and IPTV.

3.2 Digital Subscriber Line (DSL) Access Technology

DSL has been the most popular technology in access network. Digital Subscriber Line technology is a set of technologies, each differing in the first letter (ADSL, VDSL, HDSL, and SDSL). The set is often referred as xDSL technologies. It has been designed for digital transmission across existing local loops, combining cost effectiveness and acceptable performance.

DSL technologies are composed for a wide range of technologies. Many reasons have contributed to the popularity of DSL technologies, these include but are not restricted to, the facility of its deployment; the fact that it requires low infra structure investments since it shares telephone line. It provides security using dial-up modem or T1 connection. It offers asymmetric data rates which matches with internet applications requirements for home users. DSL is several times faster than ISDN. Several reasons has driven the evolution of DSL, factors such as increase bandwidth demand and also end user requirements for symmetric services, the purpose of operational simplicity, and the technology evolution in layer 2 transport ATM to Ethernet layer 2.

The problem of DSL is that, due to attenuation and crosstalk, it is impossible to achieve long range and high speed simultaneously. The farther is the customer located from the local exchange the lower is the data rate that can be provided. So there is a trade-off between copper length and bandwidth.

Asymmetric Digital Subscriber Line – ADSL

ADSL technology is used to transport data in addition to the regular telephone services from the central office to the home. It makes uses of the existing telephone wires so that it can deliver broadband data services. The interesting point is that it uses the existing local loops infrastructure and it requires a simple addition of modems at the customer termination and broadband service access points (Digital Subscriber Line Access Multiplexers - DSLAM) at the exchanges are sufficient.

ADSL provides a considerably higher downstream data rate than the upstream rate. That’s why it is called asymmetric. It was designed to adapt to the residential customer, that need higher data rate for downstream (from the Internet to resident) than for upstream (from the resident to the Internet). Therefore it is not the most suitable for business corporations that need high data rates in both directions.

The data rate that it can provide depends on several requirements:

- the length of the twisted pair: the longer the twisted pair, the lower the bandwidth that it can provide;

- The wire gauge: that is a measurement of how large a wire is, either in diameter or cross sectional area. This determines the amount of electric current a wire can safely carry;
- Presence of bridge taps: it is a long-used method of cabling for telephone lines. One cable pair (of wires) will "appear" in several different terminal locations (poles or pedestals). This allows the telephone company to use or "assign" that pair to any subscriber near those terminal locations. Once that customer disconnects, that pair becomes available at any of the terminals. The bridge tap affects the network depending on where it is located, the farther away from the customer's location, the better.
- Cross-talk interference and so on.

Ignoring bridged taps, currently ADSL can deliver for downstream up to 6.1 Mbps for a maximum distance of 12,000 feet (3.6576 km), and 8.128 Mbps for a maximum distance of 9000 feet (2.7432 km) over a single unloaded 24 gauge twisted pair. Upstream data rates currently range between 64 Kbps and 800 Kbps.

Services such as Triple-Play are extremely difficult to provide with ATM DSLAM, and IP DSLAM is a necessity. Currently, operators are increasingly opting to provide Triple-Play services, which include voice, video and Internet, by deploying IP DSLAM in the access network layer.

Today, ADSL standardization and roll-out continue, and new versions such as ADSL2 and ADSL2+ enhance its performance even further [28]. ADSL2 adds new features and functionality to ADSL and it was standardized by ITU-T in 2002 (G.992.3 and G.992.4). ADSL2+ was standardized by ITU-T in 2003 (G.992.5) and it doubles the downstream bandwidth, thereby increasing significantly the downstream rate for telephone lines shorter than 5000 feet (1.524 km). The speeds drop off as the distances increase.

VERY HIGH DATA RATE DIGITAL SUBSCRIBER LINE – VDSL

Bandwidth increases demands have driven the industry, from ADSL to bonded very-high-bit-rate DSL. VDSL can achieve very high data rates and offers more bandwidth than ADSL by bringing fiber closer to the customer, however, it has a distance limitation over which such data rates can be achieved. VDSL can achieve a downstream data rate of 52 Mbps and an upstream data rate of 6 Mbps over a distance of up to 1000 feet (0.304 km approx. 300 meter). Due to its distance limitation, the longest distance it can be transported is currently 5000 feet, for which it can achieve 13

Mbps downstream and 1.6 Mbps upstream. Some of the applications of VDSL are to deliver high quality video, access to the Internet and regular telephone services [28].

Evolution of VDSL has lead to VDSL2 which increases the bit rate from 20 Mbps to up to 100 Mbps. This improvement is possible with the use of power spectral density (PSD) shaping, which allows adaptation of the signal spectral density to the transmission channel and local noise conditions. PSD shaping tools provide the ability to adapt VDSL2 carrier power to maximize performance and compatibility with adjacent xDSL lines.

Others variations of DSL technologies exist, Single Line Digital Subscriber Line – SDSL, Single-Pair High-Speed Digital Subscriber Line (SHDSL) and High Data Rate Digital Subscriber Line – HDSL The table3.1 summarizes a set of the most common used xDSL technologies and their main characteristics.

Table 3.1 xDSL Technologies Main Characteristics

Name	**Meaning**	**Data Rate**	**Mode**	**Applications**
DSL	Digital Subscriber Line	160 Kbps	Duplex	ISDN Service, Voice and data communication
HDSL	High Data Rate Digital Subscriber Line	1.544 2.048 Mbps	Duplex	T1/E1, LAN access, server access
SDSL	Single Line Digital Subscriber Line	1.544, 2.048 Mbps	Duplex	Same as HDSL plus premises access for asymmetric services
ADSL	Asymmetric Digital Subscriber Line	1.5 to 9 Mbps 16 to 640 Kbps	Downstream Upstream	Internet Access, VoD, interactive multimedia
VDSL	Very high data rate Digital Subscriber Line	13 to 52 Mbps 1.5 to 2.3 Mbps	Downstream Upstream	Same as ADSL plus HDTV

Despite its many advantages, DSL cannot be seen as the definitive solution for the access network. DSL alone cannot meet the challenges of future broadband applications such as High-Definition TV, which may require very high bandwidth. Some of the most innovative DSL solutions, like VDSL are designed to achieve very high bit rates, but within a range limited to a couple of hundred meters. Two of most critical limitation of DSL are [28]:

- Attenuation is caused by progressive loss of the electrical energy of DSL signal in the transmission line. Attenuation is higher in longer loops, and it also depends on the frequency of the signal being transmitted.
- Crosstalk is the electromagnetic coupling of a signal from one communication channel to another, and it occurs when some of the transmissions signal energy leaks from the cable. Because copper pairs are grouped into binders and one binder may contain many copper pairs, as a result signals transmitted on one pair of wires couple into the other wires in the same cable.

In general with DSL technologies there is a trade-off between distance and capacity.

3.3 Cable Access Network

Cable access network is the combination of fiber optics and coaxial cables, for this reason this architecture is known as the hybrid fiber coaxial (HFC) architecture [28]. The fiber carries the signals over most of the network, and the coaxial is only for the last kilometer or so.

Cable network architecture consists of the headend, multiple optical fiber trunks extending from the headend, and coaxial cables. The headend transmits the TV channels which are distributed in a broadcast way to the homes over the cable network. Each fiber trunk extending from the headend terminates at an optical network unit (ONU). From the ONU, a number of coaxial cables fan out into the neighborhood, each serving a number of homes.

Data-over-cable service interface specification (DOCSIS) provides high-speed access to the home over an HFC. It permits a transparent bidirectional transfer of IP traffic between the cable system's headend and the homes. This is realized using a cable modem termination system (CMTS) at the headend, and a cable modem (CM) at each home. The CMTS is a packet switch that is equipped with network interfaces and interfaces to the data-over-cable system. The network interfaces are used to communicate with one or more MAN/WAN networks to which it is connected, and the interfaces to the data-over-cable system are used to transmit and receive data from the CMs over the HFC cable network. The maximum distance between the CMTS and a CM is 100 miles, but it is typically limited to 10 to 15 miles [27].

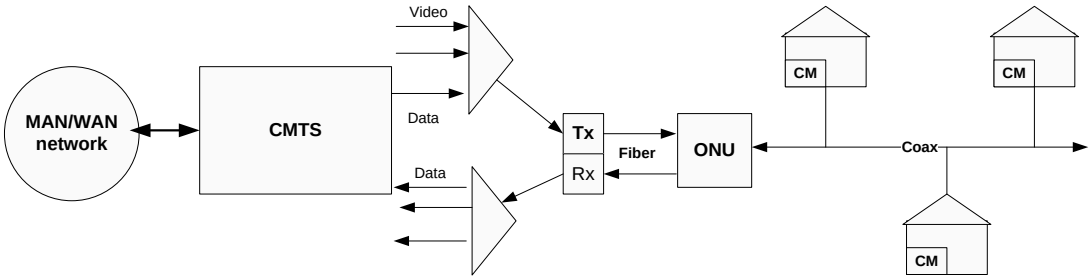

Fig 3.2 The DOCSIS Reference Architecture

Data that is transmitted to the CMs is modulated onto a carrier; it is then multiplexed with all of the television signals and the other signals in the downstream direction. The resulting signal is transmitted out on the optical fiber which terminates at the ONU, and from there it is distributed to all of the homes attached to the coax cables that fan out from the ONU. The data stream transmitted by the CMTS is extracted by each CM, from where it extracts the IP packets destined to it. On the upstream side, each CM transmits IP packets towards the CMTS. These packets are modulated on a carrier ranging from 5 MHz to 42 MHz. Multiple carriers can also be used. A specially designed MAC, referred to as the DOCSIS MAC, assures that there are no collisions in the upstream direction [27].

3.4 Wireless Access Network

Next generation wireless systems are envisioned to provide high-speed Internet access to home and mobile users, high quality multimedia services, including video-conferencing, high resolution image and file transfer over mobile and hand-held devices. However, providing a high-performance, scalable and cost-effective wireless infrastructure requires new system and network architectures.

The radio access network (RAN) constitutes one of the biggest challenges. The access network provides the vital link for backhauling user traffic and control signals to the backbone network.

3.4.1 Spectrum Management

The electromagnetic spectrum is fundamental resource in a wireless communication system. This spectrum is divided into several bands that are used for specific applications. The frequency band associated with an application determines the propagation characteristics of the Radio Frequency (RF) channel. In particular, the frequency band determines how much energy density is left in the signal at a given

distance from the transmitter under given terrain, foliage, and weather conditions. Also propagation impairments vary according to the frequency band.

One of the general rules regarding the use of the radio-frequency spectrum is that as new applications are developed, the frequencies assigned for handling them tend to increase. This is due to the fact that use of the spectrum is regulated by the government, which is responsible for licensing the use of the bands of the spectrum. Thus, it is only in the higher end of the frequency spectrum that very large bandwidth can be made available for these new applications. Unfortunately, the technology for supporting applications at these very high frequencies becomes more challenging as the propagation impairments become very severe. Also, it takes a long time to develop economically viable semi conductor devices that can operate at higher frequencies [29].

3.4.2 Broadband Wireless Access Network

Wireless broadband access technologies refers to high-speed wireless services that service providers deploys within a metropolitan areas or areas where installing physical cable has high costs, such as remote rural areas to provide Internet access and other services.

Broadband Access in Wireless networks faces several challenges. One of them is related with the optimum management and allocation of spectrum and bandwidth limitations. Another factor is impairments due to noise from the environment or weather conditions and interference that the signals suffer.

A broadband wireless access network consists basically of two principal components: the customer premises equipment (CPE) that enables a user in the customer's network to access variety of services, and the base station that controls the CPEs within a coverage area. The network is divided in a set of small sector or also called cell, with a physical limited coverage area. The base station consists of many access points or wireless hubs, each of which controls the CPEs in one sector. The access points are connected to a multiplexer, such as a switch, which aggregates the traffic from different sectors and forwards it to a router that is connected to the service provider's backbone IP network [29] according to the scheme depicted in figure 3-3.

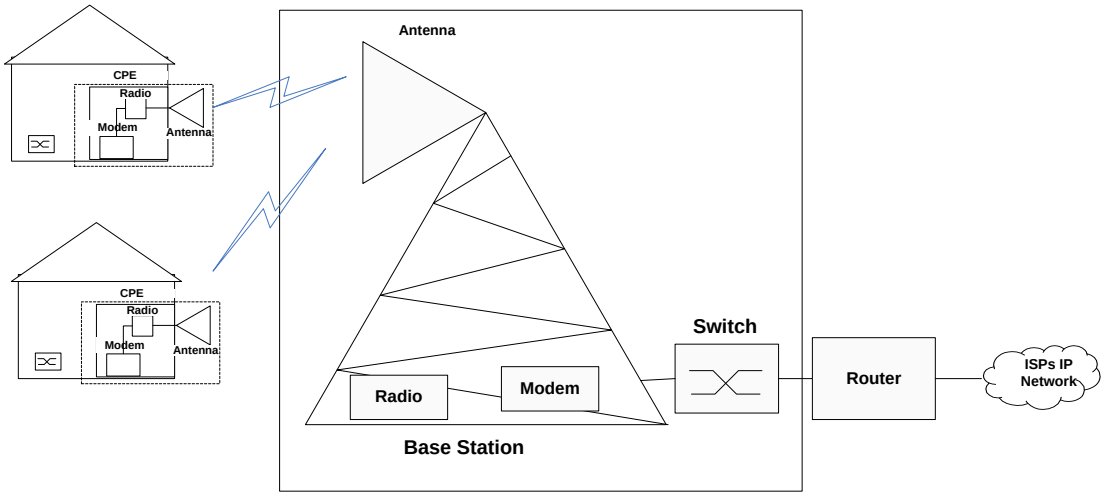

Fig 3.3 Fixed Broadband Wireless Access Network Architecture

The distance between the CPE and the base station depends on how the system is designed and the frequency band in which it operates. If it is designated as a line-of-sight (LOS) system, the distance is generally less than 8 km. Typically systems that operate above the 20-GHz band are LOS systems. However, most of the early deployments of fixed broadband wireless access networks were based on LOS technologies because, non-line-of-sight (NLOS) system were still very expensive to deploy. NLOS systems use more advanced modulation schemes to overcome the transmission impairments.

The air link capacity available to each sector depends on the modulation scheme used. The most commonly used modulation schemes are quadrature phase shift keying (QPSK) and different variations of the quadrature amplitude modulation (QAM) which the most commonly used being 16-QAM and 64-QAM. QPSK is mainly used in the upstream direction, which is the direction from the CPE to the base station, and 64-QAM is used in the downstream direction (or the direction from the base station to the CPEs). The 16-QAM can be used for either direction. QPSK is functionally identical to 4-QAM, which means that it has a lower modulation order than 16-QAM [29].

The figure 3-3 depicts the fixed broadband wireless access networks architectures and components. The wireless hub provides a wireless interface for receiving and transmitting data from and to the CPEs. The wireless hub is connected to the backhaul router via a switch. The switch can be an Ethernet or ATM switch. The router is the default gateway to the Internet and the service provider's IP backbone network. There are three components parts of the CPE: the modem, the radio, and the antenna. The

modem provides an interface between the customer's network and the fixed broadband wireless network, while the radio provides an interface between the modem and the antenna.

3.4.3 Broadband Wireless Technologies

Broadband wireless offers users ubiquitous and continuous coverage mobility. In order to support this service mobility, a network of interconnected and overlapping mobile base stations that seamlessly hand-off users while moving across adjacent cells is deployed. Each mobile base station has a ray of coverage which can be up to few kilometers. The cells towers are connected to each other by a backhaul network that also provides interconnection to the wireline Public Switched Telecommunications Network (PSTN) and other services.

Two advantages of wireless technologies are that first there is no need to re-wire the building or run cables all over the campus and second is that it facilitates mobility. This includes both (1) the ability to move devices around without having to move cables and rearrange spaces; and (2) the ability to stay continuously connected over a limited coverage area. The first situation is typically referred as local mobility and this is one of the key advantages of WLANs over traditional wireline LANs. The second type of mobility is one of the key advantages of mobile systems such as 3G.

The major broadband wireless access network technologies are as follows:

- 3G/ 4G
- WiFi
- WiMAX

3.4.4 Third and Fourth Generation (3G and 4G)

Third generation mobile technologies (3G) allow mobile operators to offer integrated data and voice services over mobile networks. The concept of 3G Systems was to provide a global mobility with wide range of services including telephony, paging, messaging, Internet and broadband data. The International Telecommunication Union (ITU) started the process by defining the standard for the third generation, the International Mobile Telecommunications 2000 (IMT-2000). In Europe, ETSI (European Telecommunications Standards Institute) was responsible of UMTS standardization process. Third Generation Partnership Project (3GPP) was formed to continue the technical specification work.

The mobile cellular systems began with the limited analog cellular (first generation), however it has vastly improved and are still widely deployed around the world. Each

new generation offers significant “revolutions” in performance and capabilities compared to its predecessor. In wireless access network, this often means assigned a new frequency band to the new technology generation. The third-generation is a generic term used for the generation of mobile communications systems, which provide enhanced services such as voice, text, and high-speed data as depicted in figure 3.4.

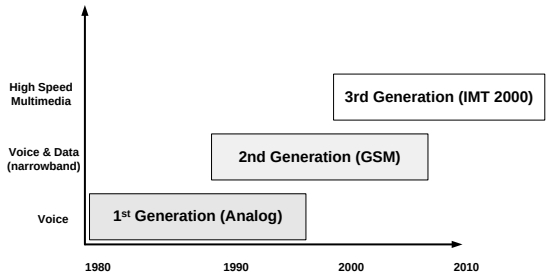

Fig 3.4 Mobile Communication Evolution

The **First Generation** started in the early 1980’s. It utilizes analog technology over switched networks and supported voice-only capabilities. These systems were characterized by very limited features, poor voice quality, and limited radio coverage.

The **Second Generation** started one decade later (1990’s). 2G is based in Digital Technology, although it’s still utilizing the circuit-switched networks. The main goal was improving voice quality, coverage, and capacity. The world’s four primary mobile digital wireless standards currently deployed around the world use technologies such as GSM (Global System for Mobile Communications), TDMA (Time Division Multiple Access) (IS-136) and CDMA (IS-95-B) (Code Division Multiple Access), all supporting speeds ranging from 9.6 kbps to 28.8 kbps. CDMA and TDMA were widely deployed in U.S, while GSM was deployed as the common standard in Europe.

The **2.5 Generation (2.5 G)** is referred as Enhanced Second-Generation Mobile Standards. It was built upon 2G standards by providing increased bit-rates and bringing limited data capability. This generation includes at least one of the following technologies: high-speed circuit-switched data (HSCSD), General Packet Radio Services (GPRS), and Enhanced Data Rates for Global Evolution (EDGE)). The Data rates range was increased from 57.6kbps to 144kbps.

The **Third Generation** is the generation of mobile service capabilities, such as, higher capacity and enhanced network functionalities, which allow advanced services

and applications, including multimedia. Third generation aims to converge telephone, Internet and broadcasting media in a single device

3G is the wireless network technology that provides high speed bandwidth (high data transfer rates) to handheld devices. This high data transfer rates allow 3G to offer multimedia services combining voice and data. To differentiate 3G from 2G the ITU defined higher and detailed performance levels then those obtained from 2G mobile networks, in particular minimum data speeds, for various specific radio operating environments.

IMT-2000 is the global standard for third generation (3G) wireless communications. It covers key issues such as frequency spectrum use and technical standard. It provides a framework for worldwide wireless access by linking the diverse systems of terrestrial and/or satellite based networks.

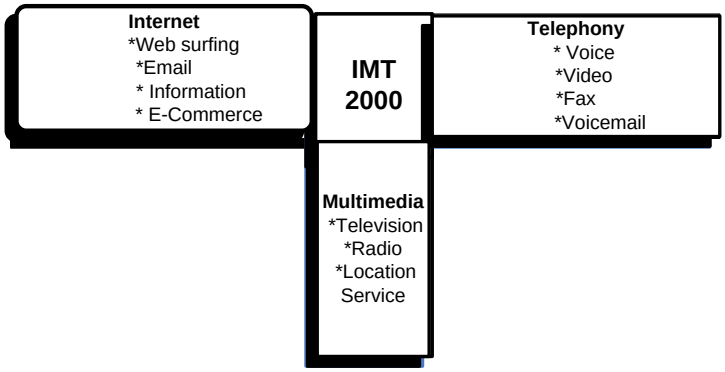

Fig 3.5 Convergence of Services in IMT-2000

Forth Generation

The fourth generation (4G) mobile communication systems are expected to provide a wide variety of new services, from high-quality voice and high-definition video to high-data-rate wireless channels. The 4G systems will not only support the next generation of mobile service, but also support the fixed wireless networks. There is no formal definition for what 4G is; however, there are certain objectives that are projected for 4G. Technically, 4G stands for one integrated, IP-based environment for all telecommunications requirements including voice, video, broadcasting media and Internet that utilizes both fixed and wireless networks [43].

3G networks are inadequate to accommodate WLANs as access networks, which offer data rates of 11 Mbps. 4G will be capable of providing bandwidth between 100 Mbit/s and 1 Gbit/s both indoors and outdoors, with quality and high security. Fourth

generation will support several types of broadband wireless access communication systems, not only cellular telephone systems. 4G networks are likely to use a combination of WiMAX and Wi-Fi technologies [44].

Although, 4G does not have any solid specification yet, the key design parameters rely on general proposals. The desirable characteristics of 4G are [43]:

- Carrier frequency: 5GHz;
- Channel bandwidth /operator: 50MHz
- Target data rate: 100 to 1000 Mbits/s;
- Channel is assumed to be extremely frequency-selective;
- Ubiquity: Seamless Communication, Next-generation internet supporting IPv6, Mobile over IP.
- Multiplexing options: single-carrier (SC), multi-carrier (MC) (including OFDM).
- Multi-access options: TDMA, CDMA.

3G still possesses bandwidth limitations; 4G core networks are all IP based and are extended to radio access nodes, hence the limitation of circuit switching are eliminated. These networks will be incorporating advanced IPv6 protocol.

3.4.5 WiFi

Wireless Fidelity or WiFi was standardized by IEEE 802.11b wireless Ethernet standard that was designed to support wireless Local Area Networks (WLAN). The goal of WLAN's is to replace office cabling, to enable tether less access to the Internet and, to introduce a higher flexibility communication. WiFi technologies make uses of two technologies to set up WLANs; one is infra red light (e.g., at 900 nm wavelength), the other one, is radio transmission in the 2.4 GHz license-free ISM (Industrial, Scientific and Medical frequency) band [41]. For campus network, radio wave transmission is widely deployed to connect computer and other network devices together by the use of a single shared channel.

The standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to upper layers to allow interoperability. These characteristics demand the specification of some access rules to guarantee that terminals transmit in different time intervals without collision. These specifications are defined in the Medium access control (MAC) layer, which represents a fundamental part of WLAN standard.

Terminals with access mechanism for wireless medium and radio associate to the access Point. The AP connects to distribution system (infrastructure network) that connects several AP and wired network to form a single network.

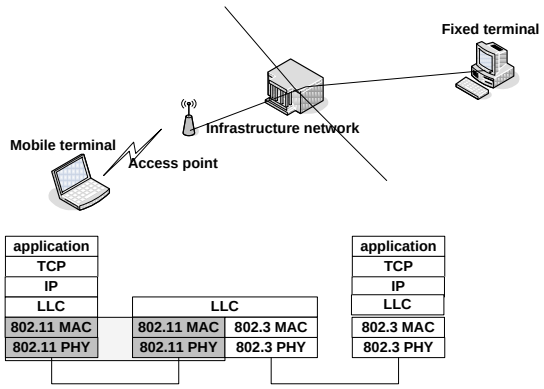

Fig 3.6 Architecture of an Infrastructure-based IEEE 802.11

The IEEE 802.11 standards only cover the physical layer and medium access MAC. The MAC layer comprises medium access, fragmentation of user data, and encryption. The PHY layer provides a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer.

Some PHY techniques are Frequency hopping spread spectrum (FHSS) and Direct sequence spread spectrum (DSSS) [41].

Frequency hopping spread spectrum (FHSS) is a technique that assign different hopping sequences to separate different network therefore making possible the coexistence of multiple network. For security purposed in each time we peak one frequency randomly. So if a sniffer gets a packet it has access to just one part of the message. The channel quality and communication quality is high because the noise is distributed among all range of frequency.

Direct sequence spread spectrum (DSSS) is another PHY technique spread spectrum method separating by code and not by frequency. DSSS technique expands the bandwidth of a signal by replacing each data bit with n bits using a spreading code. In other words, each bit is assigned a code of n bits, called **chips.**

Multiple users share a common medium, therefore important issues includes collision detection, delay, fairness (backoff's), synchronization, power management and roaming.

There are three basic access mechanisms that can be used by the MAC. The first and mandatory method is based on Carrier sense multiple access / collision avoidance (CSMA/CA), the others two are based on a mechanism called distributed coordination

function (DCF) and point coordination function (PCF), which relies on the listen-before-talk paradigm, coupled with random access delays called "backoffs" [42]. The DFC only offers asynchronous service, while PCF offers both asynchronous and time-bounded services but needs an access point to control medium access and to avoid contention.

Carrier sense multiple access (CSMA) technique is used to solve the problem with hidden terminal. It implements collision avoidance via randomized back-off mechanism. This technique requires every station to listen to the channel for a time interval called the DCF interframe space (DIFS) before transmitting. In wireless the receiver uses an acknowledgement message to inform the sender about successful received MAC frame. The lack of acknowledgement informs the sender that the sent frame has not been received by the receiver due to collision or error and thus, there is automatic retransmission of packets.

DFC prevents collision by implementing a mechanism through which the stations must senses the channel and only transmits when the channel is idle. If the channel is busy an additional mechanism of random delay (the backoff) is implemented. This operation is called collision avoidance. Therefore, DFC protocol is long-term fair, since each station has the same probability of accessing the channel.

WiFi LANs operate using unlicensed spectrum in the 2.4 GHz band. The current generation of WLANs supports up to 11 Mbps data rates within 300 feet of the base station. WLAN is usually deployed as the last-mile solution connected to a wireline backbone corporate or campus network. The communication takes place between the wireless nodes and the access point. The access point control the medium and also acts as a bridge to other wireless and wired networks. Although each base station supports a limited coverage area, it can be extended by implementing multiple base stations. This solution has been adopted by business company and university campus.

3.4.6 WiMAX

Customer's increasing desire to have Internet anytime and anywhere constitute another challenge for access network design. Mobility seems to be an important challenge in access network. WiMAX (Worldwide Interoperability for Microwave Access - IEEE 802.16) was initially developed as a fixed wireless technology. This fixed WIMAX (IEEE 802.16d) has the potential of bring broadband internet access to the millions of people worldwide who are not connected to a wired network infrastructure. With the new IEEE 802.16e standard, mobility was introduced.

For WiMAX deployment, a very important issue is the properly dimension of the network by calculating the required number of base stations and their optimal placing. There are several physical aspects to be taken into account. The MAC is structured to support multiple physical layer (PHY) specifications, each suited to a particular operational environment. For operational frequencies from 10 - 66 GHz, the PHY is based on single-carrier modulation. For frequencies below 11 GHz, where propagation without a direct line of sight must be accommodated, three alternatives are provided, using OFDM, OFDMA, and single- carrier modulation. The channel bandwidth is divided into smaller subcarriers which are orthogonal with each other. Subsets of these subcarriers can be assigned to individual users. The physical layer is well adapted to the NLOS propagation environment in the 2 – 11 GHz frequency range and it is fundamentally different from the CDMA modulation used in the UMTS technologies. Another feature which improves performance is the adaptive modulation, which is applied to each subscriber individually according to the radio channel capability. WiMAX also provides flexibility in terms of channel bandwidth and carrier frequency. Mobile WiMAX uses time-division duplex (TDD) as duplex mode. In TDD mode duplex transmission is carried in alternate time slots in the same frequency channel. Both the uplink and downlink traffic use the same frequency f0 but at different times. TDD is best suited for the transportation of asymmetric traffic and it allows service providers the flexibility to manage bandwidth allocated to each direction. An important feature of the WiMAX system is the use of advanced antenna techniques such as beam forming using smart antennas and the build in support of MIMO techniques.

3.5 FTTx Access Networks

Applications that are bandwidth-intensive like high speed Internet, videoconferencing or high-definition television (HDTV) has imposed demand for ever increase bandwidth requirements. This situation is being “pushing” fiber closer and closer to the customer premises.

DSL have been a very successful technology for broadband internet access, but due to its distance limitation and attenuation and crosstalk, many operators have already started to deploy new access networks based on optical fibers. Fiber optical communication systems have many advantages over more conventional transmission systems. One of them is, they are less affected by noise and carry extremely high data transmission rates over very long distances. Another reason is that they can support an

enormous variety of services simultaneously. For these reason, optical fiber communication seems to be a promising choice to fulfill the increasing demand on bandwidth via the vast available capacity of the fiber optics and its economic costs.

Re-building the network with new higher bandwidth connections to every home is impractical due to the cost. An evolutionary solution which reuses the existing network seems to be more reasonable. In the FTTx access networks, optical fiber replaces copper in the distribution network. For example, in fiber to the curb (FTTC) or cabinet (FTTCab), the capacity of access networks is sufficiently increased to provide broadband services to subscribers. Decreasing the copper length means the fiber comes closer to the user, which can be the first step in deploying FTTH.

3.5.1 Fiber to the X Access Networks - FTTPremises, FTTNode/ Cabinet and FTTCurb

Optical fiber has many advantages over copper and cable technologies. These include improved performance and capacity as it offers high-bandwidth over long distance for a group of user at a site; it is not susceptible to electromagnetic interference and noise, lower bit error rates and there is no crosstalk.

Depending on the fiber deployment strategy, several alternatives are available, using all fiber architecture or hybrid architecture, a combination of fiber and copper. According to criteria's such as cost, different solution can be deployed.

There are three possible ways of delivering broadband fiber access network: the feeder portion, the distribution portion, and the drop cables to the subscriber's premises (home or building). According to how far the fiber goes, the architecture can be fiber-to-the-node or cabinet (FTTCab), fiber-to-the-curb (FTTC) or fiber-to-the-premises (FTTP) and that determines the architecture of fiber access network.

Access network plays an important role in providing high-speed broadband to the subscribers. **Fiber-to-the-Premises or FTTP** can be classified as fiber-to-the-home (FTTH) when serving residential subscribers and fiber-to-the-building (FTTB) when serving building deployment such as a multi-floor office building. FTTP architecture involves laying optical fiber all the way from a central office to the termination point (the home or business) and it offers the most future-proof solution in terms of pure bandwidth capabilities. However, there are cases where it is not the optimal solution because of cost associate with the deployment and existent infrastructure [31].

The figure 3.7 depicts an example of deployment of fiber-to-the-premises (homes and

buildings) architecture, presenting that this architecture is a pure all fiber deployment. Compared with the others possible architecture it's more expensive.

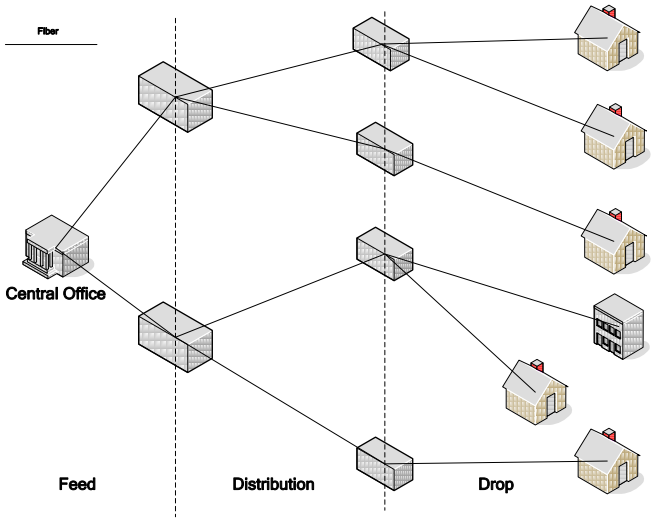

Fig 3.7 Fiber to the Premises (Home and Building) Architecture

Fiber-to-the-Cabinet or FTTCab, was initially denominated in ITU standards Fiber to the Node (FTTN). It is a fiber and copper local loop architecture. With FTTCab, fiber is installed from the CO to copper local loop aggregation points known as Feeder Distribution Interfaces (FDIs). And from there, it uses the Digital Loop Carrier (DLC) and Digital Subscriber Line Access Multiplexer (DSLAM) installed at a FDI and typically serving several hundred subscribers.

FTTCab brings the fiber optics to a feed point and from there traditional copper cable is used to connect the node to the homes. It provides the necessary bandwidth required for today's voice, video, and data services while taking advantage of existing infrastructure.

Fiber-to-the-Curb (FTTC), like FTTCab, is a hybrid architecture composed by fiber and copper local loop architecture. The difference between them lay in distance or node that the fiber reaches. In FTTCab, fiber is installed till copper local loop aggregation points, which tend to be up to about 5000 feet (1.524 km) from subscribers. In contrast, with FTTC, fiber is installed closer to the subscriber typically within 500 feet of the 8-12 subscribers it serves. With FTTC network architecture the fiber is installed in the feeder and distribution portions of the access network, and DSL copper from there to businesses and homes. This closeness to subscribers allows for much higher DSL rates than are possible with FTTN. Although, it can meet today's bandwidth

requirements with the increasing demands for more bandwidth, the question that should be asked is for how long [31].

FTTN and FTTC are hybrids architectures which combine fiber with copper local loops and are less expensive solutions due to the fact that they made use of already installed copper infrastructure. Considering deployments and installation costs, they seem to be the primarily choices, since they leverage existing facilities as much as possible. FTTN has the potential for faster return on investment, yet it may require a complete overhaul at some point, depending on consumer bandwidth demand. Therefore, the cost should not be the predominantly reason for choose FTTN over FTTP, others factors such as bandwidth future proof must be taken into consideration. The migration to FTTP should be taken into consideration, in a way that makes the process easy if future bandwidth demands exceed bandwidth capabilities of the current infrastructure.

Fiber Deployment

The figure 3.8 shows the most important components of FTTx equipments. There are:

- **Optical Line Terminals (OLT)** - Located in Service's provider central office, this equipment serves as the point of origination for FTTx transmissions coming into and out of the network.
- **Optical splitters/splitter hubs** - A focal point for the main fiber feed in a neighborhood or development, where the optical signals from a fiber link are split off to serve multiple customers over individual strands of fiber.
- **Optical Network Terminal (ONT)** - The termination point for fiber at the home or business building, where the optical signal is converted into voice, data or video feeds to equipment in the customer's premises.

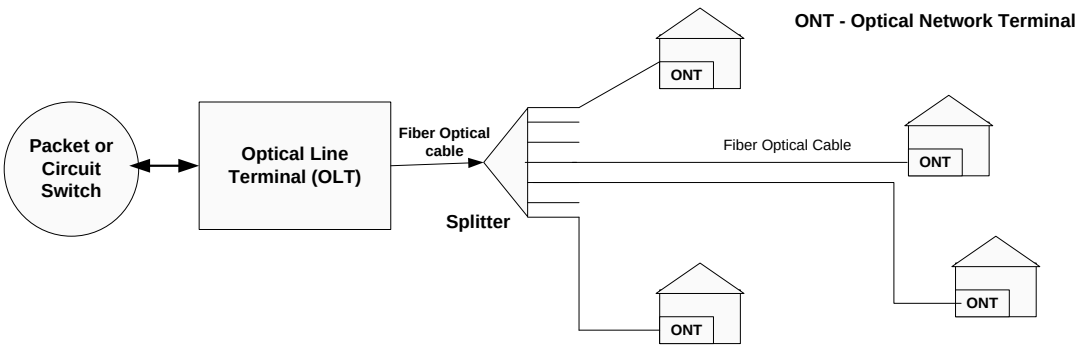

Fig 3.8 Technical Components of FTTP

3.5.2 Passive Optical Network

Originally, point-to-point optical fiber systems were deployed for business customer. It is in fact the simplest fiber infrastructure topology, but this solution is very expensive. This has led to the use of passive optical networks (PON) which is point-to-multipoint network rather then point-to-point fiber for home or business uses. PON makes possible to share infrastructure (fiber) and bandwidth between several customers. This has two primarily advantages, first the exchange-end-interface cost is shared between many end users, and the point-to-multipoint architecture is also well suited to the delivery of broadcast services.

For several reasons such as cost-efficiency of access networks, passive optical networks are considered to be most promising technology, as they can provide high bandwidth which can support reliable yet integrated data, voice, and video services to end users. The advantageous characteristics of PON include long distance transmission over 20 kilometers of single-mode fiber. It can offer symmetrical data transmission and high bandwidth on both the upstream and downstream links, with facilitate the availability of multimedia services. By using passive components (such as optical splitters and couplers) PONs represents an excellent evolutionary path for current access technologies such as cable and DSL and it minimizes fiber deployment compared to FTTC or FTTH.

In PON, the optical signal is shared between customers using passive optical splitters combined with time-division multiplexing (TDM) techniques for downstream and upstream directions.

PON architecture comprises several standardized variants such as Broadband PON, Gigabit PON, Ethernet PON and the two most used variants today are:

- Gigabit PON (GPON – standardized by ITU)
- Ethernet PON (EPON, ratified by IEEE).

Although GPON also supports Ethernet (next to ATM), the ubiquity of Ethernet tends to favor EPON. EPON reaches speeds of 1.25 Gb/s up and downstream and accommodates split ratios up to 1:16, while GPON is standardized at 2.5 Gb/s downstream and 1.2 Gb/s upstream and accommodates split ratios up to 1:64. The next step is to upgrade these PONs to 10 Gb/s.

GPON is based on ATM as in BPON, but additionally support Gbps rates, better encryption, as well as a new frame-oriented mode that can better accommodate native TDM and variable sized IP/Ethernet frames.

In EPON, Ethernet frames are carried in their native format on the PON. This greatly simplifies the layering model and the associated management. Services are all mapped over Ethernet (directly or via IP).

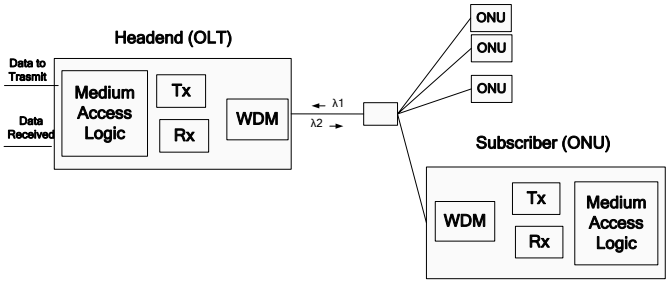

Fig 3.9 Passive Optical Network Architecture

3.6 Access Network Solution for Campus Network

Subscriber's requirements for new services, including voice, data and video information in interactive and broadcasting mode represents key forces for evolution of access networks. Local networks based on traditional networks principles are becoming "bottleneck", limiting subscriber's access to modern services.

On the way of migrating to Next Generation Network, the ultimate goal is to build campus networks utilizing the existing investments for legacy TDM service, and at the same time be able to correspond to the All-IP networks at minimum cost. The network migration must consider the compatibility with the existing network. One of the critical aspects of migration toward Next Generation Network (NGN) is Quality of Service. Circuit Switched (CS) access networks traditionally provide guaranteed QoS to customers by means of one or several dedicated time slots which are connected end-to-end. Contrary, Packet switched (PS) network do not provide dedicated circuit for end to end connection, so dedicated mechanism such as RSVP, Diffserv or Intserv are required.

One strategy of migration towards next generation access network for campus network is using PON. PON can provide broadband fixed access to wireline networks and also accommodate the wireless networks such as WiMAX base stations or WiFi and 3G Nodes B. Hu, Wang, , et al. (2008) [48] propose a method for providing wireless over a Passive Optical Network. According to this solution, the WiMAX base station can be directly connected to the ONU (Optical Network Unit) via Ethernet interface,

while TDM/ATM interface for the 3G Nodes B is carried over Ethernet employing pseudo wire (PW) technology or to transmit the TDM signals transparently over the PON network, using subcarrier multiplexing (SCM).

DSLx technologies, hybrid-fiber coax and FTTx techniques are the wired techniques described in this work, there are other techniques such as providing the feed over electricity cables (PLC – Power Line Communications) and Satellite for wireless access. Relatively to PLC much more intensive research need to be done about it support for campus network access and Satellite is not economically suitable for campus network.

4 NETWORK MANAGEMENT

Network is composed of many complexes, interacting components of hardware and software – from links, switches, routers, servers, hosts, and other devices that comprise the physical components of the network and of many protocols. However, as the complexity of the network increases, so does the relevance of network management. Network Management is about planning, organizing, monitoring, accounting and controlling activities and resources in the network.

Network management main functions involve monitoring and controlling the devices connected in a network by collecting and analyzing data from them. Traditional Network Management structure is based on a client/server approach, which uses a query-response model constitute of a centralized network management station (client), a managed device (server), management protocol and management information [39].

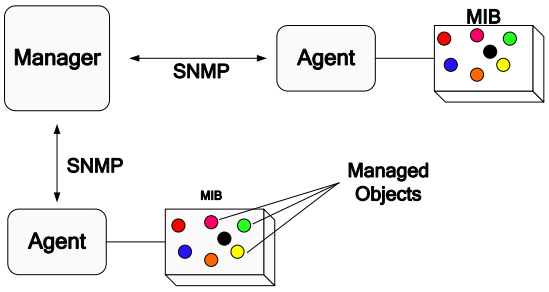

Fig 4.1 Management Structure

Traditional Network Management System (NMS) employs a central manager which is responsible to periodically poll managed devices usually using simple network management protocol (SNMP) through Get or Set commands to configure (changes variable value) or retrieve information about running status. It works as a client and asks information to the managed devices which acts as a Server. Managed device provides management information to NMS by responding to the request sent by the NMS. Management protocol is used as a mechanism for communication between NMS and a managed device. Management information provides piece of information used by NMS to configure the managed devices.

Client/server approach is not the most suitable for modern computer network, due to the huge amount of management traffic that it generates, it affects considerably the throughput and it may cause a processing bottleneck in the manager.

Distributed management solves the problems of centralized management such as excessive processing load by the manager, heavy usage of network bandwidth because of SNMP constant polls. Improved by the utilization of mobile agents, which are software code programmed and dispatched to remote managed device to execute pre-configured function, is an efficient and promising approach.

4.1 FCAPS Model

There are several management reference models which serve as conceptual frameworks for organizing different tasks and functions that are part of network management. One of them is FCAPS model. This model divides management functions into five categories: the fault management, configuration management, accounting management, performance management, and security management. Another reference model is the Operations, Administration, Maintenance, and Provisioning (OAM&P) model. In the later, management functions are categorized a bit differently. Although these are the most prominent reference models, they are not the only ones. The figure 4.2 groups the network management functions.

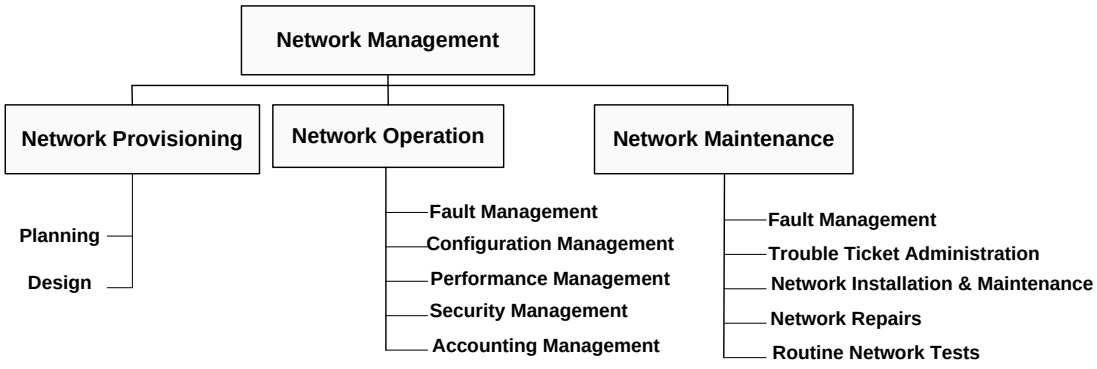

Fig 4.2 Network Management Functional Groupings

The International Organization for Standardization (ISO) Network Management Forum divided network management into five functional areas [22]:

- **Fault Management**

Fault management deals with detects and take actions to faults conditions in the network components. Fault management function deals with monitoring the network to

ensure that network is operating as expected and reacting when this is not the case. It also deals with faults diagnosis and alarm management processing functions. Effective fault management is critical to guarantee service availability and when there are outages to keep it to a minimum.

Mobile agents can be programmed to monitor and analyze to help detect when a defined threshold is about to be exceeded and report to a manger.

- **Configuration Management**

Configuration management includes functionality to perform operations that will setup a network, deliver and modify configuration settings to equipments in the network and services. This includes the initial configuration of a device as well as updating and/or configuration changes. Configuration is the core of network management since it deals with setting up a network so that it can deliver service

Configuration management functions include the configuration of all the network components, as well as auditing the network to discover running configurations, provides backup and restore procedures in case of failures.

Mobile agents can facilitate the process of configuration management which is a complex process. Usually the network administrator has to perform the entire task manually which can lead to some misconfiguration and can be time consuming. MA can be programmed with the necessary parameters and dispatched to a remote managed device that needs to be configured.

- **Accounting**

Accounting function is necessary to provide record of services being provided to user and to be able to assess the cost/benefit ratio of running services, to keep cost under control relative to the services that are actually provided, and to use consistent data for decisions on whether to perform services in-house or outsource them. Obviously, accounting management needs to be highly robust; highest availability and reliability standards apply.

Mobile agent added value to account management is similar to that described in configuration management.

- **Performance Management**

The goal of performance management is to measure, analyze, monitor and gather information about different network components. Measure and make available various aspects of network performance so that network performance can be maintained at an acceptable level.

Performance management involves three main steps. First, performance data is gathered on variables of interest to network administrators. Second, the data is analyzed to determine normal (baseline) levels. Finally, appropriate performance thresholds are determined for each important variable so that exceeding these thresholds indicates a network problem worthy of attention.

Management entities continually monitor performance variables. Systems are configured with a pre-defined performance threshold so that when that value is about to be exceeded, an alert/alarm is generated and sent to the network management system.
Performance of networks is measured according to metrics. Some examples of performance metrics are these:

- **Throughput**, measured by a number of units of communication performed per unit of time. The units of communication depend on the layer, type of network, and networking service in question.
- **Delay**, measured in a unit of time. Again, you can measure different kinds of delay, depending on what layer or networking service you are dealing with.
- **Quality** is in many ways also performance related and can be measured differently, depending on the networking service.

Instead of querying the managed node for every fixed and analyzing the performance from management station, MA can be dispatched to analyze the node locally.

- **Security Management**

Security management encompass aspects that are related to securing network from threats, such as hacker attacks, the spread of worms and viruses, and malicious intrusion attempts. Security domain has two important aspects that need to be distinguished: security of management, which ensures that the management itself is secure, and management of security, which manages the security of the network. Those aspects are depicted in Figure 4.3 and are explained in the following subsections.

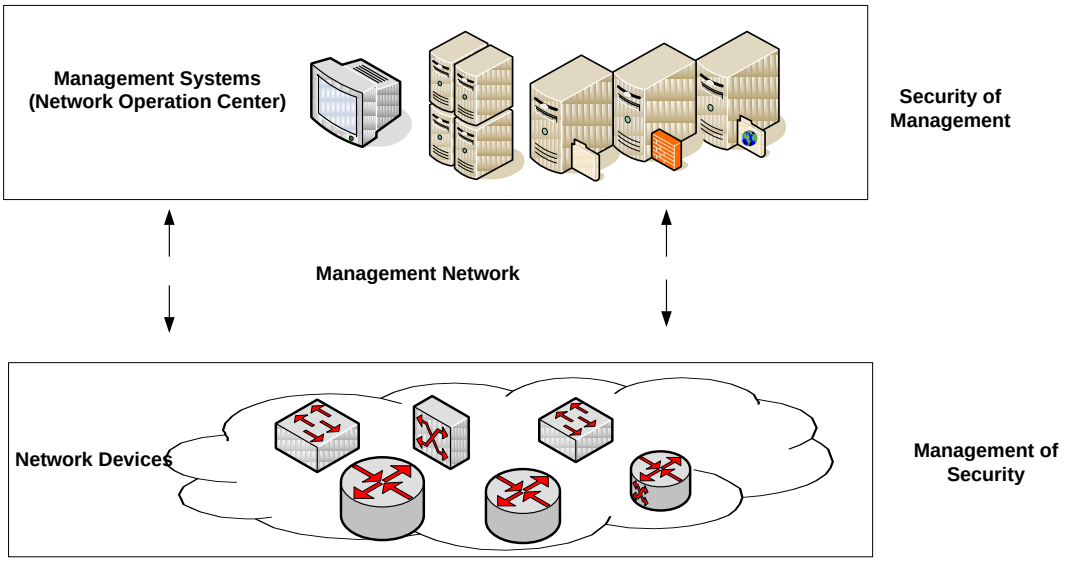

Fig 4.3 Security Domains [29]

Security of Management

Security of management deals with ensuring that management operations themselves are secure. A big part of these concerns ensuring that access to management is restricted to authorized users.

Management of security

Management of security deals with managing the security of the network itself, Common security threats include but are by no means limited to hackers attacks who try to obtain unauthorized control of a system that is connected to the network, Denial-of-service (DOS) attacks try to overload portions of a network by generating illegitimate traffic and Viruses and worms that attempt to corrupt and possibly destroy systems along with their file systems, and all the consequences of those attacks.

Management of security involves other functions such as intrusion detection; definition of Security Policy Plan, implementation of mechanism and techniques such as port scan to gather information about network vulnerabilities before it can be find out for a hacker and used to perpetuate an attack.

In fact, security is a very important area of network, but it is behind the scope of this thesis, since it worth of a dedicated thesis only about it. Plenty of information are available that must be taken into consideration when planning network security.

4.2 Network Management Protocol - Simple Network Management Protocol

As network equipments and traffic increase as so network complexity, several protocols for network management have been proposed. ISO (International Organizaiton for Standardization) defined CMIS/CMIP (Common Management Information Services / Common Management Information Protocol). IETF (Internet Engineering Task Force) defines SNMP (Simple Network Management Protocol). Both protocols are typical centralized system using a client / server model. However SNMP is widely accepted as standard and used because the architecture that is structured as manager and agent is relatively clear and simple and also the implementation is not difficult.

Simple Network Management Protocol (SNMP) is a widely accepted industry management protocol standard. It is the most dominant network management protocol used particularly in the data-networking world. It was defined by Internet Engineering Task Force (IETF) standards back to the late 1980s. SNMP was developed to ensure transmission of management information between any two nodes, which facilitates network administrators to search for information at any node on the networks for the purpose of configuring, modifying, locating fault, troubleshooting and generating reports. Those standards also include the Management Information Base (MIB) specification language and standard definitions, Structure of Management Information (SMI), and its successor, SMIv2 and even the architecture of agent implementations.

SNMP system consists of Network Management Station (NMS) and multiples managed device which contains Agent that interact with the NMS. It employs a client-server architecture, which means clients (NMS) initiate communications by sending a request to server (agent). The agent receives and processes the request packets from NMS, and responds to it by returning the corresponding management variables obtained from MIB information. Servers passively await such requests or they can send trap to the manager in case of unexpected event happen.

There are actually three versions of SNMP: the original SNMP also referred as SNMPv1 (RFC 1155), SNMP version 2 (SNMPv2c – from RFCs 1441 to 1452) and SNMP version 3 (SNMPv3 – RFC 2570 and there is also RFC 2271 which define the SNMP protocol currently and future versions). SNMPv3 defines a series of access control management functions for network security, in addition to the functions defined in SNMPv2c and SNMPv1.

SNMPv1 and SNMPv2c lack security functions, especially in the aspect of authentication and privacy. In these versions security is based on the type of community representing a group of managed devices. Each NMS controls access to the devices via the community name list, for example, public community that has read-only access or private community that has read-write access. However, agents do not verify whether the community names used by the senders are authorized. Besides that, SNMP messages are transmitted without encryption, which exposes the community name, brings potential threats to security. To avoid the lack of security in SNMPv1 and SNMPv2c, IETF develops the SNMPv3 protocol, which is described in RFC2271 through 2275 and RFC2570 through RFC2575 in details.

Security of SNMPv3 is mostly represented by data security and access control. **Message-level data** security provided in SNMPv3 includes the following three aspects:

- **Data integrity** – It ensures that data will not be tampered by means of unauthorized modes and the data sequence will only be changed within the permitted range.
- **Data origin authentication** – It confirms the received data belongs to which user. Security defined in SNMPv3 is user-based. Hence, it authenticates the users that generate messages instead of the particular applications that are used to generate the messages.
- **Data confidentiality –** Whenever a NMS or agent receives a message, it will verify when the message was generated. If the difference between the generating time of message and the current system time exceeds the specified time range, the message will be discarded. Thereby, it ensures that the message has not been tampered with in-transit on the network and prevents processing of received malicious messages.

SNMP Protocol Architecture

SNMP is designed according to a centralized model. This protocol assumes network to be collection of managed objects (hosts, routers, switches, bridges etc.) and each managed object runs a SNMP agent that continuously updates Management Information Base (MIB) with network management statistics. MIB is stored locally in managed object (figure 4.4)[31].

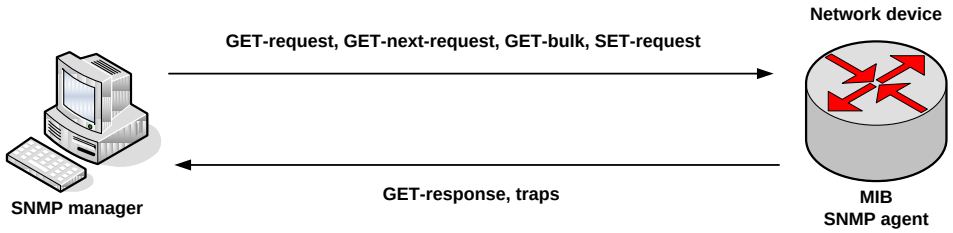

Fig 4.4 SNMP Architecture

There are four basic components of SNMP protocol:

1. Managed nodes or network elements, each of which contains an agent;
2. At least one Network Management Station (NMS);
3. Management information;
4. A network management protocol, which is used by the NMS and the agents to exchange management information;

The agent contained in managed node implements the SNMP protocol. The agent is capable of sending, receiving, and parsing SNMP messages. The agent is capable of retrieving the necessary information from the device MIB to answer queries from the NMS and to send trap messages (unsolicited notification messages).

A Network Management Station (NMS) is a host responsible for the management of network nodes, it has the capability to send SNMP requests and receive and parse SNMP replies and trap messages to/from managed nodes.

There are two approaches for the management system to obtain information from SNMP agent [31]:

- **Polling** – as monitoring functions, network management system periodically queries network nodes to collect information about it status or to configure it. The management information is the information that is exchanged between managed nodes and NMS. The managed object is not a managed device. A managed object is an abstract concept - it is the definition of some kind of information. For example, suppose we had a device whose location could be changed at will. We could define a managed object called "location" and the corresponding definition could be "the location that the device is at", it is basically one instance of managed device.
- **Traps** – agent has the capability to when an unexpected event happens on the network node to send a trap to network management system to inform about the situation that had occurred. The management system then polls

the network device to get further information. A trap contains the network device name, the time the event occurred and the type of event. The drawback related to trap is that when a lot of events occur, the network bandwidth may be tied up with traps. One solution is to define thresholds to limit and prevent the send of trap.

There are five different operations performed by SNMP:

1. "GetRequest" to fetch a value from a specific variable. The Get operation is used to poll information from a managed agent.
2. "GetNextRequest" to fetch the next value in a MIB category without knowing its exact name.
3. "SetRequest" to store or upgrade a value in a specific object or variable. With the Set command manager send information to an agent. This is one way of configuring different components from a managed device.
4. "GetResponse" to get a response from an agent as a reply to a fetch or a store command. The agent will respond to a poll performed by the manager.

"Trap" to automatically generate "alarm" from an agent when an important event has happened. A Trap is a kind of alarm which is automatically generated and sent from an agent to the management device when unexpected event occur.

SNMP uses the User Datagram Protocol (UDP) as the transport protocol for passing data between managers and agents. It was chosen over the Transmission Control Protocol (TCP) because it is connectionless thus it requires no acknowledgements which could overload network and lead to a huge bandwidth consumption. With UDP there is no end-to-end connection made between the agent and the NMS before datagram is sent. Since there is no acknowledgment of lost datagrams at the protocol level, it's up to the SNMP application to determine if datagrams are lost and retransmit them in case of necessity. This is typically accomplished with a simple timeout and number of retries. The NMS sends a UDP request to an agent and waits for a response. The length of time the NMS waits depends on how it is configured. If the timeout is reached and the NMS has not heard back from the agent, it assumes the packet was lost and retransmits the request. The number of times the NMS retransmits packets is also configurable [21].

For traps, the situation is somewhat different. If an agent sends a trap and the trap never arrives, the NMS has no mechanism of knowing that it was ever sent. The agent

doesn't even know that it needs to resend the trap, because the NMS is not required to send a response back to the agent acknowledging receipt of the trap [21].

The advantage of UDP is that it requires low overhead compared to TCP, so the network traffic is reduced and consequently bandwidth use optimized and network's performance enhanced. SNMP has also been implemented over TCP, but this is more for special-case situations in which one is developing an agent for a proprietary piece of equipment. In a heavily congested and managed network, SNMP over TCP is not an effective option.

SNMP uses as default the UDP port 161 for sending and receiving requests, and port 162 for receiving traps from managed devices. If defaults are changed, the NMS must be made aware of the changes so it can query the device on the correct ports.

4.3 Management Information Base and Structure of Management Information

Management Information Base (MIB) is a collection of related managed objects, which are defined in a structure like a tree. MIB is like the structure of a database. MIB structure contains a set of group of managed objects according to logical functions. There are some standard MIB modules which all devices that meet the SNMP standard must support and there are others MIB modules that are vendor-specific or private MIBs that contain definitions of managed objects specific to that vendor's products. Figure 4.5 depicts an example of the definition of MIB object:

```
ospfIfIpAddress OBJECT-TYPE
    SYSTAX IpAddress
    ACCESS read-write
    STATUS mandatory
    DESCRIPTION “The IP address of the
OSPF interface”
    ::={ospfIfEntry 1}
```

Fig 4.5 Example of the Definition of a MIB Object

Managed object is an abstract concept of a real resource of the system. It contains permission for reading-writing access and each change on these values will be reflected and performed in the real resource.

The data is kept on the managed device and the agent knows how to retrieve the data or to send an instruction to change a value.

SNMP identifies the managed objects by using the hierarchical structure to name them. The hierarchical structure is like a tree, in which, the nodes of the tree represent the managed objects. As stated before MIB module is a collection of managed object - whether standard or private – and each managed object has a unique identifier, called **object identifier**. The object identifier is a set of name or a string of integers, separated by dots, that places the object at a specific node in a logical tree, which is called the **Management Information Tree**. The name/integers represent the nodes in the path from the root to the object itself included. Management objects that are related are organized in groups and sometimes subgroups forming a hierarchy to avoid a very long object nodes branching.

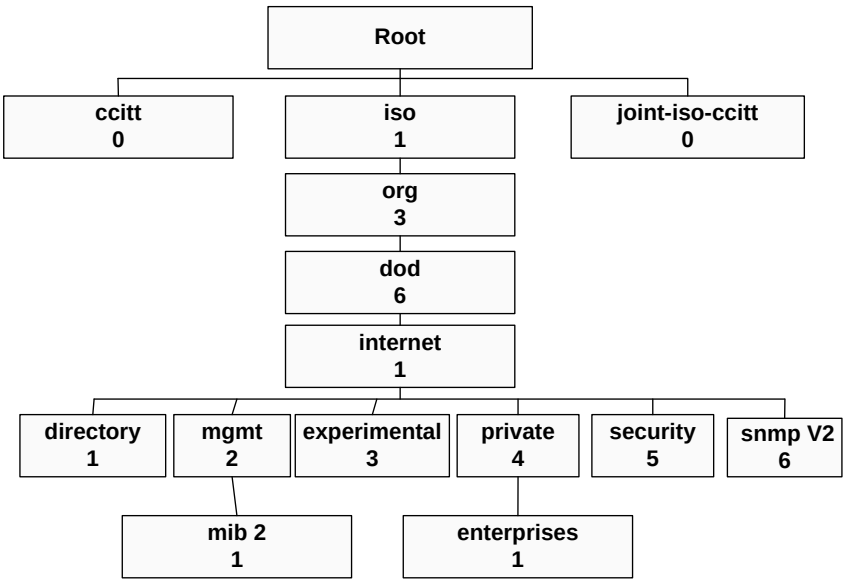

Fig 4.6 Structure of the Management Tree

Object identifier is an ASN.1 type which allows identifying an object type by a sequence of name or integer as it is depicted in figure 4.6 of MIB structure. Thus, looking at figure above, all objects in the standard MIBs have an object identifier that begins with 1.3.6.1.2.1 and all objects in the private (vendor-specific) MIBs have an object identifier that begins with 1.3.6.1.4.1.

There are five basic attributes of a managed object:

①**Object type** (object identifier and descriptor) - unique ID and name for the object

②**Syntax** - used to model the object

③**Access** - access privilege to the managed object

④**Status** - implementation status (current, deprecated, or obsolete)

⑤**Definition** - textual description of the semantics of the object type

ASN.1 is a formal notation, used for describing data transmitted by telecommunications protocols, regardless of language implementation and physical representation of these data. The SMI uses an adapted subset of ASN.1.

Structure of Management Information (SMI) was specified in RFC 1155 with the goal to provide a common scheme for representing data and RFC 2578 - Structure of Management Information Version 2 (SMIv2). SMI is a general framework in which MIB can be defined and constructed to provide a standardized way of representing management information.

For that SMI must provide:

- A standardized technique for defining the structure of a MIB (where to find data, i.e. information structure)
- A standardized technique for defining individual objects (syntax + value of each object)
- A standardized technique for encoding object values.

There are set of operations that are not allowed in SNMP. These include Add or Delete an object instance from MIB (which means to change the structure of MIB).

Due to the fact that SNMP is designed according to a centralized model, it has several drawbacks such as lack of distribution, a low degree of flexibility, re-configurability, efficiency, scalability, and fault tolerance [39]. This causes to consume a lot of bandwidth, computational overhead and a reason for traffic jam at the manager host.

4.4 Network Management with Mobile Agents

Traditional Network Management Systems (NMS) are by nature centralized systems. However, with the increasing managed devices and therefore management data, plus the complex heterogeneous network configurations and management, centralized network management is not the most suitable for current networks. Major problem areas are heterogeneity and proliferation of networks components, complexity of topologies, scalability, bandwidth limitations constraints etc. For these reasons, it is becoming necessary to change network management paradigm. Distributed management with mobile agents (MA) can play an important role in the problem solving and provide an effective solution for network management. Mobile agents can be dispatched to desired managed devices and interact (poll) with SNMP agent locally, thus saving on costly WAN bandwidth.

The primary goal of using mobile agents in management of telecommunication network is **reducing network traffic** by using load balancing and building scalable and reliable distributed network management system [18] (figure 4.7).

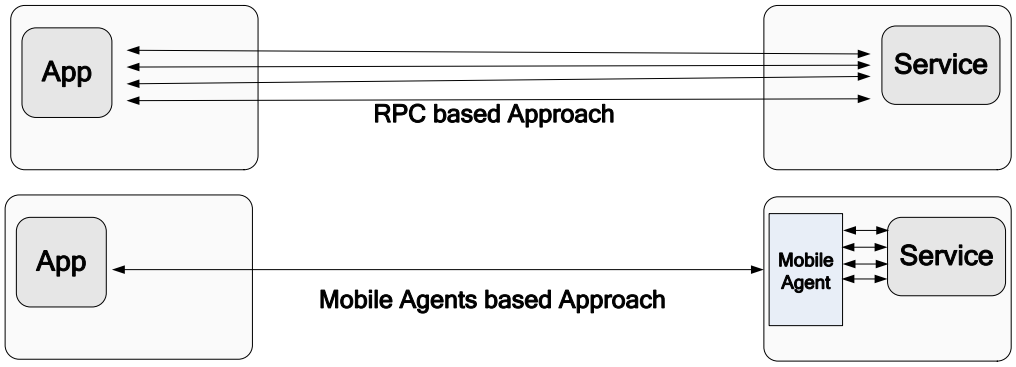

Fig 4.7 Comparison between Centralized Network Management and Mobile Agent Approach

According to IBM Intelligent Agent definition [40], "Mobile Agent is a software entity that carries out some set of operations on behalf of a user or another program with some degree of independence or autonomy, and in doing so employs some knowledge or representation of a user's goals or desire".

An agent is a software program that has the purpose of executes predefined code or function. It works through delegation of function by a master entity. The principle of the mobile agent approach is that a local method call is much faster than a remote procedure call.

Mobile agent is an emerging technology with several important characteristic that are: mobility, autonomy, authority (delegation), and capability of learning from new environment, etc. As showed in figure 4.7, they offer advantages such as, reduction in network workload and network latency, non-centralized management, and direct manipulation at remote hosts. These characteristics further improve the process of design, implementation, and maintenance of distributed systems. A mobility characteristic allows mobile agents to migrate to a remote computer within the network for execution. Arriving at the remote computer, they are authenticated and obtain access to local services and data. The process is described in figure 4.8.

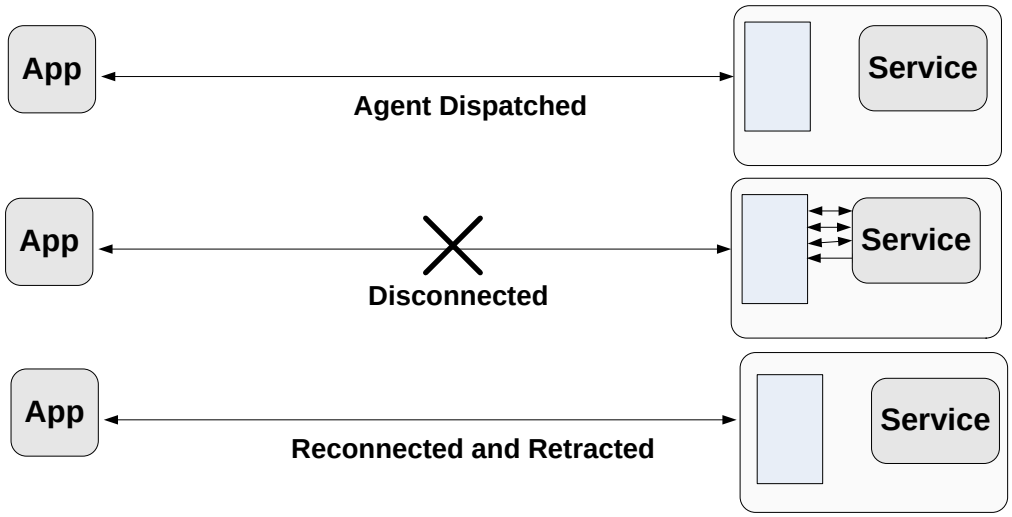

Fig 4.8 Mobile Agent Mobility Scheme

Mobile agents offer several advantages for performance monitoring such as, accurate information collected since its works locally no delays are involved, data are manipulated locally reducing greatly network traffic, filtering operations can be performed directly in the managed node.

4.4.1 Mobile agent descriptions

Furthermore, considering a mobile agent as a moving software agent, it generally consists of the following components:

- **Itinerary** - This is the place where the route and also current position of the agent is recorded, so that we know exactly where the agent is. This is an essential part of a mobile agent; since the agent is moving, it needs to know where to start and where to go next and ultimately, where to end. It is an aglet travel plan.
- **Code** -This is the part where the code of the program is stored. By definition, an agent is a software entity, which means it is a program that can be executed. Without this code part, an agent will not be created or able to perform any tasks, not even moving. Moreover, this part controls what's the agent will do.
- **State** – this is where the status of the agent is recorded.
- **Host** - This is where the server position is stored. It is quite vital since an agent is only running on the Agent Transfer Protocol (ATP). The agent has

to remember where it came from so that it will be able to return to the server after the tasks assigned are completed.

Mobile agent's framework can be used in network management into three different areas, namely fault management, configuration management, and performance management.

4.4.2 JAVA

Mobile agents are mostly programmed using Java language. Java is an object-oriented programming language, and more than that, there are several properties of Java that make it a good choice for mobile agent programming [16].

According to the creators of the aglet [25], the following are advantages of using Java for mobile agents:

- **Platform Independence** – Java is abstracted from its environment via the Java virtual machine. This provides a uniform environment for Java applications to execute in.
- **Secure Execution** – Through its byte code verifier and security managers, Java programs are protected from many types of attacks via buffer overruns or rogue pointers.
- **Multithreaded** – Since agents should be autonomous, they should be able to operate in parallel. One way to achieve this kind behavior is to let each agent run on its own thread. Multithread programming supported by Java can easily do this.
- **Objects Serialization** – Java allows the serialization of objects into a binary format, suitable for transfer across a network. This is vital as one of most important characteristics of mobile agents is mobility.

They also specify some of the drawbacks of Java as follows:

- **Inadequate Support for Resource Control** – Java has no mechanism for regulating the resource consumption of an object. For example, a denial of service attack could flood a host and infinitely loop to consume CPU resources.
- **No Protection of References** – Anyone that has a reference to an agent can call its public methods. There is no inherent way to regulate who can call these methods. Aglets get around this by providing a proxy object.

4.4.3 IBM's Aglets Platform

There are number of mobile agent frameworks available today, both commercial

and as research prototypes. Voyager developed by ObjectSpace is a product family consisting of an Object Request Broker (ORB) and an application server supporting mobile agents. Grasshopper is an agent development platform launched by IKV in 1998. It enables the user to create agent applications enhancing electronic commerce application, dynamic information retrieval, telecommunications services and mobile computing.

Aglets Software is a framework to make easy the development of agent applications. It was initially developed by IBM's Tokyo Research Laboratory, initiated in early 1995. IBM's Aglets is open source project licensed under the IBM Public License and can be downloaded from sourceforge website①. The goal of IBM Aglets is to bring mobility feature to the applets (Aglet means agent plus applet) and to build a network of Aglets.

Developers of IBM Aglets define Aglets as "Java objects that can move from one host to another in the network. That is, an aglet that executes on one host can suddenly halt execution, dispatch to a remote host, and restart executing. When the aglet moves, it takes along its program code as well as the states of all the objects it is carrying. A built-in security mechanism makes it safe to host untrusted aglets [23]".

Tahiti server is an application program that provides aglet server runtime environment. Tahiti has an easy to use graphical interface and provides a user interface for monitoring, creating, dispatching, and disposing of agents as well as enables setting the agent's access privileges to the agent servers. On a single computer multiple servers can be run by assigning them different port numbers. The figure 4.9 shows the Tahiti graphical user interface.

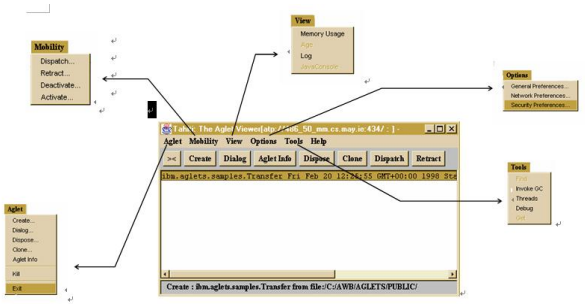

Fig 4.9 Tahiti Server Functionalities

Aglet system uses migration through sockets mechanism. During a migration, an

① http://sourceforge.net/projects/aglets/

Aglet sends a request to the Aglets Runtime Layer. The layer converts the Aglet by serialization into the form of byte array consisting of its data and code. The resulting byte stream is passed to the Agent Transfer Protocol (ATP) through the Agent Transport and Communication Interface (ATCI) that makes it protocol-independent of system (important for heterogeneous networks) [23].

The Agent Transfer Protocol (ATP) is an application-level protocol for distributed agent-based systems. It is used for transferring mobile agents between network systems [17]. An ATP request consists of a request line (request), header fields, and content. The request line specifies the method of the request, while the header fields contain the parameters of the request [20]. When an aglet invokes dispatch method, it passes an URL as argument which uses ATP as protocol:

```
this.dispatch(new URL("atp://host/port"));
```

The Aglets use weak migration, Aglet system does not transfer system classes, it assumes that all the system classes are available at the destination. That reduces necessary transfer but has an impact on security and compatibility.

Architecture of Aglets

The basic idea of this paradigm is to distribute the processing throughout the network: that is, send the code to the data instead of bringing the data to the code.

Aglet runs inside a **Context.** A context is an aglet's server. The Aglet Context is a platform where Aglets are maintained, executed and managed. One node in a computer network may host multiple contexts. As referred above, IBM Aglets uses Tahiti Server as context.

Each Aglet is surrounded by **Aglet Proxy**. A proxy is a representative of an aglet. It serves as a shield for the aglet that protects it from direct access to its public methods. The proxy also provides location transparency for the aglet. That is, it can hide the real location of the aglet. One Aglet sends the message to another via Aglet Proxy [20]. As depicted in figure 4.10:

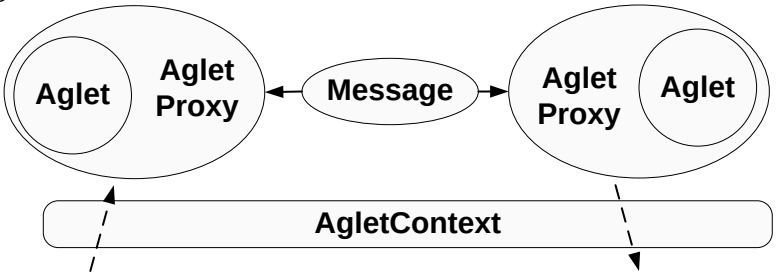

Fig 4.10 Aglet API

A **message** is an object exchanged between aglets. It allows for synchronous as well as asynchronous message-passing between aglets. Message-passing can be used by aglets to collaborate and exchange information.

An **identifier** is bound to each aglet. This identifier is globally unique and immutable during the lifetime of the aglet.

Aglets are mobile in two different ways: actively and passively. The active approach is characterized by an aglet being dispatched from its current host to a remote host. A remote host pulling an aglet away from its current host (retracting) characterizes the passive type of aglet mobility.

The Operation of Aglet

The abstract class Aglet defines the fundamental methods that control the mobility and lifecycle of an aglet. The figure 4.11 summarizes the fundamental operations that can be performed over an aglet: creation, cloning, dispatching, retraction, deactivation, activation, and disposal.

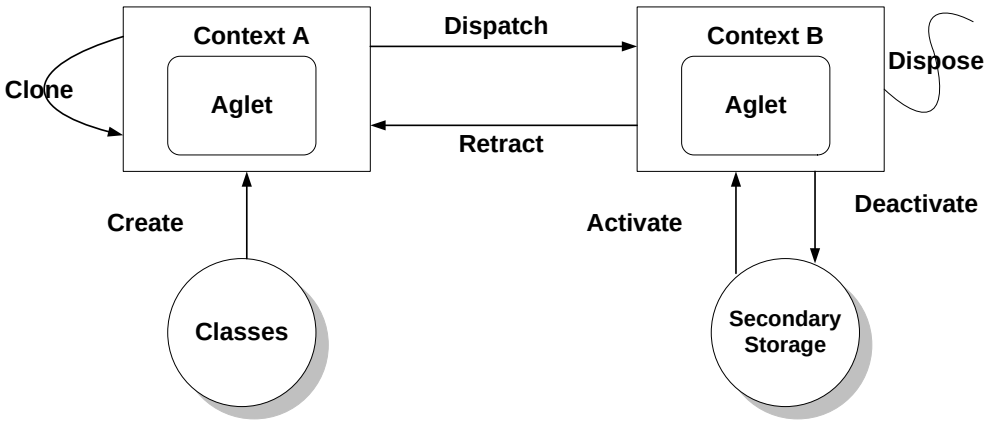

Fig 4.11 The Lifecycle of an Aglet

- The **creation** of an aglet takes place in a context (aglet server). The new aglet is assigned an identifier, inserted in the context, and initialized. The aglet starts executing as soon as it has successfully been initialized.
- The **cloning** of an aglet produces an identical copy of the original aglet in the same context. The differences are the assigned identifier and that execution restarts in the new aglet. Notice that execution threads are not cloned.

- The **dispatching** of an aglet is the process of move an aglet from one context to another. The process requires remove the agent from its current context and insert it into the destination context, where it will restart execution (execution threads will not migrate).
- The **retraction** of an aglet will pull (remove) it from its current context and insert it into the context from which the retraction was requested.
- The **deactivation** of an aglet is the ability to temporarily remove it from its current context and store it in secondary storage. **Activation** of an aglet will restore it in a context.
- The **disposal** of an aglet will stop its current execution and remove it from its current context.
- **Messaging** between aglets involves sending, receiving and handling messages synchronously as well as asynchronously.

Aglets Limitations

Since Aglets is a middleware for developing distributed applications, it must be evaluated with respect to scalability and fault tolerance, which are two very important issues for distributed robust software infrastructures.

When discussing scalability, it is necessary to first state with respect to which variable; in a Multi Agent System, the three most interesting variables are the number of agents in a platform, the number of messages for a single agent and the number of simultaneous conversations a single agent gets involved in. IBM Aglets distributed architecture clusters of related agents can be deployed on separate agent containers in order to reduce both the number of threads per host and the network load among hosts.

From a fault tolerance standpoint, Aglet does not perform very well due to the single point of failure represented by the aglets server (Tahiti Server). A replicated aglet server would be necessary to grant complete fault tolerance of the platform.

Furthermore more research should be done for improving the mobile agents technology, with more standardization and improved programming environment.

4.4.4 Simple Prototype Practical Management with Mobile Agents

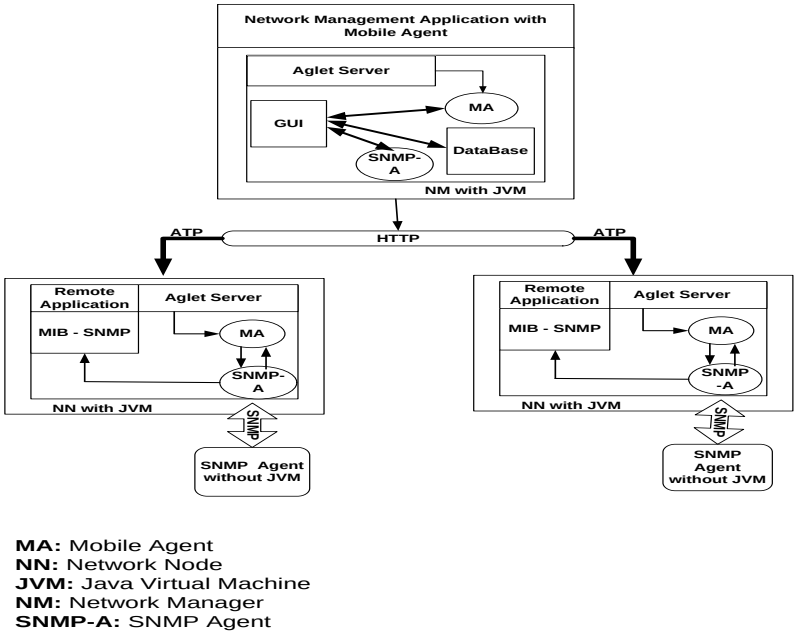

Fig 4.12 Proposed Architecture for Network Management with Mobile Agents

SNMP is supported for almost all network components such as servers, routers or Switches. The main idea behind the use of SNMP is the capture of management data through the exchange of a wide number of messages between manager and managed nodes. With the utilization of MA management operations can be done locally reducing greatly network traffic. Therefore, the integration between SNMP-Agent and Mobile Agents constitute an important factor for interoperability between centralized and distributed systems.

In the proposed architecture (figure 4.12), mobile agents are created and dispatched to remote network nodes (NNs) where they interact with SNMP –Agent to change configuration or retrieve information. The mobile agent is able to migrate from one node to the next, get the required data, and move on. The operation of the systems is that initially the SNMP-A is configured on each of the hosts. MA makes a request to the SNMP-A which will read the MIB, and passes the data to the MA, which will then migrate to the next host in the itinerary.

The operation on each host is:

1. Mobile agent arrives at the host, and communicates with SNMP-A
2. The SNMP-A reads the MIB content
3. Mobile agent leaves the host and carries on its migration

4. Finally, when the mobile agent returns to its NMS, it displays the results of the visits.

Agent proxy is used to allow asynchronous communications between the mobile and the SNMP-A. It is used to access remote methods in the same way that would be done locally.

The interface SNMP-Java (GUI) is implemented based in SNMP4J API. The API is a java library for the construction of network management systems based on SNMP. SNM4J provides components for basic SNMP operations (SNMP GET, GETNEXT, GETBULK and SET).

Aglets runs inside a Aglets server (Tahiti Server by default) so one need to install Aglets or write a program which can act as an agent server on every machine you want to send an agent to. The Tahiti server is the context where the agent lives, and it allows the user to view and manage the mobile agents which have migrated to the host. For NN that doesn't have the requirements for running Tahiti Server or JVM, MA will interact with SNMP-A and then SNMP-A is responsible to retrieve information from the node.

The aglet can perform SNMP operations by using a set, get, get-next commands through java class that provides SNMP operations and that can be serialized.

A database system can be used to store the information about network node status and network management information.

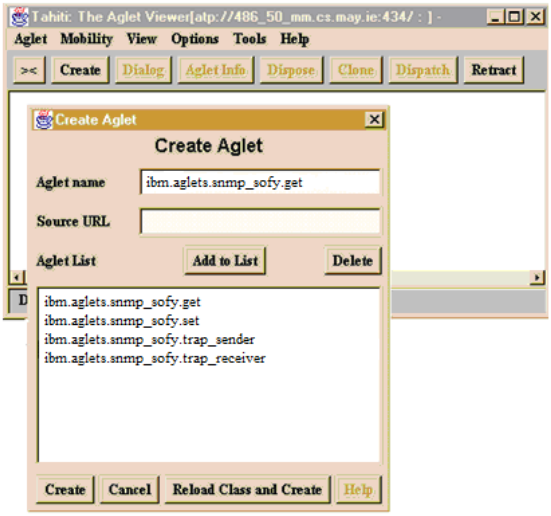

Fig 4.13 Creation of an Agent

com.ibm.aglet.Aglet: it's the abstract class that defines the fundamentals methods used

to control the mobility and lifecycle of aglets. Some of fundamentals methods and they semantics are:

- dispose (): dispose the agent;
- dispatch (URL): move aglet to another destination specified in the URL
- deactivate (long duration): aglet is put to sleep till the activation method is called.
- getAgletInfo (): get information about the aglet.

Some example of pseudo-code for Aglets operations are displayed below:

Aglet Structure

```
public class snmpAglet extends Aglet {
      public void onCreation(Object init) {
        System.out.println("Agent created!");
      }
      public void run() {
        doJob( "get MIB variables");
      }
      public boolean handleMessage(Message msg) {
        if (msg.sameKind("Display OID information ") {
                System.out.println("Asterisk Server");
               return true;
         }
        return false;
      }
       public void onDisposing() {
        System.out.println("Agent will be Disposed!");
      }
}
```

Agent Mobility

When an aglet is dispatched, cloned or deactivated, it's converted (marshalled) to a representation of bytes from where it will be restored (unmarshalled) later. For this process to occur, a java object serialization mechanism is used. Therefore all the objects that compose aglet status should be serialized (implemented interface java.io.Serializable) or be declared as transient.

```
public class MyAglet {
      static int class_variable = 0;
      public void onCreation(Object init)
      {
        class_variable = 10;
        dispatch("atp://next.place");
      } public void run() {
        if (class_variable != 10) {
              System.out.println("Class
      variable never get
        transferred!");
        }
      }
}
```

Message exchange through Aglet.handleMessage ():

The communication between aglets is thorough the exchange of messages. The reception of a message for an aglet is specified through the method handleMessage():

```
MyAglet extends Aglet {
      public boolean
      handleMessage(Message msg) {
        if (msg.sameKind("doJob")) {
                    doJob();
        }
        else if
      (msg.sameKind("shutdown")) {
              deactivate(0);
        }
      }
 }
```

The messages are not send directly to the aglet, but to the aglet proxy. A proxy is a protection for the aglet which interacts with the aglet so at first the proxy should be obtained.

AgletProxy proxy = anotherAglet.getProxy();

SNMP Prototype GUI:

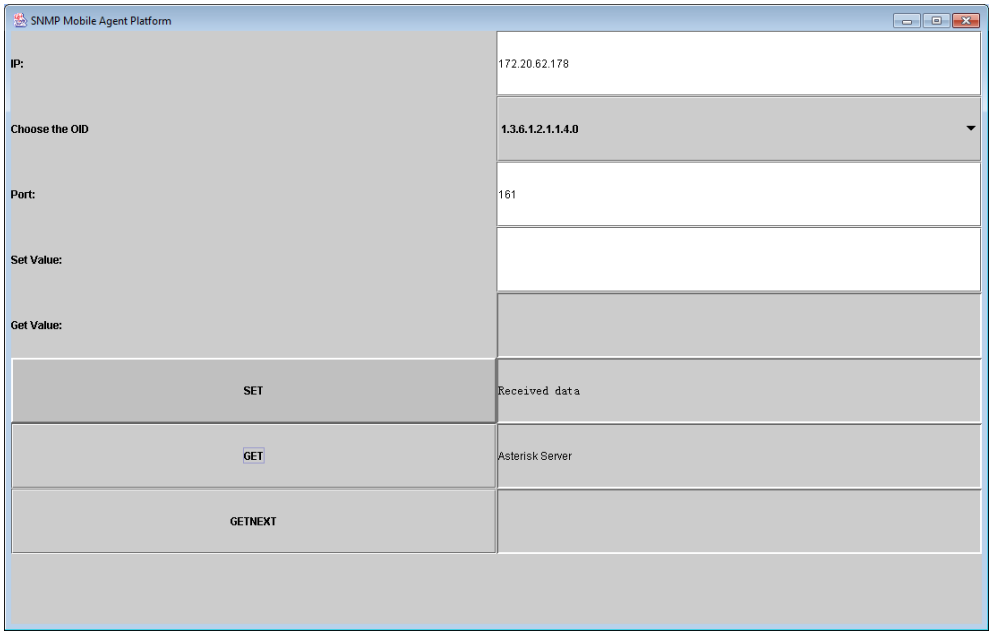

Fig 4.14 Prototype of SNMP Application

This prototype goal is to program mobile agents for network management. Therefore it has not been our goal to develop a MIB application. The application has been developed with two previous conceptions: that the snmp-agent is already configured in the network node and the administrator already knows the OID he wants to retrieve. To retrieve the MIB structure many open source application exists that can be used, one example that was used during the development of this prototype is MIB Browser[①] (figure 4.15) which is free for non-commercial use.

This prototype application works as followed:

1. The program prompts the network administrator to input an IP address. This field was left open so that the administrator can retrieve information from any network node in the network by imputing the referred IP address.
2. Then he chooses one OID from the list. For this prototype a set of the most useful OID variable was used.
3. Input the port address, by default 161
4. In case that the administrator wants to configure the network node by setting new value to a variable it should input the value in the field **Set Value** and press the button **Set.** In case that he wants to retrieve information, after finish the steps 1, 2 and 3 he press the **get or get next** button.
5. The application display error information in case that some error has occurred.

[①] www.ks-soft.net

6. An agent will be dispatched to the node and interact with SNMP-A through the command set or get search the information from the MIB variables (get command) or change to the new value (set command) and the required information is displayed in a same window.

Fig 4.15 MIB Browser GUI

5 CAMPUS NETWORK ARCHITECTURE BASIC SIMULATIONS

5.1 TEST ENVIRONMENT

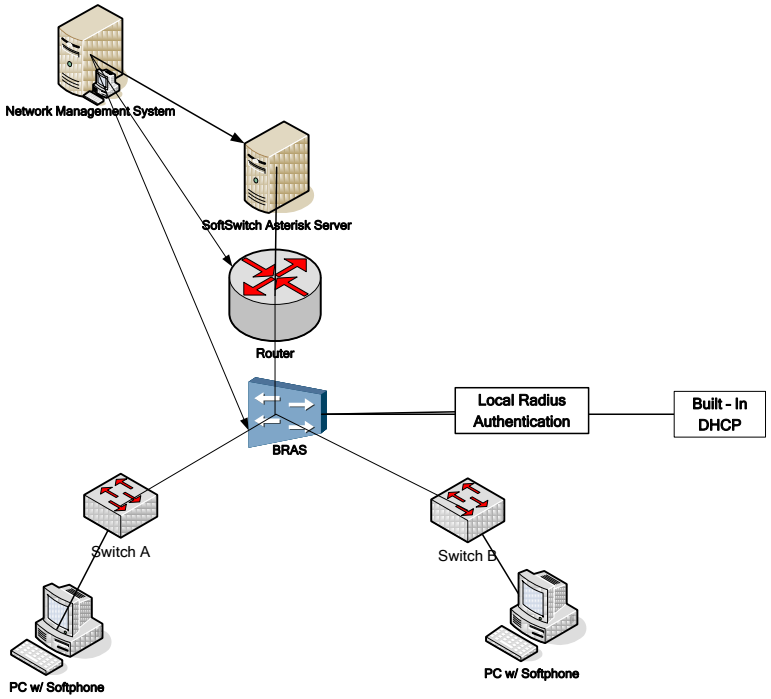

Fig 5.1 Network Architecture Simulation General Scenario

The simulation will be divided in four phases:

Phase 1 – Configure the Broadband Access Server (BAS), Router and Switches used in the experiment. Configure and test BAS VLAN Service and PPPoE Service;

Phase 2 – Install Asterisk Server, Softphones and Server Monitoring tool – SIPp software;

Phase 3 – Configure Network Management System;

Phase 4 – Perform the all integrated tests with the three components: BAS, Asterisk System and Network Management.

5.2 Broadband Access Server

5.2.1 VLAN Service

Virtual Local Access Network (VLAN) is a secure mechanism to separate data from different users and aggregate traffic reducing network traffic. VLANs are a fundamental part to delivery different types of services such as so called Triple Play Services. Packets can be tagged in two different ways: by packets that carry the same type of services or packets that belongs to the same user can be tagged with the same VLAN tag. In BAS, VLAN access authentication mode is used to verify the user's access right according to the access port and the VLAN ID (the VLAN ID can be set through the LAN Switch accessed by the user) in the user packet[15]. The simulation is as shown in figure 5.2:

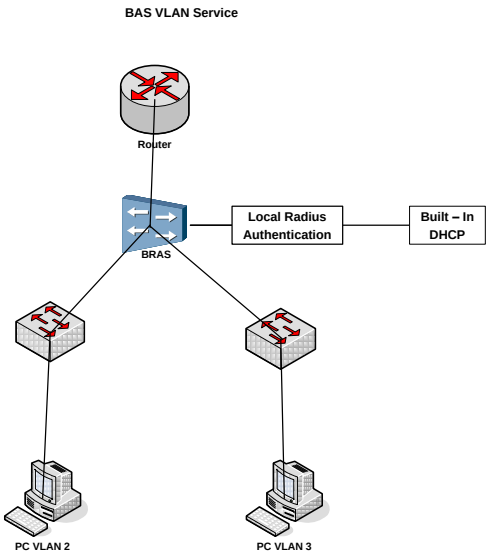

Fig 5.2 BAS VLAN Access Authentication Service Functions Configuration

BAS is configured with VLAN trunk (one port or a group of ports carrying multiple VLANs). VLAN trunk affixes different 802.1Q labels to one port or a group of ports to differentiate packets of different VLANs.

For these experiments the binding authentication (where BAS generate accounts automatically according to VLAN information at the user access port) was choose in these simulations. To configure VLAN services on the BAS the following steps are followed (Figure 5.3):

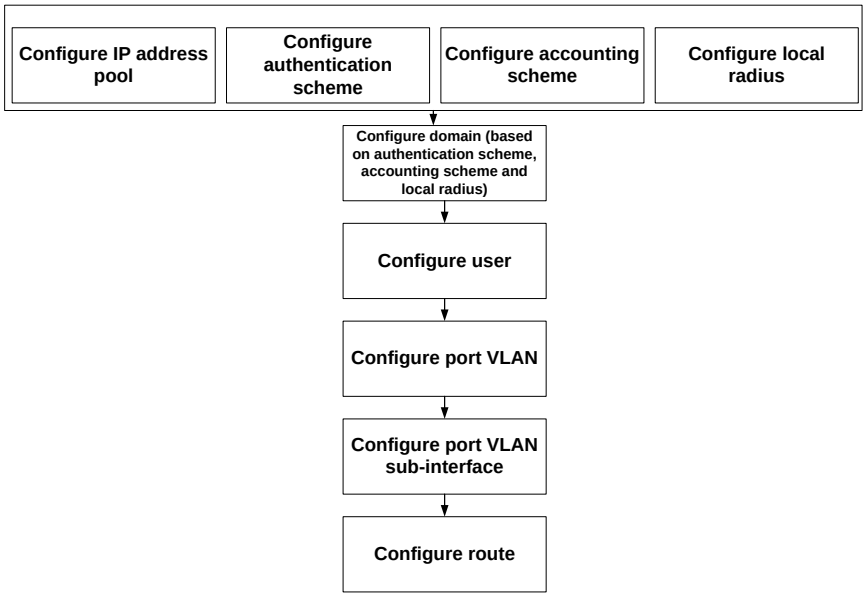

Fig 5.3 Steps for VLAN Services Configuration

The graph depicts configuration procedure of the VLAN Access Authentication Service.

Step 1: Configuration of IP address pool (including IP pool name, gateway, submask, section and DNS server.)

Step 2: Configuration of Authentication and Accounting Scheme local radius (authentication and accounting scheme name and authentication mode – local or radius server).

Step 3: Configuration of domain - Configure domain (reference to authentication, accounting and local radius) – define a domain isp name, assign the ip pool to be used and also assign an authentication and accounting scheme previous defined.

Step 4: Configuration of user, portvlan, VLAN sub-interface and route - Configuration of user, portvlan as access layer 2 subscriber, VLAN sub-interface as access-type interface and default route for the system.

In appendix A there is a detailed commands and screenshots of all the steps followed for the configuration of the BAS.

5.2.2 Broadband Access Server – PPP0E Service

Point-to-Point Protocol over Ethernet (PPPoE) is another authentication mode that allows users to access the network. Through PPPoE virtual dialing, users can establish point-to-point connections to the BAS, and thereby obtain online services. The network diagram and configuration procedures are almost the same as used in VLAN service except that the service is different, therefore the first procedure is configure the PPPoE virtual template[15] the procedure steps are depicted in figure 5-4.

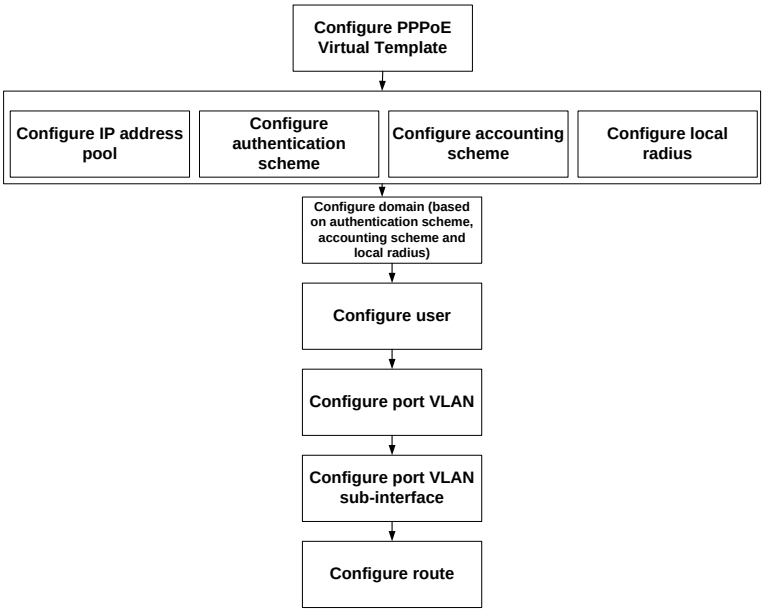

Fig 5.4 Steps for PPPoE Services Configuration

The first step to configure the PPPoE is to configure virtual template. The following steps are basically the same of those followed to configure VLAN. The only difference with VLAN is the configuration of virtual template. Therefore these steps will not be displayed here.

In appendix A there is a detailed commands and screenshots of all the steps followed for the configuration of the BAS.

5.3 Asterisk

Asterisk is open source software which provides almost all the services available in private PBX and added services. Asterisk system consists of different type of components, such as Asterisk server, gateways, telephone hardware and SoftPhones. To evaluate Asterisk performance and capacity to handle calls a set of performance tests was carried out. The experiment structure is depicted in figure 5.5.

The first step of this test was the installation and configuration of the Asterisk server and SIP client softphones on the computers. The files Extensions.conf and Sip.conf have been configured. The SIP softphones are then configured with SIP extensions created in SIP.conf. In order to perform VoIP calls to another SIP extension, the softphone must register itself as an extension on the server, which also gives it the presence status on the SIP server.

A basic scenario, an audio and video call is established between two computer running softphone X-Lite[①] which supports Session Initiation Protocol and Asterisk server performing the SIP registration between them.

Test requirements:

Asterisk server - running in a Celeron (R) Dual-Core CPU T3000 @ 1.80 GHz.

SIPp[②] is one of the most popular sip stress software. Its open software used to perform the stress-test of Asterisk server.

Wireshark software is used to analyze traffic.

SIPp is a test tool / traffic generator for the SIP protocol. It establishes and releases multiple calls with the INVITE and BYE methods. SIPp can also send media (RTP) traffic through RTP echo and RTP / pcap replay. Media can be audio or video.

SIPp can be used to test many real SIP equipments like SIP proxies, SIP media servers, SIP gateways, SIP PBX. It has the capacity to generate thousands of user agents calling a SIP system. VoIP uses several protocols for establishing SIP session and transfer streams such as SIP and RTP.

Wireshark is complete software for capture and analyze packets and network traffic. It provides different type of filters according to protocol, TCP or UDP data, etc. It has the capability to updates list of packets in real time. Wireshark permits analyze the complete process of initiating, establishing and terminating SIP session, all the negotiation performed by Asterisk Server to establish a connection between two users.

A multitude of factors can interfere in the performance of Asterisk, such as server capacity, bandwidth, protocols used, codec's, terminal equipments etc. as well as which service is being used (audio and video calls, voice mail, conference etc).

5.3.1 Simple audio and video call or Conferencing between 2 users using Softphones

The principle of this simulation is to perform Simple audio and video Call between two computers (A and B) running Softphones.

Three computers are used: one of them as Asterisk server, the other two as clients. The clients ran softphones; that is: software that simulates a telephone.

① http://www.counterpath.com/x-lite.html

② http://sipp.sourceforge.net/ - Download and further information about SIPp

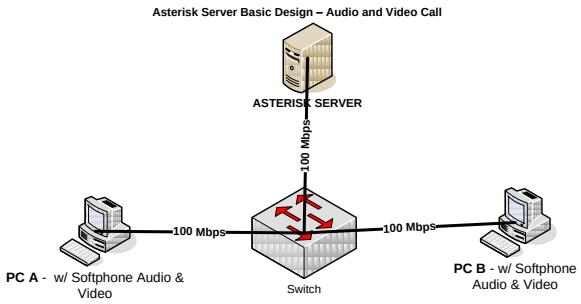

Fig 5.5 Basic Audio and Video call with Asterisk works as VoIP Server

Fig 5.6 Softphone Software

After downloading the software we had configured the phone according to user information configured in sip.conf on asterisk system. To make calls through asterisk server first clients must register with the server. After configuration of softphones it registers with server. Once registered, asterisk creates a route to its computer. That means asterisk will know where it should redirect the connection to in case somebody calls the user extension.

The dialplan is one of the most important and fundamental part of asterisk system. It is the kernel of the asterisk system because it's the place where we define the rules for inbound and outbound calls, configure applications like voice mail, conference, IVR and so on. Asterisk dialplan is totally customizable, it consists of a set of rules that we define to tell asterisk how to behave and what to do with any number dialed or received. The Dialplan configurations of asterisk are done using extensions configuration file; It is where extensions are added, where one defines actions to be started when a call is received, etc. The dialplan is made up of four main concepts: contexts, extensions, priorities, and applications.

Above is an example of part of the code configured in files extensions and sip.conf to run the experiment.

Table 5.1 Asterisk Dialplan Basic Configuration for Audio and Video calls

extensions.conf	sip.conf (audio call)	Video call
[incoming_calls]	[fofa]	[101]
exten =>104,1,Dial(SIP/fofa)	type=friend	type=friend
exten =>104,2,Answer()	secret=1206	username=101
exten =>104,2Hangup()	qualify=yes	secret=hidden
	nat=no	host=dynamic
exten =>105,1,Dial(SIP/teja)	host=dynamic	context=caboverde
exten =>105,2,Answer()	canreinvite=no	callerid=Video Phone <101>
	context=incoming_calls	disallow=all ; better for custom-tunning codec selection
		allow=ulaw
		allow=alaw
		allow=gsm
		allow=h263 ; H.263 is our video codec
		allow=h263p ; H.263p is the enhanced video
		codec
		dtmfmode=rfc2833 ; inband is not supported in compressed codecs like gsm, so we better set it to rfc2833
		canreinvite=no ; canreinvite must be set to 'no'
		qualify=yes
		nat=no

5.3.2 Asterisk Performance Evaluation

In this simulation SIPp software is used for calls generation and emulation to measure the maximum call asterisk server can handle and analyzed load and call success rate by number of calls completed and summary reports from SIPp Software.

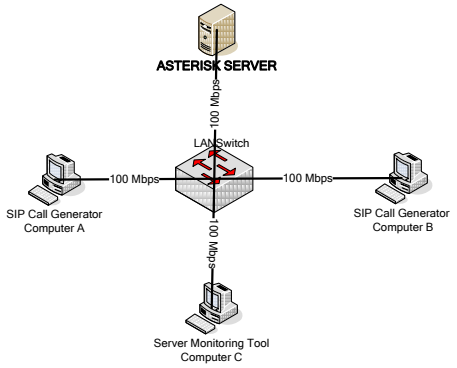

Fig 5.7 Asterisk Performance Evaluation

As can be observed in the fig 5.7 four computers are used to evaluate the Asterisk performance. According to the figure diagram, computer A generates calls and computer B receives calls. Computer C runs Wireshark software which is configured to capture and analyze data generated by SIP and RTP call sessions.

The test was performed using different amount of calls starting from 10 to up to 500 calls per second.

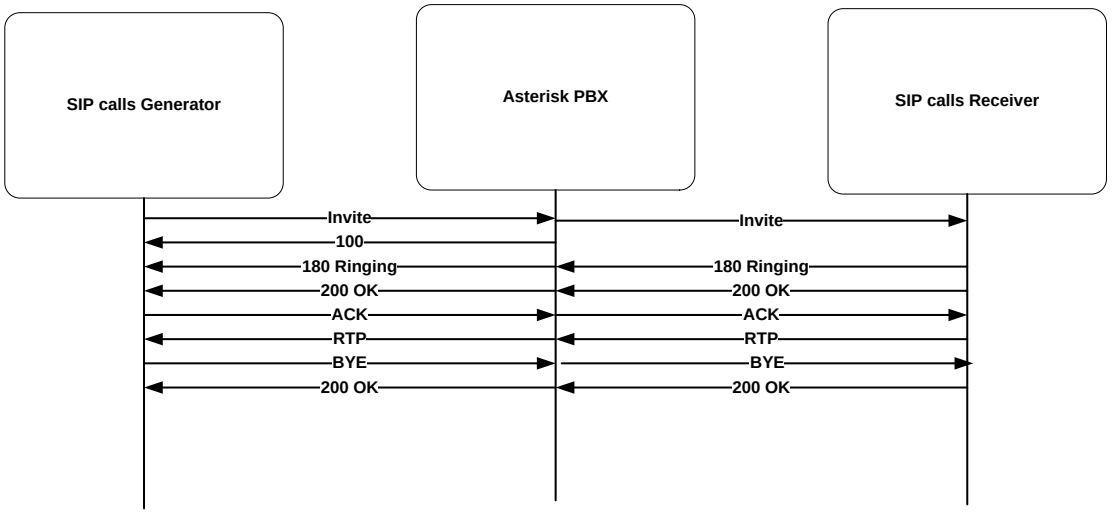

Fig 5.8 SIP and RTP Messages Flows

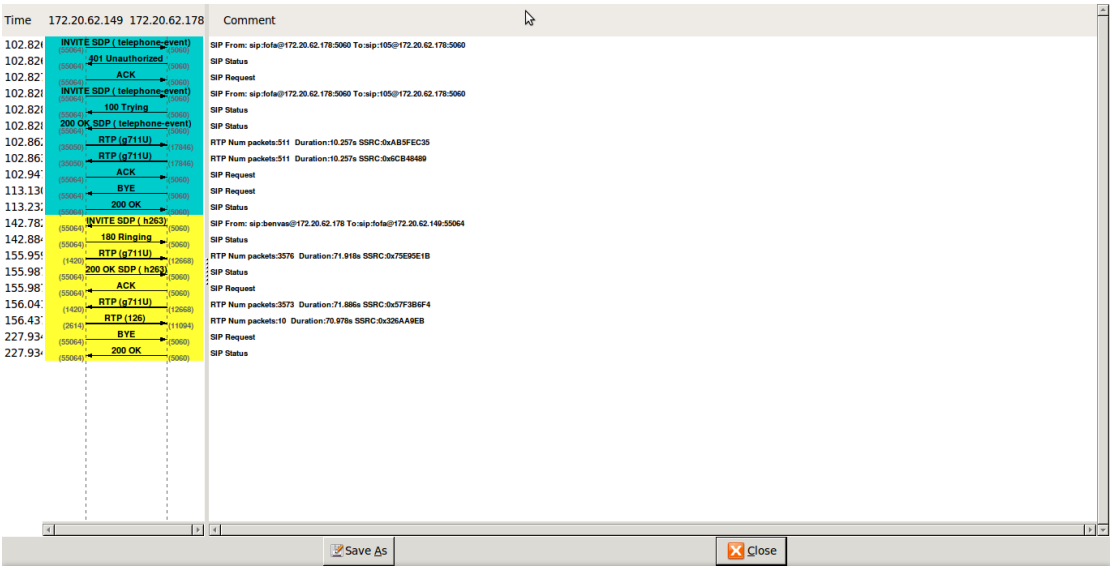

Fig 5.9 SIP and RTP Messages Flows Captured with Wireshark

The figure 5.9 depicts an example with SIP basic functions of messages exchanges, of a typical call scenario establishing, where exists a user terminal that wants to communicate with another terminal. It displays the parameters negotiation of an initiation, establishment and termination.

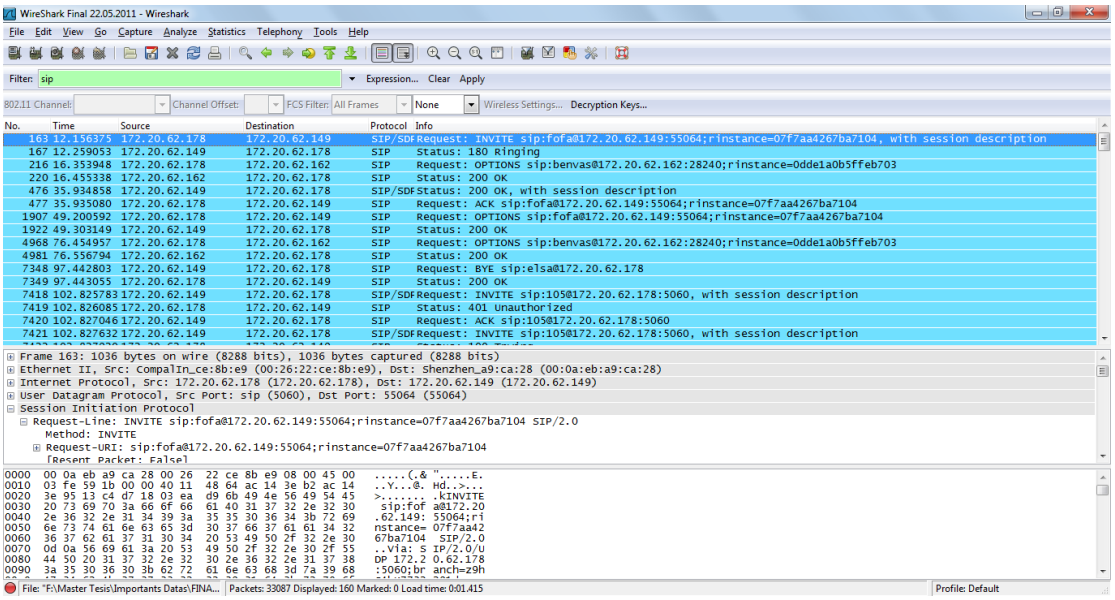

Fig 5.10 SIP Messages Flows

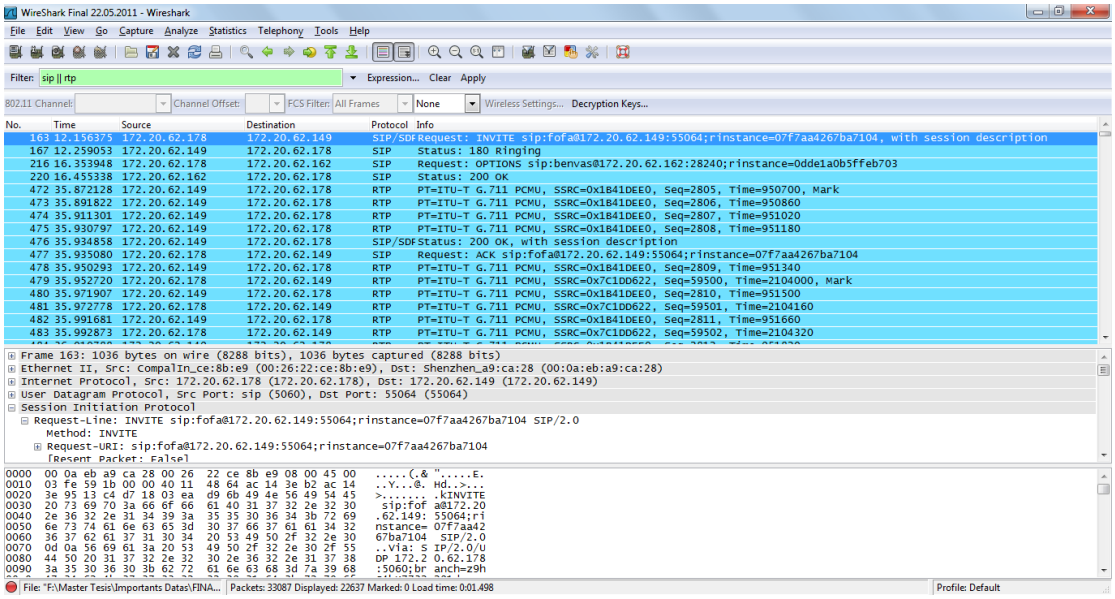

Fig 5.11 RTP Messages Flow

The softphone sends REGISTER requests. Then sends ACK responses and then receive 200 OK responses by the server if the client is able to authenticate successfully. We were able to successfully establish successful call between two user agents. With wireshark protocol analyzer we see the complete passing of the SIP messages (figure 5.10).

The goal is to evaluate the capacity of Asterisk to handle point to point simultaneous call, which means the maximum number of calls for that there, is no retransmission of messages due to timeout message because Asterisk does not reply.

To evaluate the maximum volume of calls Asterisk can handle, the software SIPp is used and configured with different calls limits as parameter.

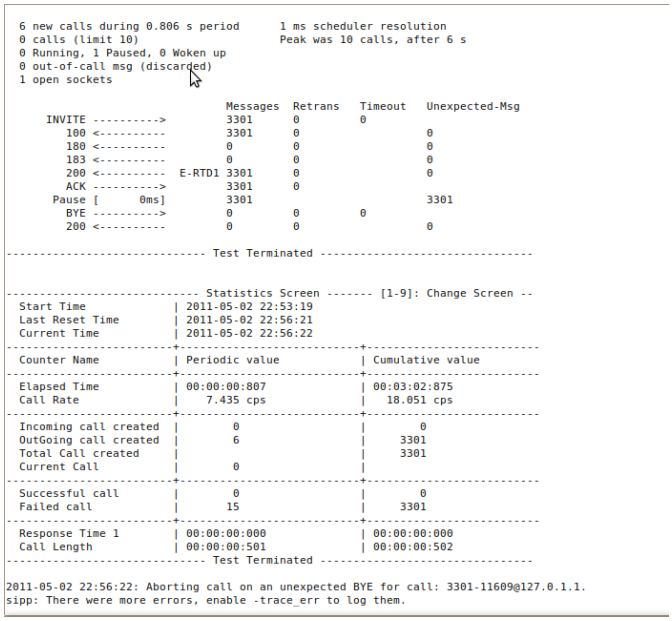

Fig 5.12 Maximum Calls per Second =10

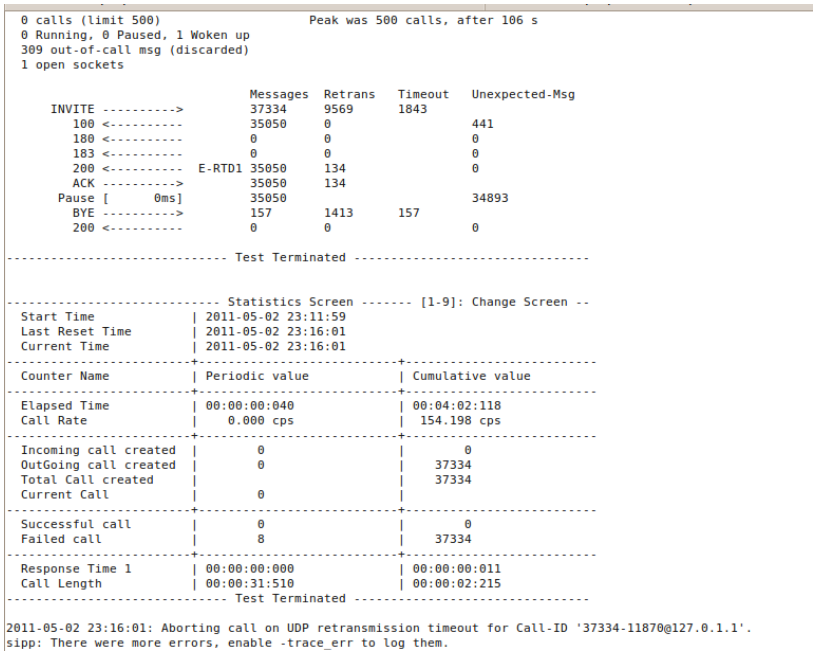

Fig 5.13 Maximum Calls per Second = 500 Simultaneous Calls

A set of tests was performed with an average duration of 4 minutes. The variable used to test the server load was the maximum simultaneous calls.

The best condition is all calls complete without any unexpected message and without any message loses. In our simulation, the amount of messages was high due to the fact that we've not configured the mailbox and Asterisk generates warnings in through messages alerting for that situation.

The maximum call limits was 10, 25, 50, 100,200 and 500 simultaneous calls using peer-to-peer calls with the same codec between sender and receiver, g711 and gsm. In appendix B there is all the results for different calls limits.

Table 5.2 Asterisk SIPp Stress Results

Observed Variable	**10**	**25**	**50**	**100**	**200**	**500**
SIP flows	3301	10774	17224	34512	62604	37334
B. C- G711	796.25 Kbps Kbps	1990.63 Kbps	3981.25 Kbps	7962.5 Kbps	15925 Kbps	39812.5 Kbps
B.C Gsm 13 kbps	286.25 Kbps	715.63 Kbps	1431.25 Kbps	2862.5 Kbps	5725 Kbps	14312.5 Kbps
Failed Calls	15	10	42	139	131	8
Peak calls	10 calls after 6s	28 calls after 5s	50 calls after 8s	100 calls after 11s	200 calls after 31s	500 calls after 106s

B.C - Bandwidth Consumption

Transnexus [49] have carried out an intensive Asterisk test and conclude that, for a server hosting Asterisk, each One GHz of CPU processing capacity can manage 100 simultaneous calls without codec translation (G711 ulaw) or 30 simultaneous calls with G711 ulaw to G729 codec translation. This proof the result achieved in our simulation for 500 simultaneous calls (using 1.80 GHz CPU processor), the retransmission was 9569 calls due to the limited capacity of the computer where Asterisk Server was running. A low percentage call failing may be acceptable for very heavy traffic conditions.

The capacity of Asterisk server is affected by different parameters. The server CPU capacity is one of the predominant factors that affect the performance of the system. The utilization of transcode or not which means the codec conversion between different codec types constitutes another factor for Asterisk performance.

5.4 Network Management with Mobile Agent - Simple management functions to manage BAS and Asterisk with Mobile Agent

In this simulation a simple prototype mobile agents was used. Tahiti server was

installed in the machine that Asterisk server was running and mobile agent was dispatched to collect simple information about Asterisk status. Asterisk with pre-programmed functions such as collect statistics information and do simple configuration.

For BAS, SNMP Agent was first configured and through the snmp-local agent some management information was collected and simple variable configured through set commands.

The purpose of this experiment is to demonstrate the advantages of using mobile agents in network management. Those advantages include reducing network traffic and building scalable and reliable distributed network management system since commands and configuration was performed locally in Asterisk Server.

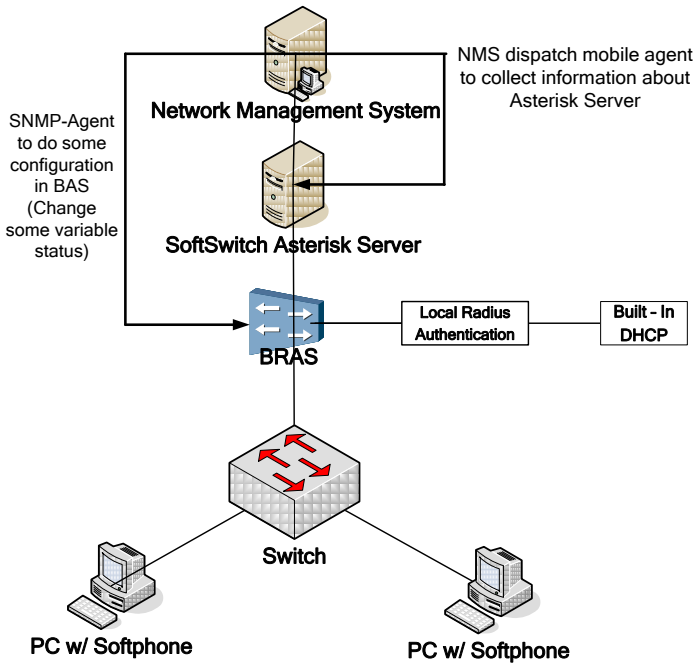

Fig 5.14 Network Management with Mobile Agents

6 CONCLUSIONS AND RECOMMENDATION FOR FUTURE WORK

6.1 CONCLUSIONS

With the constant evolution and ever increasing bandwidth requirements, predicting the future of information technology topic have never been so challengeable - and it follows that building an access network that is "future-proofed" and suitable for next-generation technologies is a major challenge for today's network architecture design. Today's network is in constant evolution – and what is enough today will almost certainly be too little tomorrow. With that in mind, future-proofing the network wherever possible should be a major consideration.

This thesis proposes network architecture and entities suitable for university campus requirements today and future-proof. It is built in open standards, modular and flexible way which makes it easy for future-growth. It provides ways to respond to actual challenges faced by university campus network and also it provides an evolutionary path for NGN. A very important characteristic for this architecture is that it allows the convergence from many network to one while it is open, this means it's not vendor dependent and as so no single service provider or vendor owns the technology and controls its definition and development. This make possible that the architecture be adopted as a standard and be widely deployed. With a layered model which divides the architecture into a number of key components, each components providing a set of functions and interacting with each other. It offers transport flexibility with IP being the fundament transport technology.

The proposed architecture offers several advantages, build in a modular way allow Campus University to be adapted and evolutes according to the demands. Because most of university have already implemented their network infrastructure and rebuild it from scratch may not be economical feasible, an incremental approach to adapt to the proposed architecture can be adopted. The evolution procedure shall be complete steadily in a way that it not affects the existent services. However this adoption should be build for future. We use several strategies to ensure flexibility, reliability and scalability. Using a layered architecture makes it easy to grow and the mobile agents make the management distributed, thus the scale of the network is no more an obstacle.

Several access network key technologies have been described in this research. Campus access network technologies can support multiple access modes, which offers the flexibility to the university to choose the appropriate access mode according to the actual network conditions and realizes smooth integration and evolution of PSTN to NGN. An efficient solution incorporates hybrid solution comprising optical fiber and wireless access. The backbone of optical connections offers high bandwidth while wireless networks enable mobility and ubiquitous broadband communications. Wireless access offers many advantages for campus network such as mobility, facility in deployment as well as bandwidth scalability in terms of the number of users. Optical access can provide high bandwidth required by new emerging services such as multimedia services. Such networks represent an excellent evolutionary and flexible path for current campus access technologies. Different architectures are available for fiber deployment such as FTTP, FTTC or FTTCab which can be chosen according to university requirements.

Asterisk as softswitch is the core of the proposed architecture and NGN. It provides call control functionality, controls the media gateways and access devices, processing signal protocols, generates Call Detail Record. It also supports interoperability between circuit-switched network and data switched network. Asterisk supports integrated access between analog and digital users. Asterisk supports a multitude of multimedia standard protocols, such as SIP, h.323, RTP protocols, etc.

Traditional network management is based on centralized management. It has the advantage of centralizing information about the whole network in one place and locates the network faults quickly. However it has several drawbacks as well, there are often an overload processing at network manager side and the exchange of messages between manager and the managed device leads to a huge consume of bandwidth and lead to heavy traffic generation in the network which may cause network bottleneck. A network management model using mobile agents has been proposed in this thesis in a way to overcome the drawback of traditional management. To take advantage of distributed network management, we purpose a flexible and scalable architecture Network Management with Mobile Agents which improves conventional SNMP architecture effectiveness. This make possible take advantages of SNMP as well as the performance effectiveness of Mobile Agents. The proposed model is a hybrid model, which provides an additional component to network management system. The system has been prototyped based on an SNMP4J package and IBM Aglet mobile agent system.

Network management with mobile agents has the advantages of flexibility, scalability, easy to be integrated, security, and customization, and also the benefit of run on any platform. As we use java technologies, networks can be managed from any platform with JVM.

In the university campus network process of migrating to broadband next generation network, there is no “one size fits all” solution. The best solution is careful analyzing today’s network campus requirements and keeps in mind future prospects and then based on architecture model design a network plan that meets each unique situation.

6.2 FUTURE WORK

As future works this thesis aims to provide improvements in the architecture and propose it as a standard for Campus next generation network architecture.

Do a more intensive research about method to provide Wireless over Passive optical network and Simulate the proposed solution with hybrid access network composed by optical fiber backbone and Wireless in the last mile solution.

Research Asterisk core and upgrade it with more sophisticated softswitch capabilities. Further research and simulation will be done by to improve its functions as a softswitch. In case of more than one Asterisk server (cluster of Asterisk server) being deployed, the integration with SER[①] – SIP Express Router (SIP proxy) is very important to manage the load balancing, allowing system redundancy and scalable SIP register.

Based on open source solutions implements a complete platform for network management with mobile agents by incorporate advanced functions in the mobile agents platform, improving its mobility algorithms and provide Web solution as it is current trend and it permits that the platform can be used from everywhere to manage the network.

① http://iptel.org/ser/

DEDICATION

It's in Christ that we find out who we are and what we are living for. Long before we first heard of Christ ... he had his eyes on us, had designs on us for glorious living, part of the overall purpose he is working out in everything and everyone.

Ephesians 1:11 (Msg)

Dedicated to the Author of life whom I love and have completely surrendered my life: GOD.

To my parents, Benvindo and Fofa,
my sisters and brothers: Elsa, Teja, Angelo, Elly and Valdir
my beloved Helder, Lorena, Helio and Tiago, with my eternal love…

ACKNOWLEDGES

First of all, I thank the almighty God for all His love, care and protection.

I thank my parents, sisters and brothers, niece and nephews, and all my relatives and in laws, for their love and encouragement. You are the light of my life and you are forever in my heart.

I would like to thank my advisor, Mr Hu Zhi-Yuan, at College of Communication in Chongqing University, for his valuable knowledge and all his suggestions, efforts, patience and his encouragement during these two years in China and toward the successful completion of this thesis.

I'd like to thanks all my teachers in the college of communication from Chongqing University for the transmission of knowledge, all the efforts made and their friendship.

I thank my labmates – Chinese students, for always being there to help me in whatever I needed and make my life happier and easier in China. You have been my second family in China. I want you to know that I appreciate it and may God bless you all.

I thank all my true and good friends from home for their support, prayers and friendship, and my gratitude to Acolytes group and Scouts movement for contributed in my spiritual and individual grow.

I thank my new friends (those I've met here in China) for all the moments shared and our unique get together in Xuelin. I'll keep them all in my good memories about China..

My gratitude to China Scholarship Council and Government of Cape Verde to gave me this opportunity to pursue my master degree here in China.

REFERENCES

[1] Yuan, S. and Wang, W. (2010) "A Campus Network Security Emergence Response - Technical System Based on Emergency Log", IEEE Journal.

[2] Razak, M.R.A. and Ali, A.H. (2006) "The Impact of Voice Traffic on UniKL-BMI Campus Network", in Proc. of the Electrotechnical Conference, MELECON 2006. IEEE Mediterranean, IEEE Journal.

[3] Gigabit Campus Network Design—Principles and Architecture - http://www.cisco.com/warp/ public/cc/so/neso/lnso/cpso/gcnd_wp.pdf, 10/05/2010

[4] Campus Area Network basic information – (1999) http://www.freewimaxinfo. com/campus -area-network-can.html, 10/19/2010

[5] Imran, A., M. A. Qadeer, and M. J. R. Khan (2009) "Asterisk VoIP Private Branch Exchange", http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05164214&tag=1, IEEE Journal.Mahle, P. VoIP Telephony with Asterisk 2003 USA.

[6] Network Wired and Wireless technologies http://www.netgear.co.uk/home_ newnetwork_ wiredwireless.php, 10/19/2010.

[7] Xia, S., Zhang J., Yang J., and Ni J. (2010) "A content-based Self-feedback E-Governemnt Network Security Model" – 2010.

[8] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05521604 in Proc. of 2009 Fourth International Conference on Internet Computing for Science and Engineering, pp 194-198

[9] Carpenter C., Middleton N., Duffett D., and Plain I., (2009) Asterisk 1.4 - The Professional's Guide – Implementing, Administrating, and Consulting on Commercial IP Telephony Solutions.

[10] RFC 2705 - Media Gateway Control Protocol (MGCP) Version 1.0 http://www.ietf. org/rfc/rfc 2705.txt, 10/19/2010.

[11] Standford H. R. and Marsha L. S. (2006) Computer Networking, Pearson Education Asia and Tsinghua University Press.

[12] Kaufmann, M., (2007) Network Analysis Architecture and Design 3rd.Edition USA.

[13] University of Maryland Information Technology Ten Year Plan (2007) http://www.oit. umd. edu/ ITCouncil/materials/10_Year_Campus_IT_Plan031407.pdf,11/10/2010.

[14] IBM Aglets Project website - http://sourceforge.net/projects/aglets/ 10/19/2010.

[15] SmartAX MA5200F Broadband Access Server Operation Manual, (2006), Huawei Technologies Documentation http://www.huawei.com, 09/12/2010.

[16] Zhao, V. Q., Wang H., and Zhang Y., A Comparison Study of Three Mobile Agent Systems. Agent Transfer Protocol website - http://www.trl.ibm.com/aglets/atp/atp.htm, 10/19/2010.

[17] Application of Mobile Agents in Managing the Traffic in the Network and Improving the Reliability and Quality of Service Aglets Specification 1.1 Draft - http://www.trl.ibm.com/aglets/spec11.htm, 10/19/2010.

[18] Building Applications with Aglet (1998) – http://www.trl.ibm.com/aglets/spec11.htm#Building 10/19/2010.

[19] Mauro D. R. and Schmidt K. J. (2001) Essential SNMP - http://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_01.htm, First edition, published July 2001.

[20] Clemm, A., (2006), Network Management Fundamentals (2006) – Cisco Press.

[21] Lange D., Java Aglet Application Programming Interface (J-AAPI) White Paper - Draft 2 – (1997) http://www.trl.ibm.co.jp/aglets aglets@yamato.ibm.co.jp - IBM Tokyo Research Laboratory.

[22] Stallings W., (1999) SNMP, SNMPv2 and RMON: Practical Network Management, Addison-Wesley.

[23] EDUCAUSE Center for Applied Research (ECAR) (2005), "Network Funding Models: Cornell University, University of California at San Diego, and University of Wisconsin – Madison" http://net.educause.edu/ir/library/pdf/ers0502/cs/ECS0501.pdf, 02/10/2011.

[24] NGN Access Single Line Multi-Service - ITU-BDT Regional workshop on NGN Economics,http://www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S4-Migration.pdf, 09/17/2010

[25] Perros G. H., (2005), Connection Oriented Networks SONET/SDH, ATM, MPLS and Optical Networks, John Willey & Sons, England.

[26] Hens J. F., and Caballero M.J, (2008), Triple Play – building the converged network for IP, VoIP and IPTV, John Willey & Sons, England.

[27] Wong, Kong et al, (2009), Wireless Broadband Networks Willey (2009) Maeda, Y., Kikuchi, K., and Tokura, N.; (2001) "ATM Access Network Architecture", IEEE Journal, pp 687-691.

[28] CCM Conectcom, (2008), The book on Next Gen Networks FTTx 2008, ADC Telecommunications Broadband Forum, Next Generation Access http://www.broadband-forum.org/, 12/20/2010.

[29] Yang K., Ou S.,Guild, K., and Chen H., (2009), Convergence of Ethernet PON and IEEE 802.16 Broadband Access Networks and its QoS-Aware Dynamic Bandwidth Allocation Scheme, IEEE Journal on selected areas in Communications, vol. 27, no. 2, February 2009

[30] Teare D., and Paquet C. (2005), Campus Network Design Fundamental – Cisco Press, 2005.

[31] Network Protocols Handbook Second Edition, (2005) Javvin Technology.

[32] CISCO Qualiy of Service Overview, http://www.cisco. com/en/US/docs/ios/ qos/configuration/ guide/qos_overview.html,12/20/2010

[33] Federal Communications Comission - FCC, Telecommunication Act of 1996 - http://www. fcc.gov/telecom.html, 10/25/2010.

[34] ITU-T Recommendation Y.2001 (12/2004) - General overview of NGN - http://www. itu.int/en/ITU-T/gsi/ngn/Pages/definition.aspx, 10/28/2010.

[35] Kurose, J., and Ross K., (2005), Computer Networking – A Top-Down Approach Featuring the Internet, 3rd Edition -2005 pp 734-736.

[36] Michael J. Wooldridge and Nick Jennings - Intelligent agents III: agent theories, architectures, and languages – August 12-13, 1996 – pp 23.

[37] Schiller J., (2004), Mobile Communications, Second Edition – 2004, pp 201-230.

[38] Giarre L., Neglia G., and Tinnirello I., (2009), "Medium Access in WiFi Network : Strategies of Selfish Nodes" IEEE Signal Processing Magazine. pp 116.

[39] Govil J., and Jivica (2008) "4G : Functionalities Development and an Analysis of Mobile Wireless Grid" in Proc. of First International Conference on Emerging Trends in Engineering and Technology, pp 270-275.

[40] Khan A. H., Qadeer M. A., Ansari J., and Waheed S. (2008), "4G as a Next Generation Wireless Network" in Proc. of 2009 International Conference on Future Computer and Communication. pp 334-338.

[41] International Telecommunication Union –What really is a Third Generation (3G) Mobile Technology.http://www.itu.int/ITU-D/imt-2000/DocumentsIMT2000/ What_really_3G.pdf 03/25/ 2011

[42] Rash, W. (2005). "Open source pbxes: Free flexibility" InfoWorld; 1/31/2005, Vol. 27 Issue 5 (2005).

[43] Huitema, C. (2003). IETF RFC 3605: Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP), Oct. 2003, http://tools.ietf.org/pdf/rfc3605.pdf 04/04/2011.

[44] Hu, Wang, , et al. (2008) System and method for providing Wireless over a Passive Optical Network (PON) USA 03/13/2008 http://www.freepatentsonline.com/20080063397.pdf 11/02/2011

[45] TransNexus (2008) –Performance Benchmark Test for Asterisk B2BUA – October 3, 2008

[46] RFC 5346 - Operational Requirements for ENUM-Based Softswitch Use – Internet Engineering Task Force.

APPENDIX

A Broadband Access Server Configuration

VLAN Access Authentication Service Steps for Configuration

Configuration procedure steps of the VLAN Access Authentication Service.

Step 1: Configuration of IP address pool

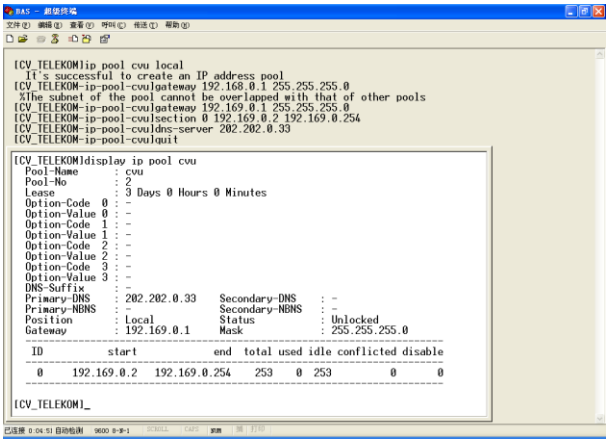

Fig 00 Vlan IP Address Pool

Step 2: Configuration of Authentication and Accounting Scheme

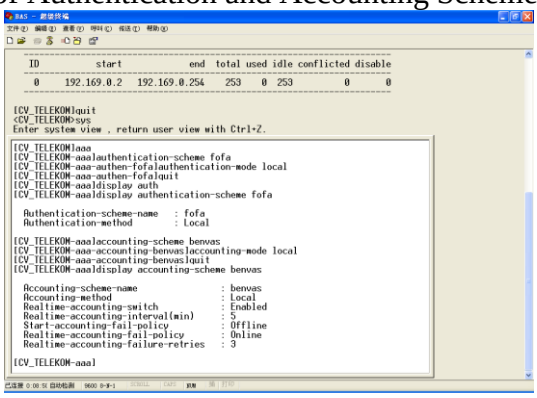

Fig 01 Authentication and Accounting Scheme and Local Radius

Step 3: Configuration of domain

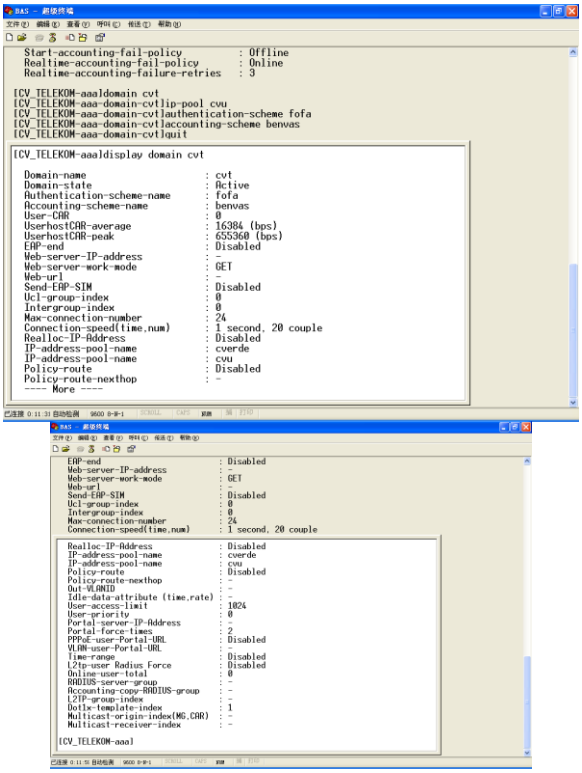

Fig 02 Configure Domain (reference to Authentication, Accounting and Local Radius)

Step 4: Configuration of user, portvlan, VLAN sub-interface and route

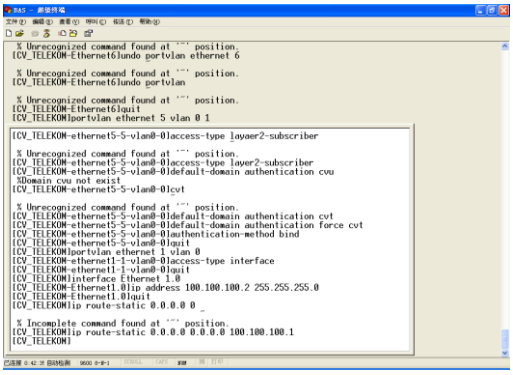

Fig 03 Configuration of User, Portvlan, VLAN sub-Interface and Route

PPPoE Access Authentication Service Steps for Configuration

The first step to configure the PPPoE is to configure virtual template. The following steps are basically the same of those followed to configure VLAN. The only difference with VLAN is the configuration of virtual template. Therefore these windows will not be displayed here.

Step 1: Configuration of Virtual Template. The others steps are the same as those followed to configure VLAN services.

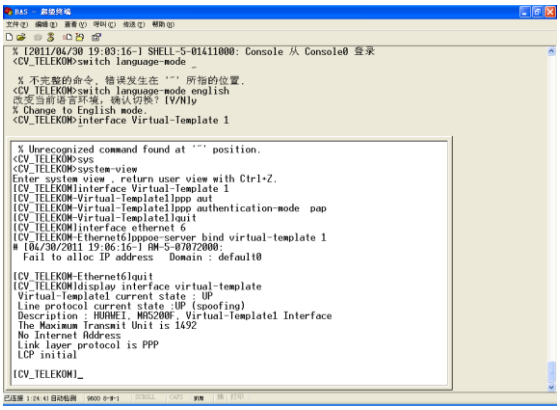

Fig 04 Configuration of Virtual Template

APPENDIX B SIPp Stress Calls

```
  0 calls (limit 25)                    Peak was 25 calls, after 5 s
  0 Running, 1 Paused, 0 Woken up
  0 out-of-call msg (discarded)
  1 open sockets

                                Messages  Retrans   Timeout   Unexpected-Msg
      INVITE ---------->         10774     0         0
         100 <----------         10774     0                   0
         180 <----------         0         0                   0
         183 <----------         0         0                   0
         200 <----------  E-RTD1 10774     0                   0
         ACK ---------->         10774     0
       Pause [      0ms]         10774                         10774
         BYE ---------->         0         0         0
         200 <----------         0         0                   0

------------------------------ Test Terminated --------------------------------


------------------------------ Statistics Screen ------- [1-9]: Change Screen --
  Start Time             | 2011-05-02 22:57:22
  Last Reset Time        | 2011-05-02 23:01:10
  Current Time           | 2011-05-02 23:01:10
-------------------------+---------------------------+--------------------------
  Counter Name           | Periodic value            | Cumulative value
-------------------------+---------------------------+--------------------------
  Elapsed Time           | 00:00:00:206              | 00:03:48:249
  Call Rate              |    0.000 cps              |   47.203 cps
-------------------------+---------------------------+--------------------------
  Incoming call created  |        0                  |        0
  OutGoing call created  |        0                  |    10774
  Total Call created     |                           |    10774
  Current Call           |        0                  |
-------------------------+---------------------------+--------------------------
  Successful call        |        0                  |        0
  Failed call            |       10                  |    10774
-------------------------+---------------------------+--------------------------
  Response Time 1        | 00:00:00:000              | 00:00:00:000
  Call Length            | 00:00:00:502              | 00:00:00:501
------------------------------ Test Terminated --------------------------------

2011-05-02 23:01:10: Aborting call on an unexpected BYE for call: 10774-15110@127.0.1.1.
sipp: There were more errors, enable -trace_err to log them.
```

Figure 06 Maximum Calls per Second = 25 Simultaneous Calls

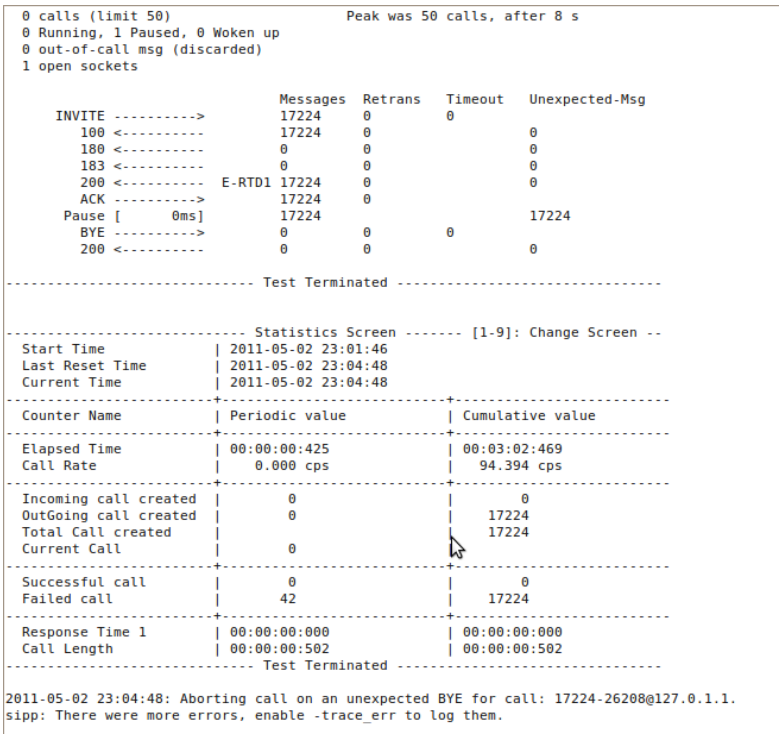

Figure 07 Maximum Calls per Second = 50 Simultaneous Calls

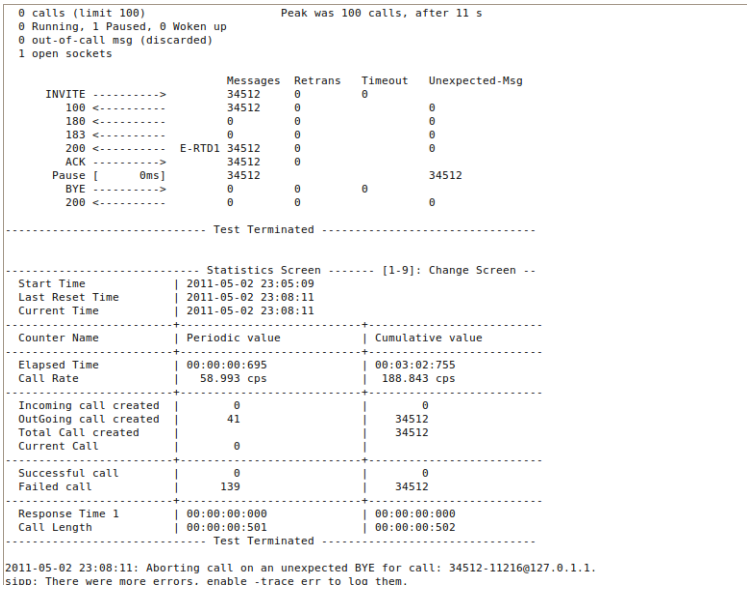

Figure 08 Maximum Calls per Second = 100 Simultaneous Calls

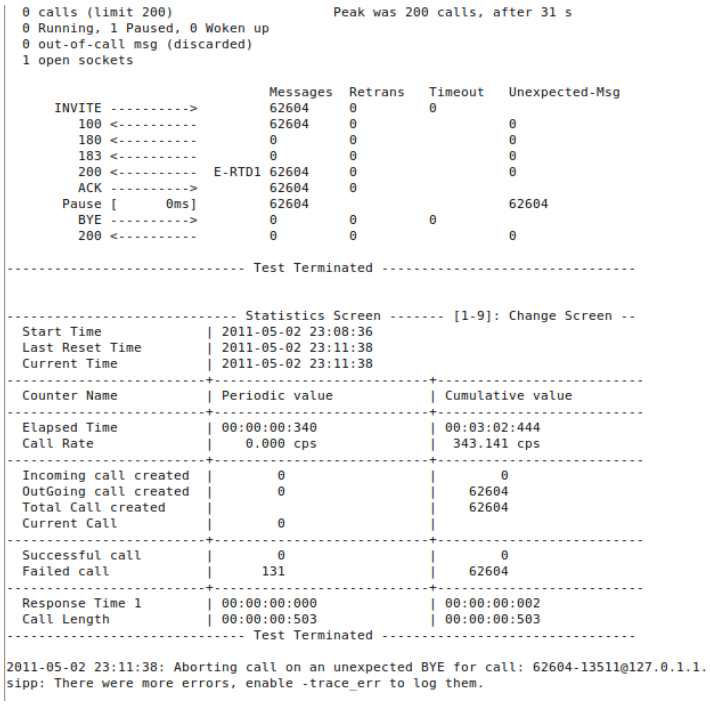

Fig 9.10 Maximum Calls per Second = 200 Simultaneous Calls