Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE @ DIRECT®

Computer Communications 26 (2003) 679–690

computer communications

www.elsevier.com/locate/comcom

Operation management of IP broadband access networks

Ammar Rayes*

Cisco Systems Inc., 170 West Tasman Drive, San Jose, CA 95134, USA

Received 8 July 2002; accepted 8 July 2002

Abstract

The last several years have seen significant advances in broadband access technology, including greater bandwidth, improved quality of service capabilities, multicast, and better applications availability. Customers today have several choices of broadband access technologies, namely Digital Subscriber Lines (DSL), Cable, wireless, and most recently Ethernet or Fiber to the home or business, as the first/last mile access is now an emerging technology gaining significant momentum specially Europe and Asia Pacific.

Ensuring profitability from these services requires a comprehensive service management architecture that enables service providers to carefully plan, quickly provision, efficiently operate, and accurately bill these services. Once the user is connected to the network, service providers must monitor and ensure the Quality of Service. In this paper, we first provide an overview several IP broadband access technologies including Ethernet to the home/business, IP DSL, Wireless, and Cable. We then define an integrated Operation Support Systems/Network Management Systems (OSS/NMS) architecture including description of fault, configuration, accounting, performance, and security management functions. Several traffic-engineering algorithms are then discussed and simulation results are compared. Finally, an intelligent capacity allocation algorithm for IP network is introduced.

Keywords: Broadband access technology; Digital subscriber lines; Ethernet; Traffic-engineering

1. Introduction

The Internet is penetrating all aspects of society and becoming an indispensable part of our daily lives. With the enabling applications such as emails, the WWW, online shopping, banking, video-conferencing, distant learning, entertainment, which often entail exchange of large amount of data, the Internet access speed is an important issue. Internet access is in fact becoming a commodity service from a service provider perspective. It has little customer loyalty and is driven by price and quality.

There are many broadband access technologies including Ethernet-to-the-Home (ETTH) and Ethernet-to-the-Business (ETTB) (collectively known as ETTx), wireless, cable, and IP digital subscriber line (DSL).

Ethernet is the dominant technology in LAN due to its simplicity, low cost, ubiquity (300 million ports installed worldwide), and very high speeds. In the last four years the industry has seen a jump from shared 10 Mbps, to switched 100 Mbps, to switched 1 Gbps, and now up to switched 10 Gbps Ethernet. These factors have allowed LAN network managers to put more and more mission critical applications on their networks. In the WAN, service providers have used technologies such as DWDM to scale the long-haul networks. This has enabled service providers to more cost-effective by utilizing their investment in fiber. By extending Ethernet to the last mile, service providers can deliver true multi-services to the end-users. ETTx offers new opportunities for service providers. However, it entails laying fibers to the customer premises, which may be expensive.

Wireless provides mobile connection to the Internet and voice networks. Due to the noisy transmission media, it can support up to 2 Mbps in the optimal case, for the 3G (third generation) wireless systems, such as IMT-2000 and CDMA2000.3x. In practical environment, the actual speed can be much slower. However, the ubiquitous access capability has gained much market interest.

Cable access can provide connection speed up to 6 Mbps. With cable connections to most of the household in North America, it gives the cable operators quick presence into the Internet access market. The lack of switching capability in the cable network limits its two-way communications capability. Significant infrastructure upgrade is needed.

* Corresponding author.
E-mail address: rayes@cisco.com (A. Rayes).

0140-3664/03/$ - see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0140-3664(02)00200-1

DSL uses the current twisted copper pairs in the Plain Old Telephone Service (POTS) to provide Internet access. There are many flavors of DSL technology, e.g. Asymmetric ADSL (ADSL), G.Lite, Very-high-data-rate DSL (VDSL), etc. The downstream bit rate ranges from 1 Mbps by G.Lite to up to 52 Mbps by VDSL. The actual speed depends on the specific implementation and the distance between the customer premise and the central office (CO), i.e. the loop length. The almost 100% market penetration of the twisted pairs make DSL is strong contender in providing Internet access.

Possessing the access technology is only half of the battle for service providers. The ability to manage the network efficiently and in a timely fashion is essential in the current competitive market place. Network management can be defined as the set of operation support systems that service providers use to deploy, configure, maintain, and monitor the network and the services that are carried over it. They can also be used to study the network behavior and determine the future network expansion plans. Network management is also used for user authentication and network security to protect the network from malicious users and to maintain the network integrity. Other important issues include service order management, billing, to name a few. These are all crucial for the service providers' market penetration and profitability. The objective of this paper is to discuss the integrated management of IP (Internet Protocol) broadband access networks.

This paper is organized as follows. In Section 2, we will give an overview of the few popular broadband access technologies. The integrated network management problem is discussed in Section 3. Section 4 studies the traffic modeling and network-dimensioning problem, which is an essential component in network management. An intelligent capacity allocation algorithm is proposed. Conclusion remarks are given in Section 5.

2. Broadband Access Technologies

2.1. Wireless Access

Fig. 1 shows the wireless access architecture. A mobile terminal with IP capability establishes a wireless link to the base station transceiver (BTS). The corresponding base station controller (BSC), with IP capability provides the actual attachment to the packet-based wireless network. It can be either the GPRS (GSM Packet Radio System) or CDMA system for the 2.5G wireless systems. Alternatively, it can be the 3G wireless systems. Through an access router at the edge of the IP core, the wireless network communicates with the Internet Service Provider (ISP).

The main difference between the IP wireless access and traditional wireless access lies in the enhancement of the BSC to be IP-literate. The IP wireless network is packet-based with IP capability. For example, the GPRS system consists of the Servicing GPRS Support Node (SGSN) and the Gateway GPRS Support Node (GGSN). GPRS uses GPRS Tunneling Protocol (GTP) to deliver IP packets to the mobile terminal. On the other hand, the 2.5G CDMA wireless system consists of the Packet Data Service Node (PDSN) and it uses Mobile IP for packet delivery.

Although the access speed through the wireless domain is limited, wireless access provides the unique tether less access to the Internet. It allows subscribers to communicate anywhere they are traveling.

2.2. IP DSL

Fig. 2 shows the IP DSL architecture. The IP DSL switch is an IP-aware DSL switch, capable of switching permanent virtual circuit (PVC's) and soft-PVC (SPVC's), yet support IP Quality of Service (QoS) and IP DSL switch. Connections to the ISP or private Virtual Private Network (VPN) are established by setting up tunnels using tunneling protocols such as Layer 2 Tunneling Protocol (L2TP). The IP DSL switch pushes the Layer 3 functionalities toward the network edge. It is a distributed architecture in the sense that it distributes the CPE aggregation and thus the L2TP aggregation among the IP DSL switches at the network edge. It makes the network more resilient to switch failure and provides better scalability.

The DSL architecture with IP DSL switches allows full IP functionalities for both consumers and businesses. These include basic Internet access, online shopping, online banking, multicast video, e-commerce, distance learning, secure Virtual Private Network (VPN) using Multiprotocol

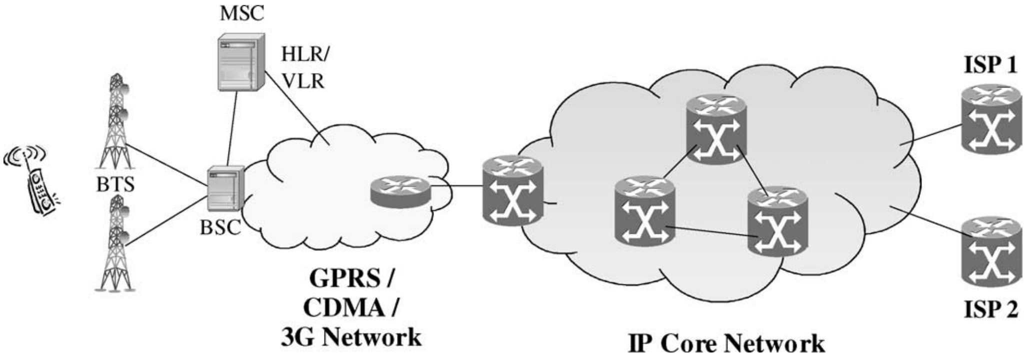

Fig. 1. Wireless Access Architecture.

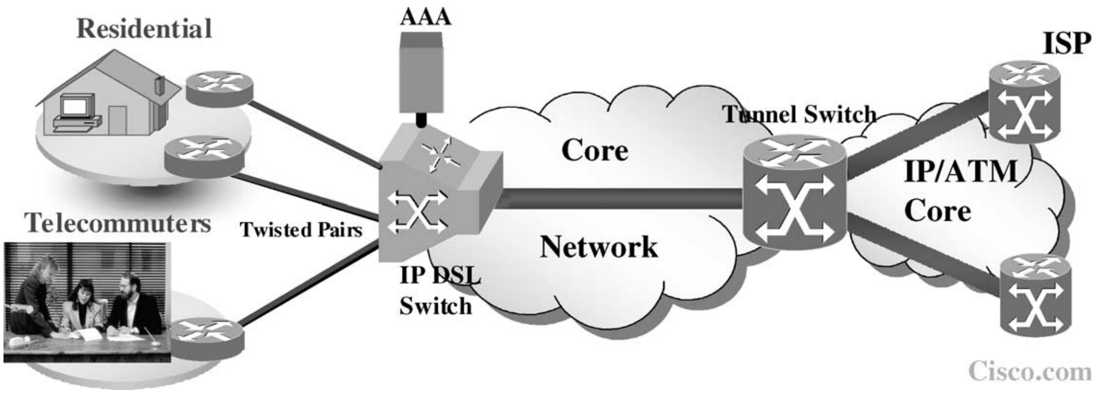

Fig. 2. IP DSL Network Architecture.

Label Switching (MPLS) technology. The distinctive feature of DSL is the use of the existing twisted copper pairs for both analog voice and Internet access. The thousands of miles of copper pairs in the ground is a multi-billion dollars infrastructure. DSL allows traditional telephone service providers to leverage their existing infrastructure to offer broadband IP access. IP Internet traffic in the twisted pairs is routed to the DSL networks, freeing up the analog voice networks, which are not originally designed to handle packet traffic that can be more persistent with longer call holding time than analog voice. As a result, better Internet service is provided while call blocking is reduced in the analog networks.

2.3. Cable Access

The cable access architecture is shown in Fig. 3. At the customer premise end sits the CPE device, which is the cable modem. Personal computers are connected to the CPE through Ethernet. Using cable, the CPE links to the access provider network through the access router. Links to the Internet or Corporate sites are then made from the Network Access Provider (NAP).

The highly penetrated cable network gives the cable providers an advantage in gaining presence in the ISP industry. However, switching capability needs to be installed in order to provide more interactive services.

2.4. Ethernet to the Home/Business Architecture

Fig. 4 shows the ETTX architecture, a variant of FTTx. ETTx is particularly suitable for SOHO (small office, home office) and multiple dwelling units including high-rise apartments and campus dormitories. Each dwelling unit has Ethernet connection to the Ethernet access switch in the basement of the apartment, providing 'always-on' broadband access. The connection speed can be 10 or 100 Mbps and easily upgradeable to the gigabit range as the cost becomes commercially feasible. At the customer premise end, set-top box, personal computers, IP phones and other appliance are connected to the Internet through the residential gateway. The Layer 3 access switch in

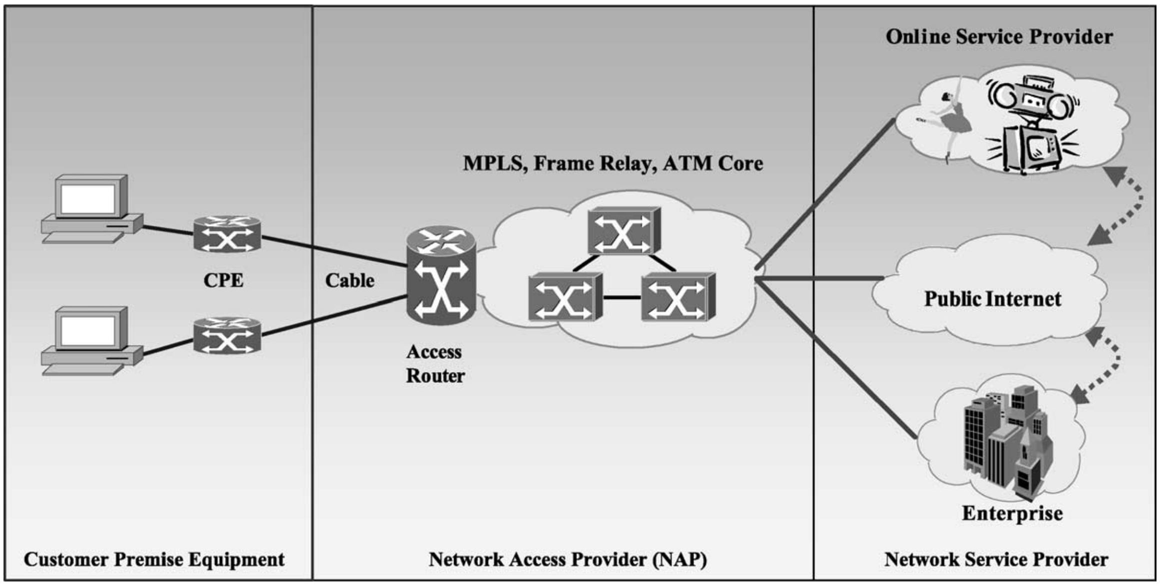

Fig. 3. Cable Access Architecture.

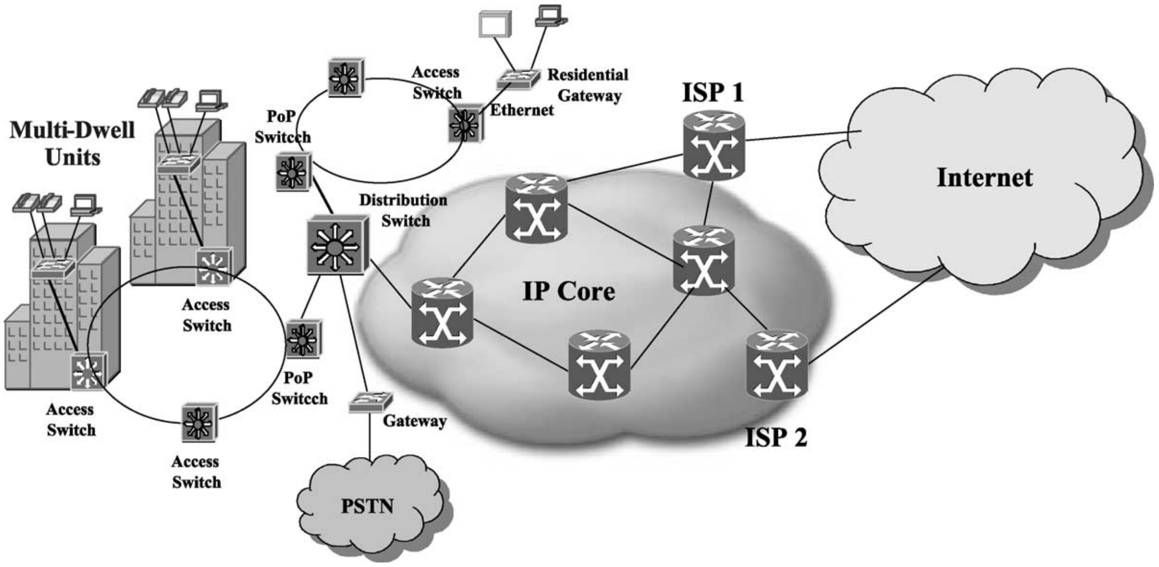

Fig. 4. ETTx Architecture.

the basement provides the aggregation for all the units in the apartment, and it pushes Layer 3 services to the network edge. The access switch is then connected to the fiber-based IP Core through the distribution switch.

With Layer 3 capability at the access edge, ETTx architecture facilitates IP service offering, enabling a wide range of value-added services. These include entertainment applications such as gaming and video-on-demand, information services such as remote training, e-learning, video conferencing and web-browsing, transactional services such as on-line commerce, online banking and online trading, and voice over IP based on the H.323 or other protocol. To support voice service, the residential gateway will provide the analog-to-IP conversion and the public-switched network gateway is needed to provided the IP packets-to-TDM digital signals conversion. With ETTx high 'last-mile' connection speed, broadcast-quality video streaming is made possible. The ability to distribute streaming video content and popular movies allow service providers to expand their service offerings and gain additional revenues, as well as adding more value to existing services to capture incremental revenue and reduce churn.

3. Integrated Network Management

The abbreviation FCAPS is often used in the literature to refer to the integrated management of various types of networks. It refers to the Open Systems Interconnection (OSI) five functional areas: fault management, configuration management, accounting management, performance management, and security management. Fig. 5 shows an overview of the Operation Support Systems / Network Management Systems (OSS/NMS) stand-alone functions based on the Tele-management Operation Map (TOM) [14] while Fig. 6 shows the OSS/NMS process. This section outlines the flows of the OSS/NMS functions, with emphasis on performance analysis, Quality of Service (QoS), Service Level Agreement (SLA) security management, and traffic engineering requirements.

3.1. Network Optimization and Capacity planning

Network optimization and capacity planning provides a long-term view of network demands and requirements. It computes network element growth rates, and generates a long-term capacity expansion plan. The network administrator who wants to do hypothetical (what-if) studies typically carries out the capacity planning function to determine the required capacity as well as optimal equipment locations (or homing arrangements) based on forecasted or expected demands.

In general, network optimization problem can be formalized as a non-linear programming with an objective to minimize the cost of adding resources (e.g. DSLAMS, transmission capacity) to the network and the overall constraints (e.g. end-to-end packet lost and delay) being satisfied.

3.2. Performance Data Collection

Once the network is in place, the Data Collection function collects and forwards data on a regular basis to the appropriate module. For instance, alarms and related fault statistics data is forwarded to the fault module to provide comprehensive diagnosis capabilities including alarm correlation and pinpointing. Traffic statistics data is typically forwarded to the performance module for data analysis and detection of potential performance exceptions (based on the collected and trending data). Traffic statistics as well as network topology data may also be forwarded to the planning module to estimate the base exogenous traffic

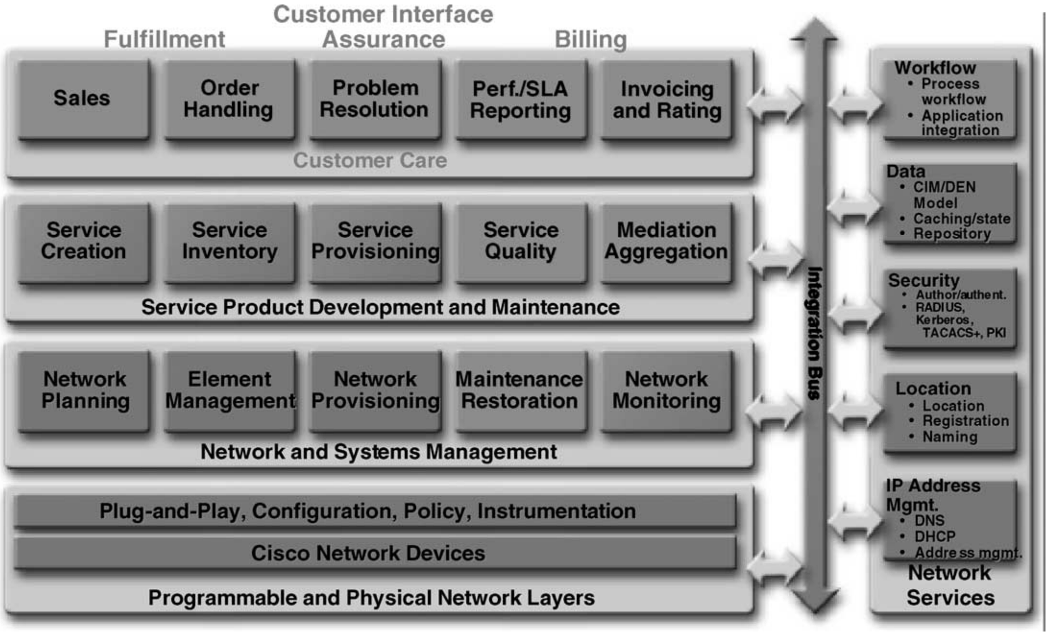

Fig. 5. Overview of NMS/OSS Requirements.

load [13]. Estimated growth factors can then be used to estimate the future forecasting traffic loads. Finally, traffic statistics can also be used as the basis to observe traffic trends and estimate the load for use in network engineering. It should be noted that the data collection functionality has been implemented in several element management systems especially for IP networks.

3.3. Performances Management

Performance Management is the process of converting raw traffic measurements into meaningful performance measures. It can be divided into real-time (or near-real-time/short-term) and long-term management. Real-time performance management typically includes snapshots of the behavior of bottleneck network elements (such as backbone link elements that affect the operation of the entire network) as well as mission-critical applications. The real-time performance management process is a mechanism to guarantee that enough bandwidth is reserved for time-sensitive traffic while other applications that are sharing the same link get their fair share without interfering with the mission-critical traffic. Another example of real-time performance management is the constant monitoring of high-priority customers' services (such as

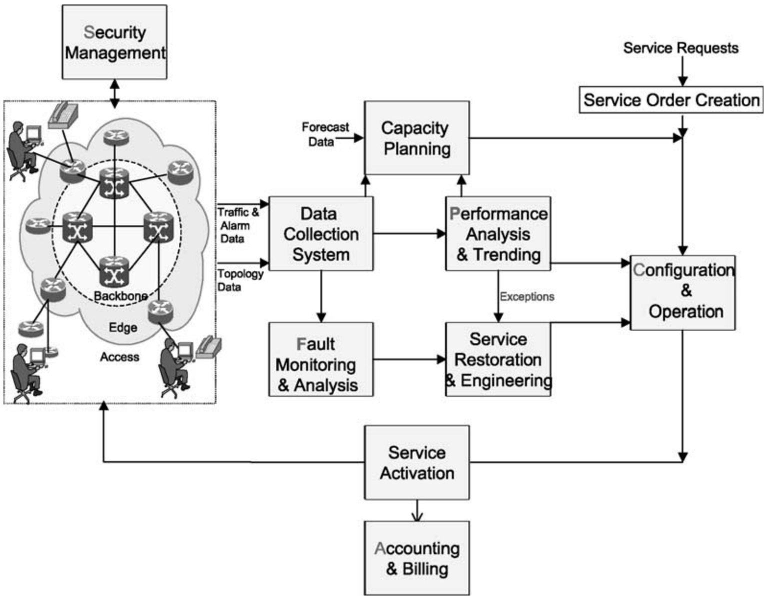

Fig. 6. Process Flow of Network Management Functions.

gold) as well as customers who have been complaining about the performance of their services.

Long-term performance management, on the other hand, supports studies that monitor the ability of the existing networks to meet service objectives. The purpose of this type of study is to identify situations where, corrective-planning action is necessary. This is needed when objectives are not being satisfied and, where possible, to provide early warning of potential service degradation so that corrective plan can be formulated before service is affected.

Typically, raw traffic measurements are collected, validated by data collection systems (or element management systems), and then stored in a database. One of the most critical steps in developing comprehensive management methods is to identify the required measurements as they provide the basis for:

- Performance monitoring—it helps network planners or engineers identifying faults in the network. This can be called fault performance that include threshold crossing alerts, transmission errors, etc.
- Performance quality assurance—it helps to determine whether or not SLAs are met by monitoring the QoS performance.
- Performance control—an example of this can be traffic shaping algorithms that actually change the network behavior to achieve a performance target.
- Traffic performance—it includes traffic engineering and planning.

Examples of IP performance raw traffic measurements include:

- Number of packets received per interface,
- Number of packets transmitted per interface,
- Number of packets dropped due to mild congestion[1] per interface,
- Number of packets dropped due to severe congestion per interface,
- Number of packets dropped due to protocol errors,
- Amount of time a network element is in a mild congestion state,
- Amount of time a network element is in a severe congestion state,
- Number of times a network element enters a mild congestion state, and
- Number of times a network element enters a severe congestion state.

For the OC3 interface of the IP DSL switch, some examples of the performance raw traffic measurements include:

- Errored seconds,
- Severely errored seconds,
- Code violation seconds.

For the ATM interface of the IP DSL switch, some examples of traffic measurements include[2]:

- Number of ingress cell count,
- Number of egress cell count,
- Number of ingress/egress CLP $= 0$ cell count,
- Number of cell dropped due to congestion,
- Number of cell dropped due to HEC violation, and
- Number of cell dropped due to protocol error.

For the DS3 interface of the IP DSL switch, some examples of the performance raw traffic measurements include:

- P-bit errored seconds,
- P-bit severely errored seconds,
- Unavailable seconds,
- Line coding violation seconds, and
- C-bit coding violation seconds.

The performance management process then converts the validated raw measurements into meaningful network element loads (utilization, packet loss ratio, delay, jitter, and so on). Next, it calculates statistics to characterize the *load* for traffic engineering purposes (such as average peak values and/or average busy season). The process then computes network element performance measures (route delay, end-to-end packet loss, average and peak packet loss, and so on) based on the characteristic engineering loads. Finally, the performance management process compares the calculated performance results, short and long-terms, with the service objectives to identify service or performance exceptions.

3.4. Fault Management

The Fault management process is similar to the real-time performance process except that it uses the collected alarms and fault statistics to detect and correct problems by pinpointing and correlating faults through the system. It simplifies the service provider's ability to monitor customer services by providing status of the subscribed services. The ability to monitor a service inherently includes all the network elements that comprise a service. Examples of fault data for DSL lines include:

- Loss of Frame seconds since last reset,
- Loss of Signal seconds since last reset,

[1] Mild and severe congestion states are typically defined by the network administrator per service. For instance, the thresholds for gold IP services should be lower than bronze and silver services so that network operators have more time to react to any potential problems before gold services are affected.

[2] The backbone of the DSL access network is mainly ATM based. IP service in most cases are carried over ATM.

- Loss of Power seconds since last reset,
- Errored Seconds since last reset,
- Number of initializations attempts since last reset,
- Received data blocks since last reset,
- Transmitted data blocks since last reset,
- Corrected data blocks (data blocks with error but corrected) since last reset,
- Uncorrected data blocks (data blocks with uncorrectable errors) since last reset,
- Number of previous intervals with valid data since last reset, and
- Number of previous intervals with no valid data since last reset.

3.5. Service Level Agreement

Service Level Agreement (SLA) reports are intended to correlate fault and performance data and then provide end users and network operators the freedom to establish quality and grade of service objectives that are specific to their applications. SLA reports are intended to be tailored to a specific customer or organization. Examples of IP SLA metrics include:

- Service Availability: the percentage of time each polled element was active and running,
- Network Latency: the elapsed time between receipt of last bit in a frame at network ingress to delivery of first bit in same frame at network egress,
- Jitter: the variation in network latency,
- Response Time: measures how quickly the network moves information,
- Loss Ratio: percentage of sent frames discarded or not received,
- Mean Time To Repair: average down time (from when an outage is detected until it is reported fixed),
- Mean Time Between Failure: the average down time between consecutive failures,
- Throughput: the total traffic volume (usually, in bits per second), and
- Network Uptime: the percent of time the network is operating without a 'hard' failure, usually better than 99.9 + percent.

3.6. Traffic Engineering

Traffic Engineering is perhaps the most challenging function of the management process for IP networks. It represents the action that the network (or network administrator) should consider in order to relief a potential servicing problem before the service is affected. This may include re-homing, re-routing, load balancing, and congestion control. Traffic engineering is also an essential input for capacity expansion[3], network dimensioning, and network planning.

The development of appropriate models for traffic engineering depends primarily on a clear understanding of quality and grade of service requirements and the statistical characteristics of the traffic. While there are more than a hundred years of experience in traffic engineering circuit-switched networks, engineering IP-based networks is new. Traffic engineering functionality has been added through the use of tunneling mechanisms or forced route algorithms.

Several traffic models and network dimensioning methods for packet networks have been proposed in the literature [3,7,10,11,13]. In general, the models can be divided into two categories: models that exhibit long range dependency (such as the fractional Brownian motion model, on/off model with heavy-tailed distributions for the on/off duration, and M/Pareto/∞ models) and Markovian models that exhibit only short-range dependence (such as on/off models with exponential on/off distributions, Markov-modulated Poisson process, and Gaussian auto-regressive models, which typically have exponentially decaying correlation functions). The on/off model has been proposed to model voice over IP calls with an alternating of active periods (talk spurts) and silent periods. The parameters of the on-off models can be estimated from actual traffic traces or by using typical default values. More traffic modeling details and simulation data will be discussed in Section 4.1.

Finally, traffic-engineering methods depend on the function of the network element. For instance, traffic techniques for IP edge routers include packet classification, admission control, and configuration management whereas congestion management and congestion avoidance are typical considerations of backbone routers or switches.

3.7. Configuration Management

Configuration management deals with the physical and geographical interconnections of various IP network elements such as routers, switches, multiplexers, and links. It includes the procedure for initializing, operating, setting, and modifying the set of parameters that control the day-to-day operation of the networks. Configuration management also deals with service provisioning, user profile management, and collection of operational data, which is the basis for recognizing changes in the state of the network.

The main functions of configuration management are creation, deletion, and modification of network elements and network resources. These include the action of setting up an IP network or extending an already existing network, setting various parameters, defining threshold values, allocating names to managed IP objects, and taking out an existing network elements.

"Another important function of configuration and provisioning management is the synchronization between the OSS/NMS systems of the various network management layes (NMLs). For instance, some service providers prefer

[3] Capacity expansion typically is an optimization process that involves a set of algorithms that determine the required network resources (capacity) to meet a specific set of performance objectives.

to have the network element (i.e routers, switches) as the master of the configuration data. In this case, the database of the NML systems (e.g. EMS, Inventory management system, provisioning management system, etc.) must synch up with the network element by obtaining regular updates (e.g. every some time interval or very time a change has been saved) or by discovering the changes of the network every so often. Other carriers prefer to have the OSS/NMS as the master of the data given that the physical network element may exhibit christophic failure where all the provisioned data is obliterated. In such case, the network element can be simply replaced quickly where the latest saved configuration data is downloaded form a OSS/NMS system. The shortcoming, however; is that all changes to the network element itself must be entered manually (or via synch up again) into the OSS/NMS systems."

3.8. Security Management

The flexibility of IP broadband access networks, especially ETTx, introduces new challenges to hardware vendors as well as service providers. The most important challenge is perhaps the network and service security. Business and residential customers are reluctant to subscribe to these services unless the service providers can prevent malicious users from spoofing their IP addresses and 'tapping' into their communications. The first issue is commonly known as IP spoofing and the latter is referred to as default gateway spoofing. In addition, many local government agencies require service providers to implement strict security and traceability techniques to monitor subscribers (which user has which IP address) at all time. Service providers are extremely concerned about the network security and subscriber privacy.

Secure Address Resolution Protocol (ARP) Discovery (SAD) is proposed to address both IP spoofing and default gateway spoofing [15]. SAD uses an ARP Access Control List (ACL) to restrict ARP request access. However, this requires that all Layer 3 switched to support this feature. An alternative solution is to use OSS/NMS to prevent IP spoofing.

The OSS/NMS can prevent the IP spoofing by building a binding relationship between the MAC address (Ethernet address) and the IP address and put it in the static ARP table in the first layer of Layer 3 switch. This assumes that the Layer 3 access switches support DHCP Option 82 so that a one-to-one relationship with the port, IP and MAC address can be built. In addition, Option 82 is also required to monitor traffic flow / usage of specific subscribers which may be required for security tracing and usage-based billing. For instance, Cisco NetFlow Collector can monitor traffic flows on particular ports and then Option 82 can be used to identify the port user/subscriber.

Security management also includes authorization and other essential secure communications issues. Authorization establishes what a user is allowed to do once the user is identified. Authorization usually follows any authentication procedures. Issues related to authentication and authorization include the robustness of the methods used in verifying an entity's identity, the establishment of trusted domains to define authorization boundaries, and the requirements of uniqueness in namespace.

3.9. Billing and Accounting Management

Billing and accounting management deals with the generation and processing functions of end-user usage information. This includes measuring the subscribers (and possibly the network resources for auditing purposes) and managing calls detail information generated during the associated call processing. Of growing importance in IP networks are the records created in the application servers. Such records are the source of content and services delivered by the network. Billing data collection and mediation systems between the IP architecture and the extant billing platforms may aggregate usage-related raw data and produce usage detail records. The access usage detail data can then be transferred to a billing system to render invoices to the subscribers that use IP services. Fraud detection and subscriber-related profile information, such as authorization to charge, is also a function of accounting and billing management.

Several billing approaches have been considered for IP networks ranging from flat-rate, such as the voice-world Call Detailed Record (CDR) approach, to a full IP-usage based. A known working IP-usage approach is to integrate the IP rated records with existing telephony customer care

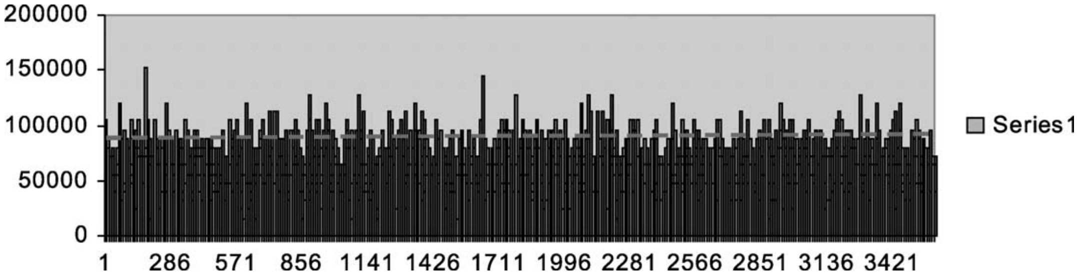

Fig. 7. Observed bit rate in a link carrying voice traffic.

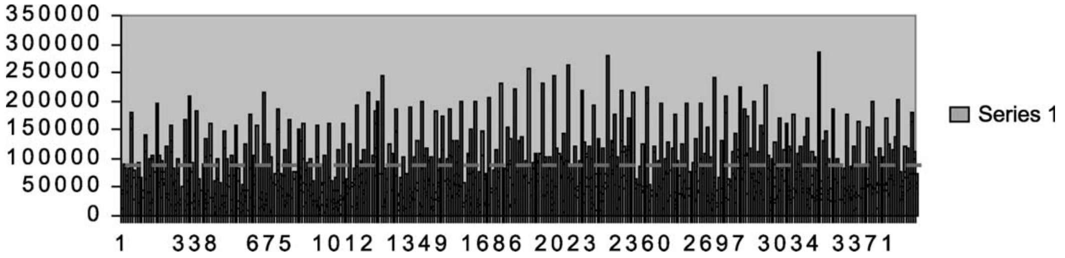

Fig. 8. Observed bit rate in a link carrying IP traffic.

and billing systems. Such arrangements exists and are fully functional in the both the US and Europe.

Another important requirement for IP billing and accounting functions is an interface to the SLA profiles and the resulting performance and fault reports. This includes the generation of automatic credits for customers that their SLA agreements were validated.

4. Traffic Modeling and Network Dimensioning

Traffic measurements have shown that IP traffic is bursty over a wide range of time scales [5,12]. Figs. 7 and 8 show typical normalized utilization of a T1 link carrying voice traffic and IP, respectively, over an observation period (in seconds). While both links have the same mean utilization, the variation of the IP traffic is much greater than that of the voice. Finding a simple network dimensioning model that accurately reflects the important characteristics of the traffic over the IP core is a very challenging research problem, e.g. [1,2,4,6,8] and [9]. Traffic modeling is not the focus of this paper, however, it is crucial in traffic prediction for traffic engineering and capacity planning. Some traffic models reported in the literature are reviewed. Then, an intelligent capacity allocation scheme is outlined and described.

4.1. Network Traffic Models

Poisson models have been used extensively to model the behavior of traffic carried by the telephone networks. Readers are referred to [2] for details on the Poisson modeling for network dimensioning.

The Markov-modulated Poisson Process (MMPP) [6] has been widely used to model various B-ISDN sources, such as voice and video, as well as to characterize the superposed traffic. It has the property of capturing both the time-varying arrival rates and the correlations between the inter-arrival times.

The *on/off* model is often used to characterize Variable Bit Rate (VBR) traffic. In this model, traffic is alternating between *on* state and *off* state. Traffic is generated during the *on* period at a constant rate, whereas no traffic is generated during the *off* period. The lengths of both periods are independent and exponentially distributed. By knowing the mean of both *on* and *off* periods, different calculations can be obtained which are useful in traffic modeling. Typical VBR sources include video-conferencing and computer network applications.

Studies of Ethernet and WWW traffic patterns [12] have shown that considerable degree of correlation exists in the traffic bursts in such streams. To capture the long-term dependency, or the self-similarity nature, the Fractional Brownian Motion (FBM) has been proposed as a convenient mathematical representation. It accounts for the observed peakedness as well as the long auto-correlation of the traffic. FBM model can be described by three parameters (m, a, H), where m stands of the mean rate, a for the peakedness, and H for the Hurst parameter, which is a dimensionless measure of the persistency of the correlation in data rate, $0.5 \le H < 1$.

If the traffic is exactly self-similar, the bounds on the queue length distribution can be used in buffer sizing [8]. In such an analysis, we are effectively using the queue length distribution of an infinite buffer system as the storage for the variation in packet loss probability with finite buffer size. The cell probability with a buffer size of B is approximated by the probability that the queue length exceeds B in an infinite buffer system:

$$P(V > B) = \mathrm{e}^{-cB^{2-2H}}$$

$$c = c(\rho) = \text{const.}\ \rho^{\frac{1}{2H-1}}(1-\rho)^{\frac{-H}{H-\frac{1}{2}}}$$

where, ρ is the channel utilization, a is the variance of the FBM process, and H is the Hurst parameter.

Besides the FBM process, *on/off* model with on and off periods exhibiting heavy tail is another convenient way to represent self-similar traffic. A heavy-tailed distribution of the *on* period can be justified by the transmission of extremely long files occasionally by a source. A heavy-tailed *off* period is related to human behavior. An *on/off* model with on and off periods being independent and Pareto distributed, is often used to model self-similar traffic. The probability density function of the Pareto distribution is

$$f(x) = \beta\alpha^{\beta}x^{-\beta-1}, \qquad \alpha, \beta x \ge 0, \qquad x \ge \alpha,$$

and the cumulative distribution function

$$F(x) = 1 - (\alpha/x)^{\beta},$$

where, β is the shape parameter. If $\beta \le 2$, the distribution has an infinite variance, and if $\beta \le 1$, it has infinite mean

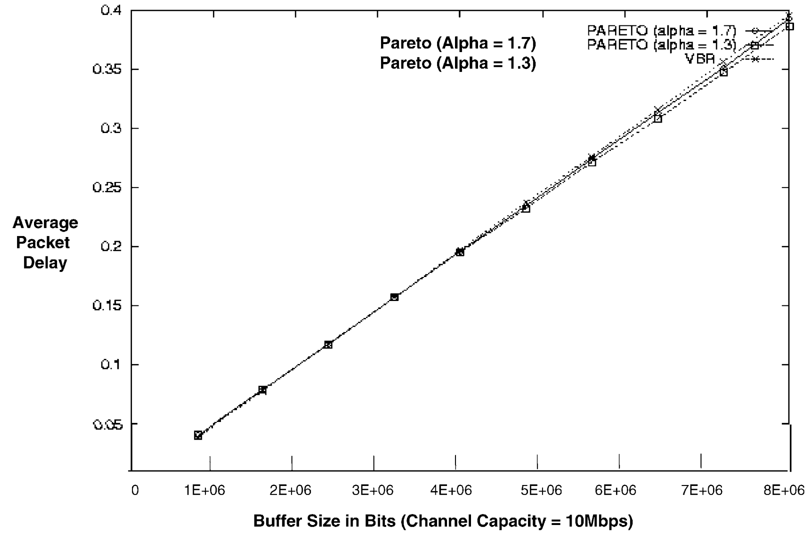

Fig. 9. Average packet delay as a function of buffer size for Pareto ($\alpha = 1.3$, $\alpha = 1.7$) and VBR traffic.

and α is the location parameter, computed in terms of the Hurst parameter of the FBM process. In particular, $H = (3 - \alpha)/2$

Fig. 9 shows a plot of the required buffer size to achieve a given average packet delay objective for two different Pareto traffic sources with different values of α *(*$\alpha = 1.7$ and $\alpha = 1.3$*)* and one VBR traffic source. Note that as α decreases, the average delay of the Pareto traffic source slightly increases, approaching that of the VBR. Note that $1 < \alpha \leq 2$.

Fig. 10 shows a plot of the required buffer size to achieve a given packet loss objective for two different Pareto traffic sources with different α*(*$\alpha = 1.7$ and $\alpha = 1.3$*)* parameters and one VBR traffic source. Note that as the α parameter increases, the packet loss probability of the Pareto traffic slightly decreases, approaching that of the VBR. One of our current research focuses is to investigate on the behavior of the Pareto when α*?* is varied. The goal is to determine the condition when the on/off exponential traffic behavior can be used to approximate accurately the on/off Pareto behavior, so as to avoid the computation of the Hurst parameter H (a complex variable to approximate).

4.2. An Intelligent Capacity Allocation Algorithm

The Intelligent Capacity Allocation Algorithm is shown in Fig. 11. It is self-adaptive and uses statistical predictions, self-corrections, and heuristics to choose the best capacity allocation and adapt the parameters for the next computation. The algorithm has three major sections.

Traffic Analysis and Prediction analyzes the traffic and estimates the parameters of the expected traffic flow. It is composed of three modules, the Traffic Parameters Analysis

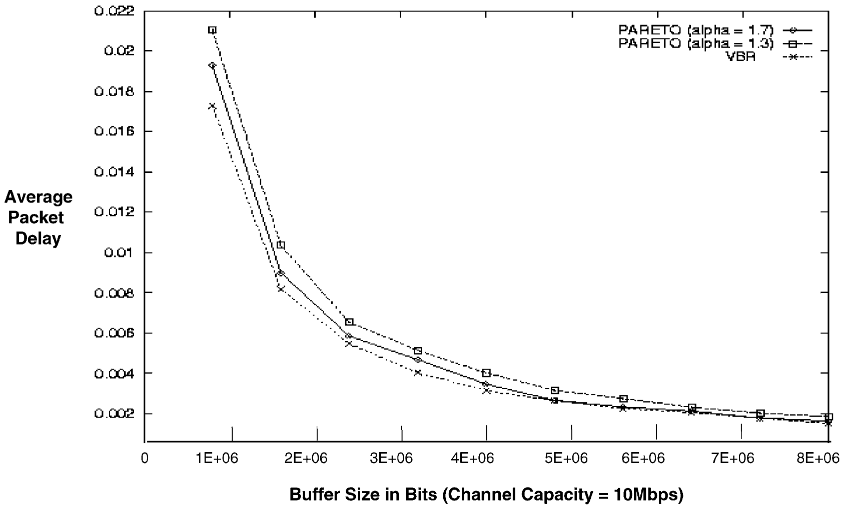

Fig. 10. Packet loss probability as a function of buffer size for Pareto ($\alpha = 1.3$, $\alpha = 1.7$)? and VBR traffic.

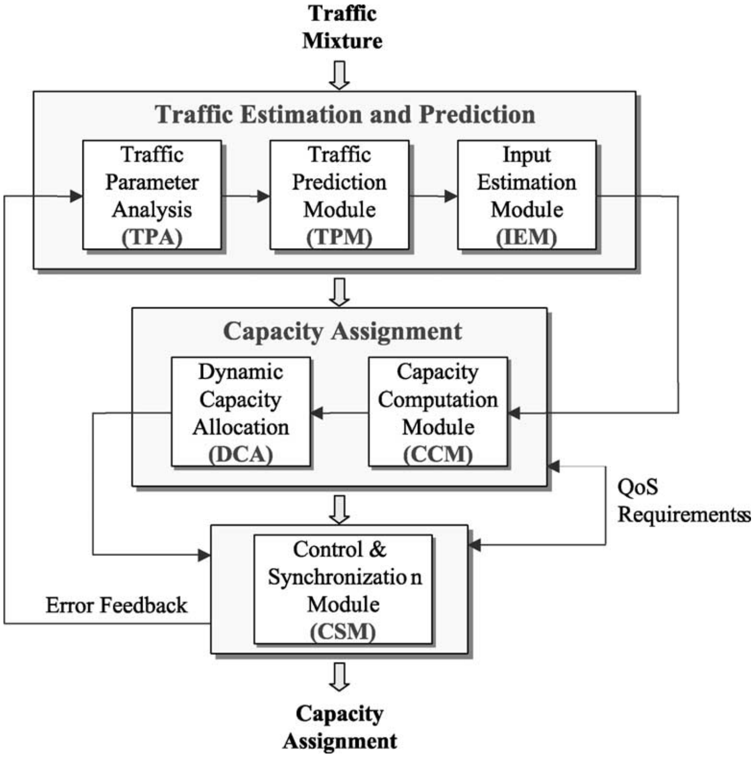
Traffic
Mixture
Traffic Estimation and Prediction
Traffic Parameter Analysis (TPA)
Traffic Prediction Module (TPM)
Input Estimation Module (IEM)
Capacity Assignment
Dynamic Capacity Allocation (DCA)
Capacity Computation Module (CCM)
QoS Requirementss
Control & Synchronizatio n Module (CSM)
Error Feedback
Capacity
Assignment

Fig. 11. Intelligent Capacity Allocation Algorithm.

Module (TPA), the Traffic Prediction Module (TPM), and the Input Estimation Module.

Capacity Assignment computes the required capacity for the expected traffic flow according to different models and assigns the appropriate value. It is composed of two modules: the Capacity Computation Module (CCM) and the Dynamic Capacity Allocation (DCA).

Control and Synchronization synchronizes between the two previous sections and handles the error estimation.

Each section contains a set of modules that perform independent tasks.

Traffic Parameters Analysis Module (TPA) observes the input traffic in the specified period of time that is assigned by the Global Control Module. These parameters should be enough to completely describe all of the characteristics of the input traffic. The required parameters are:

1. The mean bit rate.
2. The variance of the bit rate.
3. The peak bit rate.
4. The mean burst length.
5. The variance of the burst length.
6. After computing the input parameters, TPA provides them to the TPM.

Traffic Prediction Module (TPM) predicts the future traffic characteristics. It takes as input the traffic parameters from the TPM and the error feedback from the Global Control Module (GCM) and produces an estimation of the predicted traffic parameters. The conventional approaches for the prediction are either based on Time Series models (Kalman filter, double exponential model, etc.) or Artificial Neural Networks (ANNs). Because of the complex behavior of the traffic, we believe that the ANNs are more accurate in the prediction of the data traffic than other methods. The result of TPM is then transmitted to the Input Estimation Module (IEM). The IEM then prepares the parameters that will be used in the computation of the capacity allocation for the next interval of time, and to the Global Control Module (GCM), which constitutes the central system of the algorithm.

Input Estimation Module (IEM) prepares a set of parameters for the computation of the capacity by each capacity allocation model according to the predicted parameters provided by TPM. All the parameters are specified in the relative sections describing the capacity models. The IEM transmit its output to the Capacity Computation Module.

Capacity Computation Module (CCM) computes from the parameters delivered by the IEM, three different required capacity allocations (FBM, Gaussian, SEHMM) according to the assigned Quality of service. The CCM delivers the three computed capacities to the Dynamic Capacity Allocation Module (DCA).

Dynamic Capacity Allocation (DCA) chooses the appropriate capacity allocation according to a heuristic built on the notion of *labeling graphs*. A labeling graph is a decision tree that strengthens the decision of the chosen capacity algorithm each time that decision is made. The constraints of the algorithm are the buffer size variation and the predicted traffic load.

Global Control Module (GCM) coordinates the functionalities of TPM and the DCA. This module compares the required and the observed QoS. The result is then used to adjust the DCA heuristic. It also compares the last traffic prediction parameters and the new observed ones. The error is then fed back to TPM to adjust the results of the new iteration accordingly.

The unique feature of the Intelligent Capacity Allocation Algorithm lies in the fact that more than one traffic model is taken into consideration for faster convergence to a good approximation of the capacity and to adapt the appropriate model to each particular traffic pattern.

5. Conclusions

This paper described architectures and OSS/NMS for IP-based broadband networks including ETTx, wireless, IP DSL, and cable. The OSS/NMS functions included fault management, configuration management, accounting management, performance management, and security management. Traffic engineering algorithms and models to simulate different types of IP traffic are then introduced. The simulation model accepts a multiplexed traffic stream of these sources as input and computes the needed equivalent capacity to achieve specific QoS objectives. Results of the model show that the multiplexed traffic patterns provide results as predicted. Finally, the paper described a self-adaptive Intelligent Capacity Allocation algorithm. Further research is still required to define each function of the capacity allocation algorithm.

References

[1] D. E. McDysan, D. L. Sophn, ATM: Theory and Application, McGraw-Hill, New York, 1994.

[2] A.K. Erlang, Solution of some problems in the theory of probabilities of significance in automatic telephone exchanges, Elktroteknikeren 13 (1917) 5–13.

[3] P. Karlson, A. Arvidsson, Modelling of Traffic with High Variability Over Long Time Scales with MMPPs, Dept. of Telecommunications and Mathematics, University of Karskrona/Ronneby, Sweden.

[4] K.R. Kishnan, A.L. Neidhart, Queuing Performance of Bottlenecks in IP Networks Carrying Only Voice, Bellcore Report May (1995).

[5] W.E. Leland, M.S. Taqqu, W. Willinger, D.V. Wilson, On the Self-similar Nature of Ethernet Traffic (Extended Version), IEEE/ACM Transactions on Networking 2 (1994) 1.

[6] K.S. Meier-Hellstren, W. Fisher, The Markov-Modulated Poisson Process (MMPP) Cookbook, Performance Evaluation 18 (1992) 149–171.

[7] N. Fonseca, M. Zukerman, ATM Dimensioning and Traffic Management and Modeling, Proceedings of the IEEE Globecom'97, 1997.

[8] Norros, A Storage Model with Self-similar Input, Queueing Systems 16 (1994) 387–396.

[9] R.O. Onvural, Asynchronous Transfer Mode Networks: Performance Issues, second ed., Artech House, Inc, 1995.

[10] S. Robert, J.-Y. Le Boudec, A modulated Markov Model for Self-similar Traffic, Internationales Begegnungs und Forschungszentrum für Informatik, Schlob Dagsthul, Saarbrücken, Germany, 24–29 September, 1995.

[11] S. Vaton, Modélisation Statistique de Trafic sur Réseau Local: Application au Contrôle Dynamique de Bande Passante, PhD Thesis, Ecole Nationale Supérieure des Télécommunications (ENST), December 1998, France.

[12] Walter Willinger, Murad Taqqu, Robert Sherman, Daniel Wilson, Self-similarity through high-variability: statistical analysis of ethernet lan traffic at the source level, IEEE/ACM Transactions on Networking 5 (1997) 1.

[13] Ammar Rayes, Integrated management architecture for IP-based networks, IEEE Communications Magazine April (2000).

[14] Telemanagement Forum, http://www.tmforum.com/.

[15] Marco Foschiano and Christophe Paggen, Secure ARP Discovery (SAD) 1.0, Cisco Systems, 2001.