A Multiservice Architecture for Dynamic Bandwidth Allocation and Traffic Engineering Applications

Y. L. Takahashi-Iturriaga, J. Martínez, V. Alarcón
Departamento de Ingeniería Electrónica
Universidad de las Américas – Puebla
Ex-Hacienda Santa Catarina Mártir
San Andrés Cholula, Puebla. México 72820
e-mail: uc@mail.udlap.mx

Abstract

The primary goal of this paper is to analyze bandwidth control techniques in order to propose an architecture to improve bandwidth usage. Network architecture employs several techniques in order to manage, predict and handle traffic issues due to Ethernet's best effort delivery system. Bandwidth allocation, traffic engineering and a post analysis resulting architecture are presented in that order. Ethernet's resources are dissected in order to study each component separately and present a traffic-effective architecture at each hierarchical level. The analysis reported in this paper indicate that by improving each topology hierarchical level, network performance is increased globally.

1. Introduction

A Multiservice IP Network brings the advantage of a Quality of Service (QoS) approach managing several real time applications such as VoIP – Voice over IP – , Video and critical Data, and a technology, based on the current infrastructure. The Multiservice network can be used on every network. Although IP is a connectionless protocol it can still be allocated over an ATM – Asynchronous Transfer Mode – network in order to provide a better performance and a variety of protocols outside and within the CPE – Customer Premises Equipment –. This paper proposes a network architecture involving some components that can be found on every network, such as Carriers – telecommunications providers – management, services and customer applications, which are hosted in a remote terminal and is used to connect via the Access Tunnel to the Corporate Network. Controversy has arisen over information management, due to both variable packet length and header length such as IP. Most ATM networks use the AAL5 Layer (ATM Adaptation Layer Type 5, recommended for LAN Emulation) and add only 8 header bytes on every packet, so if another protocol is being taken from source to destination, another 8 bytes are added on a VCC (Virtual Channel Conection). AAL5 can handle up to 18 header bytes.

Multiprotocol carrying hurts network performance due to AAL restriction of building 5 bytes header length and 48-load long packets. TCP/IP represents a 40% or 50% on modern networks' traffic, where most packets use Ethernet's MTU – 1.500 bytes – as a length reference [1], [2]. In order to improve network's performance, efficient data transportation, measure management, buffer management and traffic engineering must be watched closely. The rest of the paper is organized as follows. Section 2 comprehends a brief description of Data Management. Section 3 presents the proposed architecture, its characteristics and recommendations. Section 4 describes the recommended applications to be used on the proposed architecture, and Section 5 presents the conclusions of this paper.

2. Data management and transportation

While using ATM, the header can be suppressed since the packet is already working on a connection-oriented technology. ATM supports QoS, therefore, there is no need to use sequence numbers or time tagging; destination always receives cells in the correct order.

QoS is very helpful when voice or video must be transported; ATM gives two options to do so; AAL1 and AAL2 [1]. IP and Frame Relay, on the other hand, support several encoding techniques, and due to this variety of options, packets lengths vary from one to another. Besides length, IP Networks running over ATM should be aware of different traffic types. There are two types of traffic; deterministic and random traffic. The first model has a tight control over the time and how a packet was delivered, but there is a lot of administration work to be done in order to model both, source and destination. Random traffic, on the other hand, uses statistics on how both source and destination behave [3].

Bursty traffic is generated when a source station generates inconsistent traffic, resulting into traffic burstiness. Traffic burstiness is expressed as follows [1], [3]:

$$burstiness = \frac{peakrate}{averagerate} \qquad (1)$$

Source Activity Probability, SAC is given by [3]:

$$SAC = \frac{1}{burstiness} = \frac{averagerate}{peakrate} \qquad (2)$$

These formulas can be used in order to predict a LAN behaviour (e.g. WAN burstiness is close to 1) while dial-up burstiness varies depending on the application in process.

2.1 Traffic parameters

Some variables define traffic behaviour; such variables are called traffic parameters. Resource Reservation Protocol – RSVP – uses the Token Bucket Algorithm – TBA – to discover specific flow parameters. TBA verifies two parameters; average rate in datagrams per second (r) and deposit depth. RSVP adds three more parameters to the TBA, Political Minimal Unit (m), Packet Maximum Size (M) and Peak Speed (p), where m and M involve application information and all headers from layer 3 up [1], [7].

ATM parameters are fixed upon a contract between user and network therefore QoS can be assured. PCR (Peak Cell Rate) and CDVT (Cell Delay Variation) are considered in this contract. PCR is reversely proportional to the time interval between cells, while CDVT is specified as a function of the number of cells transmitted. The Maximum number of consecutive cells – MBS – is the number of cells that can be sent at peak rate and is defined in terms of "Burst tolerance". Traffic shaping assures that an ATM cell flow is constant, in order to avoid cell elimination. Every cell must be checked, and does not pass directly through deposits.

2.2. Measure and Prediction

Measuring a network performance is complicated; the network must be up functioning in order to make tests; the advantage is that every little detail is being analyzed; therefore the network is monitored and measured instantly. Predictive analysis involves simulation, and its costs. Queuing is used when there are not enough resources to be shared at the network. In ATM networks this contention takes place between connections, which are current, and also the ones to be accepted [4]. This method allows a device to form a queue in order to process and dispatch cells considering well established criteria, such as cell priority, length and so forth. Queuing is described depending on the arriving pattern, number of service channels and system's capabilities. Systems may have deterministic arrivals, in which events can happen at defined amounts of time, or may have stochastic arrivals, where events are random, and arrivals should be considered in groups, not individually, one should consider that the length of each group is variable [1], [2].

3. Proposed Multiservice Architecture

Architecture should always be deployed as in a three level hierarchical topology – Backbone, Service Access and Network Access – so that the network may offer scalability, easy management and high efficiency. This Multiservice network allows traffic using several different protocols to flow in the same network. The result is a direct connection to customers, providers, and partners through a Corporate Network strong enough to hold every little piece together, including remote mobile users. A network example using this topology is presented in Figure 1.

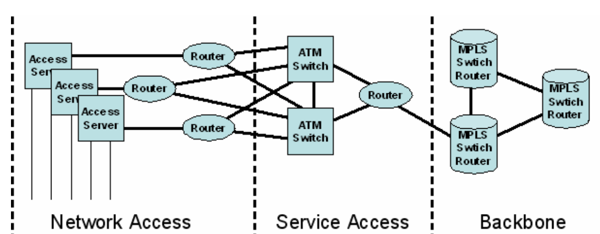

Figure 1. Hierarchical Network

The user-generated traffic is classified according to the associated QoS to the application. Traffic should be prioritized and modeled in order to organize queues on the inbound switch interface. A Multiservice architecture offers privacy based on the Multi Protocol Label Switching tag, scalability in order to provide service to different locations and users and flexibility to add new network branches, the use of different media, and bandwidth increments.

3.1. Backbone

The Backbone is responsible for a differentiated transportation of the customer's information throughout the network. At this level, no packet analysis is made whatsoever, due to other priorities such as bandwidth efficient utilization and fast traffic switching. Among the main activities that should be performed by the backbone are path capabilities improvement, congestion control, load balancing and the use of alternative routes. Packet switching must be done as fast as possible. This layer is to be considered a WAN deployment layer; therefore traffic analysis should be made at Service Acces or Network Access layers.

3.2. Service Access

Distribution layers should assure access between users and the backbone; it must support multiprotocol switching and is responsible for Transport Protocol. Services classification should take place in this layer as well as the network security politics defined to end user. Most of the functional processes occur at this layer. All devices placed at this layer are responsible for VPN (Virtual Private Network) establishment as well as users generated packets routing. Layer three routing protocols are used at this topology layer also. CAR – Commited Access Rate - is requested, handling bandwidth, expected burstiness and maximum burstiness. When packets arrive from CPE (Customer Premises Equipment) priority is assigned to each one and from this point on is handled based on this priority. Extended lists verify if these packets comply with the parameters set by CAR, if the bandwidth and TCP or UDP comply, then packets are prioritized, otherwise are discarded or considered best effort packets.

3.3. Network Access

This layer includes all the CPEs and is responsible to connect the client internal network with the network, or a VPN. Standard protocols should be used at this level; no special configuration is required in order to implement a VPN. Network privacy over the PSTN (Public Switched Telephone Network) is achieved by placing a point-to-point connection on the same network, therefore VPNs are isolated and there is no need for tunneling and encryption. Markov chains congestion control method fits exactly traffic management requierements at this level.

3.4. Bandwidth Calculation.

Last-mile bandwidth is calculated by considering all applications bandwidth requirements, and is expressed as follows:

$$TBW = \sum_{i=1}^{n} ABW_i \qquad (3)$$

TBW is the total bandwidth required in the last mile, while ABW is the bandwidth used by every application, where *i* is the number of applications in the last-mile link and *n* determines the maximum number of such applications. An usage factor for each application should be considered in the calculation of each application bandwidth. Load balance is a must between links, and the maximum number of E1 links is up to 6, after which a E3 should be considered. In the United States dedicated links at 1.544 Mbps are called T1s, while in Mexico and Europe the rate used is 64Kbps for a DC0, and 2.048 Mbps for E1s, other rates are available for commercial use, but availability depends on your local Carrier.

4. Recommended applications for the proposed architecture

In order to assure QoS, an IP Network should be able to anticipate traffic demands, stability and service. So, in order to predict the impact on the demands of the resources a record should be kept. There are two ways to do so: Hard State in which connection oriented technologies save information for every connection that is made, and is deleted when is no longer necessary. The Soft State, as in RSVP, information flow is only valid through a pre-defined period of time, after which the information must be refreshed or deleted [5]. Both ways have to deal with scalability issues, since behaviour is related to every network user. Using the ATM's VPs, IP packets are classified in order to transport them along the network. Packet arrival can be represented as a Poisson distribution, where many packets from many sources arrive simultaneously to one port, then inbound and outbound speeds should be considered within the analysis, otherwise the Poisson distribution is invalid. In order to analyze packet flow, sources should be taken as only one source. There is a phenomenon called Self Similar Traffic, where similarities and Long-Range Dependence – LRD –are present in a large variety of traffic types, these similarities are presented on various technologies as well [1], [4].

4.1. Buffer Management

When using FIFO – "First In-First Out" – there is no priority control, and if a packet arrives when the buffer is full it is discarded. On ATM QoS enables priority point to point. There is another method called RED (Random Early Detection), which anticipates congestion by discarding packets using probability, it has no priority control whatsoever, while ATM, on the other hand, has two levels of priority, and to do so uses PBS (Partial Buffer Sharing). Another way to help avoid congestion is to divide the buffer in equal virtual partitions and distributes them among the sources, then RED can be applied on every part of the divided buffer, and again, no priority is considered. On IPv4, the Type of Service (ToS) field can be used to determine packet priority; as for IPv6 there is a Priority field already in place and is used on priority queues, which may postpone low priority packets that result in data loss. ATM's traffic control reserves resources. WFQ – Weighted Fair Queuing – shares the buffer by considering different weight to every buffer partition. WFQ and queuing is a good approach to solve delays and flow loss, although data loss can still occur [2].

4.2. Analytic routing models.

While QoS seems to be efficient, it has faults on delay and data loss due to time restrictions. Therefore network monitoring and ports costs are a must. A network with an N number of nodes all of them fully interconnected results in a balanced network, for distance can be considered unitary to any node. Hierarchical networks have an average distance of three between nodes, but they are cost-efficient and easy to manage and modify. Tree hight (H) is the number of levels of ramifications, and the tree is considered complete only if each level has at least one node, which is, a full three grade hierarchical network which has N nodes, where N is:

$$N = \sum_{i=o}^{H} D^{i} = \frac{D^{H+1}-1}{D-1} \qquad (4)$$

IEEE's 802.1d Spanning Tree Protocol (STP) re-directs all traffic to the root – upper level – in order to be sent to its final destination, therefore the average distance increases due to traffic way through the root [1], [2], [5]

4.3. TE, Traffic Engineering

Multi Protocol Label Switching is designed to work on connectionless-oriented networks, and it's all it takes to get a nice TE and routing control on ATM networks. IP routing can be improved with PVCs and flooding technology put together. MPLS labels help ATM cells pass through switches, and allow the use of hierarchical groups' traffic. Within design processes, the more complicated the model is, the tougher the calculations get. While designing, costs must be considered along with performance and service quality as well as a detailed performance analysis. Network modeling involves growth analysis and escalability as well as fault-tolerant links and dynamic routing defining network performance. Capacity, efficiency, availability and error rate are considered the most important parameters to measure in order to model a network´s performance, and should be analyzed so that design turns out as the result of an exhaustive study, including traffic patterns, varieties and network behaviour. Design must be cost effective.

When traffic load is known, hierarchical routing improves costs between dedicated links, if traffic load is variable, or bursty should be used oher routing methods. Traffic patterns may differ, a static routing algorithm cannot adapt immmediatly to the fact that traffic loads may not have peak hours simultaneously. Dynamic Non Hierarchical Routing (DNHR) or Dynamic Controlled Routing, (DCR) both work on connectionless oriented networks where the load waiting time varies. MPLS can be used over Internet over an optimized multipath – OMP MPLS – approach, where packets are discarded randomly. Designing cost criteria is one the most important issues to consider because performance is directly affected with costs. Dynamic routing is considered an adaptive method with which service is assured; nonetheless it also represents bandwidth consumption when devices pass updates among themselves.

4.4. Dynamic Allocation.

Bandwidth can be negociated or shared in time divisions or among the numbers of applications. Dynamic allocation adjusts periodically, depending on the network's requierements; should bursty traffic occur, a time variation bandwidth requirement may happen.

Traffic models are of great relevance to QoS, and one issue is its own complexity of applications sharing one channel with traffic patterns that differ between applications. Traffic may have repetitive patterns in a wide time range; therefore an efficient approach comes when bursty traffic is described statistically with similarity. Self similar traffic is associated with those objects which whose appearance does not change despite of the scale they are working on, and are called fractals. Statistic models, like Markov Chains help reduce burstiness, but may still be a very important issue to take care of. A network based on fractal nature should involve different control methods. Self–similarity is very important when it comes to network performance, for example all web applications present similarities and are very important in order to determine the similarity phenomena on the network [4], [7].

These similarities within processes do not depend on the computer application, but on how traffic is managed within the network, and is an effective way to work with help traffic through bottlenecks and buffer capacity. Self similar traffic can hurt network performance, due to delays on queueing systems and cell loss, and but can be controlled with layer 3 and layer 4 protocols. Similar traffic dos not handle buffer congestion, therefore cell loss is decreased and traffic flow throughout devices is improved [4].

When bursty traffic does not vary in time, it implies that there are periods in which a great activity takes place and hurts congestion control, therefore a dynamic congestion control is a serious issue to consider. Dynamic control measures recent traffic and does not necessarily adapt to changes immediately, due to network conditions. Congestion avoidance design engineered to the last – considering variables such as buffer size – is difficult due to information traffic not behaving in a predictable fashion during periods of great traffic, when patterns can vary within days or even months and congestion occurs.

Packet loss and retransmisión rate decrease as traffic similarity increases within a reliable flow control method. The average time a queue lasts can help understand how much network control depends on similarity, and it occurs when a distribution has decreased in measures lower than those on Poisson distribution on the system. Increments on network resources such as bandwidth and buffer capacity result as a linear improvement in network performance. However, when buffer size is huge, delays on queueing systems are generated. Increasing the bandwidth – considering a buffer with great capacity – decreases the waiting time under similarity conditions, therefore E1s and other great bandwidth links can be used, to relieve cell loss and delays when time sensitive applications are on track.

The bigger the load is, the higher the similarity grade can become. Due to its bursty nature, cell loss and network delay are very common problems, especially on multimedia applications [4]. Dynamic BandWidth Allocation – DBWA – comes hand to hand with similar traffic, and each can be managed separately, in order to comply to networks needs and user requierements on how their traffic should be managed along the network. MPLS may be considered a powerful help when it comes to packet manage on WAN links.

5. Conclusions

Since a real time application uses most of the network's bandwidth and requires a high QoS level. This type of traffic should be compressed in an orderly fashion otherwise traffic may get bursty. Therefore in this paper a multiservice architecture for dynamic bandwidth allocation and traffic engineering applications has been proposed. Bit rate changes abruptly based on traffic priority. ATM networks may represent a great step forward, with services such as high speed, bandwidth on demand and high multiplexion capability. Statistic multiplexion improves bandwidth utilization and decreases burstiness and costs, yet traffic peaks may result in network congestion. Multiplexed information transmission, along with DBWA improves resources use. DBWA, is used to help time sensitive applications, or high priority applications minimize data loss, sometimes a loop back controlled source data rate. Traffic may be shaped in a server controlling rates, delay and buffer size. These results have been proven effective in a laboratory basis network; it employs a combination of traffic management with great improvement on network's performance. Due to different task being executed on three levels, design should consider working with MPLS Traffic Engineering techniques on Network Access layer, while ATM switching and buffer management over the backbone layer.

6. References

[1] J. M. Pitts & J. A. Schormans, ”Introduction to IP and ATM Design and Performance“, Wiley, 2001

[2] T. M.. Chen & S. S. Liu, “ATM Switching Systems”, First Edition, Artech House Publishers, 1995.

[3] B. Zheng & M. Atiquzzaman, “Traffic Management of Multimedia over ATM Networks”, University of Dayton, January 1999

[4] Z. Sahinoglu & S. Tekinay, “Self-Similar Traffic and Network Performance“, New Jersey Institute of Technology, January 1999

[5] W. Zitzen, “Metropolitan Area Networks Taking LAN’s Into The Public Network”, Telecommunications, pp. 53-60, June 1990.

[6] D. McDysan, “QoS and Traffic Management in IP and ATM Networks”, McGraw-Hill, 2000.

[7] K. Lindberger, “IP over ATM Network Management major Issues”, November 2001.