iaes
Institute of Advanced Engineering and Science

International Journal of Information and Network Security (IJINS)
Vol.1, No.1, April 2012, pp. 9~27
ISSN: 2089-3299

The Transmission Multicast and The Control of QoS For IPv 6 Using The Infrastructure MPLS

WAYAWO-MANDATAAugustin , LIU Lan
Wuhan University of Technology
122, Luoshi Road Wuchang-wuhan, Hubei Postcode: 430070
telephone: +86-2787658253 P.R.China
e-mail: www.whut@whut.edu.cn

Abstract

Recently there has been several literatures about congestion control in an Unicast/Multicast environment and also some authors tried to be exhaustive as they discussed about managing Quality of Service (QoS) under DiffServ and IntServ. Although Multiprotocol label Switching (MPLS)Traffic and routing control, and as well as IPv6 control QoS were discussed by certain researchers these decades, however finding a paper about MPLS and the way to control QoS for IPv6 is quite difficult. MPLS routing control and multicast transmission are concerned with the handling of traffic flows during normal predictable network conditions. Overload control addresses the handling of traffic flows during unexpected or unusual conditions such as holidays, catastrophes (e.g., earthquakes), or equipments failures. To save network resources, multicast transmissions are more and more adopted by operators when the same information has to reach several destinations in parallel, such as in IPTV services, radio broadcast and video-clip s reaming. Though, with respect to unicast transmissions, multicast sessions make the routing problem more complex with huge sets of trees to be evaluated. Multicast focuses on the scenario whereby an entity transmitter needs to forward a datagram to others 'multiple' receivers. In this work, we use to create an Multicast Environment Group to share data with opening UDP Tunnel and overlay topology to control message just like in an VPN, and give better management of QoS. Experimental results will be provided to show the performance of the proposed technique compared with Unicast transmissions solutions in terms of bandwidth utilization and the QoS control as well as to illustrate the importance of the Congestion control in an MPLS Environment.

Keywords*: maximum 5 keywords from paper* (9 pt)

1. Introduction

Communication networks have entered an era of fundamental change where market and regulatory forces have finally caught up with the relentless advance of technology as: (1) The explosive of growth of multimedia personal computing and the World Wide Web, demonstrating the value of network-based services. (2) The deregulation of the telecommunications industry opening the door to new access network technologies (digital cellular systems, cable modems, high-speed DSL modems, direct broadcast satellite systems, satellite constellation network, broadband wireless cable) that will cause telecommunications infrastructure to migrate towards a flexible packet-based backbone network technology. (3) The explosion in available bandwidth due to optical transmission technology and the entry of new national and global backbone service providers. (4) The emergence of the Internet suite of protocols as the primary means for providing ubiquitous connectivity across the emerging network of networks. (5) The predominance of data traffic over voice traffic dictating that future networks will be designed for data, and that telephone voice service must eventually operate possibly solely over the Internet.
To do so, network operators are supposed to deploy best communication services that will bring infrastructures (Hardware) and software together to achieve customers' needs and requirements [1]. The purpose of congestion control is to eliminate or reduce congestion. If done properly, performance should improve. For a novice, it is tempting to claim that congestion can be solved by just allocating a large buffer. However, this solution merely delays congestion from happening. Worse yet, when congestion kicks in, it will last much longer and will be more severe. In the worst case where the buffer size is infinite, packets can be delayed forever.

Thus, the main architectural elements of the network of networks that will emerge in the next ten years are becoming more evident[1]. In this work we are going to show how building an Communication Service of Alternative Group (CSAG), IPv6 transmission Multicast over MPLS using IPsec can handle (manage) QoS requirement. To achieve this objective, we focus on: Transmission Multicast, CSAG building in IPsec, the IPv6 Multicast on regard with the QoS implementation - and finally we will show how to handle QoS over an MPLS environment.

2. Related Work

There is a little panel of knowledge on QoS-based multicast routing. The article by Jun Hong Cui, Li Lao & company[2] proposes a remarkable architecture, called Aggregated QoS Multicast (AQoSM), to provide scalable and efficient QoS multicast in Diff-Serv networks. The main idea of AQoSM is to separate the concept of groups from the concept of distribution tree by ''mapping'' many groups to one distribution tree.

Received March 11, 2012; Accepted March 30, 2012

Firstly multicast groups can now be routed and rerouted very quickly by assigning different labels (e.g., tree IDs) to the packets. Therefore, we can have load-balancing and dynamic rerouting to meet QoS requirements. Secondly, the groups aggregation on some trees leads to route state reduction and less tree

management overhead. Thus, AQoSM enables multicast to be seamlessly integrated into Diff-Serv without the violation of the design principle of Diff-Serv to keep network core ‘‘QoS stateless’’ and without sacrificing the efficiency of multicast[2]. Finally, They found that by doing an efficient resource utilization and strong QoS support can be achieved through statistical multiplexing at the level of aggregated trees; then they give a design of a detailed MPLS-based AQoSM protocol with efficient admission control and MPLS multicast tree management.

The article by Hao, Zegura and Ammar[3] proposes a remarkable end-to-end QoS-based anycasting architecture which consists of four major issues, namely client demand prediction, signaling protocol between resolver, server agent (SA) and BB, server selection/sorting algorithms, and resource reservation granularity. Server selection is achieved in two steps. In priority, the SA selects a list of candidate server domains based on server information and client requirements. Then, signaling occurs in either a forward or backward direction to reserve resources from the server domain for the client domain. The server information in the SA is gathered by self- ‘‘pushing’’ from each server. The server selection algorithm can select all feasible domains or select the closest server domains from all feasible server domains.

Thirdly and finally it needs to determine which candidate server domains should be tried. Three sorting algorithms were studied: random, widest first and a probabilistic balancing algorithm. Random sorting is applicable for both signaling protocols. The other two algorithms can be used only in backward signaling.

Ayman El-Sayed Ahmed EL-SAYED in "Application-Level Multicast Transmission Techniques Over The Internet" [4], introduce a proposal for building an alternative group communication service that shifts the multicast support from core routers to end-systems. His proposal, called Host Based Multicast (HBM), operates at application-level and provides an

efficient multi-point data distribution service for one-to-many or many-to-many communications. With this approach end-hosts (running the application), dedicated servers and/or border routers automatically self-organize into an overlay distribution topology where data is disseminated. This overlay topology can be composed of both unicast connections and native multicast islands (e.g. within each site). Therefore it offers a group communication service to all hosts, even those located in a site that does not have access for any reason, to native multicast routing.

Finally his works investigate the use of HBM to build a fully secure but efficient group communication service between several sites using an IPSec VPN environment. We show that HBM and the IPSec VPN environment naturally fit with one-another and lead to the concept of Virtual Private Routed Network (VPRN). The motivation of his HBM proposal is usually to offer an alternative to the lack of deployment of inter-domain multicast routing. Another motivation is sometimes to go beyond the limitations of multicast routing protocols.

Nicolas Bonmariage and Guy Leduc in" A Survey of Optimal Network Congestion Control for Unicast and Multicast Transmission" [5], used an optimal problem of congestion control by formulating an technical issue of both unicast and multicast transmission; they shown that decentralized theoretical solutions are derived by applying duality theory. Based on these results, actual generic algorithms and implementations are proposed for solving these problems in a distributed way.

In "A location prediction based routing protocol and its extensions

for multicast and multi-path routing in mobile ad hoc networks"[6], Natarajan Meghanathan proposed a new location prediction based routing (LPBR) protocol for mobile ad hoc networks (MANETs) and its extensions for multicast and multi-path routing. The objective of the LPBR protocol is to simultaneously minimize the number of flooding-based route discoveries as well as the hop count of the paths for a source–destination (s–d) session.

During a regular flooding-based route discovery, LPBR collects the location and mobility information of nodes in the network and stores the collected information at the destination node of the route search process. When the minimum-hop route discovered through flooding fails, the destination node locally predicts a global topology based on the location and mobility information collected during the latest flooding-based route discovery and runs a minimum-hop path algorithm.

If the predicted minimum-hop route exists in reality, no expensive flooding-based route discovery is needed and the source continues to send data packets on the discovered route.

Similarly, Natarajan Meghanathan[6] proposes multicast extensions of LPBR (referred to as NR-MLPBR and R-MLPBR) to simultaneously reduce the number of tree discoveries and the hop count per path from the source to each multicast group receiver. Finally, he also proposes a node-disjoint multi-path extension of LPBR (referred to as LPBR-M) to simultaneously minimize the number of multi-path route discoveries as well as the hop count of the paths in showing that the aim of each category of the LPBR protocols is to simultaneously minimize the number of times the underlying communication structures (single-path, tree or multi-paths) are discovered through a global broadcast discovery as well as the hop count of the paths and/or the number of links that are part of these communication structures.

The work by Nakaniwa et al[7] proposes a new application-level QoS-based anycast protocol, which considers both the server load and the network load simultaneously. The protocol improves the system reliability by introducing distributed resource management by the bandwidth broker (BB) in each domain.

The functions of the original BB have been extended to contain a route cache and a resolver. In addition, the protocol searches for the best server and the best route not by signaling with candidate servers one by one, but rather by broadcasting a search message to all candidate servers.

Rozita Yunos, Noorhayati Mohamed Noor, Siti Arpah Ahmad[8], Performance Evaluation between IPv4 and IPv6 on MPLS Linux Platform presents the performance evaluation between IPv4 and IPv6 with Linux MPLS tunnel. MPLS Linux tunneling is used to transport IPv6 data stream over IPv4 network for interoperable IPv4 and IPv6 deployment. The performance metrics such as jitter, datagram/packet loss and bandwidth were measured in both TCP and UPD traffic flow

Lin et al[9] proposed a load-balanced anycast routing scheme based on the WRS (Weighted Random Selection) method. Each router's outgoing interface is assigned a weight and selected randomly. The probability of a selected outgoing interface is proportional to its corresponding weight. By carefully determining the weights, the distribution of packets among all outgoing interfaces can be controlled. As a result, the network traffic and the server loading can be balanced.

Wu Hsu & Ming Tung[10] proposed a QoS routing protocol that integrates the network-layer and the application-layer anycast approaches. Specifically, the network-layer anycast is used inside a DiffServ network to select a path which matches a client bandwidth requirement, while the application-layer anycast is used to select the best server with the smallest Server Weight (SW). Therefore, Wu Hsu & Ming Tung [10]shown that the QoS metric precedence used in network-layer anycast is defined as bandwidth and then hop-count, while the QoS metric of application-layer anycast is concentrated on SW.

In Sender access Control Distribution for Inter-Domain Multicast groups, Salekul Islam et J. William Atwood[11] argue that classical IP multicast model makes it impossible to restrict the forwarded data to that originated by an authorized sender. Without effective sender access control, an cipher may exploit the existing IP multicast model, where a sender can send multicast data without prior authentication and authorization.

Even a group key management protocol that efficiently distributes the encryption and the authentication keys to the receivers will not be able to prevent an cipher from spoofing the sender address or replaying any previously sent data and hence, flooding the Data Distribution Tree. This can create an efficient Denial of Service attack.

They have proposed an architecture for sender access control and data distribution control in inter-domain multicast groups. For sender access control, the Protocol for Carrying Authentication for Network Access, encapsulating Extensible Authentication Protocol packets, is used to authenticate a sender and to establish an IPsec Security Association between the sender and the Access Router to cryptographically authenticate each packet.

This access control architecture is then extended to support inter-domain multicast groups by making use of Diameter agents. An inter-domain Data Distribution Tree (DDT) is distributed over different domains. Hence, sender access control will be meaningless without protecting the whole DDT.

3. IP Multicast QoS and MPLS Overview

Stimulated, categorized and presented by Stephen Deering[1988], the standard multicast model for IP networks is as follow:

- IP-style semantics. A source can send multicast packets at any time, with no need to register or to schedule transmission. IP multicast is based on UDP, so packets are delivered using a best-effort policy.

- Open groups. Sources only need to know a multicast address. They do not need to know group membership, and they do not need to be a member of the multicast group to which they are sending. A group can have any number of sources.

- Dynamic groups. Multicast group members can join or leave a multicast group at will. There is no need to register, synchronize, or negotiate with a centralized group management entity.

The standard IP multicast model is an end-system specification and does not discuss requirements on how the network should perform multicast routing. The model also does not specify any mechanisms for providing quality of service (QoS), security, or address allocation**.** A multicast address is designed to enable the delivery of datagrams to a set of hosts that have been configured as members of a multicast group in various scattered subnetworks. Multicasting is not connection oriented. A multicast datagram is delivered to destination group members with the same "best-effort" reliability as a standard unycast IP datagram. This means that a multicast datagram is not guaranteed to reach all members of the group, or arrive in the same order relative to the transmission of other packets[1]. The only difference between a multicast IP packet and a unycast IP packet is the presence of a "group address" in the Destination Address field of the IP header. The Internet Protocol enables communications across a vast and heterogeneous

[1] Chuck Semeria and Tom Maufer: Introduction to IP Multicast

collection of networks that are based on different technologies. Any host computer that is connected to the internet can communicate with any other computers that is also connected to the internet. The Internet therefore offers ubiquitous connectivity and the economies of scale that result from large deployment [1].

Conventional IP multicast routing protocols confront a severe scalability problem when there are large numbers of multicast groups ongoing in the networks. This is mainly due to state explosion and control explosion issues.
First, each router needs to maintain separate states for individual groups (or group/sources). Large numbers of groups mean large amount of state to be maintained at routers, which translates into large memory requirement and slow packet forwarding. Second, conventional IP multicast protocols establish and maintain a multicast tree per-group (or group/source). Large numbers of groups mean large numbers of trees to set up and maintain. Consequently, the number of corresponding tree setup and maintenance control messages will become huge and explode.

In backbone networks, this ‘‘state scalability’’ problem will be exacerbated, since there are potentially enormous multicast groups crossing backbone domains. A backbone domain is typically a concentration point of the global network, and its performance greatly influences the global network's performance.

Multicast is one solution. After having looked at the problem described before, it is clear we need a solution that:

- allows data to be sent to multiple receivers in an efficient way, avoiding per-receiver copies.
- is not constrained by arbitrary network limits, so it can reach anyone, anywhere on the Internet.
- differentiates between multiple and unrelated transmissions, so that a host may select the ones that are of interest for the user.

The solution that meets all three requirements is multicast**.** IP multicast has been a hot topic of research and development for more than one decade.

However, there are still some open issues that make it difficult for IP multicast to be deployed in the global Internet. Today many ISPs are still reluctant to provide a wide-area multicast routing service because of technical or marketing reasons[4].

3.1 Congestion Control Protocol in multicast Routing

The routing mechanisms assume that a given source transmits its packets to a single destination. For some applications such as teleconferencing, a source may want to send packets to multiple destinations simultaneously. This requirement calls for another type of routing called Multicast Routing. Multicasting on the Internet is implemented by employing three types of protocols. The first type of protocol is employed by a host to join and leave a multicast group. The Internet Group Management Protocol (IGMP for IPv4) is An example- and Multicast Listener Discovery (MLD for IPv6.

The second type of protocol is called a Multicast Interior Gateway Protocol (MIGP) and is employed by multicast routers to enable multicast communication within an Autonomous System (AS) which is a network of routers under the control of a single administrative domain. Distance Vector Multicast Routing Protocol (DVMRP) Multicast extensions for Open Shortest Path First (MOSPF) Protocol Independent Multicast (PIM) or Core-Based Tree (CBT) are some others examples of MIGPs.

The third type is employed by border routers, that interconnect two ASes to allow multicast communication across ASes. Border Gateway Multicast Protocol (BGMP) is an example of that protocol[5].

The multicast forwarding state scalability is one of the critical issues that delay the deployment of IP multicast. With traditional Internet protocols, each router is required to maintain a forwarding entry for each multicast session whose distribution tree passes through the router. When there is a very large number of concurrent multicast sessions, the number of the corresponding multicast forwarding entries at routers is also very large. This could consume more router memory and might also result in slower packet forwarding as each packet forwarding involves a routing table lookup. This is the forwarding state scalability issue in providing scalable IP multicast. In general, the bandwidth saving with multicast routing becomes more substantial as the number of destinations increases. There are many ways to generate a multicast tree. One approach that is used in multicast backbone (MBONE) is called reverse-path multicasting. MBONE is basically an overlay packet network on the Internet supporting routing of IP multicast packets[2]

3.1-1. Congestion Control in Multicast Transmission.

Congestion occurs when too many packets try to access the same buffer pool in a switch.

The basic objective is to best exploit the available network resources while preventing sustained overload of network nodes and links. For example, consider the communication network shown in figure 1. Suppose that nodes A, B and D send bursts of packets to node Z simultaneously. Assume that the aggregate incoming rate of the packets is greater than the rate at which the packets can be transmitted out. In this case the buffer in node Z will build up. If this situation occurs sufficiently long, the buffer eventually may become full and start rejecting packets. When the destination detects the missing packets, it may ask the sources to retransmit the packets. The sources would unfortunately obey the control and send more packets to node Z, making the congestion even worse. In turn, node Z dis-

[2] Chuck Semeria and Tom Maufer: Introduction to IP Multicast Routing

cards more packets and this effect triggers the destination to ask for more retransmissions. the result is that the network throughput at the destination will be very low

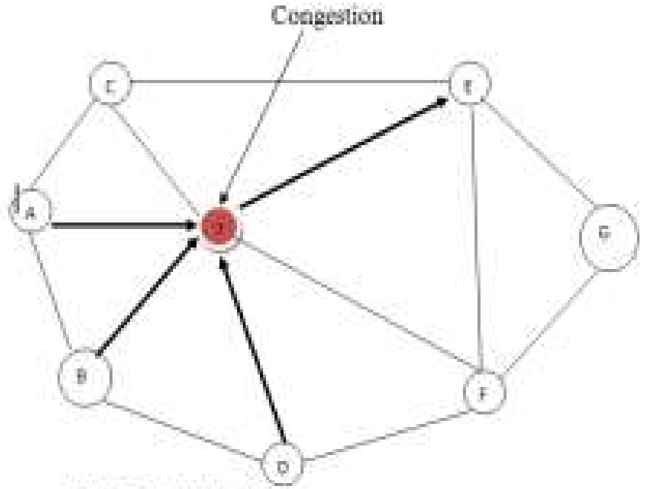

Fig0: Congested switch

By this idea we can easily formulate a principle of an optimization theory framework.
We introduce firstly some notation:

Let L = {1, . . . ,L} be the set of unidirectional network links. Each link l ∈ L is characterized by its capacity c_l. We consider a set S = {1, . . . , s} of sources using these links.

Each of these sources is characterized by a strictly concave utility function U_s which is a function of the transmission rate x_s of that source.

We consider that the rate of the source must lie within some interval I_s, i.e. $x_s \in I_s = [b_s, B_s]$. We denote by S_l the set of flows using link l:

$$max_{x_s \in I_s} \sum_{s \in S} U_s(x_s), \qquad (1)$$

$$\text{subject to } \sum_{s \in S_l} x_s \leq C_l, \quad l= 1,...., L. \qquad (2)$$

A unique solution to this problem exists, since the objective function is strictly concave and the feasible set is convex. Concave utility functions are suitable and have been used extensively for traditional elastic data services in the Internet, turning problem into a convex optimization problem.[5]

However, for delay and rate sensitive services and many services in wireless networks, non-concave utility functions (e.g. sigmoïdal-like ‘‘S’’ functions) are more realistic, although requiring more complex algorithms to find the global optimum of problem. We now give some comments on this particular formulation. The congestion control problem is not only considered for a particular flow between two end nodes but instead at the whole network level, all the receivers being simultaneously introduced in the sum of utilities[4,1]. The purpose of congestion control is to eliminate or reduce congestion. If done properly, performance should improve. It is not tempting to claim that congestion can be solved by just allocating a large buffer; furthermore, the solution to this optimization problem is thus meant to be a global optimum for all network users.

Although the congestion constraints introduced for the links seem unavoidable in the problem formulation, one might question the use of utility functions or more generally the choice of the objective function. The objective function translates in mathematical terms the actual quantity to be optimized. Besides this formulation considerations, an issue to be also considered for a given optimal solution is the impact of the choice of a particular class of functions on the properties of the resulting algorithm, such as convergence and stability. The above classical formulation for the unycast case can readily be generalized to the single rate multicast case, where the considered rates are now multicast session rates[5].

Let M denote the set of all multicast groups in the network and, for any m ∈ M, let R_m denote the set of receivers for group m. To express the link capacity constraints in the layered case, we need an expression of the flow rate of a multicast group m on a given link l, based on the choice variable x_r representing the rate associated with receiver r. If we consider a hierarchically encoded layered stream, the rate on a link upstream to a subset of receiver is the maximum of all rates reaching this subset of receivers, so that the cumulated rate of multicast group m on link l is simply max$r \in_{S_l} \cap R_m x_r$. The problem can now be formulated as

$$\max_{x_r \in I_r} \sum_{r \in_R} U_r(x_r), \qquad (3)$$

$$\text{subject to } \sum_{m \in_M} \max r_{\in_{S_l \cap R_m}} x_r \le C_l, \quad \forall\, l \in \text{L} \qquad (4)$$

where R =$U_{m \in M} R_m$ is the set of all multicast receivers, considering with no loss of generality disjoint sets of receivers[5]. If we assume that there exists an interior point to the set of constraints, problem is feasible. If we further assume that the utility functions are strictly concave, then this solution is provably unique.

Obtaining a distributed and scalable solution is of critical importance in the multicast case. Any derived solution must indeed scale not only at the multicast group level like in the single source single-receiver case, but also inside a given group. Although the max functions appearing in the link constraints of problem are non-linear, the constraint set remains convex and there is thus no duality gap, the utility functions being strictly concave. Duality theory, if being applied directly, would however in this case lead to a more difficult solution precisely because of these non-linearties in the constraints[4,5].
This would result in a much more complex maximization of the Lagrangian. But more fundamentally, problem is not separable anymore. The max functions indeed couple several variables together, making it impossible to reduce the global Lagrangian maximization to a set of local optimizations.

One way to circumvent this difficulty is to replace each max term by a set of linear constraints, which can always be carried out. A direct replacement would however lead to an exponential number of (linear) constraints. Obtaining a decentralized solution to problem by means of duality theory requires in fact a reformulation of the problem. One simple way to achieve this is to replace each max term appearing in the link constraints by a separate variable representing the rate on the corresponding branch of the multicast tree.
The choice variables are now the cumulated rates of the various multicast groups on each link. In the previous formulation, the receiver rates were considered. It is therefore necessary to introduce additional constraints on the feasible set of branch rates to ensure that the latter are coherent with a layered scheme, i.e. the rate on a branch cannot be greater than the rate on the parent branch but can possibly be lower if a layer is not subscribed anymore on that branch. Before giving the alternate formulation, we introduce some more notation.

We partition the set of nodes in the network in junction nodes and non-junction nodes. A junction node is a node where one of the multicast trees branches off in two or more children. We denote $\hat{R}$ the set of all junction nodes over all multicast groups and by $\tilde{R}$= R $\cup$ $\hat{R}$ the union of all junction and receiver nodes (which are assumed with no loss of generality to be logically different). We call a branch the set of links joining two junction nodes in a given tree and note $\hat{J}$ and J the set of branches ending respectively at a junction or receiver node. We also use $\tilde{J}$= J $\cup$ $\hat{J}$, We associate a rate variable y_j with each branch j $\in \tilde{J}$and denote by r(j) the receiver or junction node associated with branch j $\in \tilde{J}$. The alternate problem formulation used to solve the optimization problem in the multilayer multicast case is then:

$$\max_{y_j \in Y_j} \sum_{j \in J} U_j\left(y_j\right), \qquad (5)$$

$$\text{subject to } \sum_{j \in K_l} y_j \le c_l \quad \forall\, \text{l} \in \text{L}, \qquad (6)$$

$$y_j \le y_\pi(\text{j}), \quad \forall\, \text{j} \in \tilde{J} \text{ s.t. } \pi(\text{j}) \ne \emptyset \qquad (7)$$

where $K_l \subseteq \tilde{J}$is the set of branches that share link l$\in$ L and π(j) is the parent branch of branch j and where

$$Y_j = \begin{cases} I_r(j) = [b_r(j), \quad B_r(j)] & (1) \\ [0, B] & (2) \end{cases} \text{(1) if j} \in J \text{ and (2) j} \in \hat{J},$$

with B being any number satisfying B > max$_{r \in R} B_r$. This reformulated problem has grown in size, since we consider one choice variable per branch and not only per receiver and since we have added branch constraints to the usual link constraints.

The problem is now separable, enabling us to use duality theory to obtain a decentralized

solution. We note p_l, l ∈ L, the dual variables associated with the link constraints and q_j, j ∈ { j': π(j') ≠ $\emptyset$ }, the dual variables associated with the branch constraints, the latter variables being assumed to be identically zero for branches starting from source nodes, i.e. for branches j such that π(j) = $\emptyset$, We will directly give the expression of the objective function, to avoid the notational burden of its derivation, which is anyway similar to the unycast case. The dual objective function D is:

$$D\,(p, q) = \max_{y \in Y} L(y, p, q), \qquad (8)$$

$$= \sum_{j \in J} B_j(p, q) + \sum_{l \in L} p_l c_l \qquad (9)$$

with

$$B_j(p, q) = \begin{cases} \max_{y_j \in Y_j} \{U_j(y_j) - y_j(\tilde{p}_j + q_j)\} \\ \quad \text{if } j \in J, \\ \max_{y_j \in Y_j} \left\{-y_j\left(\tilde{p}_j + q_j - \sum_{k \in C_j} q_k\right)\right\} \\ \quad \text{if j} \in \hat{J} \end{cases} \qquad (10)$$

where $\tilde{P}_j = \sum_{l \in L_j} P_l$, is the set of links constituting branch j and C_j = {$k \in J$ π(k)= j}, the set of children branches of branch j. As in the unycast case, we see that the evaluation of the dual objective function can be reduced to a set a distinct branch optimization problems for which the only knowledge required are the p and q prices for that branch and the q prices for the children branch. This will enable the derivation of decentralized algorithm solving indirectly the global optimization problem.

The interpretation of the link prices p_l is similar to the unicast case, as they are associated with the link capacity constraints: they represent the price to be paid per unit bandwidth when the associated link is congested, and remain zero while the constraint is inactive. The cumulated prices $\tilde{p}_j$ are then the corresponding branch prices.

The interpretation of the q prices gives us an important insight into problem. If we look at the first piece of expression relative to branches ending at receiver nodes, we see that at optimality each receiver is again maximizing its individual profit, but this time the price per unit bandwidth is the sum of the price $\tilde{p}_j$ of the branch ending at that receiver and of the price q_j associated with that branch.

This latter price can be seen as the price this receiver has to pay for its usage of branches located in the tree upwards branch j. In the unicast case, the price was related to the whole path to the source. This is no longer the case here, as the path has been subdivided into a set of branches describing the multicast tree.

In his study Nicolas Bonmariage and Guy Leduc have shown that Equation(10), relative to branches ending at junction nodes can also be viewed as profit maximization, or more precisely, a cost minimization, as these nodes do not have a utility function and therefore any profit. A junction node can be thought of as being in charge of conveying to its children the layers they have subscribed to. It therefore has to pay for the resulting usage of the branch ending locally but also above in the tree. The price thus still includes the price $\tilde{P}_j$ for the branch ending at that node and the price q_j of the upper branches in the tree. But the children nodes are also charged for their usage of the tree from the source down to them, so that the price in (10) can be diminished by the corresponding amount. This is again only true for children using all the layers conveyed by their parent node, since otherwise the price for the use of the tree is zero, as a result of the slackness conditions.

We can also calculate the total profit P_m realized by a given multicast group m by summing for the receiver and junction branches the profit terms appearing in inside the max terms. We have:

$$P_m = \sum_{j \in J_m} U_j(y_j) - \sum_{j \in J_m} \bar{P}_j\, y_j - \sum_{j \in \bar{J}_m} y_j\, q_j + \sum_{j \in \bar{J}_m} y_j \sum_{k \in c_j} q_k \qquad (11)$$

or, the variables q_j being identically zero for branches starting at the source,

$$= \sum_{j \in J_m} U_j(y_j) - \sum_{j \in \bar{J}_m} \bar{P}_j\, y_j - \sum_{j \in \bar{J}_m} q_j \left(y_j - y_{\pi(j)}\right)$$

where : $\sum_{j \in \bar{J}_m} q_j \left(y_j \quad y_{\pi(j)}\right) = 0$ (Slackness conditions complementary)

At the optimality point, each group maximizes its profit, which is the sum of its receiver utilities diminished by the amount that the group has to pay for its branch usage in the multicast tree. Again, the price of a branch is zero when all the links constituting that branch are not saturated.

3.2. CSAG: fundamentals principles

A Communication Service of Alternative Group is concerning by the ability to send information to several points (receivers) at the same time, using either a one-to-many or many-to-many structures.

Although this survey purpose is to give a complete overview of CSAG techniques, we do not claim to be exhaustive. Besides we only consider the routing service (i.e. as a replacement of, or complement to, IP-multicast) and try to point at upper-level service like reliability or congestion control. If some of the solutions we introduce largely impact these upper-level services, Likewise, we will cover DiffServ multicasting or, more generally, QoS-based multicast routing. It (CSAG)also can be used as a way to bypass the multicast routing deployment problems. [11]. For instance an CSAG can be used to go beyond the limitations of traditional multicast routing. An CSAG can offer a bridging service between several multicast capable areas running different multicast routing protocols, for instance between IPv4 and IPv6 multicast islands.

A CSAG can also be used along with PIM-SSM. Since only the source *S* is allowed to send traffic to an (S, G) channel, *G* being the group addresses, no multicast back-channel is available for a receiver to provide feedback to the group. If the feedback rate is sufficiently low (e.g. with RTCP), this feedback can be unicast to the source and echoed back onto the channel. If not, such an approach quickly results in source implosion and this is the reason that an CSAG can be useful.

Communications network is a set of equipment and facilities that provides a service much like other ubiquitous utilities, and many analogies can be drawn between communication networks and others utility systems, it also provides access for gathering information much like sewer or garbage collection systems, which gather various materials from users.

In his work Pablo J. et al [2009]argue that from a mathematical point of view, a communications network can be regarded as a collection of resources (physical links) with a finite service capacity (bandwidth) [12]. The deployment of IP Multicast (i.e. at the network layer) has been limited and sparse due to a variety of technical and non-technical reasons. Therefore some researchers have revisited the issue whether the network layer is necessarily the best layer for implementing multicast functionality and have proposed application-level multicast (i.e. at the application layer) as an alternate technique for multicasting.

They enable every host to participate in group communication sessions efficiently, no matter whether it has access to native multicast routing or not. Since data is sent via unicast, flow control, congestion control, and reliable delivery services available for unicast transmission can be exploited, perhaps with minor modifications.

Ayman El SAYED (2004) has shown that in Figure 1, considering only the number of packets in all the physical links, on top of which the overlay is built in that physical topology, we found 33, 23, and 16 copies of packets for multi-unicast, Application-level multicast, and IP multicast respectively. So, with respect to multi-unicast, he found that IP multicast reduce the used resources by 52 % but the application-level by 30 %.

As we have seen early-, the deployment of multicast routing in the Internet is still far behind expectations. Therefore a first motivation for an alternative group communication service is to bypass the lack of native IP multicast routing. One proposal of an alternative group communication service is overlay Multicast.

Over load conditions result in traffic levels that the network equipment has not been provisioned for and if not handled properly can result in a degradation in the level of service offered to all network customers

In particular, we consider a model in which multicast related features, such as group membership, multicast routing, and packet duplication, are implemented at end systems, assuming only unicast IP services.

The main purpose of our study is to introduce an application-level multicast (ALMI) that is easy design, simple deployment, and with no need of routers to support native multicast. The proposal ALMI is a centralized technique with controlling everything under a single node, called *Bungbi Ndo Point* (BNP).This approach is to give:

- build a secure group communication service.
- improve the scalability,

- impact the robustness in front of node failures and overlay topology modification,
- create not bad the overlay topology.

In these points of view and to achieve these issues, we implemented a group communication services library (GCSL) for our ALMI proposal. Several performances metrics have been defined to characterize CSAG performance and impacts on the network. Some of them focus on the data path:

- **Stress:** defines the stress of a physical link as the number of identical packets it carries. The optimal value, achieved with native multicast routing, is of course 1.
- **Resource Usage:** defines this metric as the sum of the delay stress over all the links that participate in data transmissions. This metric gives an idea of network resources used by the transmission process, assuming that links with high delays are more costly.
- **Stretch:** also called "Relative Delay Penalty" , the stretch metric between a source and a member is the ratio of the delay between them along the overlay distribution topology, to the delay of the direct unicast path. Another set of metrics focuses on end-host performance:
- **Losses after Failures:** This metric counts the average number of packet losses after an ungraceful failure of a single node. It highlights robustness in the occurrence of unpredicted events.
- **Time to First Packet:** defines the time required for a new member to start receiving a data flow when joining an on-going session. Finally some metrics focus on the control part:
- **Control Overhead:** maintaining the CSAG topology has a cost, in terms of control information exchanged (number of messages processed and bandwidth).

Finally an CSAG can be used in working environments where traditional multicast routing is completely inappropriate. This is the case of ad-hoc networks where there is no fixed infrastructure. Multicast routing, designed for a fixed hierarchical routing infrastructure with well identified multicast routers, is completely defeated.

This is also the case when there is a very high number of small dynamic groups. The signaling load required by traditional multicast routing for each group prevents the whole system to scale in terms of number of concurrent groups[4].

3.2-1. CSAG and the IPsec

In Multicast transmission, data distribution control mechanism is heavily dependent on IPsec Security Association (SA). An SA is a simple connection that affords security services to the traffic carried by it. IPsec SAs have been primarily designed to protect unicast traffic; however, they can be used for multicast communication with limited security services[11].

As in OSI architecture, Internet Layer provides a single service namely best-effort connectionless packet transfer; so Internet Protocol(IP) packets are exchanged between routers without a connection setup; the packets are routed independently, and so they may traverse different paths. Therefore, IP packets are also called Datagrams.

To deliver an datagram, IP need to use Transfer Control Protocol Technique that consist of reliable connection-oriented transfer. In this category we introduce the Point-to-Point Protocol that provides a method for encapsulating IP packets over point-to point . PPP can be used as a data link control to connect two routers or can be used to connect a personal computer to an Internet Service Provider (ISP). PPP was designed to support multiple network protocols simultaneously; it can also transfer packets that are produced by different network layer protocols.

This situation arises in multiprotocol routers that can simultaneously support several network layer protocols. The MBONE is the ad hoc Multicast Backbone on the Internet and is just such a web of *MRouter* and tunnels. Its participants are sites that are interested in using IP multicasting for a variety of services on the Internet. To prevent a multicast tunnel from being used as a back door into or out of a network, the current publicly available MRouters code will only accept multicast packets through the tunnel; it won't accept unicast packets shoved through the tunnel in an attempt to bypass your firewall.[3] These solutions are often called tunneling approaches too since they create tunnels between the reflector and the end-hosts. Yet they are completely different from the permanent tunneling approaches.

The first key aspect is its application level feature. The communication between a host and the reflector can be more or less elaborated: multicast packets can be captured by **a** BPF packet filtering tool and encapsulated in unicast datagrams. A simpler solution consists in opening a UDP socket and forwarding only the payload, without the initial packet headers.

In that case the source address and port are lost but upper protocols (e.g. RTCP) may recover the source identity.

Secondly this service is usually set up for a limited time and for a limited number of groups (usually there is one reflector per group). The UMTP and Mtunnel proposals fall in this category. Permanent Tunneling proposals differ from the reflector proposals from several points of view. First of all, tunneling is performed at routing level and uses IP encapsulation. Its creation requires privileges and is usually not set up by a end-host. Secondly, if a reflector an-

[3] Chuck Semeria and Tom Maufer: Introduction to IP Multicast Routing

swers a punctual need within a well identified group of people, tunneling solutions offer permanent connectivity for a whole site.

Thirdly, tunnels are fully integrated in the multicast routing protocols and offer connectivity to all possible multicast groups.The MRouted DVMRP implementation is undoubtedly the most popular tunneling solution and has long been used in the MBONE. AMT is midway between the reflector and permanent tunneling categories. It manages the multicast traffic exchange for any groups between isolated multicast-enabled sites, yet it does not include a routing protocol, unlike DVMRP/MRouted.

Without an efficient sender access control, an attacker may exploit the existing IP multicast model, where a sender can send multicast data without prior authentication and authorization. Otherwise, in the absence of data distribution control, a compromised network entity (e.g., a router or a host) may flood the Data Distribution Tree (DDT) by inserting any number of bogus packets[11].

3.3. Application-Layer Multicast Infrastructure: Principles.

Application-Level Multicast Infrastructure (ALMI) consists of a session controller and multiple session members. A session controller is a program instance, located at a place that is easily accessible by all members (e.g. within a dedicated server). Session members are organized into a shared-tree using bidirectional links. Session data is disseminated along this tree, while control messages are unicast between each member and the controller.

The controller calculates a minimum spanning tree based on the measurement updates received from all members. To collect measurements the controller essentially instructs each member to monitor a set of other members. The ALMI principle is that the protocol automatically creates a virtual overlay topology between the various group members (sources and receivers), using point-to-point UDP tunnels between them. Everything is under the control of a single host, the Bungbi Ndo Point (BNP).

This BNP knows all informations about any members else; their features, and the communication costs between them. He is responsible of the overlay topology calculation and its setup at each member. This proposal therefore follows a centralized approach.

Figure 1 describes the control messages exchanged by the CP and each group member. Each group member evaluates the metrics between itself and either all the other group members or a subset of them (e.g. host w1 evaluates the metrics between itself and hosts w2, w3,).

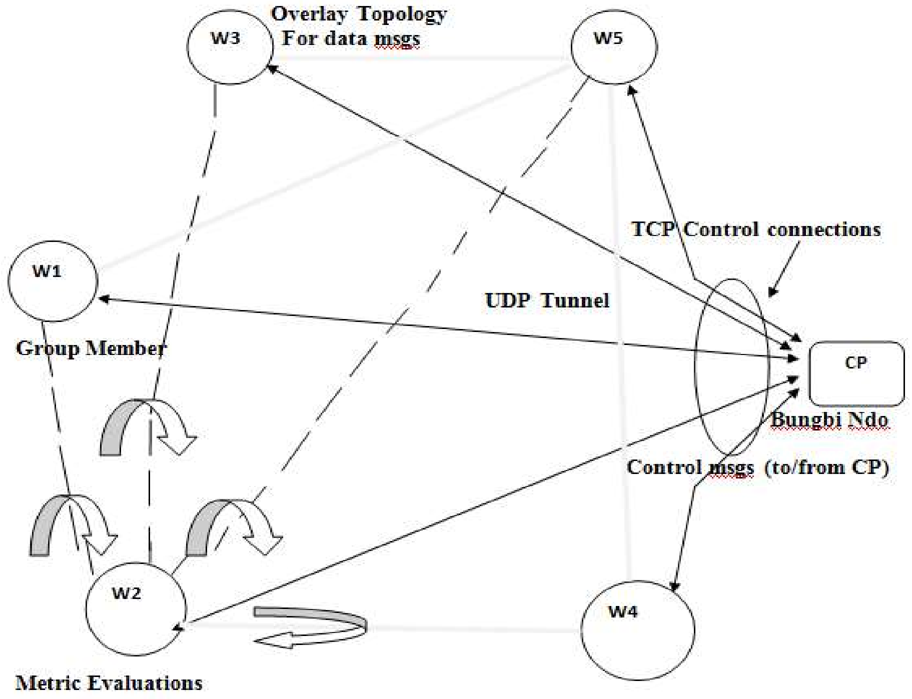

Fig1. Synoptic Scheme of ALMI connections.

Later, we will show how to bring the present architecture(ALMI) using an MPLS-Based Aggregated Quality of Service Multicast Protocol (MAQoSMP) to achieve the QoS requirements by the admission control and the MPLS multicast tree management.

3.4. IPv6 IN QoS MANAGEMENT CONCEPT.

IPv6, formerly named IPng (next generation), is the latest version of the Internet Protocol (IP). IP is a packet-based protocol used to exchange data, voice, and video traffic over digital networks. IPv6 was proposed when it became clear that the 32-bit addressing scheme of IP version 4 (IPv4) was inadequate to meet the demands of Internet growth. After extensive discussion it was decided to base IPng on IP but add a much larger address space and improvements such as a simplified main header and extension headers. IPv6 is described initially in RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, issued by the Internet Engineering Task Force (IETF). Further RFCs describe the architecture and services supported by IPv6.

The architecture of IPv6 has been designed to allow existing IPv4 users to transition easily to IPv6 while providing services such as end-to-end security, quality of service (QoS), and globally unique addresses. The larger IPv6 address space allows networks to scale and provide global reachability. The simplified IPv6 packet header format handles packets more efficiently.

IPv6 prefix aggregation, simplified network renumbering, and IPv6 site multi-homing capabilities provide an IPv6 addressing hierarchy that allows for more efficient routing. IPv6 supports widely deployed routing protocols such as Routing Information Protocol (RIP), Integrated Intermediate System-to-Intermediate System (IS-IS), Open Shortest Path First (OSPF) for IPv6, and multiprotocol Border Gateway Protocol (BGP).

Other available features include stateless auto-configuration, enhanced support for Mobile IPv6, and an increased number of multicast addresses.

3.4-1. IPv6 Address Space and Format: Address Space.

The primary motivation for IPv6 is the need to meet the anticipated future demand for globally unique IP addresses. Applications such as mobile Internet-enabled devices (such as personal digital assistants [PDAs], telephones, and cars), home-area networks (HANs), and wireless data services are driving the demand for globally unique IP addresses.

IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides more than enough globally unique IP addresses for every networked device on the planet. By being globally unique, IPv6 addresses inherently enable global reachability and end-to-end security for networked devices, functionality that is crucial to the applications and services that are driving the demand for the addresses.

Additionally, the flexibility of the IPv6 address space reduces the need for private addresses; therefore, IPv6 enables new application protocols that do not require special processing by border routers at the edge of networks.

3.4-2. IPv6 Format

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

2001:0DB8:7654:3210:FEDC:BA98:7654:3210

2001:0DB8:0:0:8:800:200C:417A

It is common for IPv6 addresses to contain successive hexadecimal fields of zeros. To make IPv6 addresses less cumbersome, two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros).

Synoptic table lists compressed IPv6 address formats. A double colon may be used as part of the ipv6-address argument when consecutive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

IPv6 Address Type	***Preferred formats***	***Compressed formats***
Unicast	**2001:0:0:0:0DB8:800:200C:417A**	**2001::0DB8:800:200C:417A**
Multicast	**FF01:0:0:0:0:0:0:101**	**FF01::101**
Loopback	**0:0:0:0:0:0:0:1**	**::1**
Unspecified	**0:0:0:0:0:0:0:0**	**::**

Figure 2: Synoptic Table of Compressed IPv6 Address formats.

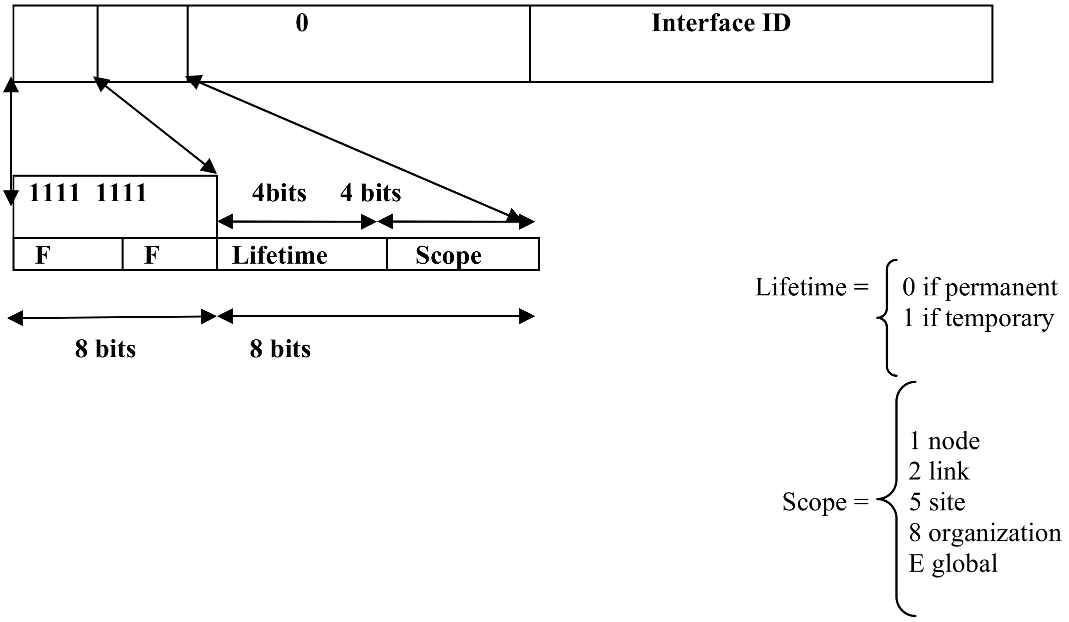

Figure 3: Synoptic Table of IPv6 Multicast Address format.

IPv6 nodes (hosts and routers) are required to join (receive packets destined for) the following multicast groups:

- All-nodes multicast group FF02:0:0:0:0:0:0:1 (scope is link local)
- Solicited-node multicast group FF02:0:0:0:0:1:FF00:0000/104 for each of its assigned unicast addresses IPv6 routers must also join the all-routers multicast group FF02:0:0:0:0:0:0:2 (scope is link local).

3.5. IPv6 QoS Management.

Talking about Quality of Service cannot make ignored the attack of messages transmitted over a link; therefore QoS handling is defined on per-hop behavior based on IP differentiated services code point, as well as Security aspect should not be neglected in data transmission within a network.

As in IPv4, path MTU discovery in IPv6 allows a host to dynamically discover and adjust to differences in the MTU size of every link along a given data path. In IPv6, however, fragmentation is handled by the source of a packet when the path MTU of one link along a given data path is not large enough to accommodate the size of the packets. Having IPv6 hosts handle packet fragmentation saves IPv6 router processing resources and helps IPv6 networks run more efficiently[13,8].

With IPv6 path MTU discovery, a router originating IPv6 traffic has an MTU cache that contains MTU values received in ICMPv6 "toobig" messages. In order to prevent an attacker from filling the MTU cache, the router keeps track of the destinations to which it has originated (sent) traffic, and only accepts toobig ICMPv6 messages that have an inner destination matching one of these tracked destinations[14].

If a malicious node has the capability to learn to which destination the router is originating traffic, it could still send a toobig ICMPv6 message to the router for this destination, even if the attacker is not on the path to this destination, and succeeds in forcing his entry into the MTU cache.

The router then starts fragmenting traffic to this destination, which significantly affects router performance. Enabling flow-label marking for locally generated traffic can mitigate this attack. Originated packets are marked with a flow label (which is randomly generated and changed every minute), and toobig messages received are checked against the values sent. Unless an attacker has the capability to snoop traffic, the attacker will not know which flow label to use, and its toobig message will be dropped.

3.6. MANAGING QoS OVER MPLS

ATM introduced the use of label switching to enable fast forwarding of cells across a network. Label switching provides a low-cost hardware implementation, scalability to very high speeds, and flexibility in the management of traffic flows. For this reasons, IP over ATM networks provided the bandwidth in the network backbone that was needed to meet the growth in Internet traffic in the last 1990s.

The need of making real-time applications such: VoIP(audio/video streaming, videoconferencing, interactive gaming, e-commerce, video distribution, networked virtual environments, GRIDs and collaborative environment....) boosted the QoS deployments in IP Networks.[1] Quality of Service (QoS) is a set of service requirements (performance guarantees) to be met by the network even in the case of transporting a datagram flow. Packet forwarding in the Internet substantiates the best-effort service model, whereby routers do not keep state information for any of the active traffic flows and every packet receives the same common service. This key architectural principle is behind the unparalleled growth in size, bandwidth and data types carried by the network, but precludes better resource allocation for applications with quality of service (QoS) demands.

In the study of Performance Evaluation between IPv4 and IPv6 on MPLS Linux Platform, Rozita Yunos & Noorhayati Mohamed Noor[8] argues that Multi Protocol Label Switching (MPLS) is architecture for fast packet switching and routing. It provides the designation, routing, forwarding and switching of traffic flows through the network. It has been proposed as a solution to overcome some limitations, drawbacks and problems associated with the network model that is nowadays currently used in the core network . Although the original idea behind the development of MPLS was to facilitate fast packet switching, currently its main goal is to support traffic engineering and provide quality of service (QoS).

MPLS is a protocol able to run below IP and on top of several layer 2 technologies (PPP, SDH/SONET, Ethernet). It enables connection-oriented paths (Label Switched Paths, LSPs) to be created within IP-based core networks The fundamental problem for providing multiple service classes in a packet network has always been the scalability of the architecture and of the routers' algorithms. In the 1990s, IntServ and DiffServ emerged from within the IETF as the two frameworks for building a network core with differentiated services. In IntServ, the applications could obtain even the strictest QoS requirements, since the architecture dictates per-flow, end-to-end resource reservations.

As a consequence of this postulate, the routers must keep running and process data and control state for every flow of packets, participate in complex signaling procedures, and cooperate with routers in the same or in other domains in order to support end-to-end service guarantees. Therefore, IntServ cannot be deployed over the global, decentralized Internet, and was never seriously considered for adoption. DiffServ arose as a simpler, more scalable, manageable, and easily deployable solution for service differentiation in IP networks. Its premise is that individual flows with similar QoS requirements can be aggregated in larger traffic groups, called macroflows, that use a certain set of forwarding rules at the core routers, furthermore to reach our purpose, we need to built an MPLS join/leave environment wherein we will show the utility of dealing with QoS requirements.

3.7. QoS Guarantees and the Service Scheduling

Switches and routers in the packet-switched networks use buffers to absorb temporary fluctuations of traffic. Packets that are waiting in the buffer can be scheduled to be transmitted out in a variety of ways. Our design goal is to achieve high state scalability and high resource utilization while satisfying QoS requirements of multicast groups with low overhead in creating an Aggregated QoS Multicast (AQoSM) to provide scalable QoS multicast that addresses the issue of QoS and routing in a unified and comprehensive way. Here we discuss how the packets delay across a network can be guaranteed to be less than a given value. The technique makes use of a token bucket shaper and weighted fair-queuing scheduling.

Let b be the bucket size in bytes and let r be the token rate in bytes/second. then in a time period T, the maximum traffic that can exit the shaper is b+rT bytes (e.g. see figure), suppose we apply this traffic to two multiplexers in tandem each served by transmission lines of speed R bytes/second with R > r. We assume that the two multiplexers are empty and not serving any other flow

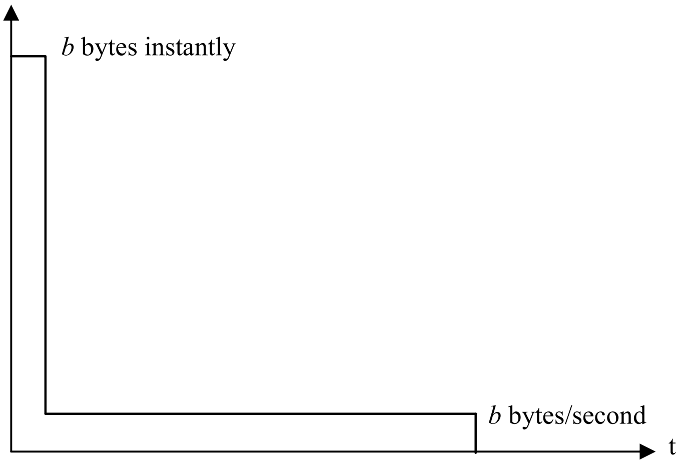

Figure 4. Maximum Traffic allowed out of Token Bucket Shaper

We also assume that the token bucket allows an immediate burst of b byte to exit and appear at the first multiplexer at t = 0, so the multiplexer buffer surges to b bytes at that instant. Immediately after t = 0, the token bucket allows information to flow to the multiplexer at rate of r bytes/second, and the transmission line drains the multiplexer at a rate R bytes/second. Thus the buffer occupancy at a given instant determines the delay that will be experienced by a byte that arrives at that instant, since the occupancy is exactly the number of bytes that need to be transmitted before the arriving byte is itself transmitted.

Therefore, we conclude that the maximum delay at the multiplexer is bounded by b / R. This architecture intends to be employed in a Diff-Serv-supported transit domain and its use is transparent outside the domain or to the application layer. AQoSM uses the concept of aggregated multicast, in which the key innovation is the decoupling of group and distribution tree concepts. Many groups can be multiplexed on a single tree. More importantly, a group can be switched easily between distribution trees.

This simple feature leads to a proliferation of new properties and advantages. First, the creation and management of trees become more efficient. We can create trees on-demand and route a group very quickly. Second, group rerouting becomes a viable option: it is a matter of assigning different labels (i.e., tree IDs) to its packets at the entrance points. This opens new possibilities for load-balancing and fault tolerance: we can now start to look at sophisticated load-balancing and failure recovery schemes.

Now, consider the second multiplexer. At time t = 0, it begins receiving bytes from the first multiplexer at a rate of R bytes/second. The second multiplexer immediately begins transmitting the arriving bytes also at a rate of R bytes/second. Therefore there is no queue buildup in the second multiplexer, and the byte stream flows with zero queuing delay.

Therefore, we conclude that the information that exits the token bucket shaper will experience a delay no greater than b / R over the chain of multiplexers. Suppose that the output of the token bucket shaper is applied to a multiplexer that uses weighted fair queuing. Also, suppose that the weight for the flow has been set so that it is guaranteed to receive at least R bytes/second. Then it follows that the flow from the token bucket shaper will experience a delay of at most b / R seconds. This result, however assumes that the byte stream is handled as a fluid flow.
[Parekh 1992] had shown that if packet-by-packet weighted fair queuing is used, then the maximum delay experienced by packets that are shaped by (b, r) token bucket and traverse H hops is bounded as:

$$D \leq b / R + (H - 1) / R + \sum^{H} M / Rj \; ; \quad j=1,$$

where m is the maximum packet size for the given flow, M is the maximum packet size in the network, H the number of hops, and Rj the speed of the transmission line in link j. Also note that r ≤ R. This result provides the basis for setting up connections across a packet network that can guarantee the packet delivery time. This result forms the basis for the guaranteed delay service proposal for IP networks.

This way, we can adapt to changes in the QoS requirements, in the network load, and in the group membership. From the scalability point of view, the major benefit is that our architecture reduces the multicast state by mapping multiple groups to one tree. Finally, the admission control can be carried out on the level of aggregated trees instead of individual links, and thus is resource efficient due to statistical multiplexing of multiple groups on a single tree. Aggregated multicast was designed as state-reduction scheme, but here, it becomes a powerful tool to simplify traffic management and QoS provisioning. Aggregated multicast was designed as state-reduction scheme, but here, it becomes a powerful tool to simplify traffic management and QoS provisioning. After a new tree is computed, the admission control module needs to decide whether adequate resource is available. If not, the incoming multicast request is rejected. Otherwise, the corresponding tree is established in the network.

Once a proper multicast tree is found or established, the tree manager distributes the corresponding group–tree matching entry to the member edge routers (source routers and receiver routers) within the group. Source routers take charge of encapsulating, classifying,

and marking individual group packets, while receiver routers decapsulate group packets. A member router might act as both source router and receiver router. During the whole process,

the policy control, which preserves a policy information base, may be consulted to do a network policy administration. A picture of AQoSM is shown in Figure 5, where A, D, and E are edge routers (with A as source router and D and E as receiver routers), and B and C are core router

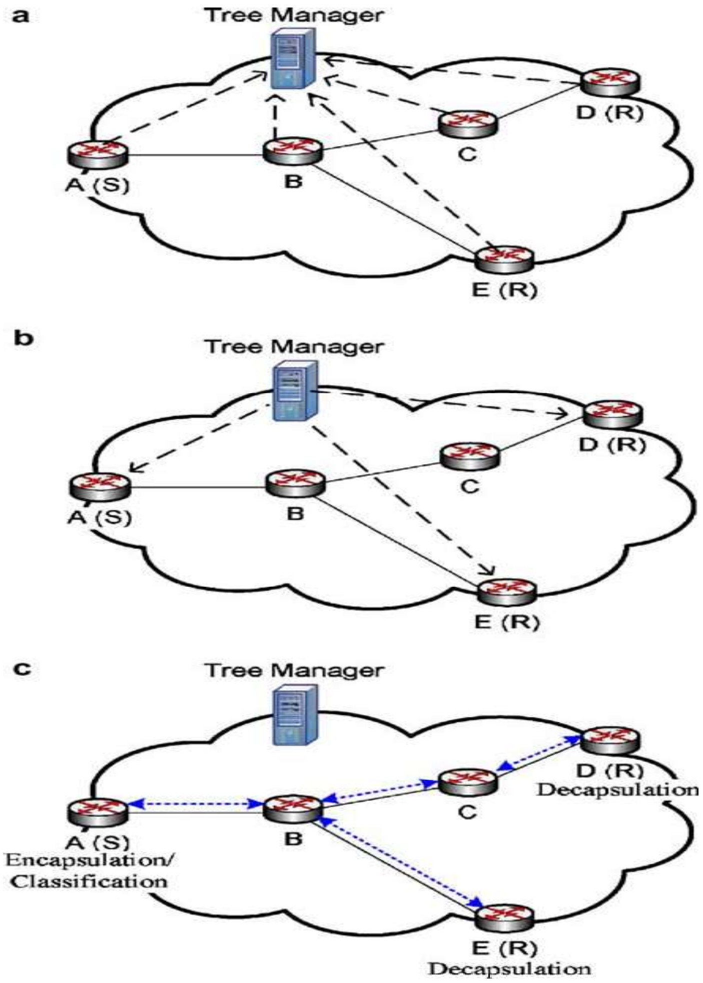

Figure 5: Picture of Aggregated QoS Multicast:
(a) membership, QoS requirement, link-state, and available bandwidth collection;
(b) group–tree matching entry distribution;
(c) multicast group packets transmitting on established aggregated multicast tree.

Establishing a tree depends on what encapsulation technique is used. If IP encapsulation is employed, then a traditional IP multicast routing protocol can be adopted. If MPLS service is available, an appropriate multicast Label Distributed Protocol (LDP) needs to be used. We will show an MPLS-based AQoSM protocol to achieve our goal.

Multiprotocol Label Switching (MPLS) emerges as an important traffic engineering technology for the Internet. It uses label switching technique. In an MPLS domain, when a stream of data traverses a common path, a Label Switched Path (LSP) can be established using MPLS signaling protocols. At the ingress Label Switch Router (LSR), each packet (FF02:0:0:0:0:1:FF00:0000) is assigned a label and is transmitted downstream. At each LSR along the LSP, the label is used to forward the packet to the next hop. MPLS-based VPNs are emerging as the popular choice by service providers to build IP VPN due to their scalability, flexibility, cost and the ability to provide IP applications with QoS across the network[1,13]

In MAQoSMP, the tree manager is implemented in a distributed fashion. We distribute the functionalities of tree manager into the core nodes within the backbone domain. The set of possible cores are advertised using the bootstrap mechanism. When an edge router receives a join message for a group g, it classifies this multicast flow into a Diff-Serv behavior aggregate based on the QoS service requested. To map this multicast group onto an aggregated tree, it determines a core using a hash function (which we call group-to-core hash function). This core is referred to as the default core C_0 for the group g.

Upon receipt of a request from g relayed by the corresponding edge router, C_0 will find or compute a proper aggregated tree for group g by conducting group–tree matching algorithm and admission control. When a multicast packet arrives at the ingress router, the Multicast Label Distributed Protocol label it, and send it to the destination.

3.8. Joining-Leaving Members

When an edge router r receives a request to join a group g from outside domains, it first uses the group-to-core hash function to get g's default core C_0, and then sends a message JOIN(g) to C_0; C_0 triggers its tree manager module to find or establish an appropriate aggregated tree (e.g., (c', T), since an aggregated tree is identified by a combination of the core's IP address and a class D address). It should be noted that this join message might activate tree switch or core switch if the existing tree could not cover group g (the details will be discussed in the following subsections). Then the corresponding group–tree matching entry is sent back to r through a message JOIN-ACK(g, (c', T)). r adds this entry to its group–tree matching table for the purpose of assigning MPLS labels to incoming packets, and employs the distributed bi-directional MPLS tree setup procedure if this tree has not been constructed.

Similarly, when an edge router r wants to leave a group g, it sends a LEAVE(g) message to its core C_0. On receiving of the LEAVE message, C_0 manipulates the group–tree matching algorithm, which might also cause tree switch or core switch. As the tree manager finds that all members in a group leave, it first sends LEAVE-ACK(g, (c', T)) message to notify the leaf routers of the tree, and then updates its own tables. If the tree is now obsolete, that is, when all groups mapped onto a MPLS tree terminate, the leaf routers remove label forwarding entries and propagate label withdraw messages to upstream routers to destroy the aggregated tree.

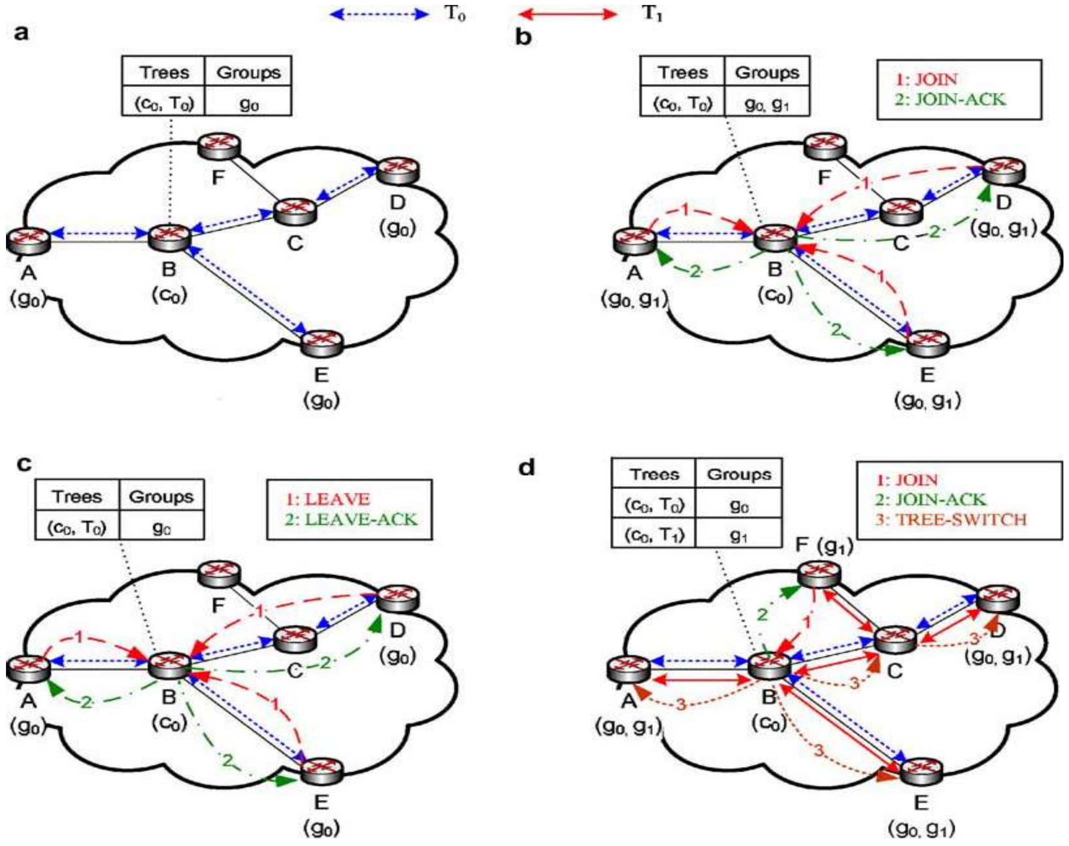

Figure 6 : getting online/offline state

(a) Initial state: group g_0 uses tree (C_0, T_0);

(b) Member join: group g_1 starts with members A, D, and E, and groups g_0

and g_1 share the tree (C_0, T_0);
(c) Member leave: group g_1 terminates;
(d) Tree switch: based on (b), a new member F joins group g_1, and g_1 switches from (C_0, T_0) to (C_0, T_1).

From a mathematical point of view, a communications network can be regarded as a collection of resources (physical links) with a finite service capacity (bandwidth). A flow using a single path is defined as a pair of objects, a route or subset of the links, and a bandwidth allocation in every link traversed[12]. Whenever a source node has packets to send to a destination and is not aware of any path to the latter, the source initiates a flooding-based route discovery procedure by sending a broadcast Multi-path Route Request (MP-RREQ) message to its neighbors, as well as if an intermediate node could not forward the data packet due to a broken link, the upstream node of the broken link informs about the broken route to the source node through a Multi-path-Route-Error (MP-RERR).

3.9. CONCLUSION

To sum up, MPLS is an efficient, effective and robust solution to achieve the requirements of IP backbone networks by allowing resource optimization and fast failure recovery.

In this paper we discuss about the problem of group multicast routing as defined by the following:

Given an existing network (Communication Service of Alternative Group) with known unicast traffic, find the optimal link capacity assignment to accommodate the multicast traffic generated by a group of multicast sources. The optimality has to be defined on the basis of the type of services conveyed through the multicast sessions and the operator objectives; yet, bandwidth usage and transmission delay are widely used in this context.

MPLS facilitates explicit routing, since the sequence of LSRs to be followed need not be carried in the packet header as in conventional datagram networks. One useful application of explicit routing is traffic engineering that is intended to maximize resource utilization in the network; the inefficient use of resource by using hop by hop routing in some situations may cause some links to be congested while some others are lightly loaded.

As we have discussed, QoS multicast provisioning is a multifaceted problem, involving routing, admission control, resource management and many other issues. Our goal is to provide efficient and practical solutions for those issues. Based on our proposed ALMI architecture, we develop a protocol using MPLS technique. Our analysis and simulation study shown that the developed MAQoSMP protocol is efficient, scalable, feasible, and implementable.

Acknowledgements.
This work is dedicated to my loved sister Patricia WAYAWO who i have lost during these research times; let God bless you in that part of world where you are. I cannot finished my knowledgements without expressing my gratitude to all of those who serve as guides, specially our professor LIU Lan who was willing, ready and available to give help and guides, be Blessed !.

***Terminology Table**:*

MPLS: Multi-Protocol Label Switching
QoS: Quality of Service
ALMI: Application Layer Multicast Infrastructure
CSAG: Communication Service of Alternative Group
ICMPv6: Internet Control Message Protocol version6
MLD: Multicast Listener protocol
IPv6: Internet Protocol version6
IPsec: Internet Protocol Security
MTU: Maximum Transmission Unit
MAQoSMP: MPLS-Based Aggregated Quality of Service Multicast Protocol
MLDP: Multicast label Distributed Protocol
LSP: Label Switched Path
LSR: Label Switched Router
ACK: Acknowledgment
DiffServ: Differentiated Service
IntServ: Integrated Service

IS: Intermediate System
HAN: Home Area Network
RIP: Routing Information Protocol
SW: Server Weight
SA: Server Agent
BB: Bandwidth Broker
OSPF: Open Shortest Path First
BGP: Border Gateway Protocol
IETF: Internet Engineering Task Force
IPng: Internet Protocol next generation
WRS: Weighted Random Selection
DVMRP: Distance Vector Multicast Routing Protocol
MIGP: Multicast Interior Gateway protocol
CBT: Core-Based Tree
IGMP: Internet Group Management Protocol
PDV: Personal Digital Assistant
BGMP: Border Gateway Multicast protocol
AS: Autonomous System
UDP: User Datagram Protocol
TCP/IP: Transfer Control Protocol/ Internet protocol
PIM: Protocol Independent Multicast
MSA: Multicast Security Association
BPF: Berkeley Packet Filter.

References.

[1] Communication Networks: Fundamental concepts and key architectures -[1999]

[2] AQoSM: Scalable QoS multicast provisioning in Diff-Serv networks, Jun-Hong Cui , Li Lao , Michalis Faloutsos , Mario Gerla. -May 2005

[3] Fang Hao, Zegura Ellen , and Mostapha Ammar, QoS Routing for Anycast Communications -August 2002.

[4] Ayman El-Sayed Ahmed EL-SAYED, Application-Level Multicast Transmission Techniques Over The Internet. -March 2004

[5] Nicolas Bonmariage, Guy Leduc. A survey of optimal network congestion control for unicast and multicast transmission. -July 2005

[6] Natarajan Meghanathan. A location prediction based routing protocol and its extensions for multicast and multi-path routing in mobile ad hoc networks. -December 2010

[7] Nakaniwa et al, An Integrated End-to-End QoS Routing on Different Service -March 2007.

[8] Rozita Yunos, Noorhayati Mohamed Noor, Siti Arpah Ahmad. Performance Evaluation between IPv4 and IPv6 on MPLS Linux Platform.

[9] Lin et al A load-balanced anycast routing scheme based on the WRS- 2007.

[10] Wu-Hsiao Hsu ,Ming-Chih Tung b, Li-Yuan Wu. An integrated end-to-end QoS anycast routing on DiffServ networks -January 2007.

[11] Salekul Islam, J. William Atwood, Sender access and data distribution control for inter domain multicast groups -January 2010.

[12] Pablo J. Argibay-Losada *, Andrés Suárez-González, Cándido López-García, Manuel Fernández-Veiga. A new design for end-to-end proportional loss differentiation in IP networks -December 2009.

[13] ChryssaA.Papagianni, NikolaosD.Tselikas, EvangelosA.Kosmatos, Stauros Papapanagiotou, Iakovos S.Venieris, Performance evaluation study for QoS-aware triple play services over entry-level xDSL connections -March 2008.

[14] Implementing IPv6 Addressing and Basic Connectivity. CISCO System -November 2010.

[15] Xingwei Wang, Lei Guo, Fei Yang, Tengfei Wua, Wei J. Multi-

layer survivable routing mechanism in GMPLS based optical networks.
- February 2008.
[16] Chun-Yen Hsu,, Jean-Lien C.Wu, Shun-TeWang, Chi-Yao Hong. Survivable and delay- guaranteed backbone wireless mesh network design. -May 2007.
[17] Chun-Hung Liu and Jeffrey G. Andrews, Multicast Outage Probability and Transmission Capacity of Multi hop Wireless Networks -October 2010.
[18] D. DiSorte, M. Femminella, G.Reali, QoS-enabled multicast for delivering live events in a Digital Cinema scenario. -February 2008
[19] Yong Xi, Mooi Choo Chuah. An encounter-based multicast scheme for disruption tolerant networks -October 2008.
[20] Wai tian Tan, Avideh Zakhor, Multicast Transmission of Scalable Video using Receiver-driven Hierarchical FEC. University of California.
[21] Tolga Girici, Asymptotic throughput analysis of multicast transmission schemes -July 2008.
[22] Reza Tadayoni , Halldo r Matthı´as Sigurðsson. Development of alternative broadband infrastructures – Case studies from Denmark -2007.
[23] Aman El SAYED, Institut Polytechnique de Grenoble: Mathématiques, Sciences et Technologie de l'information.
[24] Mojtaba Hosseini, Dewan Tanvir Ahmed, A Survey of Application-Layer Multicast Protocols -2005.
[25] ChaeY. Lee, Hee K. Cho, Discrete bandwidth allocation considering fairness and transmission load in multicast networks -March 2006.
[26] L. Sanna Randaccio, L. Atzori. Group multicast routing problem: A genetic algorithms based approach -April 2006.
[27] Hind Castel-Taleb, Mohamad Chaitou, Gérard Hébuterne, Optical MAN ring performance with traffic aggregations. -April 2010

Bibliography

I'm presently working as IT Service&Project Manager in International Commission of Basin Congo by development of hydrological applications Database. I'm Master in Communication Engineering in Wuhan University of Technology in China (2012). My main research interest areas is concerning by the control of QoS in next generation Internet Protocol (IPng)-best-effort Transmission and connection-oriented network (ATM, MPLS).

LIU Lan is currently Professor Teaching "Recognition Model" in Wuhan University of Technology; he is coordonator of Teacher's research group in this school. His main research center is concerning by the Advanced Networks Technologies.