ISSN: 0128-7680
Pertanika J. Sci. & Technol. Supplement 9(2):159-172 (2001)

Bandwidth Management for Intranets Using Multicast Firewalls

Tat Chee Wan[1], Chee Hoong Leong & Ronnie Chee Weng Thum
Network Research Group
School of Computer Science
University of Science Malaysia, 11800 Penang
tcwan@ cs. usm.my

ABSTRACT

Multimedia applications utilizing multicast transmission techniques are becoming prevalent as the number of users and types of applications proliferate. Nonetheless, the deployment of such applications throughout an Intranet is constrained by the lack of multicast capable routers and the inability to protect the network from being swamped by multicast traffic. Multicast firewalls are designed to overcome these limitations. The roles of a multicast firewall are to:

- Perform multicast packet forwarding in place of tunneling across existing routers for an Intranet
- Perform packet replication optimization via multicast group management (multicast spanning tree management)
- Perform subnet bandwidth management, by assigning priorities to multicast addresses and filtering (dropping) packets for each group according to specified criteria

This paper outlines requirements for multicast firewalls, as well as describes an implementation of a dual-LAN multicast firewall prototype implemented using Linux.

Keywords: Multicast, firewall, bandwidth management, intranet, H. 323, multimedia applications

INTRODUCTION

The development of multicasting as the vehicle for multimedia content delivery has resulted in the proliferation pf new applications that take advantage of the bandwidth optimization of multicast transmission. Nonethe less, enabling such applications to operate in an Intranet environment necessitates the use of multicast capable routers that are still in limited use. Multicast tunneling, while effective, introduces additional bandwidth requirements to support the following environment (Wan, T. C. et al. 1998):

- Lack of multicast capable routers in most Intranets constrains the development of multicast applications
- The cost of implementing tunneling to forward multicast packets among the various subnets may not be acceptable if several multicast applications are active simultaneously
- Lack of Quality of Service (QoS) capabilities in current contention-based network (e.g. Ethernet) may result in multicast data consuming all available bandwidth in each subnet, causing network congestion.

The emergence of H. 323 based system for multimedia applications has greatly increased the need for suitable mechanisms to control the flow of multimedia data through non-QoS capable network. The multicast firewall is introduced in order to overcome the bandwidth bottleneck and address the fundamental concern of deploying such applications that they use up significant network bandwidth, sometimes to the detriment of existing data applications. This device operates in parallel with existing routers to provide routing and bandwidth management of multicast traffic used by multimedia applications.

Background

Intranets are campus-wide or office-wide network that have been subneted to reduce traffic congestion. Each managed subnet using the firewall in connected to both the subnet router and the firewall in parallel. The existing subnet routers handle unicast traffic, while the firewall handles multicast traffic. This configuration is suitable for Intranets since the subnet routers are typically co-located via the use of multi-slot hubs.

The role of a firewall is to filter network packets based on some given criteria, to allow or deny access to certain network resources. However, current firewalls do not handle multicast traffic effectively, since they operate at the OSI Network Layer (Layer 3), typically in conjunction with a router. Since most routers do not forward multicast packets, the firewalls are designed to handle only unicast traffic between subnets. In addition, multicast packets are more efficiently processed at the Data Link Layer (Layer 2) since multicast data utilizes special MAC layer addresses to perform its task and can be easily identified via their MAC addresses.

Definition of Multicast Firewall

The features of a Multicast Firewall are:

- Perform multicast packet forwarding in place of tunneling across existing routers for an Intranet
- Perform packet replications optimization via multicast group membership management (multicast spanning tree management)
- Perform subnet bandwidth management, by assigning priorities to multicast addresses and filtering (dropping) packets for each group according to specified criteria.

While the first two features are present in multicast capable routers, the third features is what differentiates the multicast firewall from such routers. Bandwidth management is a basic from QoS where limits are set for the percentage of bandwidth consumed for multimedia and normal data traffic. While it is not possible to enforces QoS for contention -based networks such as Ethernet, the use of bandwidth management would ensure that multicast data do not overwhelm all available network resources to the extent that both multicast and non-multicast applications are not able to utilize the network at all. Since multimedia applications (which typically utilize multicast transmission) are able to tolerate some data loss, bandwidth management would enable such applications to share available network resources instead of requiring that a new network be setup solely for multimedia traffic.

The prioritization of multicast addresses provides additional control over the usage of the allotted multicast bandwidth where higher priority applications such as videoconferencing using a given multicast address would have better QoS compared to lower priority applications such as data delivery. Above the maximum threshold, all multicast packets are dropped.

TUNNELING VS. FORWARDING

Multicast Packet Tunneling

Although the development of VLANs has reduced the need for routers in the Intranet, routers are still needed to interconnect VLANs to each other. In this respect, VLANs are identical to physical LANs and require interLan multicast packet forwarding (Passmore and Freeman).

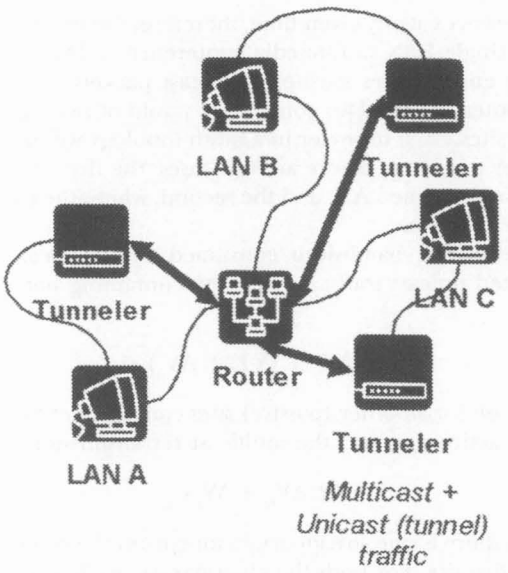

Fig. 1. Function of Multicast Tunneler and Intranet Router

Tunneling is one of the ways to support multicast applications throughout an Intranet with non-multicast capable routers. This is accomplished by placing a tunneling device (tunneler) on each LAN, whose function is to receive multicast packets, encapsulate it into a unicast packet to send it through the router to a tunneler on the other LAN which would then decapsulate it for retransmission. While this method provides a means to interconnect different LANs, it also incurs significant bandwidth in order to support a given multimedia stream (Wan T. C. et al. 1998). In addition, one tunneler is required for each Lan to support this scheme. This is the technique used in the MBONE to support multicast across the existing Internet.

Tunneling Overhead

Given that a multicast network is interconnected via a complete mesh topology, we can derive the worst case bandwidth utilization required to support a typical multimedia videoconferencing session for several participants. In a given system (Sureswaran, R. 1997), up to two participants are able to transmit their audio and video at any given time. One participant is termed the 'chairman' while the other is the 'active participant'. Other participants, termed 'passive participant' are able to observe the communications between the two.

Let the multicast video stream bandwidth for a given videoconferencing client be V_{m3} and the multicast audio stream bandwidth be A_m, assuming identical bandwidth requirements for all clients. The unicast tunneled equivalent of multicast streams are V_u and A_u where Vu =kV_m and $A_u = kA_m$. k 1 represents the overhead due to the unicast header. For simplicity, we can assume k= 1 if the overhead is negligible.

Therefore, the multimedia stream bandwidth $AV_m = (A_m + V_m)$ videoconferencing client. The respective clients perform compression, so SV_m represents the net bandwidth utilization per multimedia stream. Since full duplex transmission is generated by two simultaneously active clients (a chairman and an active client) to every client (active and

passive) of the conferences at any given time, therefore, the multicast network bandwidth utilization within a single LAN multimedia conference is $2AV_m$.

Since tunneling encapsulates existing multicast packets for retransmission via the same LAN to the router, a Multi-Lan conference would of necessity consume additional bandwidth. Given Y sites, each tunneler in a mesh topology will need to tunnel an active stream to (Y-1) other tunnelers. There are two cases: the first where both the chairman and active client is on the same LAN, and the second, where the chairman and the active client are on different LANs.

For the first case, total bandwidth consumed by the local multicast traffic and tunneler retransmitted unicast traffic for the site containing both chairman and active client is:

$$2(AV_m + (Y\text{-}1) * AV_u)_{out} \quad (1)$$

The network utilization for all other (passive) sites consisting of the unicast tunnel traffic from the chairman/active site, and the multicast retransmission is:

$$2(AV_m + AV_u)_{in} \quad (2)$$

For the second case, there is one stream originating from the chairman site, and another coming from the active site. For both the chairman as well as the active site, the total traffic due to the conference is:

$$(AV_m + (Y\text{-}1) * AV_u)_{out} + (AV_m + AV_u)_{in} = (2AV_m + (Y^* AV_u))_{total} \quad (3)$$

Whereas for the other (passive) sites, the traffic remains as $2 (AV_m + AV_u)_{in}$

Multicast Packet Forwarding

In contrast, we place the firewall device in parallel with the router to interconnect two or more subnets requiring multicast support. In this way, connectivity between subnets is provided via the router for unicast packets and via the firewall for multicast packets. Making an additional connection among the LAN segments and the firewall is easy to achieve for an Intranet environment, since most Intranets rely on hub-based subnet routers in a collapsed backbone configuration at a single firewall with N ports will suffice. In addition, no additional bandwidth is utilized to support the forwarding of multicast packets, since the forwarding function is performed within the firewall device and not via tunneling through routers.

Packet forward can be performed at the Data Link Layer(Layer 2) or Network Layer (Layer 3). For performance reasons, Layer 2 packet forwarding is more efficient and provides better throughput. Existing firewall are all based on Layer 3 processing techniques. This is due to the application (and hence IP port) specific nature of most firewall. In contrast, Layer 2 processing is used by the multicast firewall since multicasting utilizes specific Layer 2 address formats that are clearly distinguishable from other types of traffic.

Forwarding Overhead

Forwarding results in each LAN incurring constant traffic overhead regardless of the location of the chairman and the active participant:

$$2 (AV_m) \quad (4)$$

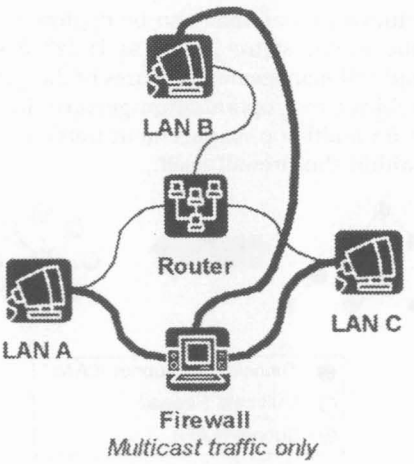

Fig. 2. Function of Multicast Firewall and Intranet Router

Therefore, it can be seen analytically that multicast forwarding will perform better in an environment where bandwidth usage is critical, since it is inherently more scalable compared with tunneling.

MULTICAST GROUP MANAGEMENT

Multicast Spanning Tree with Multiple Hops

In order to establish a multicast session among clients in different subnets, a multicast group management protocol must be operational. For H.323 based system, gatekeepers are tasked with the management of session members using H. 225 signaling (Web Proforum Tutorials 1998), (Databeam 1998), while for the Internet MBONE, IGMP is used to add or remove session members from the multicast spanning tree are used in place of complete mesh configurations to optimize the transmission of data from a multicast source to the intended receivers through an arbitrary subnet topology. Data and management packets have to be forwarded through intermediate hops in a typical multicast spanning tree (Wan et al. 1998).

Collapsed Spanning Tree with Single Hop

In a typical Intranet, a star configuration is used to interconnect the various subnets via a collapsed backbone router. Such a configuration simplifies the network topology and ensures that only inter-subnet traffic is carried on the backbone. The Multicast Firewall implements a star configuration parallel to the router to handle multicast traffic. Effectively, the multicast firewall collapses the multicast spanning tree growth and pruning is limited to control packets to and from the firewall itself, while each subnet is only one hop away from the multicast source via the firewall. In addition, multicast tree optimization is greatly simplified since the packet forwarding is performed internally to the firewall. Multicast packets replication in this scenario implies copying received data from one memory buffer to each destination subnet network interface.

Performing the group management and multicast tree optimization within the firewall eliminates the network overhead associated with spanning tree creation and protocol packet forwarding inherent in DVMRP and MOSPF that was designed for operation on the Internet rather than an Intranet (Stallings, W 1998).

Alternatively, the multicast firewall may also be deployed in environments where a gatekeeper configures the multicast tree, such as H.323 based system. The firewall complements the zone and call management features of the gatekeeper (Web Proforum Tutorial 1998) via its multicast tree optimization geature. In either case, the network overhead is similar since no multi-hop management traffic is generated as inter-subnet connectivity is handled within the firewall itself.

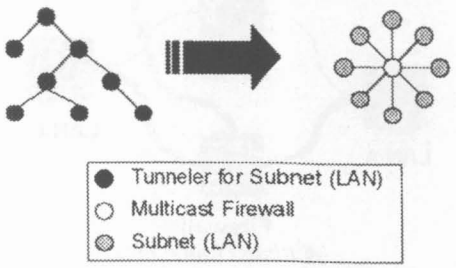

Fig. 3. Optimization of Multicast Spanning Tree

BANDWIDTH MANAGEMENT FOR PSEUDO-QOS SUPPORT

This provides the crucial functionality of the firewall. Bandwidth management is defined via:

- a bandwidth usage policy that addresses multicast traffic prioritization
- a bandwidth sampling mechanism to determine the current network load of each subnet
- a filtering mechanism that implements the policy based on the sampled network load for each subnet

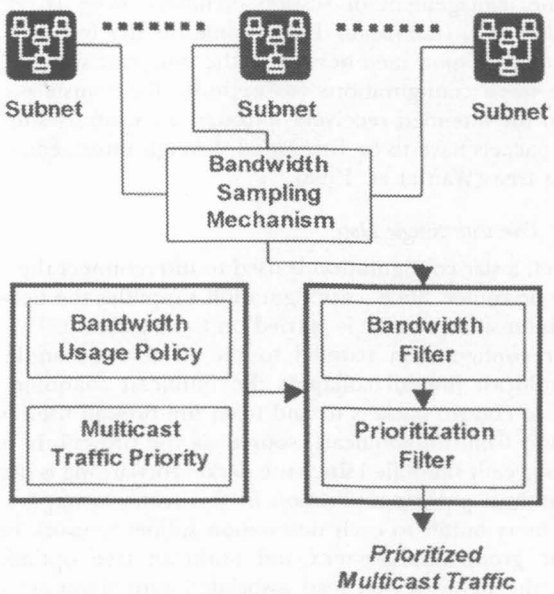

Fig. 4. Bandwidth Management Policy and Mechanism

In Ethernet type network, the lack of QoS capabilities precludes the ability to guarantee bandwidth usage for multimedia applications (Raghavan and Tripati 1998), (Web Proforum Tutorial 1998), (Databeam 1998). The multicast firewall takes advantage of the ability of multimedia applications to tolerate packet loss to perform its bandwidth management function. As such, the bandwidth management capability of the multicast firewall is not intended for guaranteeing multimedia applications QoS but instead, to provide reasonable QoS for multimedia applications by preventing multicast traffic from overwhelming the capabilities of the network to carry both normal and multicast packet forwarding into a given subnet such that the additional traffic is within the bounds specified by the network administrators via the Bandwidth Usage Policy.

Bandwidth Usage Policy

The Bandwidth Usage Policy defines the lower subnet bandwidth and upper subnet bandwidth thresholds for which multicast bandwidth management will be enabled (Figure 5). The subnet bandwidth is the value obtained by the Bandwidth Sampling Mechanism for each subnet indicating the existing traffic is below the lower subnet bandwidth threshold, then no multicast bandwidth management is required. In effect, all multicast packets that are destined for given subnet are forwarded to the subnet.

If the existing subnet traffic is above the upper subnet bandwidth threshold, then all multicast packet forwarding is disabled since the network is in a congested state. Instead of competing with other applications for bandwidth that is insufficient for multimedia applications usage, the firewall stops intersubnet multicast forwarding until subnet traffic returns to a normal level. In between the two thresholds, there is graceful degradation of QoS for multicast applications defined via the Multicast Traffic Priority policy.

The Multicast Traffic Priority is a filtering criterion that divides the available multicast bandwidth given by (upper threshold - lower threshold) into several priority thresholds. If the utilized bandwidth exceeds the given priority threshold for the packet, then it will be dropped, while packets with higher priority will still be forwarded. Multicast priority is defined based on the multicast address. While this is a crude mechanism for defining priority, most applications choose different multicast addresses for different multimedia streams and is therefore well suited to this traffic prioritization scheme.

This Bandwidth Usage Policy can be managed dynamically by the H.323 gatekeeper to fine tune allocated bandwidth for inter-subnet multicast data streams. In addition, the multicast firewall extends the basic bandwidth control offered by H.323 (request, confirm and reject) with multicast priority features.

Bandwidth Sampling Mechanism

The Bandwidth Sampling Mechanism involves determining the level of traffic on each subnet. This is achieved by placing the Network Interface Card (NIC) into promiscuous mode in order for the firewall to receive every packet in the subnet. Statistics about bandwidth utilization (traffic level), such as total packets on subnet, type of packets, and percentage utilization of subnet bandwidth, are calculated in real time in order to provide the Bandwidth and Prioritizations Filters with the necessary data to perform drop/forward decisions.

Bandwidth and Prioritization Filters

The bandwidth filter performs preliminary processing on the received packets. If the received packet is not a multicast packet, then it is automatically dropped, since it is

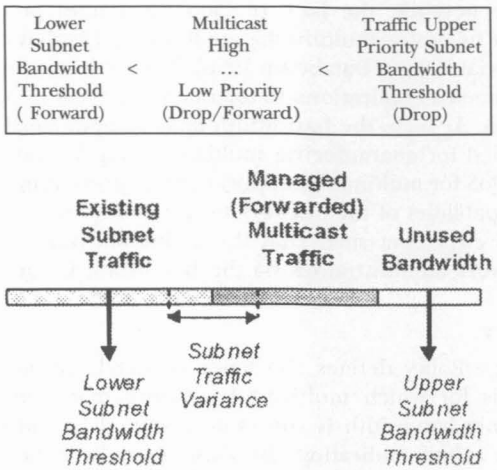

Fig. 5. Multicast Bandwidth Management for non-QoS capable network

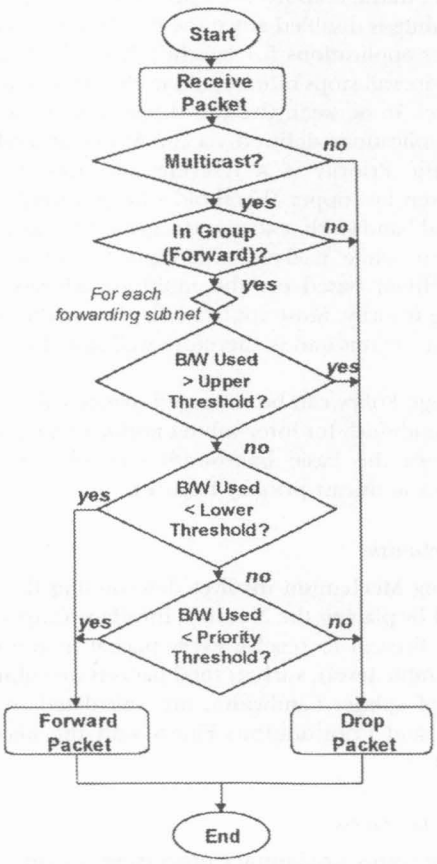

Fig. 6. Bandwidth and Prioritization Filters

handled by the Intranet router. A multicast packet is examined to determine if it should be forwarded to specific subnets based on the Multicast Group Information. If the multicast packet is to be forwarded, then the bandwidth utilization for each subnet that requires packet forwarding is examined in turn.

If the subnet bandwidth utilization is above the upper threshold, then it is dropped immediately. Otherwise, if it is below the lower threshold, then it is forwarded automatically. For bandwidth utilization in between the two thresholds, the packet must first be classified to determine its priority. Packets with priority thresholds above the current bandwidth utilization will be forwarded, while those with thresholds below the current utilization will be dropped. This is illustrated in Figure 6.

PROTOTYPE IMPLEMENTATION

A prototype multicast firewall for two subnets has been successfully implemented for the Linux environment. Linux was chosen for the implementation as it is robust and had good performance on moderately powerful hardware , while providing well established BSD style Sockets API for accessing NICs at the Data Link level. In addition, Linux provides support for multiple NICs on the same machine, making it easy to implement and test the performance of the prototype.

A web-based configuration front-end was also developed to ease the monitoring and parameter configuration of the firewall. This subsystem used Apache web server with Perl scripts to interface the firewall to HTML browsers, enabling remote management and monitoring.

In the prototype, bandwidth and priority thresholds are managed manually via the web interface. This capability can be automated in a production firewall by providing support for H.323 control signaling or IGMP protocols.

The bandwidth sampling mechanism update its statistics every second, providing a snapshot of the state of the network as a discrete sampling function.

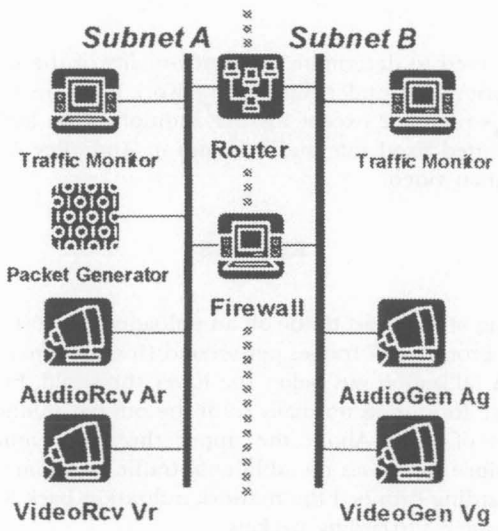

Fig. 7. Prototype Firewall Setup

Design of Experiment

The prototype firewall was attached to two isolated subnets A & B within the lab using the setup given in Figure 7, with traffic monitors and packet generators placed in each subnet to monitor and control the unicast traffic load on the resoective subnet. For the purpose of these experiments, audio multicast stream have higher priority than video multicast streams. The audio stream A and video stream V were assigned different multicast addresses so that the firewall could prioritize them appropriately. Multimedia stream generators Vg and Ag in Subnet B generate multicast data that were forwarded to receivers Vr and Ar in Subnet A via the firewall.

The firewall lower subnet bandwidth threshold was set to 10% while the upper threshold was set to 30%. Subnet A has a packet generator to simulate unicast traffic loading to test the performance of the firewall.

Experiment 1

This experiment was used to determine the functionality of the firewall in performing bandwidth management on Subnet A. VideoGen Vg transmitted video frames at 12 frames per second to VideoRcv Vr. The Packet Generator generated unicast traffic to create different loading conditions on Subnet A & B monitors on Subnet A & B monitored the packets transmitted, received and dropped, as well as bandwidth utilization on each subnet due to the multicast traffic.

Experiment 2

This experiment was used to determine the functionality of the firewall in performing bandwidth management on Subnet A. VideoGen Vg transmitted video frames at 12 frames per second to VideoRcv Vr. The packet Generator generated unicast traffic to create different loading conditions on Subnet A. Traffic monitors on Subnet A & B monitored the packets transmitted, received and dropped, as well as bandwidth utilization on each subnet due to multicast traffic and total traffic.

Experiment 3

This experiment was used to determine the functionality of the firewall in performing multicast stream prioritization under different network loads on subnet A. The settings were identical to Experiment 2 except for the addition of an audio multicast stream. AudioGen Ag transmitted fixed rate audio frames to AudioRcv Ar. In addition, audio had higher priority than video.

RESULTS

Experiment 1

In Table 1, the loading of multicast traffic on an unloaded network due to various frame rates were tabulated. From 2 to 7 frames per second (fps), minimal loss was observed as the traffic bandwidth utilization was below the lower threshold. From 12 fps to 17 fps, multicast packets were forwarded normally until the offered multicast traffic exceeded the upper threshold of 30%. Above the upper threshold, multicast packets were dropped. However, since there was no additional traffic in Subnet A, the throttling of multicast traffic forwarding dropped the network utilization back to 0%, at which point the firewall would resume forwarding packets.

The bandwidth sampling mechanism updated statistics every second.Effectively, this resulted in 50% throughput for the multicast stream since traffic in Subnet A alternated between 0% and 35% every second. In addition, a video stream Vg of 12 fps, which was

TABLE 1
VideoGen (Vg) vs. packets Transmitted (Tx), Received (Rx), and Dropped (Drp) and Corresponding network utilization for Transmit (T x BW) and Receive (R x BW) (all multicast). fsp: frame per second; pps: packets per second Net %: Network Bandwidth Utilization Percentage.

fps	pps			Net%	
Vg	Tx	Rx	Drp	TxBW	RxBW
2	26	25.5	0.5	3	3
7	92	90	2	11	11
12	157	155	2	19	19
17	223	220	3	27	27
22	288	138	150	35	17

about 19% of total network bandwidth, was chosen as the reference multicast bandwidth for subsequent experiments.

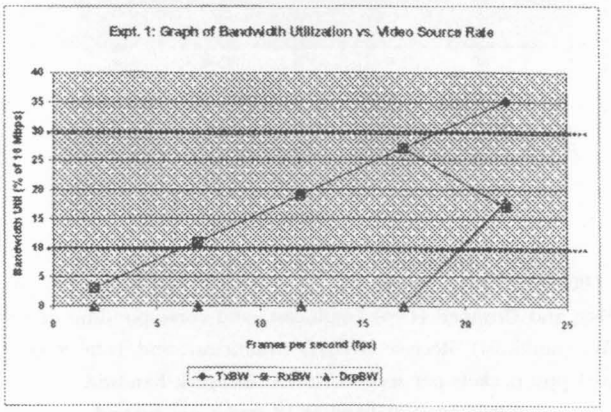

Fig. 8. Graph of Bandwidth Utilization vs. Video Source Rate

TABLE 2
Packet Generator (PG) on Subnet A (unicast) vs. packets Transmitted (Tx), Received (Rx), and Dropped (Drp) (multicast) and corresponding network utilization for Transmit (TxBW) (multicast), Receive (RxBW) (multicast), and Total Received (TotRxBW) (unicast +multicast) pps: packets per second Net% : Network Bandwidth Utilization Percentage VideoGen (Vg) fixed at 12 frame per second.

Net%	pps			Net%		
PG	Tx	Rx	Drp	TxBW	RxBW	TotRxBW
0	157	156	1	19	18	18
5	157	155	2	19	19	24
10	152	150	2	20	20	30
15	157	140	17	19	15	30
20	158	124	34	19	7	37
50	158	25	133	22	0	50

Experiment 2

As can be seen from Table 2, Minimal loss was observed when the unicast traffic level in Subnet A was below the lower threshold. Above 10% unicast traffic, the firewall started to discard multicast packets until no multicast packets were forwarded when unicast traffic level exceeded 30%. However, multicast traffic was still being forwarded with the unicast network utilization at about 30% due to the throttling effect seen previously.

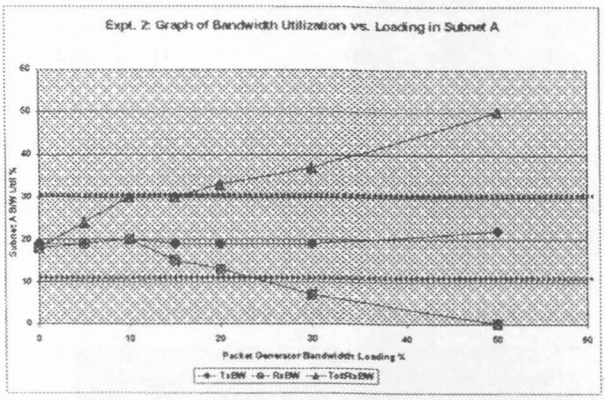

Fig. 9. Graph of bandwidth utilization vs. Loading in Subnet A for single multicast session

TABLE 3

Packet Generator (PG) on Subnet A (unicast) vs. Video (V) and Audio (A) packets Transmitted (Tx), Received (Rx), and Dropped (Drp) (multicast) and corresponding network utilization for Transmit (TxBW) (multicast), Receive (RxBW) (multicast), and Total Received (TotRxBW) (unicast + multicast) pps: packets per second Net %: Network Bandwidth Utilization Percentage VideoGen (Vg) fixed at 12 frame per second.

Stream	Net%	pps			Net%		
	PG	Tx	Rx	Drp	TxBW	RxBW	TotRxBW
A	0	9	8.5	0.5	0.5	0.5	11.5
V		157	136	21	18	11	
A	5	9	8.5	0.5	0.5	0.5	13.5
V		157	100	57	19	8	
A	10	9	8.8	0.2	0.5	0.5	17.5
V		155	78	77	19	7	
A	15	8	7.8	0.2	0.5	0.5	20.5
V		157	0	157	18	0	
A	30	9	8.3	0.7	0.5	0.5	30.5
V		157	0	157	18	0	

Experiment 3

The results given in Table 3 illustrated the effect of multicast prioritization on two different multicast stream. The high priority of the audio stream ensured that the audio

receiver encountered packet drop even at minimal bandwidth utilization due to the choice of priority levels. Since 10% bandwidth utilization was the lower threshold, while the video stream contributed lower threshold, while the video stream contributed around 19% of bandwidth utilization, selective discard of video data was initiated from the very beginning. The priority level chosen for the video data also meant that the stream became completely blocked once 15% total bandwidth utilization was exceeded on Subnet A. This ensured that the higher priority audio stream remained active even when the traffic conditions increased beyond that threshold.

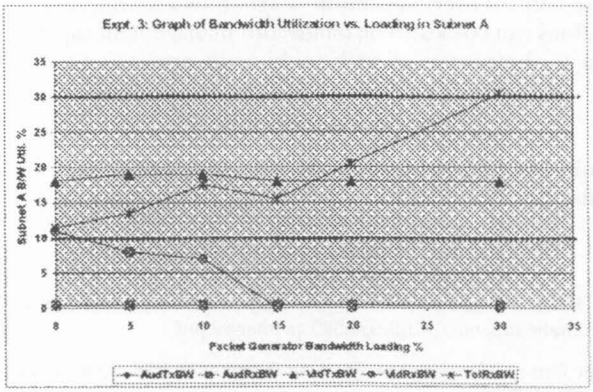

Fig. 10. Graph of bandwidth utilization vs. loading in Subnet A for two multicast sessions with dual traffic priorities.

DISCUSSION

As can be seen from the above experiments, the choice of network bandwidth thresholds and prioritization levels are critical for the operation of the multicast firewall. The ability to observe the performance of the firewall in real time via the web interface helps system administrators to determine the optimal threshold values for given network. A web-based remote management capability also simplifies administration of the firewall.

In addition, the behavior of the bandwidth sampling mechanism is important in providing fine-grain control for network bandwidth management. The prototype firewall utilized a discreate bandwidth sampling function that updated its statistics once every second. This resulted in rather erratic performance of the bandwidth filters since exceeding the upper threshold would cause multicast forwarding to cease completely for the next second. A continuous bandwidth sampling function would provide finer-grained statistics to enable the bandwidth filters to operate smoothly at the upper bandwidth threshold.

FUTURE DIRECTIONS

Work is currently being done to extend the firewall to multiple LAN's. A neural network-based bandwidth sampling estimation module is being investigated to derive a continuous sampling function, to implement smoother operation of the bandwidth filters. This will be used to address the sharp cutoff of multicast traffic experienced by the prototype firewall.

Source-based traffic shaping is another area that is being investigated in order to provide more QoS type of bandwidth management features to complement the capabilities

of the multicast firewall. The traffic shaper obtain bandwidth utilization data from the firewall in order to tailor its multicast traffic profile to meet application QoS requirements. It is expected of end-to-end bandwidth management semantics to support different classes of real -time multimedia applications effectively in Intranets.

CONCLUSION

Deployment of multicast applications such as multimedia conferencing system in a non-QoS capable Intranet is made possible by the use of multicast firewall. The firewall provides real-time control over bandwidth usage, thus ensuring that multicast and non-multicast applications can co-exist. The bandwidth management capability of the multicast firewall is crucial to the success of such multimedia applications.

ACKNOWLEDGEMENT

The authors would like to acknowledge the help of K. Saravanam, Dominic Choo Khai Shien and Christopher Aric Jihen in conducting the experiments for this paper.

REFERENCES

A Primer on the H.323 *Series* Standard, Ver.2.0, Databeam Corporation White Paper, May 1998, http://www. databeam.com/pdffiles/h323 primer-v2.pdf

FENNER W., Internet Group Management Protocol, Version 2, RFC 2236, IETF, Nov 1997, http://www.ietf.org/rfc/rfc2236.txt.

H.323 Tutorial, Web Proforums Tutorials, International Engineering Consortium, Dec 1998, http://www/ webproforum.com/acrobat/trillium.pdf

PASSMORE D., J. FREEMAN, "The Virtual LAN Technology Report," 3Com Corp. White Paper, http://www. 3com/nsc/2000374.html.T.C WAN, R. SURESWARAN, K. SARAVANAN, "Multiple LAN Internet Protocol Converter (MLIC) for Multimedia Conferencing," *Proceedings SEACOMM '98*, Penang, Malaysia, Aug. 12-14, 1998.

RAGHAVAN S. V., S. K. TRIPATHI, 1998. *Networked Multimedia System: Concepts, Architecture, and Design*, Upper Saddle, New Jersey: Prentice-Hall, , ISBN 0-13-210642-6

STALLINGS W., *High-speed network: TCP/IP and ATM design principles*, Upper Saddle River, New Jersey: Prentice-Hall, 1998, ISBN: 0-13-52965-7

SURESWARAN R. Using the RSW Control Criteria to Create Distribution Environment for Multimedia Conferencing, *REDECS'97*, Malaysia. Non 1997.

WAN T.C , R. SURESWARAN, K. SARAVANAN. 1998. Mutiple LAN Internet Protocol Converter (MLIC) for Multimedia Conferencing," *Proceedings ICIMU '98*, UNITEN, Kajang, Selangor, Malaysia, Sept. 28-30.