Simulating and Implementing a Proposed IP Multicasting Service in the Network of Isfahan University Based on IGMP-AC Multicast System

masoumeh adhami [1], iman halavati [2]

1: Kerman University of Medical Sciences, Kerman, Iran
2: Research Center for Modeling in Health, Institute of Futures Studies in Health, Kerman University of Medical Sciences, Kerman, Iran (Corresponding Author)
adhamimasomeh@yahoo.com

Abstract: In recent years, the use of internet has dramatic growth and communication services such as group chat, video conferences, online games, and simulation services which are mostly in the context of open networks such as the Internet have gained great popularity. In most of these applications, users will receive similar messages from one or more transmitters. Therefore, using techniques such as IP multicast is very useful because in this method, the data packets are sent to a group only once and they also pass through the link between two nodes only once and thus, compared to IP unicast, this method reduces bandwidths consumption. However, multicast IP, despite all its benefits, has not been widely implemented yet. One reason for this is insecurity and the lack of access control on receivers and senders of the multicast group. The openness of joining and leaving services for groups in the IP multicasting underlies a wide range of attacks usually DOS attacks. In recent years, various solutions have been proposed to address these problems. In this work, in order to solve the security problems of IP multicasting services, we will review existing models and solutions and focusing on the access control structure of IGMP-AC and evaluating its advantages and disadvantages, a new structure will be suggested to address these deficiencies. Therefore, the authors, in this work, tried to simulate and implement their proposed IP multicasting system. After successful simulation results, we have implemented this system on the network of Isfahan University and its performance have been tested in terms of some important parameters.
[Iman Halavati, Masomeh Adhami, Fatemeh Hasani, Maryam Okhovati, Kambiz Bahaadini, Alireza Adhami, Forough Jahandari, Azam Bazrafshan. **Simulating and Implementing a Proposed IP Multicasting Service in the Network of Isfahan University Based on IGMP-AC Multicast System.** *Life Sci J* 2013;10(7s):1071-1078]. (ISSN: 1097-8135). http://www.lifesciencesite.com. 171

Keywords: IP multicasting, multicast routing algorithms, access control, authentication, key group

1. Introduction

Multicast is a very good network service that delivers the data to a set of hosts who are members of a group. This service uses network bandwidth very effectively because the sender does not send the data to every host separately but it sends the data once and the routers within the network, according to their information, replicate the data on their output where it is needed.

Until now, many multicast routing protocols have been standardized by IETF including DVMRP [Waitzman, D., Partridge, C., Deering, S, 1988], PIM-SM 5 [Estrin, D., Wei, L., Farinacci, D., Helmy, A., Thaler, D., Deering, S., Handley, V., Sharma, P, 1995], and CBT [Ballardie, A, 1995]. Among different multicast routing protocols, PIM, due to its simplicity and other capabilities has more popularity in implementing intra-domain multicasting routing. PIM has its name from the fact that, it is independent from unicast routing protocols and can work with any other protocol such EIGRP - OSPF - BGP and so on [Multicast routing: PIM sparse mode and other protocols, White Paper, Spirent Communications, USA, November 2003]. Even in the case of static unicast routing, this protocol is still able to work.

Our proposed is based on an innovative method which is based on access control polynomial (ACP) [Zou, X., Shun Dai, Y., Bertino, E, 2008] over a finite field that is especially appropriate for dynamic environments where members enter log in and out frequently. This method not only meets the various requirements of security but also is secure against various attacks.

1.2. Assumptions used in this method

First, the ACP is created so that, the information is distributed in a way that only the authorized receivers with an ID in the form of $x - f(\mathrm{SIDi}, z)$ are able to acquire the information. Thus, we have the following assumptions:

- q Is a large prime number which forms f_q.
- f: $\{0, 1\}^* \rightarrow \{0, 1\}_q$ is a hash function.
- There is a reliable central server.
- Any valid user, Ui, will be provided by a password (SID_i) which is an integer smaller than q and is known only for central server

and the user. Allocating SID to a user can take place during the registration process.

ACP is a polynomial on $F_q[X]$ as follows:

$$A(x) = \prod_{i\in\varphi}(x - f(\ SIDi\ , z)) \qquad \text{Eq.1}$$

Where, φ is the group, SID_i is the password of members of φ, and z is a random integer from Fq that changes each time A(x) is recalculated. It is clear that, in this polynomial, when x is replaced with $f(SIDi\ , z)$ by a valid user having a SID_i in Group φ, the value of A(x) is equal to zero and otherwise, it has a random value.

For multicasting, an encryption key like K for all users in the group φ is calculated by server through the following polynomial:

$$P(x) = A(x) + K \qquad \text{Eq.2}$$

Then the$(z, P(x))$, where K is hidden in combination with constant value of A(x) is multicast and any valid member of group can obtain the key, K, with SID_i value using the following equation.

$$K = P(f(SIDi\ , z)) \qquad \text{Eq.3}$$

Characteristics and capabilities of ACP method are as follows [Zou, X., Shun Dai, Y., Bertino, E, 2008]:

- ACP is a simple and scalable method for implementing group communications. In addition, it features the flexibility to adapt with different access control and key management patterns.
- ACP is secure against various attacks.
- ACP is suitable for highly dynamic environments with frequent entry and exit of members. Canceling the user membership is also simple and efficient.
- ACP users do not need to be synchronized.

In this method, users only need to store a secret values and calculating the key does not need high computing and processing power. Therefore, it can be implemented in devices with low computational power such as sensors.

1.3. Using ACP in Access Control Structure of IGMP-AC Multicast System

First, we consider the following assumptions:

- AAA server is used as a trusted server in ACP method.
- All AR routers are considered as trusted entities.
- Group key is only distributed between receivers and transmitters do not need group key.
- Each member of the group (receivers) has its own SID.
- AR, in addition to the previously received states, has to keep the group key too.
- It is assumed that, greport is from the messages of Diameter protocol.

In order to shed a light on how to apply the ACP method on access control structure of IGMP-AC we suppose that, a user with SID_i has sent a new application for membership in secure group of (g_or_gs) or to leave it to the related AR. The authenticity and access control processes of this user are performed based on the access control structure of IGMP-AC. After verification of authenticity of user by AAAS, the success or failure message of user's authenticity will be sent to AR and AAAS must calculate the new group key based on SID of new user. In this step, it is required to send $(z, P(x))$ to members. Here, AAAS, using greport message, sends $(z, P(x))$ value to all ARs. Moreover, in this message, the group key will be sent to all ARs in an encrypted form with a key shared between AAAS and each (K_c)AR. The diagram of the new state of AAAS in our proposed structure is shown in the following figure.

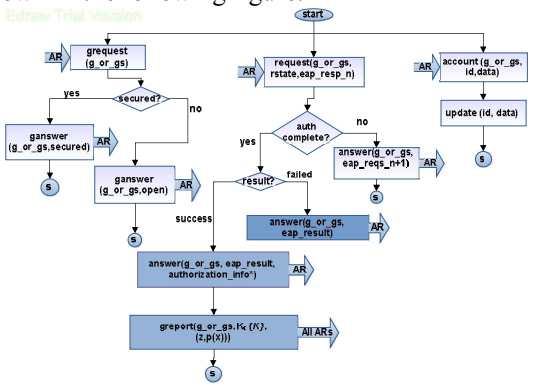

Figure 2: The state diagram of AAAS

As it can be seen, in addition to the greport message which is added to this structure, the rstate value is added in the request (g_or_gs - rstate - eap_resp_n) message that comes from AR.

AR, receiving greport message, obtains new key and sends aresult (g_or_gs , (z, p (X))) message to group members (receivers) in the related subnet (Fig.3).

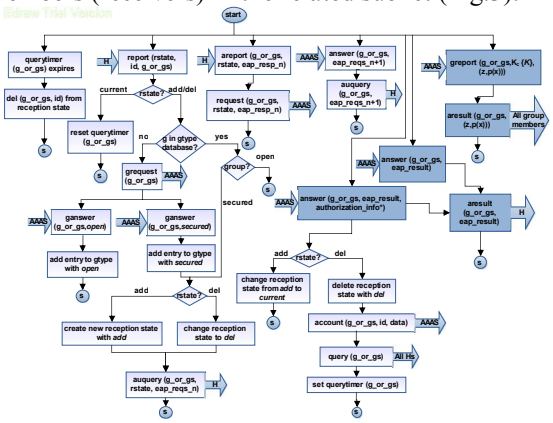

Figure 3: Diagram of AR State

2. Material and Methods

2.1. Simulating the proposed IP multicasting in Isfahan Industrial University (IUT)

Since our goals is developing an IP multicast service to be implemented in a real network (IUT network) we have tried to develop a network by benefitting simulation environment that reflects the topology of a real network through which, we can investigate the protocols and their IP multicast performance under conditions close to reality.

GNS3 Simulator Program

GNS3 is a graphical network simulator that can simulate complex networks. GNS3 enables us to run Cisco IOS on Cisco equipment on the computer. This program is based on Dynamips code. Dynamips is a program that can run, i.e. emulate Cisco IOS on the Pentium processors under Windows and Linux. The difference between simulation and emulation is that, a simulator program simulates a special job but the emulator runs a special program in a new environment with its full features. In other words, it actually runs the program in a virtual environment [Shamsi, M., 2009].

Performance Evaluation of PIM-SM Protocol in the Simulation

The following figure shows our designed network model of implementing IP multicast. As it can be seen, our network is composed form a backbone and a Host Access Network which is comparable with a medium-sized network.

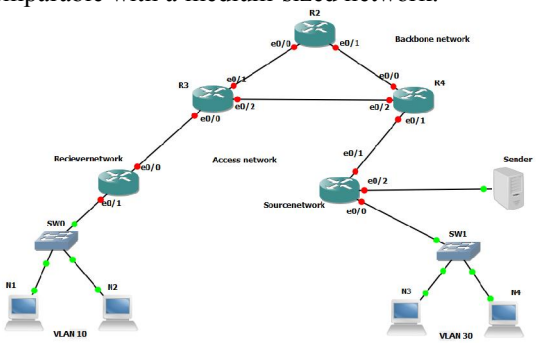

Figure 4: simulated network's model

By sending a joining request to a group from a receiver, a branch of the RPT tree will be created toward receiver from a common root. This request is sent from multicast software to the first router on the client side (LHR) through IGMP protocol. Then this router, using PIM-SM protocol, sends the request to the associated common root. Within the path to the common root, in multicast routing tables of all routers, an entry (*, G), where G is the address of mentioned group, will be entered. In this scenario, an intermediate ring with the IP address of 1.1.1.1 is selected on the R2 router R2 as a common root. Here, the request will be sent to group 239.42.42.42 by node 2. The R1 and R2 router tables and receiver network are shown in the following figures.

```
recievernetwork#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.42.42.42), 00:06:24/00:02:47, RP 1.1.1.1, flags: SJC
  Incoming interface: Ethernet0/0, RPF nbr 172.16.30.2
  Outgoing interface list:
    Ethernet0/1.10, Forward/Sparse, 00:06:24/00:02:47

(*, 224.0.1.40), 00:18:17/00:02:37, RP 1.1.1.1, flags: SJPCL
  Incoming interface: Ethernet0/0, RPF nbr 172.16.30.2
  Outgoing interface list: Null
```

Figure 5-a: multicast routing table of receiver network's router

```
R2#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.42.42.42), 00:08:53/00:03:25, RP 1.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse, 00:08:53/00:03:25

(*, 224.0.1.40), 00:20:11/00:03:29, RP 1.1.1.1, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet0/0, Forward/Sparse, 00:19:00/00:03:29
    Ethernet0/1, Forward/Sparse, 00:19:05/00:03:19
    Loopback0, Forward/Sparse, 00:20:11/00:02:45
```

Figure 5-b: multicast routing table for R2 router

```
R4#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.0.1.40), 00:21:19/00:02:57, RP 1.1.1.1, flags: SJCL
  Incoming interface: Ethernet0/0, RPF nbr 10.20.20.1
  Outgoing interface list:
    Ethernet0/1, Forward/Sparse, 00:20:25/00:02:57
```

Figure 5-c: multicast routing table for R4 router

As the above tables show, each input of the tables have an input interface and a list of output interfaces which are distinguished by the reverse path algorithm of RPF and in fact, they form RPT tree RPT. The data enter to router through the input interface and the router sends these data to all of its output interfaces i.e. multicast receivers.

Now receivers, through RPT tree, are waiting for the data sent to group 239.42.42.42. We, through the sender (Source1), will send the first ICMP package to the target group of 239.42.42.42 and they respond to this request (Fig. 6). Here, 30.30.30.6 is the IP address of node 3 and 10.10.10.3 is the IP address of node 2 which both nodes have been sent membership request to 239.42.42.42.

```
source2#ping 239.42.42.42

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 239.42.42.42, timeout is 2 seconds:

Reply to request 0 from 30.30.30.6, 452 ms
Reply to request 0 from 10.10.10.3, 816 ms
```

Figure 6: receivers respond to ICMP requests

If there were other receivers in the network, there would be responses from them. Here, in order to investigate more closely, we turned off node 3 and assumed that, our group has one receiver (node 2) and one sender.

2.2. Configuring Network Equipment for Multicast Services

In order to configure a multicast service in such a network as our scenario it is required to apply needed commands in each of equipment. Variety of equipment is use in networks such as routers, switches, hubs and so on and each of them must be configured in a way to provide multicast services. In this section we examine the configuration of each of these components.

2.2.1. Configuring routers

The corresponding configurations and commands are as follows [IP multicast, http://www.cisco.com/en/US/docs/ios/solutions_docs/ip multicast]:

- Configuring a unicast routing protocol (OSPF) on all routers
- Activating IP multicast IP on all routers

```
router(config)#ip multicast-routing
```

- Multicast routing protocol configuration (PIM-SM) on all interfaces

```
router(config-if)#ip pim sparse-mode
```

- Determining an interface on one of the routers of network as the common root
- Manual configuring common root on all routers

```
router(config)#ip pim rp-address 1.1.1.1
```

In addition, in order to membership of a router interface in a particular group, the following command will be used

```
Router(config-if)#ip pim dense-mode
```

If the multicast routing protocol PIM-DM is being used, in addition to generally activating multicast on routers, the following configuration should be applied on interfaces and there is no need to configure the common root.

2.2.2. Using Access Control List (ACL) to manually control the receivers

Despite all its benefits, multicast in not widely implemented yet. One reason for this is the lack of manual access control on senders and receivers of the multicast group.

In this section, we want to relatively restrict the access to the multicast groups using ACL and a technique called SSM [Bhattacharyya, S., 2003].

Since that, receivers communicate with the routers using the IGMP protocol, these ACLs will be written on IGMP protocols and on the receivers at their sides. Below is the example of this type of ACL [IP multicast, http://www.cisco.com/en/US/docs/ios/solutions_docs/ip multicast].

```
router(config)#ip access-list extended 100
router(config-ext-nacl)#permit igmp 30.30.30.1 0.0.0.255 239.0.0.0 0.0.0.0
router(config-ext-nacl)#permit igmp any 225.0.0.1 0.0.0.255
router(config)#ip access-list extended 101
router(config-ext-nacl)#deny igmp any 239.42.42.42 0.0.0.0
router(config-ext-nacl)#permit igmp any any
```

In the first law of the ACL, the receivers with the address range of 30.30.30.1 to 30.30.30.255, are allowed to access 239.0.0.0 group. The second rule to allow access to all receivers in the group suffering 225.0.0.1 Until225.0.0.255 Talking. And the default access is denied to others for other receptors.

In the second ACL, the access of all groups to 239.42.42.42 group is denied and the access is granted to the other groups.

On the interfaces of the routers of receiver side, using the following command, the appropriate ACL will be applied.

```
router(config-if)#ip igmp access-group 100
```

2.2.3. SSM Mechanism

Using SSM mechanism along with an ACL allows us to control the access based on sender and group in the IGMP reports.

To use the SSM mechanism, it is necessary for IP multicast receiver to use third version of the IGMP protocol in order to register in (S, G) channel. By registering in this channel, the receiver specifies that, it wants to receive IP multicast traffic sent by the sender S to the group G.

The multicast addresses in the range of 232.0.0.0/8 (232.0.0.0 - 232.255.255.255) are reserved by IANA for SSM.

IGMPv3 allows multicast receivers not only to join a particular group but also join groups including special senders. In order to appropriate access control, it is necessary to allow filtering of IGMPv3 messages not only according to the reported group addresses but also according to the address of the sender and group. This capability is provided by IGMP extended access control list.

In order to use SSM method, after establishing multicast service on the router and PIM-SM routing protocol on interfaces, we will apply the following configuration on the router followed by writing required ACLs [IP multicast, http://www.cisco.com/en/US/docs/ios/solutions_docs/ip multicast].

```
Router(config)#ip pim ssm default
```

The following command will be applied on all interfaces at the receivers' side in order to activate IGMPv3:

```
Router(config-if)#IP IGMP VErsion 3
```

ACLs are very flexible and using their different rules, we can filter multicast traffic. Here's an example of the extended access control list and commands needed for SSM groups.

```
Router(config)#ip multicast-routing
Router(config)#ip pim ssm default
Router(config)#ip access-list extended 100
Router(config-ext-nacl)#permit igmp any 232.2.1.1 0.0.255.255
Router(config-ext-nacl)#permit igmp 20.1.1.1 0.0.0.255 232.2.1.1 0.0.0.0
Router(config-if)#ip igmp access-group 100
Router(config-if)#ip pim sparse-mode
Router(config-if)#ip igmp version 3
```

In this example, the first rule of ACL grants access to groups from 232.2.0.0 to 232.255.255.255 for all senders and the second rule grant the senders at the range of 20.1.1.1 to 20.1.1.255 to access 232.2.1.1 group.

2.2.4. Configuration of switches

As we know, in a network, equipment such as routers, switches, hubs, etc. are used.

Required switch configuration is as follows:

```
switch(config)#ip igmp snooping
```

2.3. Testing and implementing the scenario

After performing all required configurations it is time to test the simulated scenario. In order to do that, we need to have software in the receiver and senders which would be able to send or receive an audio or video file in a multicast system. In this study, we have used Unreal Streaming software in the sender as a multicast server and have used VLC multimedia player in the receiver. VLC also has the capability to be used as a server at the sender.

Figure 7 shows the Unreal Streaming software environment.

After conducting the required settings on both receiver and sender in the simulated scenario, we were able to receive the video files sent by sender.

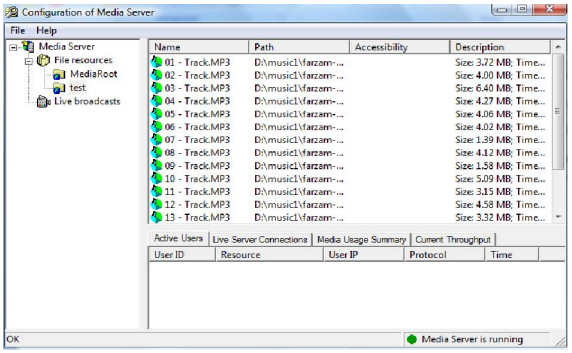

Figure 7: The environment of Unreal Streaming software

2.4. Assessment of the topology of Isfahan University's network

The topology of Isfahan University's network is a star model (Fig. 8). As it can be seen, different faculties, using a switch which is capable of performing layer 3 routing, are connected to the central switch. The central switch only performs Layer 2 switching operations. Users in the faculties connect to the network via layer 2 switches.

Given that, the structure of the universities network is the star topology, the maximum number of routing steps between a multicast sender and receiver is 2 steps (the maximum number of routers between a receiver and sender is 2). Therefore, this structure is considered as small and compact structures.

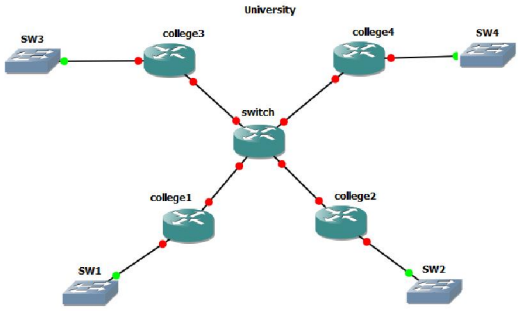

Figure 8: the typical schematics of university's network

2.5. Implementation and its difficulties

Implementing multicast services in the university was divided into two phases:

- Phase I: implementation at each of faculties and buildings separately
- Phase II: establishing multicast communication between faculties and buildings

In a real network, network manager, based on the requirements, performs other configurations such as security configuration and so on. Similarly, in our network, after required configurations, we observed that, the multicast connection is not established yet. After thorough investigation, we observed that, the security configurations of the switch were preventing the establishment of multicast communication. The configurations were the ACL which were preventing the sending of IGMP packages. Therefore, we tried to exactly adjust the ACLs by adding or deleting the proper commands to establish multicast service. We defined and applied required ACL switches in each faculty regarding two goals:

1. Establishing multicast communication
2. Control and restrict user access to multicast services

After applying the above ACLs, we were managed to establish multicast communication in the first phase.

After establishing multicast communication in every faculty, we have tried to establish the connection between faculties and the various buildings in the second phase. Since the switch of each faculty is related to other switches through a central switch, we had to apply needed configuration on this switch. As mentioned before, the central switch acts in the layer 2 and it merely provides a switching operation. This switch is capable of configuring and thus, it has been configured according to the aforementioned issues. Moreover, in the multicast path between the sender and the receiver in two separate faculties, we assumed that, where there layer 3 interface, we will conduct PIM-DM multicast routing protocol configuration. Therefore, through performing related test, multicast communication was established in the second phase.

3. Results

Upon completion of the implementation phase, we started to broadcasting multicast traffic in network of university, monitoring this traffic and measuring some important parameters of the network routers. These parameters include CPU load of routers, memory requirements of routers, and the average number of multicast packets sent in some of the router interfaces. All measurements were performed by Solarwinds monitoring software.

If we assume the university network configuration as shown in Figure 8, we can consider multicast server in a faculty and the receivers in the same or other faculty. Here, we have placed multicast server in the Faculty of Electrical and Computer Engineering and have placed some receivers in the Faculty of Information Technology and performed associated measurements in the routers of the faculties of Electrical and Computer Engineering (ECE) and Information Technology Center (ICT). Both of these routers use gigabit No. 25 interface as an upper link interface to connect to the central switch. Therefore, the above-mentioned parameters have been measured on the two interfaces.

Prior to broadcasting the video from sender, we monitored multicast traffic of mentioned interfaces to see that, how much traffic is being sent via configured multicast protocols in normal state. According to Figure 9, the input traffic of each router interface is almost an average of 2 packets per second.

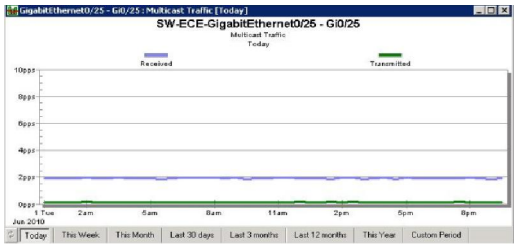

Figure 9: signaling traffic received by the ECE switch

At first, we started our test with one receiver and one sender, and then gradually increased the receivers at approximately equal intervals in order to examine its effect on increasing or decreasing each of

the mentioned parameters. The following picture exhibits the number of packets per second (pps) of multicast traffic sent by the ECE router in green color. The traffic has been sent in the period between 9:30 am to 13:30 pm and at almost 30-minute intervals, the number of receivers has been gradually increased. Furthermore, at a small interval we have used two senders on the network.

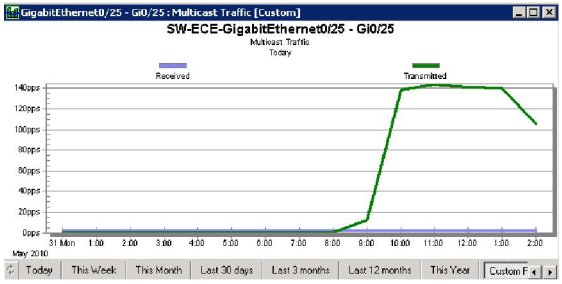

Figure 10: multicast traffic sent by the ECE router

As it can be seen in the above figure, increasing the number of receivers has no effect on pps and thus the required bandwidth since as mentioned before, multicast saves the bandwidth consumption in the network and regardless on the number of receivers, the sender sends the requested video only once and the routers replicate the video where it is needed. In the small period of placing two senders we observed an increase of the pps (Fig. 10). In addition, figure 11 shows the traffic received by the ICT router.

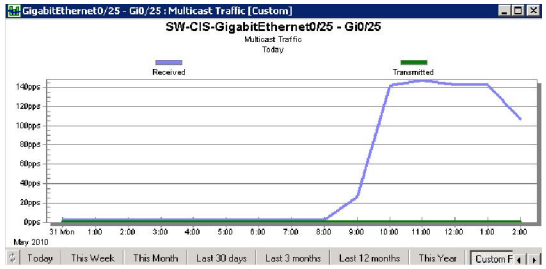

Figure 11: multicast traffic received by ICT router

Figures 12 and 13 show the average amount of CPU load of these two routers. As it is shown, multicast traffic has no significant effect on increasing the CPU load of the routers.

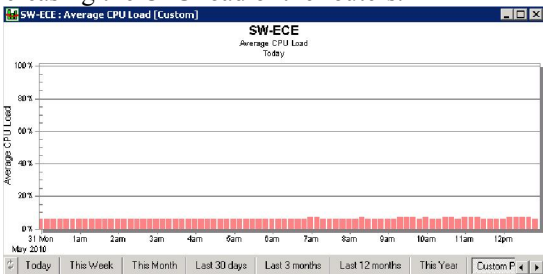

Figure 12: average CPU load of ECE router

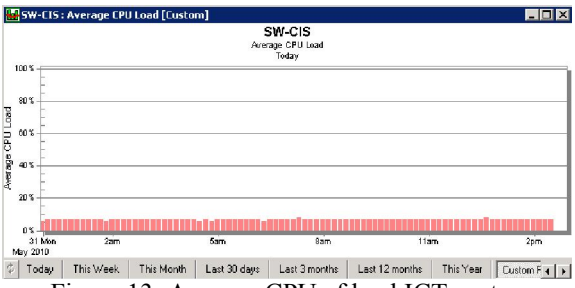

Figure 13: Average CPU of load ICT router

According to following picture, the required amount of memory, for instance in the ICT router, has not changed in comparison to previous state (before sending multicast traffic).

According to the conducted investigations, IP multicast is a very good service for multimedia broadcast in the level of local networks and ISPsthrough which, not only the network resources will not be wasted but also, via effective use of network bandwidth, the resources will be saved and thus, it can be argued that, the best way to broadcast a video for a lot of users of a local area network is benefitting multicast service.

4. Discussions

In this work, through developing a demo in the GNS3 environment we closely investigated PIM-SM multicast routing protocol and messages exchanged on the network by the protocol. In addition, we conducted the required configurations in order to establish a multicast service in a simulated network and finally, via testing the scenario, we verified the conducted simulation. After a successful simulation test, we implemented the service in the network of IUT and measured efficiency of the network and some important parameters. According to the results, multicast, through efficient use of network resources, conserves bandwidth consumption and processing load of the routers in comparison with unicast multimedia broadcast to a group of users.

Author:
Masomeh Adhami
Kerman University of Medical Sciences, Kerman, Iran
adhamimasomeh@yahoo.com

References

[1] Liu, D., Ning, P., Sun, K., "Efficient self-healing group key distribution with revocation capability", ACM CCS, pp. 231-240, 2003.
[2] Zou, X., Shun Dai, Y., Bertino, E., "A Practical and Flexible Key Management Mechanism For Trusted Collaborative

Computing", IEEE INFOCOM, Phoenix, AZ, pp. 538 - 546, April 2008.
[3] Steer, D. G., Strawczynski, L., Diffie, W., Wiener, M., "A Secure Audio Teleconference System", Lecture Notes in Computer Science, vol. 403, pp. 520-528, USA, 1990.
[4] Solie, K., Lynch, L., CCIE Practical Studies, 1st Edition, Cisco Press, 2004.
[5] IP multicast, http://www.cisco.com/en/US/docs/ios/solutions_docs/ip multicast.
[6] Hilt, S., Pansiot, J., "Using IGMPv3 to manage multicast access", Proceedings of the Fourth Conference on Security and Network Architectures, Batz sur Mer, France, June 2005.
[7] Tanenbaum, A., Computer Networks, Fourth Edition, University of Michigan, USA, 2003.
[8] Shamsi, M., Educational book starting and running GNS3, http://www. networkprof.com, November 2009.
[9] William Atwood, J., "An architecture for secure and accountable multicasting", Proceedings of the 32nd IEEE Conference on Local Computer Networks, Dublin, Ireland, pp. 73-78, October 2007.
[10] Bhattacharyya, S., An overview of Source-Specific Multicast (SSM), RFC 3589, July 2003.
[11] Islam, S., William Atwood, J., "The internet group management protocol with access control (IGMP-AC)", Proceedings of the 31st IEEE Conference on Local Computer Networks, Tampa, FL, pp. 475-482, November 2006.
[12] Kent, S., Seo, K., Security architecture for the internet protocol, IETF RFC 4301, December 2005.
[13] Rekhter, Y., Li, T., A Border Gateway Protocol 4 (BGP-4), RFC 1771, May 1995.
[14] Benslimane, A., Multimedia multicast on the internet, Second edition, ISTE Ltd, USA, 2007.
[15] Multicast Technology White Paper, http://www.h3c.com/portal/res/200806/24/20080624_634948_image006_608769_57_0.gif.
[16] Handley, M., Jacobson, V., "SDP: Session Directory Protocol (draft2.1)", Internet Draft (February 1996), January 2004.
[17] Handley, M., Stephen, R., "Multicast Address Allocation Protocol (AAP)", Internet Draft <draft-malloc-aap-*.txt>, Agust 1998.

2/17/2013