An Approach for QoS Measurements in IP Multicast Networks MQM - Multicast Quality Monitor

Falko Dressler

University of Erlangen-Nuremberg, Germany
email: falko.dressler@rrze.uni-erlangen.de / fd@acm.org

Abstract

MQM - Multicast Quality Monitor represents a new approach to measure QoS within an IP multicast environment. Existing tools stop at measuring some packet loss ratio or some reachability by producing there own low-rate measurement data streams. History has shown that there are a lot of interesting parameters to measure some multimedia transmissions such as one-way-delay, round-trip-time, packet-loss-ratio and others. Also, in a multicast environment, existing tools built for unicast measurements fail because of the very different communication model. The MQM tries to fill this gap by introducing methods as well as tools for reliability and QoS measurements.

In discussion are the most common problems such as the measurement of delays requires synchronized clocks and, much more important in the multicast environment, the scaling problem. Having a large number of measurement probes distributed over the network communicating to each other and measuring various QoS values using IP multicast results in some kind of flooding and overloading the network. Shown are approaches to minimize this effect as well as to examine really required parts of the network only.

Having in mind the reason for all the tests, the applications or services, also included is a short presentation of a model for multicast networks as well as the used services which builds a very basis for the measurements.

Keywords

IP Multicast, Quality of Service, IP Performance Measurements, Network Modeling

1. Introduction

In the last years, there have been different approaches to ensure a more reliable IP multicast network. Some are intended to check the reachability of different hosts and routers via IP multicast, some are going a little further. They try to measure the Quality of Service (QoS) of the IP multicast network as well.

The most interesting approach is the Multicast Reachability Monitor (MRM), formerly known as Multicast Route Monitor (Almeroth et al, 2001). The here presented Multicast Quality Monitor (MQM) is based on the ideas of the MRM. There are implementations of the MRM for Cisco IOS (ftp://ftpeng.cisco.com/ipmulticast/#MRM) and Sun Solaris (http://steamboat.cs.ucsb.edu/mrm/). An other implementation of a multicast quality monitor is the multicast beacon (http://dast.nlanr.net/projects/beacon/).

The MQM introduces different ways to measure the reliability (chapter 2) and the quality (chapter 3) of a IP multicast network. Very different from the MRM is the inter-probe communication (chapter 4). Based on these ideas, it became possible to do some measurement. But where to measure? Additionally, information is required to place every part of the measurement system properly within the network. This question should be discussed by presenting a model (chapter 6) for a whole IP multicast system.

2. Reliability measurement

For IP Unicast users as well as for management stations ICMP messages (Postel, 1981) are used to prove the connectivity of different IP end systems. Unfortunately there is no such tool for IP multicast connections. The MRM tries to solve this problem by defining a set of Test Senders (TS) and Test Receivers (TR). The TS send a (low bandwidth) stream of packets to a specified multicast group. The TR receive these packets and inform a central Management Station (MS) about these received packets. Basically, the MQM works like that. The MQM also uses - properly placed - probes which send MQM ping requests and act on incoming requests by replying with a MQM ping response.

Due to the principles of IP multicast, it is required to ping everyone from everywhere since it is not possible to use the information of A reaches B and C and, on the other hand, B and C both reach A via IP multicast to provide any information about the connection between B and C (this is true for IP unicast as well, but in IP multicast everyone gets each response but cannot detect the state of the network using these messages). A next version of the MQM may include a more intelligent system to prevent the transmission of additional pings if not required.

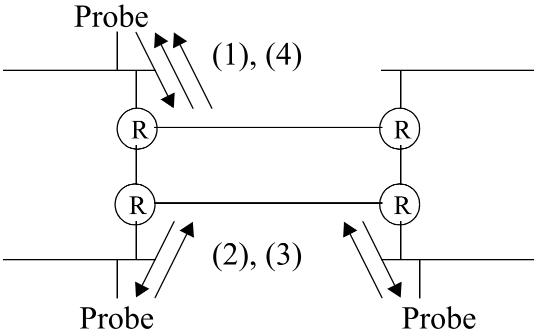

Figure 1: MQM ping mechanism

The MQM ping mechanism is shown in figure 1. For a single test, the probe sends a MQM ping request packet (1) to all the others to a well known multicast address. Other probes receive this request (2) and respond (3) back to the originator by sending a MQM ping response which is received (4) by the requesting probe. Each probe is required to send about 1 packet a minute to a well known MQM_PING IP multicast group. Lower rates do not refresh the states in the routers and result in indeterministic results. Higher rates are not required but increase the network congestion. To get more information about the state of the network, the use of unicast pings is required as well, either if there are failures in IP multicast connectivity or together with the IP multicast pings. For now, only the probes are able to do some reliability measurement of the IP multicast network. There are a few ideas how to summarize the information on a central point shown in chapter 4, MQM communication.

3. QoS measurement

The first step for QoS measurements of IP multicast networks is to define the term QoS in relationship to the multicast services and the multicast network. The most typical IP multicast applications are multimedia communications. Such real-time services depend on the current packet loss ratio, the absolute delay and the variation of the delay, the jitter. Most of these applications do use Real-time Transport Protocol (RTP) (Schulzrinne et al, 1996) as the transport protocol. This protocol already offers nearly all the information to measure the QoS of the network as it implements sequence numbers and time stamps into each packet. So RTP has been selected for the most QoS measurements.

3.1 Delay (one-way and round-trip)

The only measurement done by the MQM which is not based on RTP, is the delay. According to the research work of the IP Performance Metrics WG (IPPM) of the Internet Engineering Task Force (IETF), the most important information for real-time services is the one-way delay. The MQM introduces its own ping mechanism to measure both, the one-way delay (based on the work of the IPPM WG) in each direction and the round-trip time. Due to possible synchronization failures of the clocks of different probes, the correctness of the one-way delay may vary. This problem has been discussed at the IETF. The result was to make use of GPS clocks at each measurement probe. Nevertheless it should be possible to work with NTP synchronized clocks because most applications for which the tests are done do not depend on delays lower than 1 ms. Also GPS equipped probes would be very expensive.

The measurement of the delay is based on the reliability measurements. The same ping messages are used to calculate the one-way delay in both directions and the round-trip time. To ensure, that the ping response message belongs to the ping request sent from a particular probe (please note, every probe gets every ping message because they are multicasted through the network), the IP address of the requesting probe is included in both messages, the ping request as well as the ping response (see also chapter 6).

3.2 Packet loss and jitter

To measure packet loss and jitter, MQM makes use of RTP streams. There are two ways to do this: passive and active. Passive measurement means that the probes join an existing multicast session and decode the information of the received RTP packets. This procedure has no impact on the network but it is only useful if information about current sessions, active senders and their location is available. In the active way, the probes simulate typical transmissions with at least a little impact on the network. Simulating high bandwidth video transmissions may disturb other active IP connections (unicast and multicast) and raise the network congestion.

Using the model shown in chapter 6, it is possible to identify the parts of a particular network which are responsible for the most critical IP multicast applications. Based on these information, the probes can be placed properly within the network. It is necessary to distinguish between the two most important types of IP multicast communication: a broadcast from a single server (one-to-many communication model) and a conference between several end systems (many-to-many communication model).

A typical example of a broadcasting station is a video server (http://www.uni-tv.net). Such video broadcasts have some common properties. So they stream data mostly all the time at high data rates. If there are such services located in the network of interest, it would be a good idea to use this RTP stream to measure the packet loss ratio as well as the jitter. All the measurements are passive which means they do not affect the network if the probes are placed on the way of an active data transmission through the network. Figure 2 shows a typical situation. There is one sender which broadcasts a session to some receivers. If the probes are placed properly on the network, usually near the receivers, maybe somewhere in the path, it became possible to measure the current QoS without any impact on the network itself.

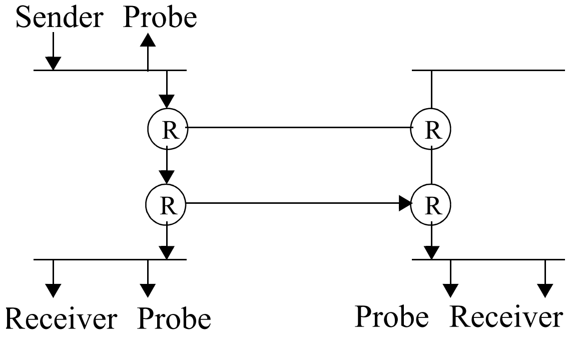

Figure 2: Passive QoS measurement

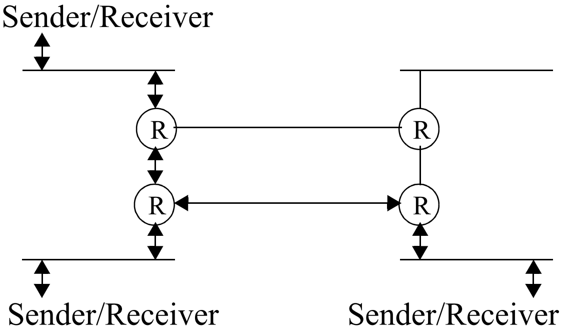

Figure 3: A typical conference

Most conferences are based on the following ideas: they last only for a short time, they are announced (start at well known times) and the location of the members is almost known but is expected to vary for different conferences. The idea is, to provide information about the current quality of the IP multicast network to all participants of a upcoming / running session. To allow this, it is required to configure all probes in involved parts of the network to simulate typical conference applications by sending simulated RTP streams. So all the probes do receive just the same traffic like if the real conference would be already active. So it is possible to simulate the traffic of a meeting and measure the QoS of the IP multicast network which allows to compute the expected QoS for the upcoming conference. In figure 3 an IP multicast network is shown which has been used by a typical conference. There is a number of participants. Everyone is sending and receiving traffic. Based on the knowledge about the network and the placement of the systems, it is possible to simulate this type of conference by configuring some intelligent probes to produce some simulated traffic and to receive and analyze it (see also figure 4). As well, the same configuration can be used to monitor a running conference.

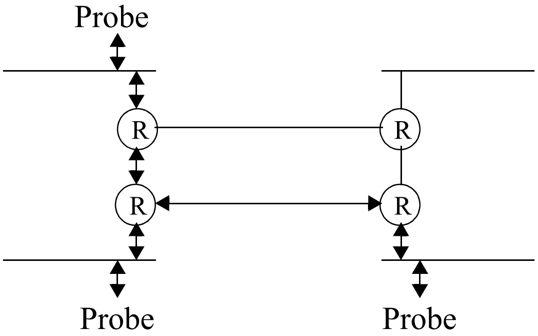

Figure 4: Active traffic simulation based on the knowledge about the conference

4. Inter-probe communication

The last two chapters have shown how to use intelligent probes to measure the reliability and the QoS of an IP multicast network. Not yet mentioned is the inter-probe communication. There are three different types of such communication:

4.1 Detecting new probes

The design of the MQM is based on the knowledge of the structure of the network and the used services. So the starting configuration will include some known probes. To provide a more flexible system, it should be possible to include more probes dynamically. The appearance of a new probe can be detected by listening to the MQM_PING multicast group. All the probes are required to periodically send ping requests to measure the reliability. The management station can join this group to detect new probes.

4.2 Starting the simulation of a RTP stream / starting analyzing a RTP stream

This is done using the same beacon mechanism as defined in MRM. The central management station can start and stop the QoS measurement via a beacon message sent to the same well known IP multicast group which is also used for the MQM_PING messages. Within this message, the manager tells the probes which RTP stream to analyze and, if required, which probe should simulate which type of traffic. Due to the use of the unreliable transport protocol UDP (Postel, 1980) for these beacon messages, they cover a maximum time to live (hold time) and the management station should send these beacon messages periodically.

4.3 Transferring the measured data to a central management station

All the described mechanisms allow the intelligent probes to measure the reliability and the QoS of an IP multicast network, partially controlled by a central manager. The idea of MQM is to let the probes save all these information locally. The transfer of these information to the management station should be done on a periodical base using the TCP protocol. The protocol ensures the reliable transport of the measured data. Not yet defined is who is required to start this transfer, the probes or the management station. Since it should be allowed to a user to force the presentation of the current situation of the network, the management station should be able to initiate this transfer. So, the current version of MQM is focused on the management station to control nearly everything, the QoS measurement (RTP analysis) and the transfer of the measured data from the probes.

5. Message format

The message format of the MQM uses the same principles as the MRM does. For the inter-probe communication, a separate header (MQM header) has been defined. Also, the beacon messages from the management station to the probes uses the MQM header. Table 1 shows the major MQM header format. Table 2 and 3 define header extensions for different MQM packet types. All values within the tables are in Byte.

Pos	Size	content
0	1	version
1	1	padding
2	2	type

Table 1: MQM Header format

Pos	Size	content
0	4	MQM header
4	4	IP address from the originator
8	4	timestamp sender
12	4	timestamp receiver

Table 2: MQM ping message format

Pos	Size	content
0	4	MQM header
4	2	hold time
6	2	message length
8	4	target probe address 1
12	4	multicast group address 1 (1st bit is used to specify if to receive or to transmit to this group)
...	4	target probe address n
...	4	multicast group address n

Table 3: MQM beacon message format

Currently, there are only three packet types: MQM_PING, MQM_PONG and MQM_BEACON. Since the transport of the measured data is an out-of-band mechanism which uses TCP for the communication, there is no MQM packet type for reporting messages. The MQM header is part of every MQM message. The encoding of the rest of the packet depends on the type value in the header. Not shown in the tables is some kind of example. The packet format has been included just to provide a more detailed view on the ideas of the MQM.

6. A model for IP multicast services

As shown in the previous chapters, it is very difficult to find proper places to deploy measurement probes and to use the computed results to provide better reliability and quality to these services.

6.1 Modeling IP multicast networks and services

One idea to solve this problem is to generate a model of the network including the overlying services. This chapter should give an overview to such a model (Dressler, 2001). The model should be able to include important functions from OSI Layer 1/2 (Physical and Link), Layer 3 (Network) and Layer 7 (Application, the services). The primary result of such a model is to find out which parts of a network are required for a particular service. This can be done by attaching various routing algorithms.

The basic objects for the model of the network are shown in figure 5. Based on these objects, it is possible to generate models of complex networks and to calculate a best route through the network. The current implementation includes the Dijkstra algorithm for route calculations. The objects are extensible to include parameters such as CPU load, bandwidth of an interface or a loss ratio of a link allowing a recalculation of the routes through the network based on more exactly information about the network.

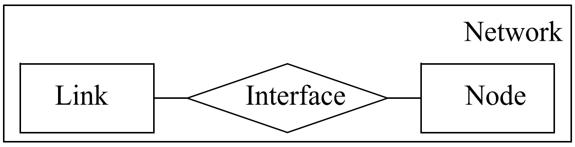

Figure 5: Basic objects to model a network

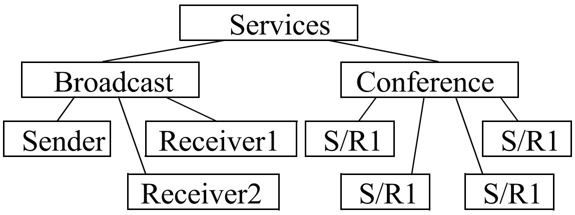

Figure 6: Example of service objects

Besides the model of the network, the representations for the services have to be modeled. Each object of class service stands for one multicast transmission which may use more than one multicast group (figure 6). Based on the concept of analyzing the most important services within the network first and using these information together with a detailed model of the underlying IP multicast network allows to extract the involved parts of the network.

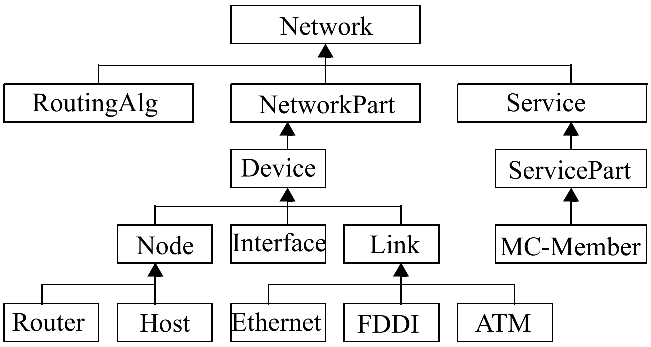

Figure 7: Object hierarchy

Summarizing the already presented objects and their capabilities, figure 7 shows the class diagram which has been used to implement the model in JAVA. This implementation called MRT (Multicast Routing Tool) has been done by Juan Ceballos-Mejia at the University of Erlangen-Nuremberg (Ceballos-Mejia, 2000) as a part of his masters thesis.

6.2 Using the model for measurements

In the last chapters an overview of a method to model an IP multicast network including the network itself, the applications / services and the participating hosts has been presented. Also, some real measurement tools have been introduced. The final question is 'How do I use this model to measure reliability and quality of IP multicast services?'.

The current implementation allows to model a network and check for optimum paths for IP multicast transmissions using the attached routing algorithm. To find the best way, the algorithm uses the constants out of the modeled objects such as bandwidth of a particular interface or the hop count. The following figures 8 and 9 show the mechanism. Using the information about the network and the service one can find out which parts of the network are used for this service.

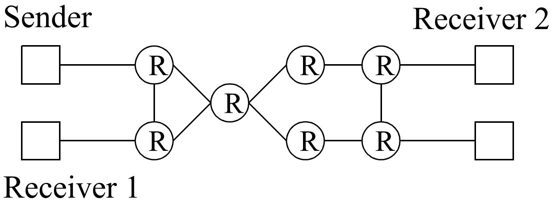

Figure 8: physical network

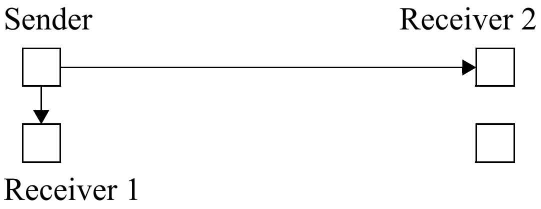

Figure 9: logical data flow

After all, this is only a first step to find all the required parts of the network for a particular service. Our implementation allows already to incorporate dynamic information about the current state of the network. The most interesting values are the state of a node, the state of an interface, the packet loss ratio from an interface and the load of a node. Also, the routing tables of the routers (IP unicast and IP multicast) have to be examined to get closer to the real behavior of the IP network. Based on these dynamic data and the knowledge about the network, the tool allows to find the used components and paths for the current situation and a particular service (figure 10). The current implementation includes an open interface to retrieve dynamic data. This includes also values such as the CPU load mentioned in chapter 6.1.

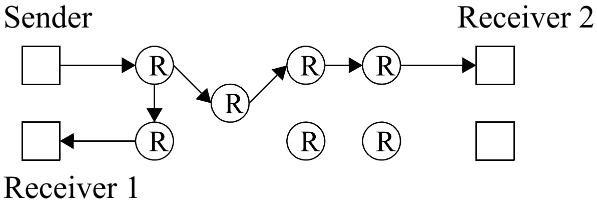

Figure 10: real packet flow

Describing the complete IP multicast network including the most critical services in this model, it is possible to use the attached routing algorithm to find proper places to implement the intelligent probes and to deploy the MQM measurements. The same model can also be used for offline analyzing of the used paths for the services and for offline simulation of the behavior of the network.

7. Summary

To summarize the introduction to MQM the most important common grounds and differences between MRM and MQM should be compared. This includes also some a summary of the functions of the MQM.

7.1 Common practices

Both, the MRM and the MQM use distributed probes (TRs and TSs). This allows to measure just these parts of an IP multicast network which are between these probes. Also, both tools are designed to measure some important QoS values like packet loss or the jitter by analyzing RTP streams.

7.2 Major differences

The first major difference is that the MQM design distinguishes between the test of functionality (reliability) and the measurement of the QoS of an IP multicast network. The first one is done without any involved central intelligence. This is very important because if there is a problem with parts of the network, the MRM is only able to detect the border of the problem but cannot look behind. With the MQM model, it is possible to check the function also behind the problem. Also, the measurement of the reliability of the MQM is done with only a very low impact on the network. Depending on the type of the IP multicast services, the additional congestion of the network may be very small if there are some broadcast services which can be used for the QoS measurement.

A real enhancement to the MRM is also the measurement of the one-way delay as a basis for real-time services. Another difference is the out-of-band transfer of the results of the tests. MRM uses the same mechanism to report to the management station as for all other communication between the MS and the TRs and TSs. So the probes became more intelligent and may act basically without any central supervision. The primary idea of the MQM is to measure the QoS depending to the services (applications) in the network. Using the model (Dressler, 2001), the deployment of the measurement probes became possible based on the requirements of a particular network. The model is not restricted for a local use only. It is designed to support distributed services as well. The same applies to the MQM.

8. References

K. Almeroth, L. Wei, D. Farinacci (2001), "*Multicast reachability monitor (MRM)*", IETF draft.

J.-F. Ceballos-Mejia (2000), "*Design and implementation of a modeling tool for multicast networks*", Master-Thesis, University of Erlangen-Nuremberg.

Falko Dressler (2001), "How to Measure Reliability and Quality of IP Multicast Services?", *Proceedings to 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, PACRIM'01, Victoria, B.C., Canada.

Falko Dressler (2002), "QoS considerations on IP multicast services", *Proceedings to International Conference on Advances in Infrastructure for Electronic Business, Education, Science, and Medicine on the Internet*, SSGRR 2002w, L'Aquila, Italy.

J. Postel (1981), "*Internet control message protocol*", RFC 792.

J. Postel (1980), "*User datagram protocol*", RFC 768.

H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson (1996), "*RTP: a transport protocol for real-time applications*", RFC 1889.