MQM - Multicast Quality Monitor

Falko Dressler
Department of Computer Science IV / Regional Computing Center (RRZE)
University of Erlangen-Nuremberg
Martensstr. 1, 91058 Erlangen, Germany
fd@bsd.rrze.uni-erlangen.de / fd@acm.org

Abstract

In the last years, various approaches have been shown to measure the reliability of an IP multicast network. Some of these tools are intended just 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 MRM (Multicast Reachability Monitor, formerly known as Multicast Route Monitor [2], [4]). The Multicast Quality Monitor (MQM) presented here is mainly based on the ideas of the MRM.
The MQM introduces different ways to measure the reliability and the quality of an IP multicast network. It is designed to work for intra-domain as well as for inter-domain multicast environments. Very different from the MRM is the distinction between reachability and quality measurements and the kind of inter-probe communication. Based on these ideas, it is possible to measure reliability and quality in IP multicast networks. The remaining question is 'What to measure?' As a third part, information is required about the locations within the network where the parts of the measurement system should be placed. This question is discussed by presenting a model for a whole IP multicast system starting with the network itself but also including the services on top of it. Finally, the paper summarizes the state of the art of methods for reliability and quality measurements in IP multicast networks.

1. Introduction

IP multicast emerged as the commonly used technology for multimedia transmissions over the Internet. Examples are TV broadcasts or conference meetings. These services require a much higher Quality of Service (QoS) than other applications in the Internet. On the other hand, the deployment of IP multicast based on current implementations is not as easy as most vendors suggest. Problems occur because of mistakes in the network configuration, implementations which are not fully interoperable or due to overloaded links or exchanges points. At the University of Erlangen, we use IP multicast for video conferences since about 1993. Additionally, we installed different video servers, which are broadcasting their content via multicast [24].
Due to the best-effort characteristics of the Internet as well as due to the state-less working principle of UDP (User Datagram Protocol, [19]) which is used for IP multicast transmissions, multimedia applications typically use RTP (Real-time Transport Protocol, [22]) for their transmissions. RTP offers sequence numbers and time stamps, allowing the support of real-time applications [5].
To provide information about the current state of an IP multicast network, the Multicast Quality Monitor (MQM) should be introduced. Using this tool, a network administrator will be able to locate failures as well as to locate bottlenecks within the network. Additionally, end users can use the measurement results to get information about the current quality of the network giving an approximation of the quality of an upcoming transmission. The MQM includes active and passive measurements. Active means that the network is affected by the measurement. Data streams are simulated to test the behavior of the network in addition to the current utilization. Another way, preventing the unnecessary disturbance of the network, is to join currently active IP multicast transmissions and to analyze the RTP and RTCP (Real-time Control Protocol, [22]) packet streams.
The paper is organized as follows. Section 2 gives an overview to related work in the field of measurements in IP multicast networks. Section 3 introduces the Multicast Quality Monitor. Besides the working principles, some results of experimental measurements are shown. Section 4 shows an approach to deploy measurement tools in general and the MQM in particular based on the requirements of the most important services, which are using the network. A summarization is given in section 5.

2. Related Work

A good overview to other implementations of tools to measure the reachability and/or the quality of IP multicast networks has been given by Almeroth and Sarac [1], [21]. A first overview to available tools and the principles of QoS measurement in IP multicast networks has been given by Dressler [10].
The term reliability measurement stands for measurement methods which allow to examine the connectivity of clients over a certain amount of time. For IP unicast, a large number of management systems a available. Typically, ICMP messages [18] - the well known ping mechanism - are used to prove the connectivity of IP end systems. Unfortunately there is no such a tool for IP multicast. To fill this gap, various groups started with implementations of different ideas. Most of the resulting tools provide some kind of QoS measurement as well. The following sections summarize only a few approaches which are directly comparable to parts of the proposed MQM. Not considered are SNMP based tools such as mmon [16] because there is typically no SNMP access to all the devices in inter-domain multicasting.

2.1. mtrace / MHealth

One of the most important tools in use today is mtrace [11], which is a multicast version of the popular traceroute utility. Mtrace works by tracing the reverse path to the source of multicast traffic starting at the receiver. To allow such operations, a special feature has built into multicast routers [12]. Since mtrace requires 'mtrace-enhanced' routers, it fails if routers on the path have not implemented this feature or ignore the requests due to overload situations. Mtrace is able to provide information about the packet loss ratio on a specific path by printing out the amount of sent and lost packets for each trace. The user of mtrace is required to select the useful data and to analyze them by himself.

A graphical frontend to mtrace is MHealth [15]. It was first proposed in [14]. MHealth joins an active multicast session to receive and examine the RTCP packets in order to locate the participating end systems. Then it uses mtrace to trace the path from the source(s) toward the receivers.

2.2. Multicast Beacon

The multicast beacon [7] is the result of a research project from the NLANR (National Laboratory for Applied Network Research). It consists of a central monitoring station and of distributed clients. These clients send a low rate packet stream to a configured multicast group. Finally, they report the status of the reception of these packets to the monitoring station, allowing to compute a reachability matrix. In a large network, the test packets have a large impact on the network due to the working principle (each client multicasts its test packets to each other!) and the data rate of at least a few packets per second. Initially, the multicast beacon was not intended for reachability measurement. It has been designed for quality measurements. The streams of test packets are used to compute the packet loss ratio, the delay and the jitter. So the drawbacks of the multicast beacon in reachability measurement change to opportunities while measuring the quality of service. But one problem is still important. There is the requirement of continuously streaming the test packets between each client without any central control.

2.3. Multicast Reachability Monitor (MRM)

The Multicast Reachability Monitor [2] tries to solve the problem of reachability measurement 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 tell a central Management Station (MS) if they received some packets successfully. There is an implementation of the MRM for UNIX systems [20] as well as for Cisco Routers [17]. This allows to deploy the measurement also directly in some core networks. Based on the centrally controlled approach, it is possible to limit the by the TS generated packet stream to actually required parts of the network as well as to limit it to short periods of measuring time. The result is a much lower impact on the current operation of the network [3]. The first design of the MRM allowed only to measure the reachability. Due to the principles of the measurement, is was possible to calculate the current packet loss ratio. In a second step, the definition of the MRM was enhanced to compute some QoS parameters by using RTP streams of active multimedia sessions. Unfortunately, these ideas have been implemented only partially.

2.4. Hierarchical Passive Multicast Monitor (HPMM)

An other approach, competing directly with the MRM, is the Hierarchical Passive Multicast Monitor [25]. The idea is to place listeners along an active multicast tree. These listeners are about to receive each multicast packet without joining a multicast group. This can be achieved using mechanisms such as the BPF (Berkeley Packet Filter). To prevent network congestion, all the measurements are passive, which means that active packet streams are required. If a fault occurs, this information is passed to the upstream neighbor, which determine whether the fault is correlated to others. The agents send their monitored information to a central management station. This machine is responsible to provide a view to the entire network including possible reachability problems. This approach shows many problems. A lot of agents are required to allow measurements not only for one single multicast tree. The listeners do not join the multicast groups, this means that multi-access networks are required at each location of such agent systems. Additionally, layer-2 mechanisms such as IGMP-snooping or CGMP cannot be used to prevent network congestion in the local networks. Finally, active multicast streams are required. A pre-event analysis is not possible.

2.5. State of the art

Until now, only a few well known measurement methods are widely deployed. The network administrators are mostly familiar with tools such as mtrace but it is used only in the case of the occurrence of problems. No QoS measurements are deployed over wider areas in the multicast enabled networks. The primary reason is that all the tools show scalability problems. The most interesting approach today is the MRM. There are implementations for core routers (Cisco) as well as for end systems available. But also this approach shows some drawbacks. First, it does not distinguish between the measurement of the reliability and the quality. This results in an insufficient scalability. Additionally, the communication mechanism between the test systems and the management station leads to a heavy network usage in case of large test environment.

The Multicast Quality Monitor is directly based on the ideas of the MRM. It should solve most of the drawbacks of the MRM and of other measurement tools.

3. Multicast Quality Monitor (MQM)

This section introduces the Multicast Quality Monitor. First, the reachability measurement is discussed. The second paragraph gives a detailed view to the approach of the quality measurement. The inter-probe communication and the message format are shown next. The last part of this section is the presentation of measurement results using the MQM.

Basically, the MQM works like the MRM. The MQM also uses - properly placed - probes. All the probes implement the full functionality of the MQM. They allow reachability measurements as well as measurements of the quality of IP multicast connections.

3.1. Reliability measurement

In order to test the reachability in an IP multicast network, the probes sent MQM ping requests and act on incoming requests by replying with a MQM ping response.
Due to the principles of IP multicast routing, it is required to ping everyone from everywhere since it is not possible to use the information of A reaches B and C, and B and C both reach A via IP multicast to provide and information about the connection between B and C. To prevent an implosion of MQM ping messages, the multicast quality monitor uses a randomized delay before starting the first MQM ping request. Including more intelligence into the probes, it is possible to use ping response messages from two or three MQM ping requests to measure the reachability of the whole network between the probes.

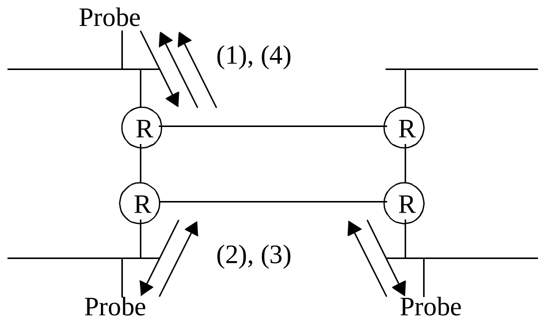

Figure 1. MQM ping mechanism

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 other probes listening to the used multicast group. The other probes receive this request (2) and send MQM ping response messages (3) toward the originator. These messages are received (4) by the requesting probe (all the other probes should also receive this MQM ping response allowing to use this information to prevent unnecessary messages, which would result in overloading the network with measurement traffic).
Each probe is required to send about one packet a minute to a configurable multicast group (we first thought about using a well-known multicast group but decided to let it be a configurable one). Lower rates do not refresh the forwarding state in the routers and result in indeterministic results. Higher rates are not required and just increase the network congestion. To get more information about the state of the network, it is necessary to use unicast pings (using ICMP messages) as well. Either, if there are failures in IP multicast connectivity or together with the IP multicast pings.
Until now, only the probes have the knowledge about the reachability in the IP multicast network. There are a few ideas how to summarize the information on a central point shown in section 3.3., MQM communication. This central management station is also required to calculate the reliability of the whole multicast network based on the reachability measurements.

3.2. QoS measurement

In order to measure the quality of service in an IP multicast network, it is first required to define the QoS parameters. The most typical IP multicast applications are audio and video 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 the applications use RTP as the transport protocol, because it already offers capabilities to inform the applications about the current situation in the network. There are sequence numbers and timestamps included into the protocol header. This is nearly all the required information to measure the QoS of the network. Therefore, RTP has been selected for the QoS measurements.
There are two groups of measurements mechanisms within the multicast quality monitor. The first one uses the MQM ping mechanism to measure the delay. The other one uses RTP streams to evaluate the packet loss ratio and the delay variation, the jitter.

3.2.1. Delay (one-way and round-trip)

The only QoS measurement from the MQM which is not based on RTP, is the delay. According to the work of the IPPM WG (IP Performance Measurements Working Group) of the IETF (Internet Engineering Task Force), the most important information for real-time services is the one-way delay. Based on the same ideas as for IP unicast, MQM uses its ping mechanism to measure both, the one-way delay 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. There are other working groups focussing this particular. The same MQM ping messages are used to calculate the one-way delay in both directions and the round-trip time. To ensure, that the MQM ping response message belongs to the MQM ping request sent from a particular probe (please note, every probe should receive every ping message because they are multicasted through the network), the IP address of the requesting probe is included in both, the MQM ping request as well as the MQM ping response. As well as for the reachability tests, multiple MQM ping response messages, initiated by two or three initial requests, can be used to prevent unnecessary requests leading to a lower network congestion.

3.2.2. Packet loss ratio and jitter

In order to measure both, the packet loss ratio and the jitter, MQM uses RTP streams [13]. There are two operation methods of the measurement tool. The passive one means that the probes join an active multicast session and decode the information out of the received RTP packets. This method has no impact on the IP multicast network but it requires information about the location of the sender and the transmission time. There can be some impact on the network, if the probes are not placed along the multicast tree from the sender toward all listening receivers. Additionally, RTCP reports are used to get information about the current quality toward receivers located in networks without installed MQM probes. In the active method, the probes simulate typical transmissions. The properties of such a simulated stream are configurable within the MQM (packet size, packet rate). Therefore, it becomes possible to test the behavior of the network without any active application. Of course, this has at least a little impact on the network. The simulation of high bandwidth video transmissions may disturb other IP connections (unicast and multicast) which are using the same parts of the network.

Using the model shown in section 4, it is possible to identify the parts of the network, which are responsible for the most critical IP multicast applications. Based on these information, the measurement probes can be deployed on proper places in the network.

It is always necessary to distinguish between the two most important types of IP multicast communication: a broadcast from a central station and a conference between several participants. A typical example of a broadcast is a video server [24]. Such broadcasts have some common properties. They tend to stream over a large period of time and they typically require a high data rate. If there are such services in the monitored network, it would be a good idea to use these RTP streams to measure the packet loss ratio and the jitter. If the probes are deployed directly on the multicast path, all the measurements are passive. Sometimes it can be useful to place some probes ’near’ the original multicast tree to include other parts of the network into the test scenario.

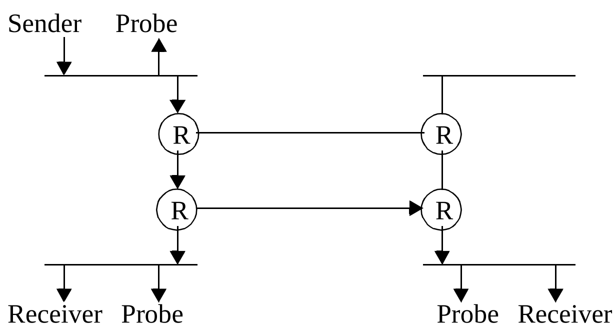

Figure 2. Passive QoS measurement using existing RTP sessions

Figure 2 shows a typical broadcast situation including the measurement probes. There is one sender broadcasting to some distributed receivers. The probes are located near the receivers (in the case of network errors of insufficient quality of service, it would be useful to have some of them located within the core network as well). It becomes possible to measure the current QoS without any impact on the network itself.

Compared with the already discussed broadcasts, most conferences are working like that. They last only for a short period of time, they start at announced times and the location of the members is almost known. At least this is true for most ’important’ conferences, one example is the conference between some managers of computing centers in Bavaria, Germany [23].

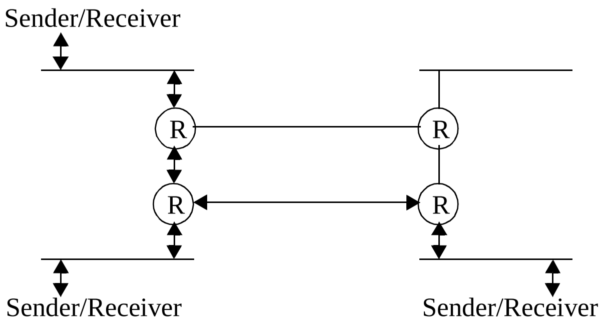

Figure 3. Setup for a typical conference

The idea is, to inform the members before they start their meeting about the current quality in the IP multicast network (to let them decide to start or to cancel the conference before they find out actual problems themselves). In order to achieve these results, probes have to be configured in all the used parts of the network to simulate the typical conference applications. This requires to initiate RTP streams like these in the real conference. Finally, all the probes receive the same traffic as if the conference would be already online. This principle allows to simulate the traffic of the meeting actively and to measure the QoS of the IP multicast network. Figure 3 shows an IP multicast network used by a typical conference. There are a number of participants. Everyone is sending and receiving traffic.

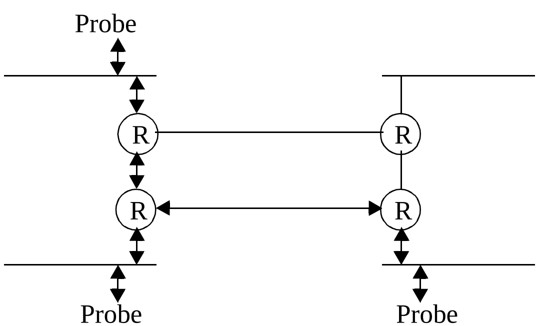

Figure 4. Active traffic simulation based on the knowledge about the configuration of the conference

Based on the knowledge about the network and the services, it is possible to simulate the conference by configuring intelligent probes to simulate RTP traffic and, finally, to receive and analyze it. This is shown in figure 4. The same configuration can be used to watch a conference and to measure the current quality without any simulation.

3.3. Inter-probe communication

The last two sections 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.

3.3.1. 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.

3.3.2. Starting the simulation of a RTP stream / starting analyzing a RTP stream

RTP streams are controlled using the beacon mechanism introduced by the MRM. The central management station can start and stop the QoS measurement via a beacon message sent to the same IP multicast group, which is also used for the MQM ping messages. Using this message, the manager tells the probes which RTP stream they should analyze and, if required, which probe should simulate which type of traffic. Due to the unreliable UDP transport of these beacon messages, they cover a maximum time to live (hold time) and the management station should send these beacon messages periodically.

3.3.3. 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 the information to the management station should be done on a periodical base. This transfer should work asynchronously from any measurements and directly unicasted to the management station using the TCP protocol. The protocol ensures the reliable transport of the measured data. Not yet defined is who should initiate this transfer, the probes or the management station. In order to allow a user to force the presentation of the current situation of the network, the management station should be able to initiate this transfer. Therefore, 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. A next version should allow a probe initiating the data transfer as well.

3.4. Message format

The message format of the MQM uses the same principles as the MRM. For the inter-probe communication, a separate header (MQM header) has been defined. Also, the beacon messages from the management station to the probes use the MQM header.

Position	Length (byte)	content
0	1	version
1	1	padding
2	2	type

Table 1. MQM header format

The MQM header is part of every MQM message. The encoding of the remaining data depends on the type value in the header. Table 1 shows the MQM header format.

Position	Length (byte)	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

Table 2 and 3 define header extensions for different MQM packet types. Currently, there are only three packet types: MQM ping request, MQM ping response and MQM beacon. The measurement of the packet loss ratio and the jitter is based on RTP streams. Therefore there is no special MQM packet type defined for these packets. The standard RTP packet header already includes all the required information. The timestamp field in the MQM ping message is used as a non-consecutive but constantly increasing sequence number as well. The sender is able to check for missing ping responses based on this mechanism.

Position	Length (byte)	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)

Table 3. MQM beacon message format

Position	Length (byte)	content
...	4	target probe address n
...	4	multicast group address n

Table 3. MQM beacon message format

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 packet format has been included to provide a more detailed view on the ideas of the MQM.

3.5. Sample measurements

This section provides the results of some measurements using the multicast quality monitor. All of them are taken between several universities in Germany connected by the German gigabit research network (G-WiN). The universities are connected by links of 622Mbps (OC-12) or at least 155Mbps (OC-3) to this network, which itself contains mostly of OC-12 and OC-48 (2.4Gbps) links. At each site, the end systems are interconnected by different kinds of university backbone networks. All the tests have been initiated from systems at the University of Erlangen.

3.5.1. MQM message based tests

We installed MQM probes at different sites within the German research network and started the measurement of the reachability between them including the measurement of the delay. Therefore, we used the results to compute the reliability of the network as well as the one-way delay and the round-trip time.

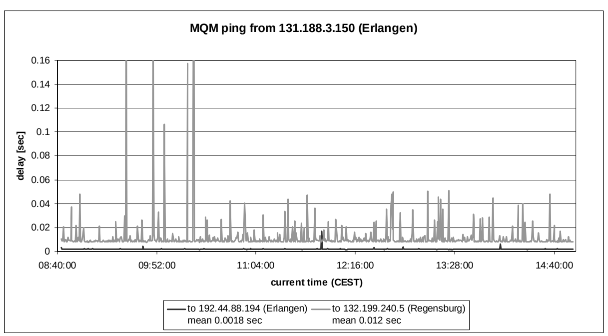

Figure 5. Delay measurement using the MQM ping mechanism

Figure 5 shows the results of a MQM ping test from a host at the University of Erlangen to another one at the same site as well as to one in Regensburg. The effect is as expected. The delay within the campus network in Erlangen is very short (about 0.0018 sec) and constant (both hosts are only two hops away). The delay to Regensburg is much higher (about 0.012 sec) and diversified.

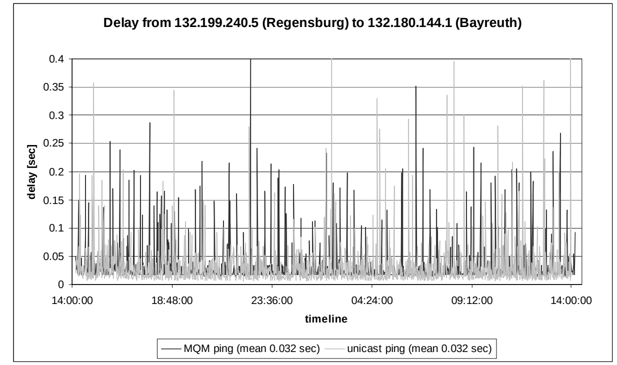

Figure 6. Delay using MQM ping (multicast) vs. ICMP ping (unicast)

Additionally, we used the unicast ICMP ping mechanism to compare the values from the unicast and the multicast test. One example is shown in figure 6. The results for the unicast ICMP ping show the same behavior as for the multicast MQM ping. The mean values for the round-trip time from Regensburg to Bayreuth is always about 0.032 sec, whether unicast is used or multicast.

3.5.2. RTP based tests

At our University, we have installed a tool, multicasting a TV channel to test multicast capabilities on the local campus network as well as of interconnections to other sites. Using this channel, we measured the quality of the transmission using the MQM tool, while the world soccer championship took place (giving us more participants than usual).

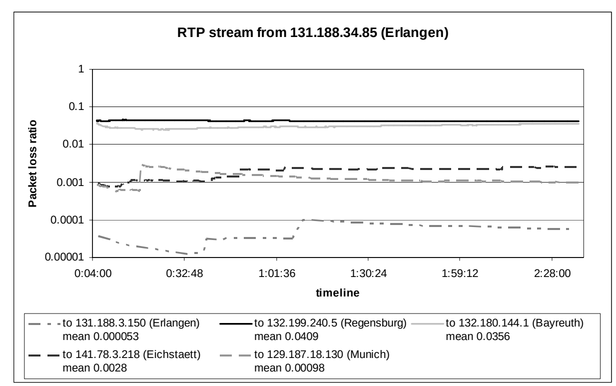

Figure 7. Measurement of the packet loss ratio using a RTP stream

Measurement examples are shown in figure 7. The ordinate is scaled logarithmically. Apparently, the packet loss ratio seems to be very constant but depends on the used parts of the network between the sender and all the receivers. It ranges from about 0.000053 for shorter paths up to 0.0409 for the transmission to Bayreuth (9 hops, high utilized links).

4. A Model for a service driven IP multicast network

As already mentioned in section 3, the multicast quality monitor (as well as all the other approaches discussed in section 2) requires very carefully located probes. A model proposed by Dressler [9] for IP multicast networks and the used services within this network should to solve this problem. This section gives a short abstract to the model. An implementation of this approach has been done by Juan Ceballos-Mejia at the University of Erlangen-Nuremberg [6] using JAVA.
Primarily, the model consists of two main parts. The physical multicast capable network and the overlying applications, the services. Figure 8 shows the object hierarchy. Additionally, an object containing routing algorithms is attached. These algorithms are used to calculate the multicast tree(s) for a particular service and therefore to identify the best locations for measurement probes to evaluate the reliability and quality of the required part of the IP multicast network. The current implementation used the Dijkstra algorithm [8] for the shortest path calculation.

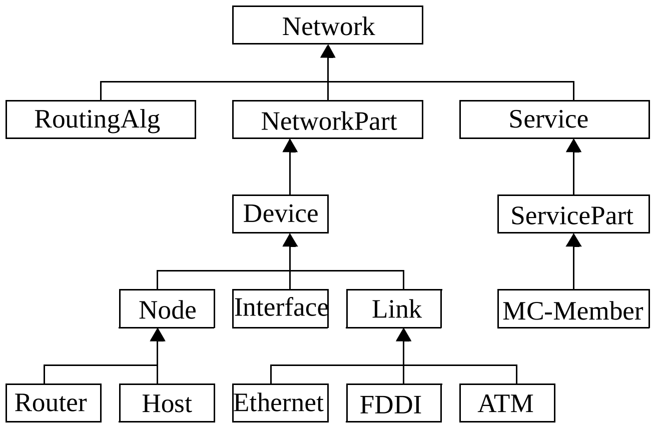

Figure 8. Object hierarchy for a model of multicast networks and services

A service is defined as a number of hosts transmitting to a set of multicast groups and a number of hosts receiving these data. Each object of class service stands for one multicast application, which may use more than one multicast group. As an example, there are different groups used for audio and video transmissions. The physical network consists of devices. The most important ones are nodes (routers, hosts) and links (network links such as ethernet, ATM or POS). Interfaces are responsible for interconnecting these two objects.
If the complete IP multicast network has been described using this model, as well as the most critical services, it becomes 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 analysis of the resulting multicast tree(s) (the used paths for the services) and for offline simulation of the expected network behavior.

5. Summary

Within this paper, a new approach to measure the reliability and the quality of service of an IP multicast network has been presented, the multicast quality monitor. Using distributed intelligent probes, is becomes possible to deploy active as well as fully passive measurements in the network. The definition of the MQM includes a new protocol for inter-probe communication. This protocol is the basis for all the reachability tests and some of the QoS measurements, in particular for the estimation of the delay, the one-way delay as well as the round-trip time. The packet loss ratio and the variation of the delay, the jitter, are calculated using the RTP protocol. This approach allows to use currently active RTP streams others than these sourced by the MQM probes. All the measurement results are transmitted to a central management station asynchronously from any measurement activity. This prevents unnecessary bandwidth consuming transmissions from and to the probes. The management station controls the measurement itself as well. Using beacon messages, simulated RTP streams can be started and the reception at the destination probes is initiated.
Completely new in this approach is the measurement of the one-way delay, which is, regarding to the IPPM WG, one of the most important values in real-time communications. Additionally, the strict distinction between the reachability tests and the QoS measurement is important in order to prevent network congestion sourced by measurement tools. The idea of the MQM is to measure the QoS depending on the services (applications) in the IP multicast network. Using the proposed model, it is possible to deploy the probes based on the requirements of the services. 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. Due to the possibility of an efficiently deployed measurement environment, the scalability of the MQM is much higher than in other approaches.
Considering the security, currently there are no authentication or authorization mechanisms included into the definition of the MQM. Therefore it is possible to introduce stealth packets if the attacker knows the multicast group used for the inter-probe communication. This allows to start denial-of-service attacks by sending beacon messages to the probes forcing them to start simulated RTP streams. So far, this was not a problem but the next version of the MQM will include authentication mechanisms into each MQM packet. Currently, the security can be enhanced by blocking the used multicast group at the border of the multicast network, which is to be examined.

6. References

[1] K. Almeroth, „Managing IP Multicast Traffic: A First Look at the Issues, Tools and Challenges,“ IP Multicast Initiative Summit, San Jose, California, USA, February 1999.

[2] K. Almeroth, K. Sarac, L. Wei, „Supporting Multicast Management Using the Multicast Reachability Monitor (MRM) Protocol,“ UCSB Technical Report TR2000-26, May 2000.

[3] K. Almeroth, L. Wei, „Justification for and use of the Multicast Routing Monitor (MRM) Protocol,“ Internet Draft, draft-ietf-mboned-mrm-use-00, IETF, February 1999.

[4] K. Almeroth, L. Wei, D. Farinacci, „Multicast Reachability Monitor (MRM),“ Internet Draft, draft-ietf-mboned-mrm-01, IETF, July 2000.

[5] I. Busse, B. Deffner, H. Schulzrinne, „Dynamic QoS Control of Multimedia Applications based on RTP,“ Proceedings to First International Workshop on High Speed Networks and Open Distributed Platforms, St. Petersburg, Russia, June 1995.

[6] J.-F. Ceballos-Mejia, „Design and implementation of a modeling tool for multicast networks,“ Master-Thesis, University of Erlangen-Nuremberg, 2000.

[7] K. Chen, M. Kutzko, T. Rimovsky, „Multicast Beacon Server v0.8,“ January 2002. http://dast.nlanr.net/projects/beacon/.

[8] E. Dijkstra, „A note on two problems in connexion with graphs,“ Numerische Mathematik 1, 1959.

[9] F. Dressler, „How to measure reliability and quality of IP multicast services?“ Proceedings of IEEE Pacific Rim Conference on Communications, Computer and Signal Processing (PACRIM’01), Victoria, B.C., Canada, August 2001.

[10] F. Dressler, „QoS considerations on IP multicast services,“ Proceedings of International Conference on Advances in Infrastructure for Electronic Business, Education, Science, and Medicine on the Internet, SSGRR 2002w, L‘Aquila, Italy, January 2002.

[11] B. Fenner, „Multicast Traceroute (mtrace) 5.1,“ December 1996. ftp://ftp.parc.xerox.com/pub/net-research/ipmulti/.

[12] W. Fenner, S. Casner, „A „traceroute“ facility for IP Multicast,“ Internet Draft, draft-ietf-idmr-traceroute-ipm-07, IETF, July 2000.

[13] C. Liu, „Multimedia Over IP: RSVP, RTP, RTCP, RTSP“. http://www.cis.ohio-state.edu/~cliu/ipmultimedia/.

[14] D. Makofske, K. Almeroth, „MHealth: A Real-Time Multicast Tree Visualization and Monitoring Tool,“ Proceedings of Network and Operating System Support for Digital Audio and Video (NOSSDAV '99), Basking Ridge, New Jersey, USA, June 1999.

[15] D. Makofske, K. Almeroth, „MHealth: A Real-Time Multicast Tree Visualization and Monitoring Tool“. http://www.nmsl.cs.ucsb.edu/mhealth/.

[16] R. Malpani, E. Perry, „mmon: A multicast management tool using HP OpenView,“ December 1999. http://www.hpl.hp.com/mmon/.

[17] „Multicast Routing Monitor,“ Cisco, Inc. http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/mrm.pdf.

[18] J. Postel, „Internet control message protocol,“ RFC 792, IETF, September 1981.

[19] J. Postel, „User datagram protocol,“ RFC 768, IETF, August 1980.

[20] K. Sarac, K. Almeroth, „Multicast Reachability Monitoring Protocol (MRM) End Host Implementation“. http://steamboad.cs.ucsb.edu/mrm/.

[21] K. Sarac, K. Almeroth, „Supporting Multicast Deployment Efforts: A Survey of Tools for Multicast Monitoring,“ Journal of High Speed Networking - Special Issue on Management of Multimedia Networking, March 2001.

[22] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, „RTP: A Transport Protocol for Real-Time Applications,“ RFC 1889, IETF, January 1996.

[23] Project „TKBRZL“. http://tkbrzl.bhn.de/.

[24] Project „Uni-TV“. http://www.uni-tv.net/index_en.html.

[25] J. Walz, B. Levine, „A practical multicast monitoring scheme,“ University of Massachusetts, Computer Science Technical Report 30-2000, June 2000.

About the author

Falko Dressler graduated in 1998 at the University of Erlangen-Nuremberg with a degree of a M.Sc. in computer science. Currently, he is working on his Ph.D. thesis at the department of computer science IV (operating systems) advised by Prof. Hofmann at the University of Erlangen-Nuremberg, which he expects to finish in 2002. His primarily research work is on IP multicast routing, Quality of Service measurements and multimedia transmissions over IP, IP multicast and ATM networks. He already contributed his research results to international conferences (including IEEE conferences) and to the IETF. He is a member of the ACM, the IEEE and the IEEE Computer Society.