Towards Autonomic Access Networks for Service QoE Optimization

Pieter Simoens*[1], Bart De Vleeschauwer[1], Wim Van de Meerssche[1], Filip De Turck**[1], Bart Dhoedt[1], Piet Demeester[1], Edith Gilon[2], Kris Struyve[2], and Tom Van Caenegem[2]

[1] Ghent University - IBBT - IMEC, Department of Information Technology
Gaston Crommenlaan 8 bus 201, 9050 Gent, Belgium
E-mail: Pieter.Simoens@intec.ugent.be
[2] Alcatel Research & Innovation
Copernicuslaan 50, B-2018 Antwerpen, Belgium

Abstract. Access networks are evolving towards an infrastructure for multiplay service delivery. IPTV is an important example of a currently popular service, transported over the access network to residential users. The QoE (Quality of Experience) requirements are very tight and it is therefore essential for a service provider to be able to provide sufficient guarantees on the service quality as perceived by the user. Since assuring QoE is a complex task, there is a need for a QoE monitoring and managing platform in access networks. We argue that this can be achieved by transforming the access network into an autonomic infrastructure that automatically detects service QoE degradation and is able to take appropriate action to restore it. A two-layered solution is proposed to achieve these goals. It consists of a monitor plane to gather the required information from the network elements and a knowledge plane to analyze the monitor information and react accordingly. We foresee a key role for the access node that connects the residential users with the access network. Examples of the functionality of both planes in the access node will be given.

1 Introduction

The current broadband access networks enable a myriad of new multimedia experiences, covering Broadcast TV, Video On Demand (VoD) and VOIP. For all these services the Quality of Experience (QoE) is of prime importance. This general term describes the service quality as it is perceived by the end-user. Packet loss, network congestion, delay and jitter are the main causes of QoE degradation. However, the appropriate actions to restore the QoE are highly dependent on the affected service and the actual network situation. We propose to automate the QoE management, so the stringent QoE requirements can be met under all circumstances and the network operator is relieved from doing

* Research Assistant for the Fund of Scientific Research, Flanders (FWO-V)
** Postdoctoral Fellow for the Fund of Scientific Research, Flanders (FWO-V)

William Donnelly et al. (Eds.): Modelling Autonomic Communications Environments 1st IEEE Intl. Workshop, MACE 2006, Dublin, Ireland, 25-26 October, Proceedings

manually this complicated task. By extending the management tool towards a pro-actively monitoring and reasoning tool, a completely autonomous and self-managing access network with high QoE guarantees is achieved.

In [1], the concept of a knowledge plane in the Internet was introduced, as an enhanced network that enables the automatic detection and recovery of faults. Here, we apply this paradigm to the access network and propose to use a two-layer approach to achieve the expected behavior. The first layer is the Monitor Plane (MPlane), which gathers monitor information in the devices along the path from edge router until the actual end device. On top of this monitor plane, a Knowledge Plane (KPlane) is deployed that guarantees the accordance of the QoE for each service with the minimum requirements as set by the network provider. The KPlane is able to identify problems and to locate the actual cause of the QoE decrease. By reasoning on the information provided by the MPlane, the KPlane can propose a solution and undertake the appropriate actions to restore the degraded QoE. Pro-active monitoring and acting of the KPlane could even avoid the drop of the QoE below the acceptable threshold. This paper elaborates on how both layers cooperate to achieve autonomous QoE management. The functionality of both layers on the access node will be presented in more detail.

This research is part of a broader and more comprehensive vision on future service-aware access networks that is under study in the integrated research project MUSE [2]. The overall goal of the MUSE project is the research and development of a future, low cost, multi-service broadband access network. MUSE is studying the QoE requirements and architecture for various services. This paper reports on the introduction of intelligence in the access network, so that it is able to guarantee autonomously these QoE requirements.

The remainder of this paper is structured as follows. In section 2 we give an overview of a typical access network and section 3 contains related work in the field of autonomic network monitoring and intelligent reasoning. Section 4 describes the architecture of both monitor and knowledge plane and their cooperation. Section 5 applies these concepts to the access node and details which actions can be taken from the access node. Finally, conclusions are drawn in section 6.

2 Access Network Overview

When observing the connection between the service provider and the device that is actually presenting the content to the user, there are a number of components with a distinct functionality, which are all presented in Figure 1 and discussed next:

- Application servers: The service provider can have a number of servers connected to the edge router in the access network. Examples are a video-on-demand or broadcast TV head-end.
- Edge router: The edge router provides the connectivity to the public Internet and to other services that are accessed from the end-devices.

- Aggregation network: To connect the edge router to the access nodes of the subscribers, an aggregation network is used. Traffic in this network is mostly transported in different classes, allowing service prioritization. More and more aggregation networks are Ethernet-based.
- Access node: The access node terminates the aggregation network and serves as an access multiplexer to provide the connectivity with the end-devices. We assume that the access node is also equipped with the ability to intercept and parse traversing packets and can decide to alter/drop these, based on dedicated network layer filtering and processing capabilities.
- User connection: In this paper, we assume the user is connected via a DSL line, offering broadband access.
- Home gateway: The home gateway connects the access network and the home network. In addition to this, home gateways typically perform a number of additional tasks like firewalling and Network Address Translation (NAT).
- End device: The end device is located in the home network and is used directly by the user of the service; it can be a Set Top Box (STB), a game console or a standard desktop pc. The connection between the home gateway and the end device might be provided over a wireless network or via a fixed cable (e.g. Ethernet).

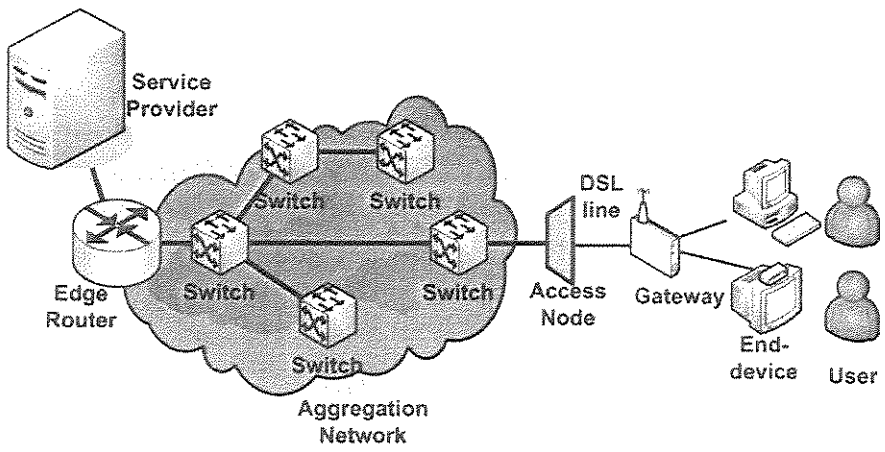

Fig. 1. An overview of the access network.

3 Related Work

In [3] a general description of autonomic computing is given. The need for autonomic computing is motivated by the steep increase in the complexity of applications, the migration from distributed heterogeneous applications to a network of interconnected distributed applications and the huge and unpredictable workload generated by these systems. A core autonomic element is comprised of four

parts: a monitor part, an analysis module, a plan module and an execute part. The core concepts defined by IBM, resurface in the autonomic access network that we envision.

For detecting and analyzing application QoE, the rmonbib working group of the ietf is developing the Raqmon framework [4]. This framework provides a mechanism for real-time reporting of QoE for devices and services. One of the strengths of this framework is that it correlates statistics on the transport network, the end-device and service specific parameters.

The concept of ontology data models is well suited to structure and arrange the available monitor data. An ontology is a data model that represents a domain and that is used to reason about the objects in that domain and their relations. These objects are instances from logical classes to which attributes can be assigned. Ontology Web Language (OWL) is a widely used ontological language, recommended by the W3C [5]. Querying on ontology languages can be performed in a number of ways, like exact lookup based on the name, but also based on properties or characteristics. Reasoners, like Racer Pro [6] and Pellet [7], allow to check the consistency of the data model. Important in the scope of this paper is however the capability of reasoners to derive and locate concepts in the data model that match the properties specified in a query. By modelling the monitoring data and the relationship between network and service components in an ontology, the reasoner can be a promising approach to realize intelligent and autonomous QoE recovery in an access network.

4 Autonomic Access Network Architecture

The autonomous access network consists of two logical layers, the monitor and the knowledge plane. Both layers are stretched out over the whole access network, from edge router up to (and including) the end-device. The MPlane monitors the status of the network and devices as well as the QoE of the running services. The KPlane is responsible for analyzing the monitor data, for detecting a decrease in service QoE and for taking appropriate actions to restore it. These two layers are distributed over the different entities in the access network and also contain central components. In this section we describe the general architecture of these two layers and their position in the access network. In Figure 2 the parts and interactions of the MPlane-KPlane are depicted.

4.1 Monitor Plane

The main function of the monitor plane is to provide a detailed view on the network by monitoring the services, switches, routers and devices, as well as their interconnecting links. As the monitoring happens continuously and across the whole network, the data must be summarized and correlated both temporarily and spatially. To do this, dedicated data structures that can easily be read out and analyzed by the KPlane are used. The MPlane exports the monitor information via an API to the KPlane. This API also allows the KPlane to

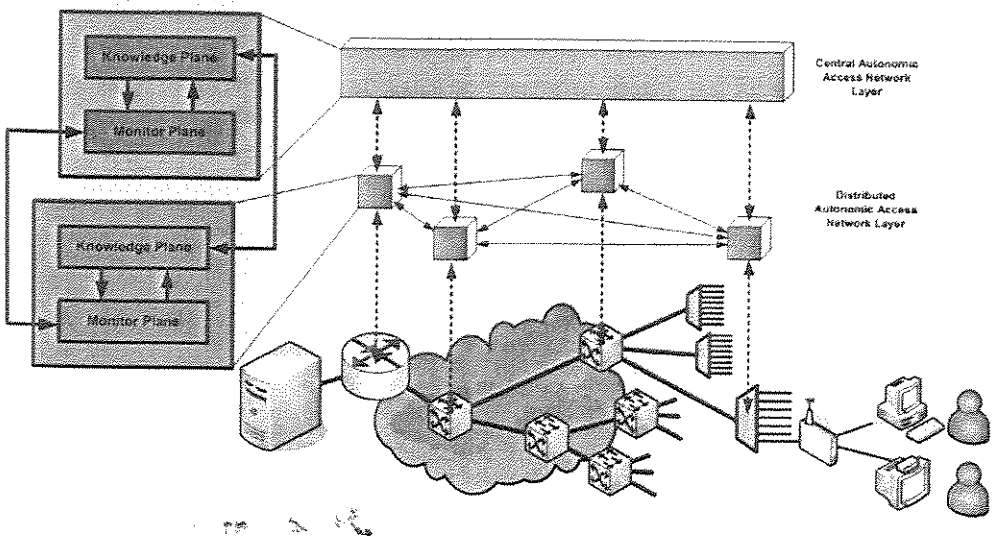

Fig. 2. An overview of the distributed MPlane-KPlane architecture.

initiate monitoring tools in the MPlane to gather additional information, or to execute additional data processing on the available data.

The MPlane is distributed over the access network and gathers data that is maintained on the devices itself for local analysis. On the other hand, there is also a central platform to which monitor information of the whole access network is pushed and that can request data from the distributed components. The decisions on where the information should be stored and can be accessed by the KPlane.

Because network monitoring is an already extensively investigated research field, a broad range of monitoring tools is available for each part of the access network. The Simple Network Monitoring Protocol (SNMP) can be used for monitoring the aggregation switches. It allows to read and write parameters on these devices and to set traps for asynchronous communication with the central managing device. The parameter structure is specified in a Management Information Base (MIB), like the MIBs defined by the rmonmib working group of the IETF [8]. IPFIX [9] is another technique to monitor switches and edge routers allowing the tracking of individual flows. Information on the quality of the access line between home gateway and access node can be retrieved e.g. from the gateway by using the TR-069 [10] interface via an Auto Configuration Server (ACS). The monitoring of the home network is perhaps the most challenging task. It is important to extend the reach of the MPlane to the end-devices since the cause of QoE degradation is often located in this part. In a previous paper [11], we argued that passive monitoring is the most viable solution. Active monitoring introduces additional traffic that is sometimes treated differently than the original data [12]. It was shown that the accuracy of active monitoring results can be problematic. By using passive monitoring, information can be retrieved on the QoE as it is experienced by the end-user.

4.2 Knowledge Plane

The knowledge plane is an autonomously acting layer on top of the monitor plane, that uses the information made available by the MPlane. Based on this information, it is able to detect the problems that may arise. Besides this proactive aspect, there's also a reactive functionality: when a problem is detected (with a QoE degradation as a result), the KPlane executes the appropriate actions to enforce a solution. A solution can involve activating service specific enhancements and/or reconfiguring equipment.

MPlane-KPlane Interaction In the MPlane - KPlane architecture, one of the essential components for realizing the autonomous character of this layer on top of the access network is the interaction between the two layers. The MPlane not only makes data available for the KPlane to analyze. Their relationship goes far beyond the simple reading of parameters from a database. In both [13] and [14], data structures are used to summarize the monitor information that can be obtained and algorithms for analyzing them and detecting anomalous behavior are described. We could use such techniques for problem detection and identification. This example illustrates the typical interaction between MPlane and KPlane, where the MPlane takes care of the actual monitoring and saving of the monitored data in dedicated data structures, and the KPlane correlates and analyzes this information to detect problems. In addition to this, the KPlane is also able to instantiate new monitor probes in the MPlane, as this might be required when the present monitor information does not provide the KPlane with enough information to determine the root cause of a detected problem. The KPlane is also able to set alarms in the MPlane to notify the KPlane when something important happens. An example of this could be the triggering of an alarm when a counter on an Ethernet switch exceeds a predefined value.

Root Cause Determination The monitor plane provides real-time updates of the status of the network. As described in the previous section, this huge amount of information is aggregated. This data has however no value on its own but must always be related to other local and global information. For example, reported packet loss is not always an indication of QoE decrease, as this might be solved by underlying mechanisms such as retransmissions so the user does not notice any service degradation. If several home networks are reporting QoE decrease for the same service, the root cause will most likely be situated in the access network. Hence, spatial correlation - comparing data generated at two or more different locations - is important. Another source of valuable information is temporal correlation of monitoring data. Both small and long term increases of e.g. jitter can then be discovered.

Monitoring information and generated alarms however are only indications of a network failure. To accurately track the root cause of the problem, the whole network context must be modeled. This model must not only contain all components of the network, but must also express their relations. As mentioned in

section 3, ontology data models are well suited for this objective, combined with reasoners to extract implicit knowledge from the data model. In the previously given example of packet loss, the reasoner could first look up the communicating entities when a connection exhibits packet loss, as each connection has a source and destination attribute. Then, by consulting the topology database, the packet route can be determined and the interconnecting link states can be queried. This results in the localisation of the congested links.

KPlane Actions A last step that the KPlane must undertake is providing a solution for any QoE decrease taking place. This can be achieved in a number of ways and is of course highly dependent on the service and the exact nature of the problem cause. For an IPTV service, the KPlane could decide to adapt the videostream by applying techniques like interleaving or forward error correction. Other actions can be the reconfiguration of the network entities, taking into account the full network topology, to avoid congestion of some access network links. This could be rerouting traffic or setting different priorities for access network traffic classes. More details will be provided in the next section.

A Distributed Knowledge Plane The KPlane is distributed and is not restricted to a central platform where all the monitor data is gathered and analyzed. This is motivated by the observation that a lot of monitor information only has local significance and should thus be analyzed locally. For instance, when the QoE of a service is deteriorating due to loss in the home network itself, this can be detected in the access node. Therefore, there is no need to inform a central platform of this observation. Possible actions to restore the service, such as retransmitting packets from the access node can also be triggered at the access node. The fact that access networks often have a tree like topology also advocates detecting and solving problems locally, since a lot of information has an explicit local scope.

Although part of the monitor information has only a local scope, other information might also be relevant in other parts of the access network. Some failures can only be detected at a higher level in the KPlane, e.g. a lot of clients, behind different access nodes can suffer from deteriorated services when some link in the access network is congested. While this information can be detected at the corresponding Ethernet switch, the appropriate action of rerouting traffic may only be taken at a higher layer in the knowledge plane that has information on the whole access network topology, in order not to degrade the QoE of more clients when the rerouting would congest even more links.

The remainder of this paper elaborates on the the MPlane and KPlane functionality in the access node.

5 Autonomic Access Node

Most access networks are organized in a logical tree-like topology (a number of extra links are added to provide resilience), with the service edge as the root node

and the so-called access nodes being the leaf nodes. Each access node connects a group of users to the network and has a dedicated physical connection to each of them. Installing an intelligent self-organizing component on the access node is motivated by many benefits. First of all, it is the nearest point to the home user that is still completely under the control of the access network provider, since access to the home network might be hindered by firewall and NAT devices. Therefore, the access node is the ideal place to determine if the root cause of a QoE degradation is situated in the home or the access network. Finally, it is the only place in the operator network where all data of all services of the same user passes through. This enables the correlation of monitoring information not only per service but also per user, which is a valuable source when taking intelligent actions to restore the QoE.

In the previous section, we detailed the architecture of the autonomous access network. We will now apply the MPlane and KPlane concepts to the access node. A range of examples of QoE restoring actions will be given. On Figure 3, a conceptual presentation of the autonomous access node is given.

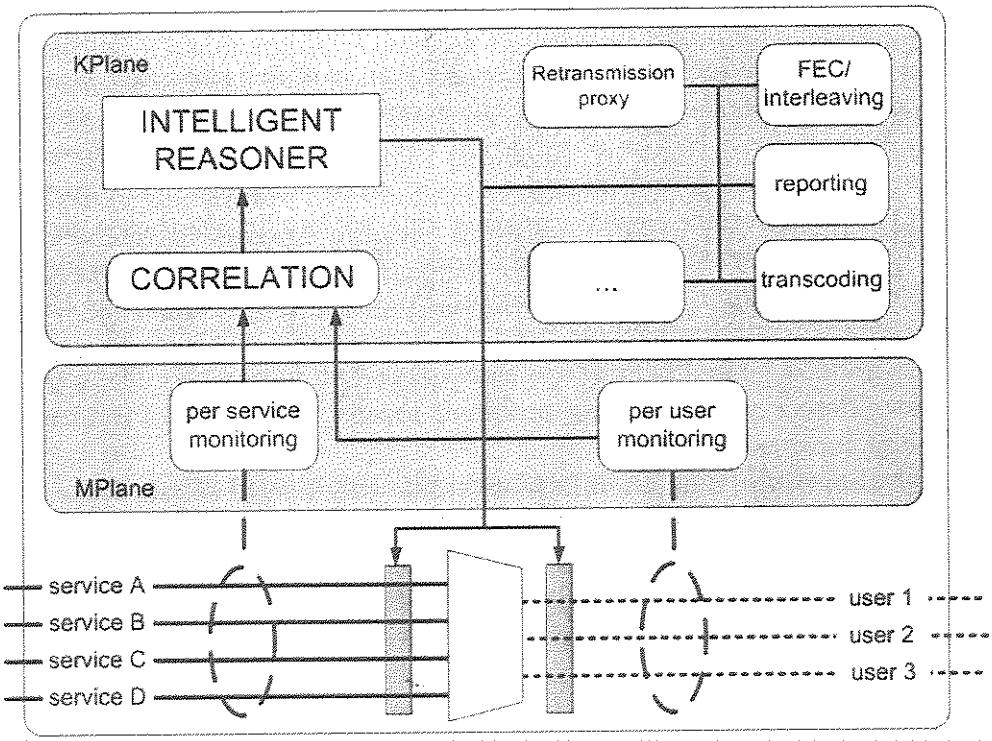

Fig. 3. MPlane and KPlane functionality in the access node.

5.1 Access Node Monitoring

The access node can easily provide information on the running services of each connected user and their QoE. It also processes IGMP join and leave messages

when a user is switching his IPTV broadcast channel, checks the link connectivity to the user, imposes bandwidth restrictions and optionally subscription conditions like up- and download limits. As such, a lot of relevant information is already present on the access node. The additional information that can be obtained by packet sniffing depends on the transport protocol that is to be monitored:

TCP TCP is reliable transport protocol that forms a cornerstone of current IP networks. It is used for internet download and web services internet traffic, but is also a candidate to transport IPTV services like Video On Demand. TCP adjusts its throughput to network congestion, using packet loss as a method to measure congestion. Packet loss is detected indirectly by timeout of acknowledgment packets. Non-congestion loss and excessive jitter cause unneeded timeouts which slow down TCP connections, since TCP will automatically downscale its sending rate. Round Trip Time (RTT), packet loss and jitter are the most interesting parameters to monitor. Monitoring RTT between client and server in an intermediate point is a rather non-trivial problem and several methodologies have been proposed in literature [15] [16]. Measuring delay jitter built up on the access line and in the home network is easier, as one can simply calculate the elapsed time between a data packet passing the access node and the acknowledgment packet sent in reply. This works well for RTT measurements in stable TCP connections. However, this approach fails to measure RTT (and thus detect jitter) when excessive jitter causes unneeded timeouts, which is something that we certainly want to detect. We are currently developing an algorithm that overcomes these limitations and is able to make a precise estimate of jitter and packet loss, based on monitoring the TCP connection in the access node.

RTP/RTCP Applications like Broadcast TV, Video on Demand and Voice Over IP often use the real-time transmission protocol (RTP [17]). This protocol is specifically designed for the timely delivery of multimedia data and is accompanied by the RTP Control Protocol (RTCP) to distribute feedback on the quality of the multimedia session as perceived by all participants. These RTCP reports contain valuable information for service monitoring such as the fraction of lost packets, the total number of lost packets since the beginning of the multimedia session and a jitter estimation between sender and receiver. The RTT can easily be derived by combining some of the reported parameters with a time tracking mechanism on the access node. To monitor services running on top of RTP/RTCP, all RTCP reports are intercepted on the access node. Packet loss taking place on the access line and in the home network can also be measured by comparing RTCP reports with the number of packets that passed through the access node.

The knowledge base can be further enriched by combined service monitoring and correlation of monitor data of different acces nodes. Additional information on the QoE of the user can be retrieved by combining monitoring information of all services of the same user. For example, if for all services an increased level

of packet loss is detected, this will results in other actions of the KPlane than when only one service is suffering from packet loss. In other situations, it will be more appropriate to compare QoE monitor information of multiple users for the same service. When all users report a decreased QoE, the cause is probably situated in the access network and it is more appropriate to undertake actions in that part. It is therefore useful to install a reporting mechanism on the access node, which communicates with a central platform, the latter having access to all other access nodes. Both summarized as raw monitored data may be provided to this central platform. If the access node concludes that actions are needed in the access network, it might send out a hint report, together with the necessary data. Data can also be provided on-demand to the central platform.

5.2 Access Node QoE Restoration & Optimization

Once the intelligent agent of the knowledge plane on the access node has determined the root cause of a QoE degradation, the required restoring actions must be undertaken. Besides a reasoning component, the access node will therefore be provided with a large set of tools to complete this task. Issuing additional monitoring data requests and reporting to the central platform are included in the list of possible actions. The following examples illustrate the autonomous and intelligent access node that we envision.

- Packet loss on the DSL line results in a QoE decrease of a user watching a video, because it causes visual distortions. Techniques like application layer Forward Error Correction (FEC) or application layer interleaving could be activated on the access node to restore the QoE and reduce the impact of packet loss.
- For some problems, the root cause detection will only be possible at a higher level. Intelligent reporting of the access node then contributes to a fast root cause detection. For example, the access node can be instructed to report on the retransmission request pattern per household or per channel.
- Sometimes the codec specifications of a multimedia stream multicast on the access network do not completely match those of the device on which a user wants to receive the stream. If the access node notifies a mismatch between the stream and a device requesting the service, it might activate a transcoding or transrating service to adapt the stream to the device specifications.

The previous examples realize the QoE restorative behavior that we require from the access network. However, we would like to emphasize that the KPlane functionality can be much broader. For instance, when a large number of users is downloading the same content, e.g. in a VOD scenario, this can be detected by the KPlane. In this case, the KPlane could decide to move the content to a VoD proxy at the access node. Since the content is only sent once from the server to the access node, the amount of used bandwidth in the aggregation network is reduced.

6 Conclusion

In order to guarantee a good QoE for multimedia services on an access network, we proposed a double-layer solution. The Monitor Plane retrieves information on the service QoE and the network status. This data is the input for the Knowledge Plane, which is provisioned with intelligence for planning and taking the appropriate actions when the QoE degrades. A key role is foreseen for the access node. We described the general architecture of the Monitor and Knowledge Plane and zoomed in on the role of the access node in this concept.

References

1. Clark, D.D., Partridge, C., Ramming, J.C., Wroclawski, J.T.: A knowledge plane for the internet. In: SIGCOMM '03: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, New York, NY, USA, ACM Press (2003) 3–10
2. Muse: Multi service access everywhere (2004-2007) http://www.ist-muse.org.
3. IBM: An architectural blueprint for autonomic computing (2003)
4. Siddiqui, A., Romascanu, D., Golovinsky, E.: Real-time application quality of service monitoring (RAQMON) framework (2006)
5. W3C: Owl web ontology language overview, w3c recommendation (February 2004) http://www.w3.org/TR/owl-features/.
6. Racer Systems: Racer Pro: The well-known Reasoner for the Semantic Web languages OWL,RDF (2006) http://www.racer-systems.com.
7. Mindswap: Pellet is an open-source Java based OWL DL reasoner (2003) http://www.mindswap.org/2003/pellet/.
8. Waldbusser, S., Cole, R., Kalbfleisch, C., Romascanu, D.: Introduction to the Remote Monitoring (RMON) Family of MIB Modules. (RFC 3577 (Informational))
9. Quittek, J., Zseby, T., Claise, B., Zander, S.: Requirements for IP Flow Information Export (IPFIX). RFC 3917 (Informational) (2004)
10. DSLForum: Technical Report 069: CPE Management Protocol (2004)
11. De Vleeschauwer, B., Van De Meerssche, W., Simoens, P., De Turck, F., Dhoedt, B., Demeester, P., Gilon, E., Struyve, K., Van Caenegem, T.: On the enhancement of QoE for IPTV services through knowledge plane deployment. In: Broadband Europe. (2006)
12. Barford, P., Sommers, J.: Comparing probe- and router-based packet-loss measurement. IEEE Internet Computing **8**(5) (2004) 50–56
13. Cormode, G., Muthukrishnan, S.: What's new: finding significant differences in network data streams. IEEE/ACM Trans. Netw. **13**(6) (2005) 1219–1232
14. Krishnamurthy, B., Sen, S., Zhang, Y., Chen, Y.: Sketch-based change detection: methods, evaluation, and applications. In: IMC '03: Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement, New York, NY, USA, ACM Press (2003) 234–247
15. Benko, P., Veres, A.: A passive method for estimating end-to-end tcp packet loss. In: IEEE Globecom. (2002)
16. Lance, R., Frommer, I.: Round-trip time inference via passive monitoring. SIGMETRICS Perform. Eval. Rev. **33**(3) (2005) 32–38
17. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications. (RFC 3550 (Standard))

William Donnelly
Radu Popescu-Zeletin
John Strassner
Brendan Jennings
Sven van der Meer (Eds.)

Modelling Autonomic Communications Environments

First IEEE International Workshop, MACE 2006
Dublin, Ireland, 25th–26th October 2006
Proceedings

multicon lecture notes – No. 2

multicon verlag
Schöneiche bei Berlin

The main challenge to making network management autonomic is to introduce the ability of the network to self-govern its behaviour within the constraints of the business goals that the entity operating the network seeks to achieve. Autonomic network management can be realised through the use of information modelling to capture *knowledge* relating to network capabilities, environmental constraints and business goals/policies, supplemented by reasoning and learning techniques to enhance and evolve this knowledge. Knowledge embedded within system models will be used by policy-based network management systems incorporating translation/code generation and policy enforcement processes that automatically configure network elements in response to changing business goals and/or environmental context. This realises an autonomic control loop, in which the system senses changes in the itself and its environment, analyses this information to ensure that business goals and objectives are being met; expedites changes should these goals and objectives be threatened, and observes the result.

The model-centric approach will deliver considerable improvements over existing statically configured network management systems, since it will support the reconfiguration of networks with minimal human intervention at all but the high-level business view. However, to deliver full autonomic network management capabilities it is also necessary to introduce processes and algorithms into the network infrastructure to maintain optimal or near-optimal behaviour in terms of global stability, performance, robustness and security. In particular, some of these processes and algorithms can be profitably modelled on various biological processes found in the natural world. Furthermore, to ensure that they act in accordance with business goals such processes and algorithms should themselves be modelled, so that their operation can be automatically configured via appropriate policies.

The IEEE International Workshop on Modelling Autonomic Communications Environments (MACE 2006) was held as part of Manweek 2006 in Dublin, Ireland, from October 25th to 26th, 2006.

ISBN 3-930736-05-5

9 783930 736058 >