A Policy Management System for Hybrid Networks

N Vardalachos†, J Rubio‡, A Galis† and J Serrat‡

† University College London, ‡ Universitat Politècnica de Catalunya

Abstract: The management of heterogeneous and hybrid networks has always been a challenge for network operators. Different frameworks and architectural approaches have been proposed and investigated in the literature. This paper describes the policy based management architecture devised for management of IP over WDM networks and is part of the work carried out in the IST Project WINMAN [1], whose aim is to develop and validate an open and flexible integrated management system for this type of networks.

1. Introduction

In recent years it has become apparent that the transportation of IP based applications will be the dominant factor in future networks. At the same time equipment for Wavelength Division Multiplexing (WDM) has matured sufficiently to give the very high capacity networks (terabit transport networks [2], [3], [4]) that will be needed for the ever-increasing amount of information. It was soon realised by the telecom industry and the research community that the convergence of those two technologies would form the solution to future networking, offering a universal, reliable and ultra-fast solution. Next generation network architectures focus on eliminating the intermediate layers between IP and optical, thus minimising encapsulation overheads and complexity. The key challenges in the deployment and use of these networks is the efficient management of their resources and migration strategy from the existing network and management infrastructure to the new one. Management of such networks in an integrated fashion is a large research area. Different approaches to network management have been developed through the years; such include approaches as the TMN, ODP, TINA-C, WBEM and Policy Based Management.

Most trends in IP-WDM integration are extensions of the distributed Internet network control approach to the Optical Layer using signalling mechanisms either in an Overlay model or a Peer model. This paper proposes an alternative approach for managing Internet services over the Optical Transport Network by extending the telecom-style policy based network management approach to the IP layer over WDM. The proposed management solution has been adopted and is being investigated by the WINMAN project.

2. The WINMAN System

The WINMAN management system has been designed by applying mainly Open Distributed Processing (ODP) principles taking also into consideration the Telecommunications Management Network (TMN) framework. The TMN architecture structures the management complexity by layering the management applications, defining a common data model, enabling re-use of management data, and specifying system interfaces. ODP goes one step further, enabling the design of management applications that are independent of distribution, the underlying infrastructure and management protocols.

As shown in Figure 1, the WINMAN architecture consists of an Inter-Domain Network Management System (INMS) for Configuration, Fault and Performance Management on top of two Network Management Systems (NMS) for both IP and WDM technologies. As shown in the figure, the management systems for ATM and SDH are considered as well although they are not going to be taken into consideration at the design and development phases. The INMS has open interfaces to the Service Management and the Network Management Systems of the different domains (WDM, IP, ATM, and SDH) and it is accessed by some categories of users through a GUI. The roles and actors in WINMAN are so diverse that other categories of users may prefer the access though an API instead of a closed GUI.

The development of the WINMAN architecture was based on a subset of the CORBA Component Model (CCM) [5] with extensions specially conceived for the integrated management of IP and WDM. This approach adheres to WINMAN all the benefits of the component-based technology. The components of the WINMAN systems could be distributed over a number of nodes connected by a Data Communication Network. The degree of distribution in that case is transparent to the components of the WINMAN solution. The components do not have knowledge on the location of the other components, whether they are collocated on the same node or running on a node thousands of kilometres away.

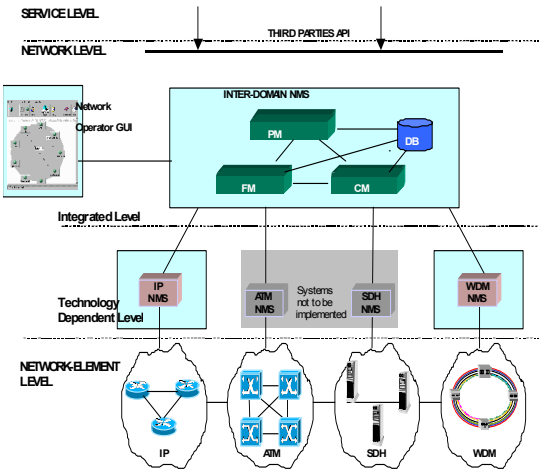

Figure 1: WINMAN Management Architecture

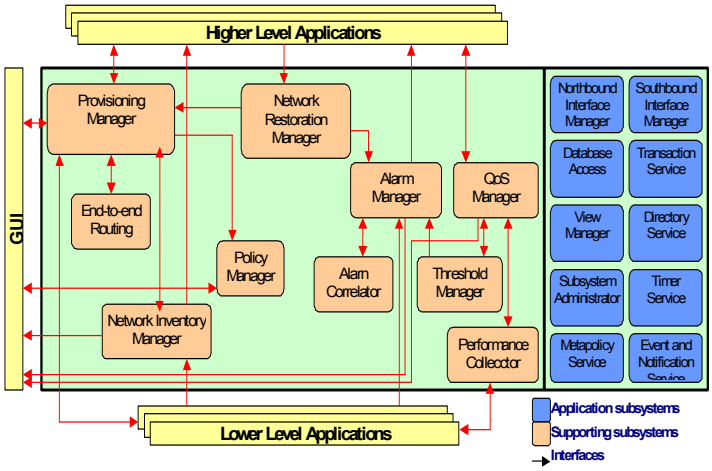

Figure 2: WINMAN Generic NMS Architecture

The INMS views all the inter-technology (inter-NMS) connections and coordinates the network provisioning, fault management and performance management between all technological domains. All these three systems share similar functionalities at their network management layer, so the approach adopted by the WINMAN project was to build a Generic Network Management System (GNMS) [6] with all the common functionalities of the three systems. The GNMS subsystems are shown in Figure 2. From that generic NMS architecture three NMSs have been specialised and further refined, and are currently being developed by the WINMAN consortium.

The Provisioning Manager is in charge for provisioning the IP services. It manages the provisioning process, including scheduling. The End-to-end Routing performs the design of the end-to-end connections inside its own network, taking into account QoS constraints and routing policies. The Network Inventory Manager is responsible to store, update, maintain and provide information about the data that WINMAN uses related to network physical resources, according to the information received from the network element layer and the GUI system. The other blocks will use these data.

The Policy Manager is responsible of managing and providing policies, necessary to make decisions in a variety of actions. For instance, it checks a provision request against the correspondent policies. Alarm and performance mechanisms can be policy oriented. The routing and the restoration mechanisms can also be controlled by policies. The Alarm Manager receives alarms from the Lower Level Application, triggers alarm correlation, stores alarm data and distributes alarms to other systems and subsystems. The Alarm Correlator filters, correlates and evaluates the alarms to find out their root cause and generate new alarms, sending the results to the alarm manager. The QoS Manager monitors and analyses the QoS data of the paths provisioned in the network and sent by the Lower Level Applications. It also provides performance data to the GUI and the Higher Level Applications. The Threshold Manager checks counters against the defined thresholds in order to generate alarms and reports if the thresholds are passed. The Performance Collector collects performance data from the Lower Level Applications. The Network Restoration Manager is responsible for the network restoration actions taken in order to prevent the disruption of the provided connectivity services. These actions are taken when alarms from the Alarm Manager arrive to the Network Restoration Manager subsystem.

The WINMAN system offers a northbound interface where Service Management Systems (SMS) might plug-in and request IP connectivity services. This interface complies with the Connection and Service Management Information Model CaSMIM [7] standard from the TMForum. The system also interfaces through its southbound interface with one or more Element Management Systems (EMSs), through an interface compliant with the Multi-Technology Network Management (MTNM) standard [8].

3. The Policy Manager

As a general remark, the operation of the Policy Manager was foreseen as a support component that becomes active in response to internal (the WO) or external events. These second type of events are to be raised by the Provisioning Manager and the End To End Routing module. Policies allow modifying the system behaviour dynamically; they are persistent but can be changed on the fly; this means than the WINMAN system's behaviour can be changed without recompiling, just adding/changing policies. The insertion or deletion of a component is known to the rest of the components by means of the infrastructure naming service. As a

supporting component, Policy Manager adds value to the system by providing services to the rest, but its presence shall not be a prerequisite for system operation. The idea is that the Policy Manager clients (WINMAN components that use Policy Manager functionality) would have a default "permit any" policy that allows their operation in case of Policy Manager absence. If the Policy Manager is running, then the policy-based value is added to the system.

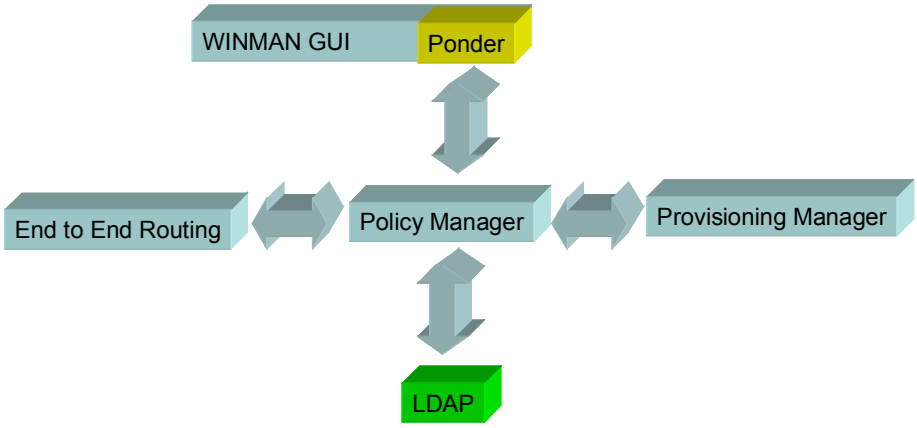

Figure 3: The Policy Manager Interactions

The Policy Manager interactions with other components can be seen in Figure 3. The WINMAN policies are managed through the WINMAN GUI. The Ponder GUI has been integrated to the WINMAN GUI in order to provide the WINMAN operator with a single interface to the system. Also, the Policy Manager interacts with the End to End Routing and the Provisioning Manager acting as a server, verifying whether use of routes (from the routing manager) or provisioning requests (creation/ modification/ deletion of routes from the provisioning manager) can be granted. Finally the policies are stored on an LDAP server (iPlanet Directory Server).

4. WINMAN Authorisation Policies Scenario

The authorisation policies can come in two flavours, positive and negative authorisations. The Ponder language supports both types. Authorisation policies are designed to protect target objects and are conceptually enforced by the target objects. In practice, authorisation policy enforcement is delegated to one or more enforcement agents that intercept actions and performs checks on whether the access is permitted. The authorisation policies for provisioning scenario describe how previously policies would define the interaction between the Provisioning Manager and the Policy Manager.

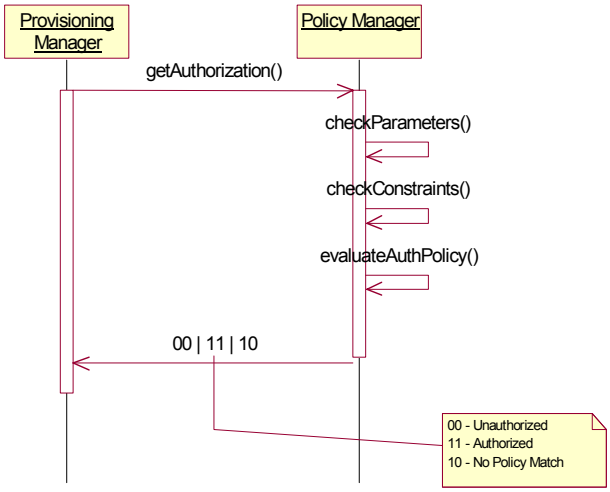

Figure 4: Authorisation Scenario

- The Provisioning Manager receives a request, and sends a 'getAuthorisation' to the Policy Manager for that request.
- The Policy Manager will then check the parameters of the request and the constraints set on the request

- Eventually, the Policy Manager will evaluate the request against the policies installed, and will return the appropriate code (00-unauthorised, 11-authorised, 10-No policy match).

5. Conclusions

This paper gives an overview of the work carried out in the IST Project WINMAN (whose main task is to develop and validate an open and flexible integrated management system for IP over WDM networks), focusing on the policy based management approach adopted by the project. The trials in the WINMAN project have demonstrated inter-connectivity across a worldwide network management infrastructure in a multi-provider and multi-domain environment [9]. Furthermore the design and the implementation of the WINMAN policy management system are described, together with a simple scenario describing a general interaction between the policy manager and the provisioning manager.

Acknowledgments

This paper describes work undertaken and in progress in the context of the WINMAN – IST 13305, a two and a half years research and development project during 2000-2002. The IST programme is partially funded by the Commission of the European Union.

References

[1] WINMAN site,www.telecom.ntua.gr/winman

[2] G. Lehr, H. Dassow, P. Zeffler A. Gladisch, N. Hanik, W. Mader, S. Tomic, G. Zou; "Management of All-Optical WDM Networks"- IEEE/IFIP 1998 Network Operations and Management Symp.; 15.2.20.02.1998, New Orleans

[3] Draft ITU-T Recommendation G.872 (ex G.otn) "Architecture of optical transport networks" Geneva (1998)

[4] G. Lehr, R. Braun, H. Dassow, G. Carls, U. Hartmer, A. Gladisch, H. Schmid : "WDM Network Management: Experiences gained in a European Field Trial" - IEEE/IFIP 1999 Integrated Network Management Symp.; proceedings, 485-498 pp, 24-28 May 1999, Boston

[5] CORBA Component Model (CCM), http://ditec.um.es/~dsevilla/ccm/index.shtml

[6] WINMAN consortium, "WINMAN Solution description R0", August 2001

[7] "Connection and Service Management Information Model (CaSMIM) Information Agreement TMF 605", Public Evaluation, Version 1.5, June 2001

[8] "Multi Technology Network Management Information Agreement, NML-EML Interface, TMF 608", Member evaluation Version 1.0, May 2001

[9] Galis, A. (ed.), -"Multi-Domain Communication Management," - CRC Press LLC, Boca Raton, Florida, USA, ISBN 0-8493-0587-X, July 2000

[10] Damianou, N., Dulay, N., Lupu, E., Sloman, M., "Ponder: A Language for specifying Security and Management Policies for Distributed Systems, V 2.3", *Imperial College Research Report DoC 2000/1* Oct. 2000.

[11] Damianou, N., Dulay, N., Lupu, E., Sloman, M., "The Ponder Policy Specification Language", *Proc. Policy 2001:Workshop on Policies for Distributed Systems and Networks,* Bristol, UK, Jan. 2001, Springer-Verlag LNCS 1995