# IP/MPLS OAM: Challenges and Directions

## A multi-technology, proactive, and autonomic management view


| Petre Dini | Masum Z. Hasan | Monique Morrow | Gerard Parr | Pierre Rolin |
|---|---|---|---|---|
| Cisco Systems, Inc. | Cisco Systems, Inc. | Cisco Systems, Inc. | University of Ulster | France Telecom R&D |
| San Jose, CA, USA | San Jose, CA, USA | San Jose, CA, USA | Northern Ireland, UK | France |
| pdini@cisco.com | masum@cisco.com | mmorrow@cisco.com | gp.parr@ulster.ac.uk, | pierre.rolin@francetelecom.com |



*Abstract*—**This paper reflects different understandings and positions on IP/MPLS OAM functions and management applications, as perceived by representatives from industry and academia. There is a clear effort to improve the state-of-the-art and to apply lessons learnt from the Ethernet/ATM approaches. A series of questions on the short-term, mid-term and long-term directions definitively arises, especially with regard to the separation of control and management functions. The questions mentioned below do not exhaustively cover the topic. Instead, the questions serve as a starting point for a discussion on methodologies to apply, on engineering requirements to consider, and on the technical challenges to resolve harnessing this next stage of evolution of heterogeneous networking. The panel guests present their perception on these issues. What are the lessons learnt from ATM and Ethernet OAM techniques that are oriented to a single network technology? What is equivalent of OAM appropriate for IP/[G]MPLS (it has to be more at link level rather than connection level)? What MPLS MIB information is intended to support OAM functions? What are the challenges on OAM in hybrid and multi-layer networks? How will management systems of next generation networks (NGN) and GRID networks make use of the OAM functions and what else is needed to smoothen the control-management interactions? What is the impact of convergent IP networking and autonomic networking on OAM functions and their distribution? How much proactiveness can management applications achieve with and without OAM functionalities?**



***Keywords-OAM; IP/MPLS; proactive management; data mining; heterogeneous networks; [G]MPLS; autonomic systems***


### I. Introduction

The basic concepts of OAM and the functional roles in monitoring and diagnosing the behavior of telecommunications networks have been long term studied (and well fixed) at the Layer 2 & Layer 3 levels. Certain OAM functions are used in many management applications for (i) defect and failure detection, (ii) reporting the defect/failure information, (iii) defect/failure localization, (iv) performance monitoring, and (v) service recovery.

It is worth to mention that each network layer has its own OAM functions. Several technology areas are covered, such as ATM OAM, SONET OAM, Ethernet OAM, VLANs, L2VPN (Transparent LAN Services), etc.

The ITU (SG13/Q3.13) recommendations and different IETF RFCs are referring to OAM functions for optical Ethernet, OAM and network management in IP-based and other networks, OAM mechanisms for MPLS networks, and protection switching for MPLS networks. However, since every exiting OAM solution is targeting one unique networking technology, there is a need for additional effort to cover heterogeneous networking technologies (NGN, GRID, Ad hoc, Sensors) and new diagnosis and management paradigms such as proactive, autonomic, partial and sporadic resources, etc.

OAM information may be used in re-active and proactive manner to monitor and diagnose heterogeneous networks. Use cases will illustrate practical use of the concepts covered by the panel discussion. A few examples summarized below indicate a concrete use of OAM functions. They clarify the nature of the problems and expose the solution adopted in a particular context.

#### A. ATM OAM-basic concepts

The operation and maintenance of the physical layer and the ATM layer for supervision at the bit and cell levels are described in ITU-T Recommendation I.610 with the objective of guaranteeing effective supervision of the UNI. In the case of the ATM layer, the portion which passes through a particular operator's network (ATM connection, VPC or VCC) can be supervised [16].

In the ATM technology, there are five independent information flows referred to as f1, f2, f3, f4, and f5. In the ATM layer, f5 cells are used for Virtual Channel Link/Connection, and f4 cells are used for Virtual Path Link/Connection. At the physical layer and transmission system, f3 cells cover transmission path, f2 cells covers digital section, and f1 cells refer to regenerator section.

The ATM layer is constantly supervised using OAM cells. The operation and maintenance of the layers above ATM (the AAL and above) have not been addressed in the ITU-T recommendations published so far.

The following OAM functions of the ATM layer apply to both the f4 and the f5 flows being performed for both VC and VP connections.

- *Fault management:* The AIS and RDI messages of the f4 and f5 flows are sent to the other network nodes via the VPC or the VCC to which the message refers (AIS and RDI have the same meaning as for the physical layer). The OAM cells indicate the type of error and error location. The fault management function performs continuity checking, verifying whether a VCC that has been idle for a period of time is still functioning. This is possible as long as the network elements send continuity-check cells along that VCC.
- *Performance management:* The OAM cells can be transmitted in either f4 or f5 flows, at fixed intervals; they are transmitted in both directions for notifying other network elements on detected errors.
- *Activation/deactivation:* Activation/deactivation of monitoring can be initiated by the operation and maintenance center (via the TMN), or by the user.

### B. *Examples*

To identify new OAM requirements on IP/MPLS and drive the development of IP/MPLS OAM solutions for the heterogeneous networks under new networking technologies, a few examples from the ATM solutions are presented below.

*Example #1:* Proactively, performance-monitoring (pm) cells are OAM cells that are periodically sent and do not mean that there is a problem with a VCC/VPC. The contents of the pm cell could indicate a problem upon further analysis (e.g., excessive number of lost cells). Continuity cells can also be sent periodically to verify the integrity of an ATM connection at the virtual path or virtual circuit level. Cells used for these purposes are referred to as f4 and f5 OAM flows, respectively (as opposed to physical layer information contained in the SONET/PDH header, where cells are referred to as f1, f2, and f3 flows - although PDH has no f2 flow). Failure to receive a continuity cell after a set interval of time can be used to flag a problem.

*Example #2:* Alarm indication signal (AIS) and remote defect indication (RDI) OAM cells do indicate a problem with an ATM connection. Loopback OAM cells are often used as a diagnostic tool for trouble location in troubleshooting.

*Example #3:* In fiber management, OAM information is provided to several sub-functions such as (i) channel management, (ii) failure indication/isolation, (iii) performance monitoring, and (iv) protection switch/fail over.

There is a trade-off between cost and complexity for implementing OAM functions, and several security aspects as well.

### C. *Extending OAM-basic concepts with new technologies*

Some OAM mechanisms are embedded into the protocols and assume there are appropriate sensors to capture state changes into the devices and networks. Device instrumentation is a keyword when considering IP/MPLS from the OAM perspective. Monitoring, diagnosis, and management functions no longer rely only on the classical FCAPS family; they are now interacting with the OAM protocol-embedded functions that must complement the former.

The paper will introduce first the MPLS OAM features (as a focused technology) and expand on heterogeneous networks. The discussion will be continued on proactive management as a complementary view on OAM control mechanisms, where different challenges will be highlighted. The positioning on emergent networks (NGN, GRID, etc.) will identify requirements for directions in supporting multi-service IP networks and autonomic networks. Conclusion will illustrate the most feasible requirements and identify the complexity of the further work.

## II. MPLS OAM

There is a paradigm shift from ATM OAM to MPLS OAM, due to technology changes. The following table is capturing the essential difference when positioning ATM and MPLS technologies, as an example.

TABLE I. ATM OAM VS. MPLS OAM

| **ATM OAM** | **MPLS OAM** |
|---|---|
| Paradigm: virtual circuits | Paradigm: Label Switched Paths |
| Bi-directional | Usually uni-directional |
| Established via ATM signaling and management | Established closely tied to control planes |
| Fixed hierarchy VP/VC | Variable label stack |
| Connection-oriented | Can be “connectionless” |
| Single route | May use ECMP |
| No penultimate popping | Penultimate hop popping |

### A. *MPLS OAM Challanges*

The existing OAM solutions focus on a particular technology. Moreover, most of the current proposals focus on single provider solutions or focus on a single aspect of the MPLS architecture or application of MPLS [15]. It is the case of using RSVP or LDP signaling where defects may be covered in some deployments, while a corresponding SNMP MIB module exists to manage this application; however, other applications (L3VPN) may handle differently (uncontrolled) these defects. To avoid inconsistencies, consistent OAM functionality must be deployed in MPLS networks. Since many MPLS applications may be concomitantly implemented, general and uniform solutions are preferred to the ad hoc point ones.

OAM functionality becomes crucial in multi-service MPLS-based internetworking for providing service level agreement (SLA/QoS) and service control/management. MPLS Layer 2 Virtual Private LAN Services (VPLS) and Layer 3 Virtual Private Networks (L3VPNs) require generic OAM functions to be homogeneously deployed. Standards organizations, such as the IETF and the ITU, have in the recent past done significant work in this area, and this subject is also being investigated by the IEEE and the Metro Ethernet Forum. New mechanisms for OAM are now in development (e.g., IETF LSP ping, ITU-T Y.1711, virtual circuit connection verification (VCCV)) focusing on the OAM impact on edge services (such as metro Ethernet) using MPLS transport or interoperability aspects with other technologies, e.g., ATM.

When implemented, the OAM MPLS functionalities require the 'Operation and Maintenance (OAM) Alert Label' to be used by the user-plane MPLS OAM functions for identification of MPLS OAM packets (similar to ATM cells).

We summarize the main OAM MPLS functionalities as proposed and experimented by many service providers.

### B. *Salient MPLS OAM functions*

The following MPLS OAM functions are under scrutiny to get generalized; these functions are directly targeting MPLS technology:

*a) Detection of broken label switch path:* This function is used to avoid hop-by-hop troubleshooting and synchronization of detection time bounds by the tools implementing it. This function is very relevant since the ICMP-based ping may return erroneous results due to inconsistencies between IP and MPLS forwarding tables or between MPLS control and data planes, as the reply path doesn't exist.

*b) Diagnosis of a broken label switch path:* This function allows the ability to detect, diagnose, and isolate a failed component (link or node); it is implemented through a path trace function. This function can be executed from both head-end LSRs and any mid-point LSR.

*c) Path characterization:* This function reveals details on LSR forwarding operations, such as ECMP, algorithms used, data/control plane OAM capabilities of the LSR, stack operations performed by an LSR, and time to live (TTL) propagation at penultimate hop LRSs.

*d) Service level agreement measurement:* This function provides ability to measure service level agreement parameters, such as availability, performance, latency, packet loss, jitter, etc.

*e) Frequency of OAM execution:* To configure how frequently the OAM functions must be executed for to guarantee consistency with the SLA related function, a special function with minimum impact on the network resources is needed. The frequency must be tuned in harmony with other technologies (ATM, SONET/SDH, etc.) and the size of the networks.

*f) Alarm supression, aggregation and layer coordination:* This function allows discarding superfluous traffic by correlating and aggregating the notifications. This requires fault notification to the LSP egress (with potential time constraints). The function may also select those LSPs that are monitored.

*g) Support for OAM interworking for fault notification:* Using multiple technologies over MPLS requires the ability to translate an MPLS defect/error into native technology's error condition (e.g., alarm suppression by the upper layer using the LSP). This requires MPLS to detect the anomaly in a bound time interval.

*h) Error detection and recovery:* This function guarantees that some well-identified mechanisms to automatically fix and recover an error, prior to customers detecting it are used. This means that the function must accept various types of automation procedures.

*i) Standard management interfaces:* Operators must have a common programmatic interface to access operations and managemnt functions and their status. This requires common information modellling of management and control of MPLS OAM functionality.

*j) Detection of denial of service attacks:* Security management MPLS OAM tools and mechanism must detect denial of service attacks against the data and control lanes. This function is related to the function presented at item (l).

*k) Per-LSP accounting and scalbility metrics:* This function must support different types of traffic accounting in order to ensure that service providers can measure traffic from an LSP to the egress of the network (some MPLS MIBs will also be required). The information can be used to design a network, to check the SLA violations, or to measure per operator partial services in a multi-provider service network.

*l) Security (LSP mis-merging security implications):* This function will most probably be provided by a series of tools that must be self-protected (aka, preventing their unauthorized use).

Review of current research in this area, e.g., setting parameters for connectivity verification and their impact on LSP recovery, trade-offs between bandwidth usage by OAM traffic and efficiency of failure/anomaly detection, and results from testbed deployments or simulations will be an indicator of how useful these OAM functions are and at what cost they will get implemented. Moreover, other aspects will be driven by the hybrid networks, where multiple technologies are used.

## III. OAM IN HYBRID, MULTI-LAYERED NETWORKS

OAM features are traditionally designed with respect to a single networking technology. Examples in case are ATM, SONET, and MPLS. Current networks are hybrid and multi-layered. A hybrid network is a network of multiple regions or layers, where each region or layer is based on different networking technology. For example, one region or layer can be TDM, another DWDM, another [G]MPLS, yet another ATM. In such a hybrid and multi-layer network end-to-end (or edge-to-edge) OAM becomes a challenge. Let us consider the network in Figure 1. The lower portion shows a hybrid Optical Transport Network (OTN) with multiple regions. Each of the regions consists of a network with a particular technology, control and signaling plane. For end-to-end circuit provisioning this network supports an end-to-end (this is in contrast with individual control and signaling plane in each region) control plane and signaling plane on top of the OTN (data plane), as shown in the upper portion of the figure. The upper control plane can be [G]MPLS supporting MPLS OAM. It is obvious from the figure that the upper portion does not have the full visibility into the whole network. Hence end-to-end MPLS OAM probes sent at the upper layer may not be able to isolate problem areas. What is needed is a layered hybrid OAM for full end-to-end performance and fault management.

The network in Figure 1 also has a number of reference points, such as UNI, ENNI, and INNI. These reference points define boundaries, which are defined based on various criteria, such as:

- UNI between different autonomous systems (AS);
- ENNI between different ASs, regions within the same AS, and
- INNI within a region.

For end-to-end performance and fault management OAM has to pass through all these reference points.

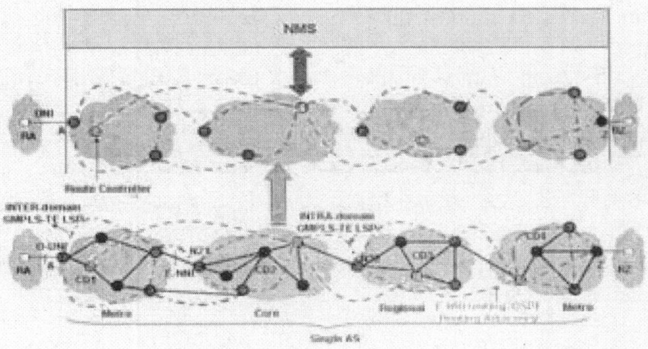


Figure 1. Heterogeneous networks

There are also challenges in managing OAM probes. Given a network one can have O(N**2) OAM probes sent from one node to another. But this may not scale well in a large network. Hence future OAM should have a way of interfacing with configuration and SLA information, so that probes can be launched automatically and in a scalable way.

## IV. PROACTIVE NETWORK MANAGEMENT

Present network management approaches are reactive (cure as opposed to prevention). Due to increasing complexity of communication networks, it is highly desirable that they should have the ability to detect symptoms of oncoming exception conditions and take measures to prevent them. This enables a degree of proactive network management that underpins acceptable QoS. To take advantage of OAM functions, a framework for achieving proactive network management in MPLS networks by deploying MIB data mining techniques is suggested. MPLS MIB attributes that have a bearing on the network management task at hand are short listed using a process called feature extraction and selection. Trends are then identified in these attributes which point to oncoming exception condition(s) followed by which control measures are taken to avoid their occurrence in the first place.

### A. *Predicting exceptions*

Increasing reliance on MPLS networks has resulted in an unprecedented growth in their size and complexity. Managing these networks is a big challenge. The problem is further compounded by the need to operate in real time. Legacy network management is reactive (*if-problem-then-recovery action*). Disruption in service due to network problems is undesirable as it results in overheads in terms of down time, lost QoS and potential financial penalty. Thus, it is highly desirable that networks should be able to predict exceptions and take proactive measures to reduce their probability of negative impact on performance. Several key challenges need to be overcome before this can be achieved. First, networks should have the 'intelligence' to predict problems and second, they need be empowered to cope with voluminous data. Third, the networks need to have the ability to alter the behavior of key network elements through their dynamic MIB attributes. Our approach attempts to address these challenges. The first objective can be achieved by identifying some means through which an early warning can be provided. An example would be, monitoring system variables and identifying trends in these variables that point to an oncoming exception condition. The second objective can be achieved through Data Mining. Traditional techniques of analytical modeling are not ideally suited to the problem under consideration since the volume of data is huge and also it changes quickly. Data mining approaches could provide viable alternatives as they improve their performance with time and also overcome the conservative approach (worst case analysis) adopted by analytical modeling. The third aspect can be addressed by using the standard MPLS MIB Community and features of SNMP v3. Several approaches have been proposed on MPLS Management including [1][2][3][4]. None of these approaches advocate proactive behavior. On the other hand, our framework employs adaptive learning techniques to support Proactive network management. Moreover, our approach involves taking local autonomous decisions and hence supports scalability.

### B. *Proactive management: A conceptual Architecture*

There is a Management Information Base (MIB) located on each LSR where statistics pertaining to the various operational aspects of that LSR are collected. Typically, MPLS MIBs consist of hundreds of variables the details of which can be found in [5][6][10][11][12][13][14]. Moreover, not all of the variables in these MIBs may be relevant to the management task at hand. Our approach entails identifying the MPLS MIB variables which have a direct bearing on the specific management task at hand (e.g. reducing end-to-end delay, maximizing buffer occupancy, providing for sustained and consistent levels of throughput per label) through a process called 'Feature Extraction and Selection'. We then advocate designing an intelligent data mining algorithm (training and validation of a suitable model) and incorporating the rules generated by the model in the production system to support loop-back. These rules will provide the network node with early warnings (symptoms of oncoming exception condition). Once these warnings are captured, pre-emptive action will be taken to avoid the exception condition. Feature selection is a process in which *'m'* out of *'n'* independent variables are chosen such that each of these strongly correlates to the dependant variable (target attribute of prediction), where *'m'* may be less than equal to *'n'*. There are several techniques that can be used for feature selection – Principal Component Analysis, Statistical t-tests, Bayesian Belief Networks, etc. Which technique to use is a matter of personal choice. The choice of a data mining technique depends on whether the learning is carried out in an offline or an online manner. In case of an offline approach the choice is governed by the accuracy and generality of the model produced by the technique whereas for an online approach, the convergence time (measured in secs/msecs) of the technique would be a dominant criterion. Note that the Simple Network Management Protocol (SNMP) standard [7] will be employed to capture the MPLS MIB data. Figure 2 embodies the conceptual architecture, Figure 3 shows our simulation framework and Figure 4 shows an example scenario where congestion avoidance is achieved through proactive management.

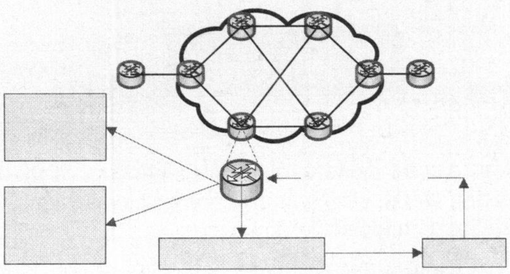

Figure 2. Conceptual Architecture

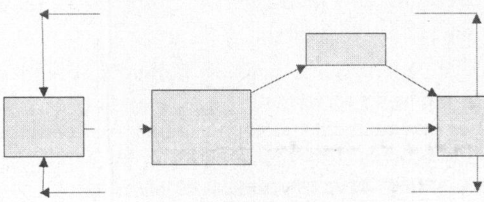

Figure 3. Simulation Framework

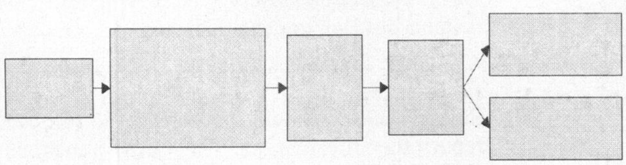

*Figure 4. Example scenario – Congestion Avoidance*

## C. *Proactiveness, data mining and OAM MPLS*

We proposed a mechanism to attack the problem of information overload (i.e. processing of MPLS MIB data in real time) and building intelligence into the network management system through the use of data mining. Our initial experiments in [8][9] have produced encouraging results and demonstrated that data mining is a viable approach to proactively detect network exception conditions. However, an offline approach was employed. We plan to investigate several data mining and statistical techniques and assess their suitability. We also intend to explore issues involved in the deployment of online learning to underpin real-time feature extraction-data mining and loop-back. To our knowledge, no standard approach exists to date that employs real-time online learning to achieve proactive network management. This is going to be a big challenge. Successful experimentation with these techniques could lead to a new breed of MPLS Network Management methods capable of proactive behavior without imposing any major requirements and overhead on existing and evolving systems. Obviously, combining the mechanism exposed above with MPLS OAM functions

# V. TOWARDS AUTONOMIC NETWORKING

In the 80's, the operators dreamed and worked hard to achieve a unique Integrated Service Data Network (ISDN) capable to serve all service needs. Currently, IP is performing this goal event if not born in operators' research projects. IP networks are becoming the communications support of all traditional telecommunications services, such as voice including mobile telephony and data including web and mail. Additionally, new ones such as triple play (video, internet and voice), P2P, Grid are hot spots now. Each of these services has specific requirements concerning bandwidth, quality of service, security, safety, flexibility, and so forth. Also, managing an internet network is a more challenging task than the management of the past dedicated networks (POT, X25, or Frame Relay…). Therefore, combining protocol functions and management functions appears as a reasonable solution. OAM functions may not only be useful in proactive management, but also capturing some behavioural aspects that are the hot target of the classical management systems.

## A. *Towards multi-service convergent IP networks*

The main advantage of a single ISDN network is in terms of operational cost reduction. This objective may be (most probably) defeated by the emergence of many different new complex technologies, user profiles, and services. The management of quality of service (QoS) over this unique network appears to be complex and difficult, as legacy classical architectures and requirements associated with them are still present:

- IP hides physical media diversity to users. However, the network infrastructure has to cope with this diversity. Radio segment have low bandwidth and a high error rate, optical network have a limited ability to change dynamically the route path…
- The network QoS is not explicitly given by an IP packet; this must be derived from flow information included in packets. However, flow

analysis is pretty complex in real time on the network, as networks use flow aggregation mechanisms.

- Traffic engineering (TE) usually serves only one aspect of service integration. TE mechanisms must be applied at different timescales. As TE mechanisms interact, this raises stability issues.
- Billing is a significant issue; yet billing on a per packet basis is not an easy task. This is fairly more complex that the traditional circuit based rating and billing current implementations.

There exist now many other aspects to be considered when innovating additional control and management functions:

- Security is becoming more and more critical, as the number and frequency of intrusions in the services (spam, denial of service, virus propagation, etc.) put on operators new and not anticipated operational costs.
- Plug and play is a mandatory requirement for those users that willing to be always connected anywhere. Additionally, user identification and context provisioning are now standard services.
- Mobility of the terminals is an issue to serve on IP networks.

### B. *Towards automatic IP network configuration and management*

Operators need methods and policies to allow for an automatic network configuration for both network and application layers.

- Flexibility: Management policies must evolve according to operational and commercial strategies, customers QoS requirement, fast resources allocation, efficient resource retrieval; this implies some inter-action with routing protocols.
- Reliabilty: Any interruption of service or any network failure have an impact on the end-user access and lead to direct loss of money. There is a need for swiftness in the infrastructure reaction (detection, repairing, etc.)
- Self-management: Evolution of autonomous systems is based on policies that correlate the next functionalities, addressing schemes, dynamic routing information, and QoS related information.
- Security: All proposals answering the above problems must be secure for ensuring the safety of autonomous networks.

On a complementary but mandatory view, monitoring networks efficiency by incorporating intelligent feedback (and here OAM functions) is expected to play a major role for:

- Intelligent measure activation and parameterization.
- Advanced interpretation of the observed measures.
- Discover Ad hoc networks or overlay networks
- Self-repairing, self-diagnosis and self-protection (autonomy).

The management systems must be able to identify the right information in order to perform automatic decision functions, in cooperation with OAM functions. Such architecture is presented in Figure 5.

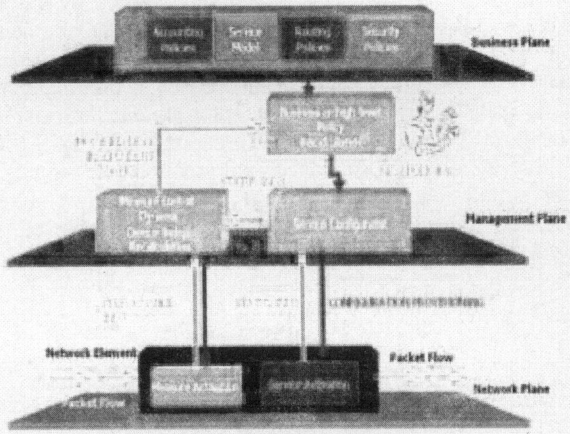


Figure 5. Control/management architecture

Decisions can be made through available "out of the box" information (MIB, etc.) and the appropriate mechanisms to be configured on the network devices;

- Listing all available mechanisms on the "off the shelf" network devices;
- Defining new features and functionalities that need to be supported by network devices.
- Defining new parameters to observe (including by the OAM functions).

The management systems need to define how and when measurements are to be performed (e.g., dynamic configuration policies). The management personnel must be available to provide stability studies (timescales and scopes), studies about the interaction among services (consistency checks).

One needs to define generic device independent models for:

- Intelligent scheduling (how often?, when?, scope?) that is needed to observe the appropriate level of detail according to the situation;
- Intelligent filters (which metrics), and
- Suitable protocols and mechanisms to retrieve and report the information. The OAM functions are part of this requirement.

In conclusion, management is now facing new challenges in term of automation required to cope with new needs and to maintain reasonable operational cost. France Telecom (and other operators) has developed projects to experiment some of the above autonomic networking concepts. It is expected that new IP/MPLS OAM functionalities will contribute to enforce the management autonomy of networks and network devices.

## VI. Conclusion

As the panel discussions will be after this paper is published, we expect that some of the directions set by the authors will be endorsed and/or challenged by the audience. It is our perception that the IP/MPLS OAM is a very challenging domain, as multi-technologies and network types are interacting with each other. The success of deploying new IP/MPLS OAM functionality is driven by the nature of the legacy networks and technologies, the network size, and the costs service providers plan to allot to the effort. We expect that most of the topics presented in the panel paper will get implemented in the next generation networks.

## References


[1] T. Nadeau, M. Morrow, G.Swallow, D.Allan and S.Matsushima. "OAM Requirements for MPLS Networks", IETF draft, Sept 2004.

[2] T. Anjali. "DiffServ/MPLS Network Design and Management", PhD Thesis, Electrical and Computer Engineering, Georgia Institute of Technology, Mar 2004.

[3] H. Lohne and J.Vea. "Mechanisms for OAM on MPLS in large IP backbone networks", Masters Thesis, Faculty of Engineering and Science, Agder University College, May 2002.

[4] F. Holness. "Congestion Control within MPLS Networks", PhD Thesis, Queen Mary and Westfield College, London University, Sept 2000.

[5] C. Srinivasan, L. Bloomberg, A.Viswanathan and T.Nadeau. "MPLS LSR MIB", IETF Tech. Rep. RFC 3813, Jun 2004.

[6] T. Nadeau, C. Srinivasan, L. Bloomberg and A.Viswanathan. "MPLS FEC to NHLFE MIB", IETF Tech. Rep. RFC 3814, Jun 2004

[7] J.Case, M.Fedor, M. Schoffstall and J. Davin. "A Simple Network Management Protocol", IETF Tech. Rep. RFC 1157, May 1990.

[8] P. Kulkarni, S.McClean, G. Parr and M.Black. "Deploying MIB Data Mining for Proactive Network Management – Experimentation and Initial Results", Submitted to IEEE Integrated Management (IM) 2005.

[9] P.Kulkarni, S.McClean, G.Parr, and M.Black, "A conceptual framework for achieving congestion avoidance through proactive network management using data mining," in *Proceedings of the 5th Annual Post-Graduate Conference on Networking, Telecommunications and Broadcasting (EPSRC PGNET), Liverpool, UK*, June 2004.

[10] A.G. Malis, T. Hsiao, "Protocol Extensions forSupport of ATM Service Class-aware Multiprotocol Label Switching (MPLS) Traffic Engineering, RFC 3496, March 2003

[11] L. Anderson, G Swallow, "The Multiprotocol Label Switching Working Group decision on MPLS Signaling Protocols, RFC 3468, Feb 2003.

[12] H Ohta, "Assignment of the OAM Alert Label for MPLS OAM Functions, RFC 3429, Nov 2002

[13] F. Le Faucheur, W Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering, RFC 3564, July 2003.

[14] T. Nadeau, C. Srinivasan, L. Bloomberg and A.Viswanathan, "MPLS FEC-to-NHLFE MIBs, RFC 3814, June 2004.

[15] T. Nadeau, M. Morrow, G. Swallow, D. Allan, S. Matsushim, OAM Requirements for MPLS Networks, draft-ietf-mpls-oam-requirements-04.txt, expires April 2005

[16] Ericsson, Understanding telecommunications: operations and maintenance, http://www.ericsson.com/support/telecom/part-g/g-8-3.shtml


## Authors' Biographies

**Petre Dini:** Petre is now with Cisco Systems, as a CTO Senior Technical Leader, being responsible for Policy-based architectures for network management, Programmable Networks and Services, QoS/SLA/Performance, Nest Generation Networks, and Consistent Network/Service Manageability. He's industrial research interests include nomadic code, performance, scalability, feature interactions, sporadic and intermittent resources, and policy-related issues in GRID networks. Petre was responsible for different industrial projects including CAD/CAM, nuclear plant monitoring, and real-time embedded software; then he was involved in various Canadian projects related to object-oriented management applications for distributed systems, and to broadband services in multimedia applications. He invented several mechanisms in the area of agent negotiation, QoS evaluation metrics, and policy for conflict resolution in feature interaction. Petre edited several books, chaired many scientific conferences and was invited speaker and panelist to tens of international events. He published over 100 papers in scientific journals and conferences. Petre was an Adjunct Professor with McGill University, Montreal, Canada, a Canadian representative in the European projects, and a senior technical manager AT&T Labs. He is the IEEE ComSoc Committee Chair of Dynamic Policy-Based control in Distributed Systems, and actively involved in the innovative NGOSS (TMF) and NGN (ITU-T) standards initiatives. Petre received his M.Eng. from the Polytechnic Institute of Timisoara, Romania, in Computer Engineering, and a Ph.D. in Computer Science from the University of Montreal, Canada. He is currently an Adjunct Professor at Concordia University, Montreal, Canada, a Senior IEEE member, and an ACM member. He is the founder of the International Academy, Research, and Industry Association (IARIA). [ www.iaria.org]

**Masum Z. Hasan:** Masum is currently a Senior Technical Leader at Cisco Systems, USA. Prior to joining Cisco he was a Principal Investigator at Bell Labs Research, USA, and a Research Associate at the University of Toronto, Canada. Masum has worked in industry and academia in Bangladesh and Canada. Masum is on the committees of a number of IFIP and IEEE international conferences. He is the Tutorial Chair of the IEEE/IFIP Integrated Management Conference 2005. He is on the editorial board of the Journal of Network and Systems Management. He also participates in the activities of international standard bodies, such as ITU, OIF and IRTF. Masum has published extensively in a number of areas of computer science discipline, including network management, active, temporal, and text database systems, computer languages and environments, structured data visualization, Internet applications, and distributed and parallel systems. Masum has a number of patent proposals approved. Masum's current work involves management and control plane issues of traffic engineering, QoS, VPN, G/MPLS, Optical, GRID and Next Generation Networks. He received a combined Bachelors and Masters in Computer Engineering from Odessa Polytechnic University in former USSR, and MMath and PhD in Computer Science from University of Waterloo, Canada.

**Monique Jeanne Morrow:** Monique is currently CTO Consulting Engineer at Cisco Systems, Inc. She has over 20 years experience in IP internetworking that includes design, implementation of complex customer projects and service development for service providers. Monique has been involved in developing managed Network Services like Remote Access and LAN Switching in a Service Provider environment. Monique has worked for both enterprise and service provider companies in the United States and in Europe. Monique has been an invited speaker and panelist at many international conferences and has spoken in several Cisco Networker Conferences. Monique is co-author of the book *Designing IP-Based Services: Solutions for Vendors and Service Providers*, Morgan-Kaufmann, 2002. Monique is active in both the IETF and ITU-T SG 13 with a focus on OAM. Monique is currently engaged in MPLS OAM standards development (IETF, ITU). Additionally, Monique is working on GMPLS and NGN topics pertinent to both carriers and NRENs. Monique has been a technical reviewer for the book, *International QoS Architectures and Mechanisms,* Zheng Wang (Morgan-Kaufmann, 2001); she has contributed a chapter on MPLS in the book, *Networks : Internet-Telephony-Multimedia, Convergences and Complementarities*, De Boeck Diffusion, 2002 (France Telecom Lead) and was content reviewer for the book, *MPLS and VPN Architectures, Vol 2,* Jim Guichard et al, Cisco Press, 2003. Monique is quest editor of several IEEE journals. Monique is co-guest editor of a forthcoming special issue of the IEEE Communications Magazine on the subject of "OAM in MPLS-based Networks. Publication is scheduled for October 2004. She is also a co-guest editor of the IEEE Communications Magazine feature topic on "Inter-Provider Service Quality on the Internet" (June 2005). Monique earned an M.Ss in Telecommunications Management from Golden Gate University, San Francisco, California, and an MBA from City University, Zurich, Switzerland. Monique is also a Cisco Certified Engineering Expert (#1711).

**Gerard Parr:** Gerard holds the Full Chair in Telecommunications Engineering and is the coordinator of the Internet Technologies Research Group in the Faculty of Engineering at the University of Ulster, Coleraine campus, Northern Ireland. Areas of research within the group include self-stabilizing protocols, interplanetary network protocols, ATM, CNNs and intelligent mobile agents in xDSL and SNMP, bandwidth provision over SONET/SDH in the presence of chaotic impulses and fuzzy inference systems for multicriteria handoff in tactical communications. Currently he is supervising PhD students ranging in topics from proactive network management to storage resource management in GRIDs. He is a founding Executive Director of the campus spin-off company (Causeway Data Communications Ltd) which is based at the Coleraine Science Park and holds a number of international patents. Gerard is a member of the UK EPSRC College (Communications Panel). He was Technology/Track Chair for Advanced Architectures and Protocols at IEEE MILCOM. He sits on the Editorial Board of the Elsevier Science International Journal of Computer and Telecommunications Networking. He has been invited to become an Expert Evaluator to the EU's FP6 for IST: GRID Technologies and Satellite Communications. He worked previously as a Visiting Scientist at the USC Information Sciences Institute in Marina Del Rey, Los Angeles on DARPA funded research projects into Fault-Tolerant and Self-stabilizing Protocols. Currently he is acting as the Senior Guest Editor for a Special Issue of the premier International Journal of Computer Networks by Elsevier which will be devoted to Advances in Military Communications Technologies and Systems. He is an active member of many international scientific conference committees. He is also an invited Member of the Editorial Panel for the U.S. International Journal of Aerospace Computing, Information, and Communications. He has published papers widely in international peer-reviewed journals, including CACM, LNCS Springer-Verlag, Parallel and International Journals Distributed Systems and Networks, Software Concepts and Tools, International Journal of Network Management and IEEE conferences including IFIP/IEEE MMNS, IEEE WCNC, and IEEE MILCOM. More recently he has been invited to become a member of the world's first UK-China Research Network for Manufacturing, Automation and Computing with 16 UK Universities and 32 of the top Universities in China. In addition he is a founding member of a recently funded EPSRC Research Network on Systems Biology which will address challenges from the Engineering-Life Sciences Interface. Gerard holds a PhD in Self Stabilizing Protocols.

**Pierre Rolin:** Pierre is the Head of Service Network, Expertise, and Research Partnership at France Telecom R&D Division. After 15 years of research at INRIA on distributed system and real time networks, he has been professor in Network and Computer Science at ENSTA. In 1991 he has created the Multimedia Systems and Networks department at ENST Bretagne. He has joined France Telecom R&D division in 1997 where he is in charge of several areas. Pierre is responsible of management, coordination and budget allocation for long term research in the fields of "software and networks" (network architecture, network management, access network, core transport networks, digital communication and coding, wireless network, optimization et dimensioning, IP networks, software engineering, distributed computing infrastructures, security). He is the coordinator for technology road map preparation and technology prospective studies. Pierre also drives the relationships with academic partners worldwide. He has published more than 50 international papers and communications, five books on LAN, MAP, ATM, Broadband Networks and Networks Principles, and holds 8 patents. He is also a scientific committee member of conferences, high education institutions, and editions such as the journal "Annals of Telecommunications". Pierre is an engineer in computer science from INSA 1974 (Institut National des Sciences Appliquées); he has achieved his PhD in 1977 and is a Doctor of Science from University of Rennes 1987 ("Measure of distributed system and networks").