Towards Automated Interactions between the Internet and the Carrier-Grade Management Ecosystems

Small or medium scale focused research project (STREP) Co-funded by the European Commission within the Seventh Framework Programme

Grant Agreement no. 258300

Strategic objective: The Network of the Future (ICT-2009.1.1)

Start date of project: September 1st, 2010 (36 months duration)

Deliverable 3.1.1
Preliminary report on IP and carrier-grade management functions analysis

Due date: 6/1/2011

Submission date: 6/1/11

Deliverable leader: TID

Author list: TID: Carlos García Argos, Óscar González de Dios, Javier Jiménez Chico, Fernando Muñoz del Nuevo.
UPC: Anny Martínez, Xavi Masip-Bruin, Marcelo Yannuzzi, Wilson Ramirez
TUBS: Mohit Chamania, Admela Jukan
ADVA: Maciej Maciejewski, Christine Brunn
MySoft: Gabriela Aronovici, Vlad Melinte, Dan Horhoianu, Viorel Ionescu, George Dan Culache
SNU: Jörn Altmann, Mohammad Hassan.

Dissemination Level

☒	**PU:**	Public
☐	**PP:**	Restricted to other programme participants (including the Commission Services)
☐	**RE:**	Restricted to a group specified by the consortium (including the Commission Services)
☐	**CO:**	Confidential, only for members of the consortium (including the Commission Services)

Table of Contents

0 Executive Summary 6

1 Introduction 7

1.1 Organization of the deliverable 8

2 Network Management Functions 9

2.1 Standard Management Functions 9

2.1.1 Fault Management 9

2.1.2 Performance Management 9

2.1.3 Configuration Management 10

2.1.4 Security Management 10

2.1.5 Account Management 10

2.2 Management Protocols 11

2.2.1 CLI (Command Line Interface) 12

2.2.2 SNMP (Simple Network Management Protocol) 12

2.2.3 NETCONF (Network Configuration Protocol) 13

2.2.4 YANG 14

2.3 Role of Control Plane in Management Functions 15

2.3.1 Protection and restoration 16

2.3.2 Provisioning 16

2.3.3 Distribution of routing 17

2.3.4 User Network Interface 17

3 3 Functional Limitations of Current IP Management Systems 18

3.1 Introduction 18

3.2 Overview of IP Network Management Systems and Features 19

3.3 Limitations of Current IP Network Management Systems 25

4 Carrier Grade Management Functions 27

4.1 Current Transport Network Management Systems 27

4.2 Functional Limitations of Current Carrier Network Management Systems 27

4.2.1 ITU-T Telecommunications Management Network (TMN) 27

4.2.2 MTOSI: 29

4.2.3 MTOSI NBI in ADVA's FNM: 30
4.3 Functional Limitations of Current Carrier Network Management Systems 31

5 Multilayer Management 31
5.1 Benefits of Network Management Coordination 32
5.2 Economic Benefits 34
5.2.1 Reduction of complexity and duplication of network devices 35
5.2.2 Reduction of manual and error prone intervention 35
5.2.3 Increase in capacity utilization 35
5.3 Current Multilayer Management Approaches 36
5.4 Integrated multilayer devices and networks management. 37
5.5 The ONE Adapter in Management Functions Standardization 38

6 Conclusions 40

7 References 42

8 Acronyms 44

Figure Summary

Figure 1. Failure Management WorkFlow 9
Figure 2. Performance Management WorkFlow 10
Figure 3. Configuration Management WorkFlow 10
Figure 4. NETCONF Architecture [JuSch] 13
Figure 5. NETCONF Entity [JuSch] 13
Figure 6. Example of relation between TMN-related Recommendations [TmnM3000] 28
Figure 7. Layers in TMN with interfaces between layers 29
Figure 8. Future Netwok Management Process 33
Figure 9. Multilayer CyMS 3D View [Cya11] 36
Figure 10. Juniper PTX [JUN11] 37
Figure 11. NETCONF Operations 47

Table Summary

Table 1. Management Protocols 11
Table 2. NETCONF Protocol Layers [YuAja] 14
Table 3. Summary of IP Management Tools 18
Table 4. Comparison of IP Network Management Tools 25

0 Executive Summary

Business services, like bank transactions, brokerage operations, etc., and the everyday more dependant Internet access rely on a complex environment based on IP, MPLS and transport networks. It is the role of network management to assure that the connection services offered by the network meets the desired quality.

The management functions, as defined by ISO are:

- Fault Management
- Configuration Management
- Accounting Management
- Security Management
- Performance Management

These management functions have been developed mainly in a per layer basis. As a result, we are facing on one hand, an IP ecosystem, dominated by individual tools, SNMP and CLI connections that need IP experts to manage the network.

On the other hand, the transport network is dominated by Network Management Systems particular to each vendor. MTOSI appears as the interface to communicate in a standard way to different NMS.

The control plane provides an automatic behaviour in the network equipment to help in some of the management functions, mainly in the fault management, with the automatic protection and restoration, and in the configuration, with the automatic set-up of paths. Although there has been an attempt to standardize the control plane for multilayer networks, that is, an automatic mechanism between devices, there has been no success so far.

In sight of the complex environment, there are two directions:

- Simplify the network
- Coordinate multiple layers

The first is trying to be achieved by a flattering of the layers, either by integrating functionality in one box, or by providing a single control plane instance for the layers. However, such approach still lacks of interoperability.

The ONE approach aims at facilitating coordination among different NMS's on a layered network scenario each interacting and communicating trough separate customizable interfaces.

1 Introduction

IP Networks are the support of today's worldwide communications, with the carrier grade transport networks serving as their aiding highways. Network management is the responsible of achieving the expected behaviour of the network. In fact, the main goal of Network Management is to ensure that the services provided by the network are offered to the clients with the desired level of performance and availability, typically based on a Service Level Agreement (SLA) [Sub10]

The typical functions of network management include **network provisioning**, **fault management** and **performance monitoring**. The first one is aimed at setting up new network services, configuring all the necessary equipment. The second one aims at detect a failure in the network, isolate it, inform about the problem, recover the service connectivity and finally, repair the source of the failure. Note that when the service is recovered by network means, it is called "*self-healing*", which leads to a quick service recovery. Finally, performance monitoring aims at detecting if the SLAs are being satisfied (typically in terms of delay and jitter).

To achieve those management functions there are a set of protocols and tools. With them, it is possible to access the network devices and configure them. To further help in the process and provide a simpler way to operate, Network Management Systems (NMS) integrate a set of these protocols and tools and customize them to the different network equipment.

However, nowadays, each section of the network that falls under the responsibility of the same department, as well as the portions of the network using the same network technology (e.g., MPLS, SDH, OTN, etc ...) uses its own NMS. Such NMS is in some cases, e.g. typically in IP/MPLS networks, just a collection of tools particularized by the Network operator. In other cases, typically in the transport network, the NMS is developed by the vendor. The reason is that the configuration of the transmission and switching devices is complex and very specific to the vendor equipment (internal layering, transmission power level, equalization, PMD compensation modules, etc).

Thus, the management of a complex operator network with many layers is based on an ecosystem of many different NMS and isolated tools, without easy interaction between them. There inter-relation between different layers in kept by in-house systems and databases, that are hard to develop and maintain. Moreover, operations involving several layers are full of manual steps and end up in long and costly processes. This isolation leads to high operational costs and a continued need of upgrades in different systems.

In order to reduce the complexity of the management of a network with multiple layers, several approaches can be followed. On the one hand, it is desired to try to reduce as much as possible the complexity of the network and, as the technology advances, to bring together layers that once started with different goals. In this sense, approaches like IP over DWDM, or integrated devices, aim at reducing this complexity. The main problem is that there are only mono-vendor solutions at the moment, which are highly avoided by operators. Also,

advances in the control plane, which have the aim of performing automatic functions, not only in one layer, but also involving two layers, like the UNI interfaces, facilitate the reduction of complexity. However, for example, although IP over WDM control plane standards have been out for a long time, there has never been a success in its use.

Other approach to follow is to develop multilayer network management systems and tools. There are some initial steps in this sense. However, most of current products are focused only on multi-layer transport networks, which are a set of connection oriented layer, with a similar philosophy.

Given that there is currently an ecosystem of different network layer with different management systems currently deployed for each network segment, the ONE approach is to enable the coordination of the different management systems and tools. Although there has been a lot of effort in the standardization of the communication between network management systems, there has not been much success, mainly due to the high complexity of the solutions and the high investment and development needed for them. In this sense, the ONE project aims at helping the management functions, levering the gap between network layers, and facilitating the communication in a simple way between IP/MPLS and transport layer NMS.

The ONE approach aims at facilitating coordination among different NMS's is an layered network scenario each interacting and communicating trough separate customizable interfaces.

1.1 Organization of the deliverable

In this document, we present an overview of the Network Management goals and functions and go on to review the standard management protocols for both IP/MPLS and Transport networks. Next, we present the state of the art in current integrated NMS for both layers and analyse the limitations of these integrated approaches. The analysis helps us to identify specific deficiencies of multi-layer management which should be addressed by the ONE adapter to enhance network OAMP, and we then present an overview of the ONE approach to deal with the aforementioned issues.

2 Network Management Functions

The network management functions keep the network running in the desired conditions. In this chapter, we briefly review these functions. In order to get a complete understanding of principles of Network Management, the reader is referred to the literature, concretely recommending the books “Network Management: Principles and Practice” from Subramanian et al. [Sub10] and “Network Management Fundamentals” from A. Clemm [Clem06].

2.1 Standard Management Functions

OSI (Open System Interconnection) model defines 5 standard management functions [Sub10]:

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

2.1.1 Fault Management

Fault management consists of detecting, diagnosing, bypassing, repairing and reporting network equipment and service failures. A complete fault management process starts with monitoring and failure identification, and upon failure identification performs error detection, notification, and necessary diagnostic tests after which faults are corrected. The error information is also stored for further analysis by the network operator.

Figure 1. Failure Management WorkFlow

2.1.2 Performance Management

Configuration Management consists of functions to maintain an accurate inventory of network resources and to configure network devices without creating network failures. Configuration management activities include defining parameters to control the network operation and network elements identifiers, collecting current network state information and changing configurations.

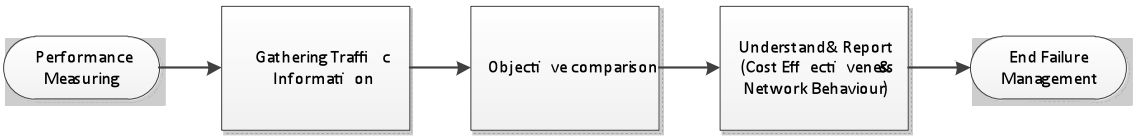

Figure 2. Performance Management WorkFlow

2.1.3 Configuration Management

Configuration Management consists of functions to maintain an accurate inventory of network resources and to configure network devices without creating network failures. Configuration management activities include defining parameters to control the network operation and network elements identifiers, collecting current network state information and changing configurations.

Figure 3. Configuration Management WorkFlow

2.1.4 Security Management

Security management is responsible for controlling access to network and management systems and protection of information against unauthorized subjects. The security process has to manage access to network element (only authorized users), detect attacks and deploy protection measures such as information encryption.
Account Management

Account management has to identify costs to be charged for a service to the corresponding network user/subscriber. These costs are measured by setting tariffs, accumulating resource usage (time, capacity…) and charging it to the subscribers.

By grouping the standard management functions along with other specialized functions, any management operation can be done to satisfy the network operator needs (e.g. capacity planning, strategic planning).

2.1.5 Account Management

Account management has to identify costs to be charged for a service to the corresponding network user/subscriber. These costs are measured by setting tariffs, accumulating resource usage (time, capacity…) and charging it to the subscribers.

By grouping the standard management functions along with other specialized functions, any management operation can be done to satisfy the network operator needs (e.g. capacity planning, strategic planning).

2.2 Management Protocols

To achieve the functions described in the last section, the different standardization bodies and current practices have defined a set of protocols to manage the network.
First of all, one the basic needs it to access the equipment to configure it and launch a set of commands. Command line interface is still used to configure many devices. In many cases, there is a template of how to configure the equipment, so the operator just connects to the device by CLI and follows the outlined steps, full of proprietary commands. Also, repeated operations are usually scripted, and run remotely in batches. The access to the device is performed by standard protocols, e.g. telnet or ssh, depending on the desired security.

Management Protocol	Benefits	Issues
CLI (Command Line Interface)	• Well defined commands & exact configuration.	Scalability (scripts needed). Multi-vendor impossible. The information presentation is hard to read & comprehend
SNMP (Simple Network Management Protocol)	• Mature standard protocol (SNMP v3 from 2002). • Very good at monitoring and alarms sending and detection.	SNMP fails to address configuration requirements in order to be a well-defined configuration protocol.
NETCONF (Network Configuration Protocol)	• Distinction between configuration and state data • Multiple configuration Data-Stores (running, start-up….) • Support for configuration change transactions • Configuration testing and validation support • Selective data retrieval with filtering • Streaming and playback of event notifications • Extensible remote procedure call mechanism	Recently converted in RFC. It is still not implemented by many vendors.
YANG (A data modeling language designed to write configuration data models for the NETCONF protocol)	• Human readable easy to learn representation • Hierarchical configuration data models • Reusabe types and groupings • extensibility through augmentation mechanisms • Supports the definition of operations (RPCs) • Formal constraints for configuration validation • data model modularity through features versioning rules and development support • Translations to XSD, RelaxNG and YIN	It is still not implemented by many vendors.

Table 1. Management Protocols

2.2.1 CLI (Command Line Interface)

CLI is the interface commonly used to access any network equipment via the console. It is used to perform command configuration directly on the network equipment and each vendor has its own commands which mean that Juniper's CLI will be different than CISCO's CLI. It automatically starts when the hardware finishes booting.

As advantages, CLI allows configuration, monitoring, service provisioning and other functions in a safe way and also supports all of the vendor specific functions which may not be available over other interfaces. In order to ensure safe practices, operators develop configuration scripts for specific hardware, and these scripts are easier to adapt into the operators NMS tools than web services.

As disadvantages, the configuration process is slow using CLI. Multiple commands have to be sequenced to set a configuration and this has driven operators to develop configuration scripts to configure network equipment when complex command combinations have to be used.

In terms of scalability, CLI usage is also a problem because multiple nodes have to be configured at the same time which again requires complex script development. Also, as commands or answers can change with network vendors and even operating system versions, the configuration scripts must be adapted when vendors upgrade their equipment operating systems.

Also, CLI interfaces use primitive data representation and do not have graphical representation, making the comprehension of complex information such as monitoring difficult.

Given the diversity between vendor OSs and even differences between OS versions of the same vendor, it is unlikely that the CLI will be standardized as a management protocol.

2.2.2 SNMP (Simple Network Management Protocol)

SNMP is an asymmetric protocol that interacts between two different entities, the management station and the agent. The agent is an element that replies to the management station request either with the management information desired or changing the request specific parameters. On the other side, the management station, depending on its complexity, can elaborate different network information representation from all the request information gathered. This management and configuration information is stored in Management Information Base (MIB) and it includes all the data elements that are used to represent the network element behaviour.

Even though the network equipment configuration can be done using the SNMP mechanisms, the most used applications of this protocol are discovery, monitoring and event notification functions.

SNMP can perform data collection from multiple network equipment in a very effective way, but as the data amount grows, the bandwidth required and latency growth significantly reduces the efficiency of the protocol.

The problems with SNMP configuration functions are related to configuration sessions in the elements [JuSch]. SNMP does not distinguish between configuration states, it does not prevent concurrent configuration changes and it cannot distinguish between two different configurations. As SNMP does not comply with these configuration requirements, the configuration requirements specified on the SNMP RFCs are very specific to avoid configuration failures [RFC3535][RFC3139].

Definitely, SNMP is not recommended for configuring equipment and, due to this, other management protocols are being developed to serve this purpose.

2.2.3 NETCONF (Network Configuration Protocol)

The main reason behind the NETCONF development is the need for a configuration interface suitable of configuring multiple vendor equipment without operating system version compatibility problems. The current configuration approach is based on CLIs (Command Line Interface) manual configuration and automated scripts that need to be adapted every time to operating system version changes which is really inefficient.

The NETCONF architecture comprises two elements:

- NETCONF Server: This element is included on every configurable network element.
- NETCONF Client: Management applications include a client. CLI can be wrapped around a client.

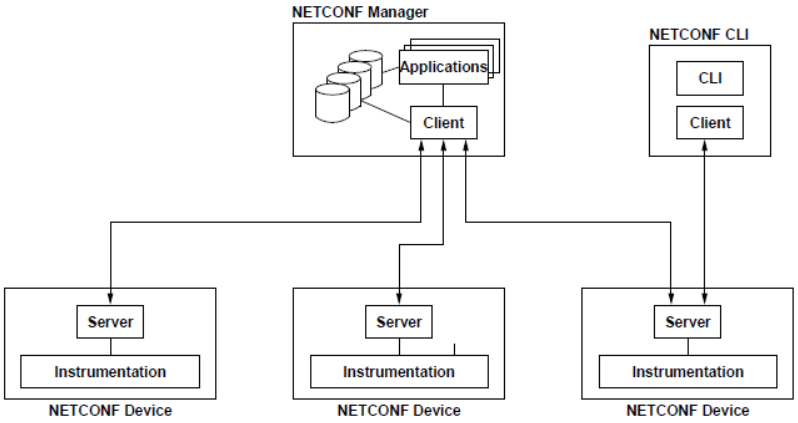

Figure 4. NETCONF Architecture [JuSch]

The IETF NETCONF working group has defined SSH, SOAP, BEEP and TLS as the allowed transport protocols when implementing NETCONF.

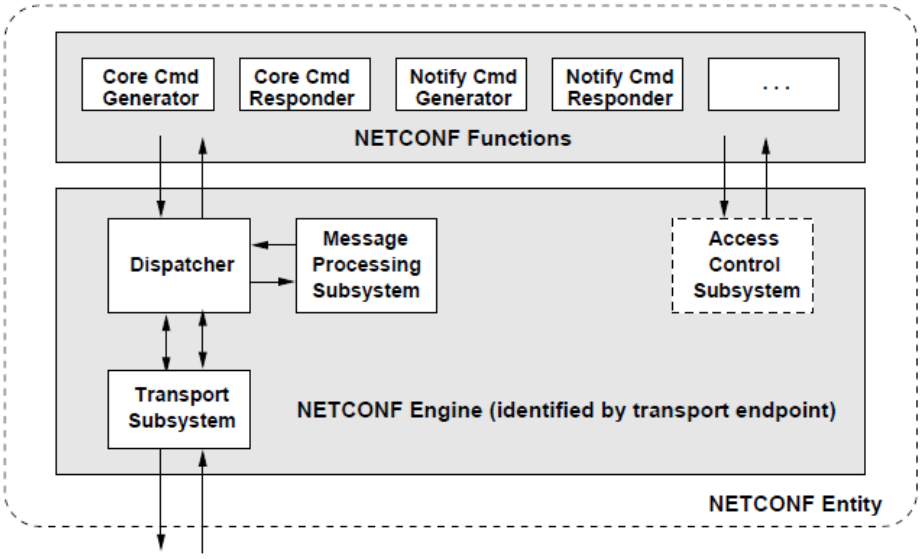

Figure 5. NETCONF Entity [JuSch]

Layer	Content & Examples
Content	Device configuration data (YANG definition)
Operation	Operations invoked as RPC methods in XML. <get-

	config>and<edit-config>
RPC	Transport independent mechanism in XML. <rpc>and<rpc-reply>
Transport	Transmission protocol between agent and manager. SSH, SOAP and BEEP

Table 2. NETCONF Protocol Layers [YuAja]

NETCONF implements a larger number of protocol operations than SNMP and it is expected to grow.

For operations, data structures are defined using XML (eXtensible Markup Language) and current standardization is focusing on the exact definitions of these data structures. This problem is the reason why the definition of YANG is needed.

NETCONF is implemented by:

Commercial Tools

- Applied Informatics - http://www.appinf.com
- Netconf Central - http://www.netconfcentral.org
- SNMP Research - http://www.snmp.com
- Silicon and Software Systems - http://embeddedmind.com
- Tail-f (ConfD) - http://www.tail-f.com

Device Vendors

- Alaxala - http://www.alaxala.com
- Cisco Systems - http://www.cisco.com
- Ericsson - http://www.ericsson.com
- Juniper Networks - http://www.juniper.net
- Nortel - http://www.nortel.com
- RuggedCom - http://www.ruggedcom.com
- Taseon - http://www.taseon.com
- Verivue - http://www.verivue.com

Open Source

- YencaP - http://ensuite.sourceforge.net
- ncclient - http://code.google.com/p/ncclient
- netopeer - http://code.google.com/p/netopeer

2.2.4 YANG

YANG is a language used to model data; in particular, it is being developed to model data for NETCONF protocol. The way YANG defines data is using hierarchical trees where each tree can have either a value or a set of child nodes.

YANG is meant to be human readable (easy to learn and comprehend data structures), modular (use of modules and sub-modules), reusable (structured types) and extensible. The YANG module translation into XML

is called YIN. YANG maintains compatibility with SNMP's SMIv2 ensuring that SMIv2 modules can be automatically translated into YANG ones (YANG to SMIv2 is not concerned).
YANG nodes definition:

- Leaf node: A leaf node contains simple data as integers or strings. It has no children nodes.
- Leaf list nodes: It is a leaf node sequence with exactly one value per leaf node.
- Container nodes: It is used to group related nodes in a subtree. Container nodes have only children nodes and no value. (Children nodes can be leaves, lists, leaf-lists and other containers.
- List nodes: A list is a sequence of list entries. List entries may contain any number of children nodes and any type of them.

Commercial Toolkits

- Netconf Central - http://www.netconfcentral.org
- SNMP Research - http://www.snmp.com
- Tail-f (ConfD) - http://www.tail-f.com

Open Source

- jYang - http://jyang.gforge.inria.fr/jYang
- libsmi - http://www.ibr.cs.tu-bs.de/projects/libsmi
- pyang - http://code.google.com/p/pyang

Utilities

- syang.el

2.3 Role of Control Plane in Management Functions

With the advent of fully reconfigurable network infrastructure, control planes were developed for both packet as well as circuit networks in order to automate the provisioning process and reduce the complexity from the NMS. Control planes were designed with three specific functionalities, namely: dissemination of routing information, automated provisioning and automated service recovery during failures.

The most commonly used control planes in transport network today are the GMPLS control plane [GMPLS], which extends MPLS to support packet switching, time division and wavelength multiplexing, and the ITU-T Automatic Switched Optical Network (ASON) [G8080] which uses standard interfaces, namely the User Network Interface (UNI), the Internal Network-Network Interface (I-NNI), and the External Network-Network Interface (E-NNI) for communications between the user and the network, two network elements inside a domain and between network domains respectively. Both the ASON and the GMPLS control plane support multiple technologies and have support for multi-layer networks, but by themselves do not solve all problems of multi-layer network management. Control plane deployments only provide basic support for features such as policy control, AAA integration and do not provide support for complex functions such as root cause analysis for network failures, inventory discovery and management, configuration and management of device specific alarms, etc. It is for these reasons that control planes are currently used as a tool by the NMS to support automatic provisioning and failure recovery, while all other management tasks are facilitated by the NMS.

Currently, control plane is only used to provision services (MPLS services in IP, and circuit services in transport) in the network and is configured to automatically restore a failed service, either on a pre-reserved backup path or by re-computing a path in the network. Also, routing capabilities of the control plane in multi-layer context are limited based on the network model (peering, overlay) used in the deployment, and upcoming standards such as the PCE are more likely to be used for multi-layer path computation in the future.

Control plane is used to provision multi-layer connections in transport networks but is rarely used in conjunction with IP networks. The primary reason here is that unlike services in the transport network, services in IP networks are significantly disrupted by changes in IP routing which may be triggered by any change in topology.Therefore, operators prefer to perform multi-layer operations as a series of controlled interactions between the two networks rather than an ad-hoc series of interactions which could significantly affect the operations of other services in the network. Also, the standardized control planes provide support for MPLS and do not support vendor-specific features of IP routing and forwarding (example Cisco's policy-based routing functions) which are used by network operators to provision services in the IP network. Finally, control planes can only perform the aforementioned functions as atomic operations, and thus cannot orchestrate complex multi-layer operations such as network engineering and policy-driven traffic offloading.

2.3.1 Protection and restoration

Protection and restoration are two main types of resilience mechanisms used in today's transport and IP network environment. While protection is one of the best recovery mechanisms, it incurs high cost to the network providers due to the low network utilization resulted by automatic protection switching. Legacy SONET network use automatic protection switching (APS), 1+1 protection, linear APS, two fiber unidirectional path switching ring(UPSR), two fiber bidirectional line witched ring(BLSR) and four fiber BLSR protection mechanisms. On the other hands, SDH networks use multiplex section protection(MSP) 1+1, MSP 1:1 and MSP1:N. They also implement two fiber sub network connection protection (SNCP), two fiber multiplexed section protection mechanisms. While transport network use protection mechanism to recover the failure, the IP networks use restoration to recover from a failures, as TCP provide opportunity for the retransmission of data if a failure occur.

For mesh networks, there are two well-known recovery methods, span protection and path protection [Vas04], whose efficiency has been evaluated in a plethora of studies, e.g. [Wan02] [Rue02]. A newer method, called local to-egress [Aut02], where the traffic is re-routed on a per connection basis between the upstream failure adjacent node and the destination node, has a good performance trade-off in terms of notification time and capacity efficiency [Gru05].

2.3.2 Provisioning

Provisioning refers to execution of complex functions that triggers the actual connection establishment between two or more points in the network. Today's network requires capability of provisioning connections that map to complex services. While control plane frameworks introduced by standardized organisations provide opportunity for automatically provisioning a link/service between the different layer of transport network, traditional network/ service provisioning is still a manual, cumbersome and time consuming process between the IP and the transport layer. Provisioning a connection between two or more nodes in the network requires algorithms for path selection and signalling to request and establish the connection. The provisioning process become more complex when it involves multi- vender technologies and multiple domain and layer in the network. Path computation, connection admission control, connection establishment between a pair of network elements and connection establishment by individual network elements are the main functions of provisioning [Ric04].

2.3.3 Distribution of routing

In BGP/MPLS IP VPNs, provider edge routers use route target to control the distribution of routes into VRFs. Within a iBGP mesh, PE routers need only hold routes marked with route targets partitioning to VRFs that have local customer edge attachments. Routh reflection commonly used for an autonomous system [Bat06], in order to simplify the process of bringing up a new provider edge (PE) router in the network. When VPNs may have members in more than one autonomous system, the number of of routes carried by the inter cluster or inter as distribution routers is an important consideration. In order to limit the VPN routing information that is maintained at a route reflector it is suggested to use cooperative route filtrating between route reflectors [Ros06]

2.3.4 User Network Interface

A User Network Interface defines the interface between the client and the network, and is used by the client to request a service from the network. The exchange of control information through the UNI is only related to neighbour discovery and signalling function. Optical Intrnetworking forum (OIF) developed two version of UNI, namely UNI 1.0 [OIF2003.249] which provide support only for SONET/ SDH data plan signals. The main functions supported by UNI 1.0 are connection establishment signalling, connection deletion signalling, status exchange signalling, auto-discovery signalling and data plane functionality.

UNI version 2.0 [OIF2003.351] which specified in the working document oif 2003.239, apart from the SONET/SDH provide support for the Ethernet signals. Since the UNI interface is of asymmetrical nature, different requirements apply to its client side (UNI-C) and the Network side (UNI-N). The UNI-C will usually be incorporated into client networks and requests typical actions such as establish connection form the optical server layer. UNI-N reside on layer 1 equipment, such as an optical switch.

3 Functional Limitations of Current IP Management Systems

3.1 Introduction

In order to help to perform the different set of management functions needed for an IP Network, a bunch of tools implementing the different management standard protocols are available in most operating systems and devices. These tools allow, for example, verifying connectivity, configuring interfaces, capturing traces to verify performance, etc. A summary of these well-known tools is provided in Table 3.

Tool	Description	Refererences
Ifconfig	Ifconfig is used to configure the kernel-resident network interfaces.	*http://linux.die.net/man/8/ifconfig*
Ping	Ping is a simple utility that sends one Echo message and wait to see if an Echo Reply is received back.	*http://www.tcpipguide.com/free/t_TCPIPCommunicationVerificationUtilitypingping6-2.htm*
Nslookup	NSLOOKUP is a service to look up information in the DNS. Is a unix tool.	*http://www.kloth.net/services/nslookup-man.php*
Dig	Dig is a command-line tool for querying DNS name servers for any desired DNS records	*https://www.isc.org/software/bind/documentation/arm95#man.dig*
Host	Host is a simple utility for performing DNS lookups. It is used to convert names to IP addresses and vice versa.	*http://www.manpagez.com/man/1/host/*
Mrtg	It will monitor SNMP network devices and draw graphs showing how much traffic has passed through each interface.	*http://oss.oetiker.ch/mrtg/*
Netstat	Netstat is a useful tool for checking your network configuration and activity.	*http://www.faqs.org/docs/linux_network/x-087-2-iface.netstat.html*
Arp/rarp	ARP is used to resolve the Ethernet address of a NIC from an IP address. RARP is used to determine IP addresses using the Ethernet address.	*http://www.comptechdoc.org/independent/networking/guide/netarp.html*
traceroute	Traceroute utilities work by sending packets with low time-to-live (TTL) fields. The TTL value specifies how many hops the packet is allowed before it is returned.	*http://www.webopedia.com/TERM/T/traceroute.html*

Table 3. Summary of IP Management Tools

These set of individual management tools are simply the basic tools for a network operator. In practice, network management still requires a high degree of manual intervention if only those tools are available. In the recent years, many Integrated IP Network Management systems have appeared in response to the increasing interest

of service providers in managing and monitoring their networks in an automated way, in order to evaluate and react to the overall performance of the Network. These Network Management Systems integrate some of the tools mentioned above, provide a unified graphical interface, and provided customized to the different network equipment and their specific data models, protocols and commands. Today, these Network Management Systems are widely used as they constitute essential elements for controlling network operations, faults, configuration, performance and security tasks.

The IP Network Management Systems are of different nature: open source, commercial tools, device specific vendor systems, and in many cases, in-house developments of the network operator.

Regarding the operating systems, typically they are Linux or Windows-based. It is clear that due to the heterogeneity of devices in current networks, multi-vendor platforms seem to provide the best solution in Network Management, whilst efforts towards standardization of network management protocols have been pushing these solutions in the same direction.

Many aspects may be taken into consideration when selecting a Network Management Tool, a commercial or a free open-source tool, monitoring capabilities (multi-vendor, protocol independent), auto-discovery features, customization degree, GUI, etc.

Next, we will present an overview of some of the most outstanding and currently deployed IP Network Management Tools, in order to evaluate the functional limitations of current systems and highlight the potential of these tools as providing inputs for coordinated functionalities in multi-layer management. The objective will be to give a technical overview of some of these tools, to understand the capabilities and features that current IP Management tools are able to provide.

3.2 Overview of IP Network Management Systems and Features

Two commercial tools lead the Network Management Software market in a competitive manner. The solutions of HP-OpenView and IBM-Tivoli constitute two of the most used enterprise-grade management systems. There are also a couple of powerful open source network management systems, Open NSM and Nagios. In this section we present an overview of these systems in order to evaluate the limitations and capabilities of the different systems.

HP OpenView Network Management Solution - A proprietary solution for IP Network Management

HP OpenView is the formal name of the HP product family consisting of Network and System Management tools. It is a suite of numerous products that allows management of applications, device availability, network conditions and status, system performance, service and program maintenance, and storage resources. HP

OpenView Network Node Manager is the SNMP-based monitoring tool for this family of products. HP OpenView has many features of which a great number is focused on usability. HP OpenView handles networks of any size and complexity and it is probably the most widely deployed application of its kind.

License

- Commercially-licensed proprietary software.

OS Support

- Supported operating platforms for host and managed systems include HP-UX, HP Tru64 UNIX®, HP OpenVMS, Linux, NetWare, Solaris, Windows, and VMware ESX.

Products

- OpenView Network Node Manager (OV-NNM) (network monitoring software based on SNMP).
- OpenView Operations for UNIX (OV OU).
- OpenView Service Desk.
- OpenView AssetCenter.
- OpenView Internet Services.
- HP OpenView SOA Manager.

Management Areas

- Network and System Management.
- Application Management.
- Event Management.
- Desktop and Software Management.
- IT Service Management.
- Security Management.
- Storage Management.

Standards Support

- The HP OpenView products support protocol, object, and service specifications defined by ITU, OSI, X/Open[R], the Internet Engineering Task Force (IETF) for SNMP (Simple Network Management Protocol), and the Network Management Forum (NMF). There is also full support for network management protocols CMIP (Common Management Information Protocol), RFC 1006 (TCP/IP), DMI and SNMP.

Graphical User Interface

- The HP OpenView windows graphical user interface (GUI) provides network operators and administrators with a consistent view of the managed environment and seamless integration of management functions, regardless of vendor or managed object type. HP OpenView windows provides a common interface that simplifies the development and use of management applications. Finally, the HP OpenView windows GUI is the key integration point for HP OpenView applications.

The core of the HP OpenView Framework is the HP OpenView Network Node Manager (OV-NNM), this is a SNMP-based monitoring tool that provides a solid solution for managing dynamic IP Networks. Some of the most outstanding features of this tool are:

- Automated network discovery.

- Broad multi-vendor device coverage.
- Device status tracking.
- Network map graphing (physical and virtual).
- Statistics and network health data gathering.
- Perform dynamic root cause analysis and advanced diagnostics such as path views and service impact analyses
- Report graphing.
- SNMP alert processing.
- Create integrated performance thresholding and reporting
- Scalable to large and complex Networks.

HP solutions are target of software integration developments for specific vendor devices, which aim to improve the initial solution and extend their reach (e.g. HP Web Jetadmin [HPJ11]).

IBM Tivoli Network Management Solution - A proprietary solution for IP Network Management

- The IBM Tivoli Network Management Solution provides the tools for managing devices in a Network in an automated approach. It includes several products aimed to:
- Collect, analyze, and project the flow of network traffic.
- Collect and analyze network events, alarms, response times, and utilization.
- Establish and adjust the network and its elements through configuration software, in order to keep it up and running.
- Network design, IP address management, network element management and mediation.

License

- Commercially-licensed proprietary software.

OS Support

- Almost all products of the IBM Tivoli Suite provide support for the following Operating Platforms: AIX, Sun Solaris, HP-UX, Linux and Windows.

Products

- IBM Tivoli NetView, is a SNMP-based distributed network management software.
- IBM Tivoli Network Manager.
- IBM Tivoli® Netcool®/OMNIbus.
- IBM Tivoli Configuration and Change Management Database.
- IBM Tivoli Monitoring.
- IBM Tivoli Storage Manager.

Management Areas

- Network Management and Monitoring.
- Service Management.
- Storage Management.
- Security Management.
- Configuration Management.

- Performance Automation

Standards Support

- Support to network management standards SNMP and CMIP.

The overall goal of these tools is to help organizations improve network visibility and drive reliability and performance.

Some of the enumerated features of the IBM Tivoli Network Manager are:

- Uses SSL and payload encryption to provide more secure connection between the management server and its clients.
- IBM Tivoli Network Manager provides automatic network discovery feature and complete visibility of the Network. Supports discovery of Layer 1, 2 and 3 Networks.
- Models and maintains information of all network devices and their connectivity.
- IBM Tivoli Network Manager easily inte¬grates with operational support systems (OSS) and other mission-critical work¬flow applications.
- Tivoli Network Manager provides valuable advanced fault correlation and diagnosis capabilities.
- Provides web-based visualization of the Network infrastructure.

Other important component of the IBM Tivoli Management Suite is IBM Tivoli Netcool Configuration Manager which automates network configuration and controls network device access. Clients can manage their device configuration changes and backups through Tivoli Netcool Configuration Manager. The main challenge of managing Network Configurations in an automated way is the lack of standardized protocols that rule over multi-vendor configuration set-up. Command-line Interface (CLI) is the common way of configuring devices, but CLI varies from vendor to vendor, or even worst it may vary through the line of products of a same vendor. In this sense, automated device configuration for heterogeneous networks is a rather challenging task. IBM Tivoli Configuration Manager features SmartModels [IBM10], which allows configuring multi-vendor network devices while providing a suitable graphic user interface along with a standard consistent language, abstracting the network manager from having knowledge of specific-vendor configuration commands. IBM Tivoli Configuration Manager is based in the use of CLI, as method of configuration, what it actually does is easy the use of any CLI by standardizing even the most complex CLI. SmartModels translates command-line interfaces into an industry-standard XML scheme that can be displayed as a common interface.

OpenNMS - An Open Source solution for IP Network Management

OpenNMS is a Java based open source network management software, licensed under the GNU Generic Public License in 2000. It aims at providing a competitive free alternative tool to products like HP OpenView, CA Unicenter, among others. OpenNMS consists of a community supported open-source project as well as a commercial service, training and support organization. It represents an application developed for scalability and integration in the enterprise. OpenNMS is used by many organizations to monitor their Network infrastructures, but also provides the functionality of monitoring services and notify of errors and statistical information of performance parameters. This platform allows users to add network management features over time. OpenNMS focuses on three areas: service polling, data collection and event management.

License

- Open Source Software.

Programming Language

- OpenNMS is written in Java.

Operating System Support

- It currently supports a variety of open operating systems, including Linux, Mandrake and Solaris, as well as Mac OS X. It also provides Windows support.

Scalability

- OpenNMS can be run distributed and scale to an unlimited number of devices.

Discovery

- OpenNMS provides auto-discovery feature, that allows to detect in an automated way all the devices on the network.
- Protocols used by OpenNMS (to discover devices and the services they run): ARP, ECHO and SNMP.

Service Monitoring

- OpenNMS is capable of monitoring over more than 25 services: HTTP, HTTPS, DNS, DHCP, IMAP, database systems, SMTP, among many other services.

Configurations

- XML-based configurations.
- Extremely configurable and customizable.
- Events are managed through configuration files.
- Availability of external tools to build events for configuration files (mib2opennms).

Other Features

- OpenNMS has developed plug-ins to integrate and interact with other network management software such as Hyperic HQ, in order to extend and complement functionalities.
- OpenNMS has MIBS already installed for most large vendors equipment but users can add their own configurations.
- Built in SYSLOG.
- SNMP trap collectors.
- OpenNMS can collect data via SNMP, HTTP(S), JMX, WMI, and other protocols.
- OpenNMS stores performance data in RRD (Round Robin Database) files.
- OpenNMS can generate network maps viewable with Adobe SVG viewer.
- It has built in reporting.
- Generates graphs from the SNMP data polled from the network
- Path outages feature, addresses the need to suppress notifications for nodes that appear to be down to the OpenNMS system due to a failure in the network path between the nodes and OpenNMS.
- OpenNMS manages internal and external events.
- It is possible to provide a complete path to an executable program. The program will be executed every time the event occurs.
- Nagios plugins may be used.

Nagios - An Open Source solution for IP Network Management

Nagios is an open source monitoring system created in 1999. Nagios stands as a powerful tool for network, server and application monitoring, with particular development in server monitoring. It is a SNMP-based management tool. A key feature of Nagios is the development of customized plug-ins by means of an open API. It counts with a powerful web-based user interface that suppors performance tracking and easy access to information. Nagios, as many open source tools, comes with a support community perhaps less active than OpenNMS support group.

Programming Language

- Nagios is written in C.

Operating System Support

- Nagios runs under Linux Operating System. No support for Windows.

Scalability

- Network Managers report scale issues for enterprise level. Visibility issues when there is too many information.

Discovery

- External tools allow to add auto-discovery features.

Service Monitoring

- Nagios provides the capability to monitor HTTP, FTP, SSH, SMTP, POP3, IMAP services.
- Plug-ins can enable the monitoring of specific services. Customized plug-ins may be written by users/developers if no existing one suits their needs.

Configurations

- It is highly configurable and customizable.
- Nagios is configured through plain text files with a special syntax.
- There are a few web-based Nagios admin interfaces written by third parties that can allow Nagios configuration via a web based interface.
- Many tasks require configuration file edition.

Other Features

- Nagios provides a notification and alerting framework. Automatic notifications can be send out to administrative contacts in a variety of different ways: email, instant message, SMS, etc.
- Easily extensible. Support of plug-ins to extend Nagios functionalities.
- Nagios allows you to write plug-ins in just about any language and run them on remote servers.
- Supports passive and active usage of SNMP. This is, in the active role Nagios can use plugins to request information from the client. Using the passive aspect Nagios can receive traps, or messages from the agent to the manager to process the information.
- Nagios stores performance data in RRD (Round Robin Database) files.
- Ability to define event handlers to be run during service or host events for proactive problem resolution.

- Simple authorization scheme that allows you to restrict what users can see and do from the web interface.
- Mobile interfaces have been developed for Nagios.
- Plugins enable the graph functionality.
- Some notable organizations that use Nagios as part of their IT management toolset are: 3COM, amazon.com, at&t, Cistera Networks, Domino's Pizza, ebay, friendster, Google, twitter, symantec etc.

Table 4 summarizes some of the main properties of the previously described Network Management Tools:

		FEATURES							
		License	Discovery Feature	Supported NM Protocols	Distributed/Centralized Management	Plug-ins	Database	Remote Device Configuration Features	Web-based GUI
TOOLS	HP OpenView	Commercial	Included	SNMP/CMIP	Distributed	Yes	PostgreSQL, Oracle Database	HP Network Automation Software	Full Control
	IBM Tivoli	Commercial	Included	SNMP/CMIP	Distributed	Yes	MySQL, Oracle Database, DB2	IBM Tivoli Netcool Configuration Manager	Supported
	OpenNMS	GPL/Open Source	Included	SNMP	Distributed	Yes	JRobin, PostgreSQL	No	Full Control
	Nagios	GPL/Open Source	Via plugin	SNMP	Distributed	Yes	Flat File, SQL	No	Full Control

Table 4. Comparison of IP Network Management Tools

3.3 Limitations of Current IP Network Management Systems

As seen by reviewing some of the most widely deployed IP Network Management Systems, despite they all aim to solve the same generalized task, each system provides different functionalities which, depending on the Service Providers real needs and requirements, makes them more or less suitable for managing their Networks.

One of the important limitations of current Network Management Systems is the lack of well set standard protocols for network device configuration. Despite the extended use of SNMP for network management monitoring functionality, this standard has not achieved any success over device configuration, on the other hand, NETCONF is figuring and pushing towards a standard willing to overcome this limitation and fill the gap of monitoring and configuration [MIJ04].

One of the main disadvantages of commercial tools is the high cost of acquiring this technology, generally only big companies can afford it. Although open source tools are free and well supported among many communities, devoted to keep forums and software up-to-date, these are not widely used in professional carrier grade networks because of limited capabilities when compared to professional proprietary tools.

Product Leadership Survey of Search Networking in 2007 [SNT07] positioned open source solutions as preferred among network managers because of their flexibility and adaptability to specific needs, avoiding licensing restraints. Many open-source management suites allow the integration by extending other tools that integrate new functions, empowering monitoring and management capabilities. Finding a proprietary solution that well suites all the real requirements of operators may be a challenging task, since customized in-house developed add-ins are not an option for commercial tools. On the other hand, competitiveness among commercial tool vendors accelerates the growth of such management solutions, in order to outstand in features and functionalities. Despite the high cost and lack of flexibility of commercial tools, they represent high-quality, high-end products that require skilled staff for the correct use of these systems.

Current open-source Network Management Systems are majorly focused on acting as Network Monitoring tools, this means they keep track of all network elements and raise alarms when any problem is detected, on the other hand, the competitiveness of commercial tools show them as more integrated solutions capable of supporting configuration functionalities, more powerful high-quality collection of data, etc.

The existence of dissimilar standards and the lack of consensus around the preferred protocols, have raised multiple interoperability issues, this refers to the ability of IP network management systems to interact with other management systems. Interoperability is an important feature of Network Management tools, considering that network management scope is so large that it is almost impossible for one product to do it all, complementary products may better adjust to real service provider's needs. The majority of commercial tools limit interoperability due to the dynamics of the business scheme and competition model. A clear example of interoperability constrains, is for example the proprietary format of processed SNMP traps by HP OpenView, which limits interaction with other management platforms. The number of third-party products a platform may support is a manner of evaluating interoperability among a tool. Interoperability issues do not only appear among the IP layer management systems but are fundamental when trying about packet and optical exchange of information, originating isolation of both layers.

Despite the potential of these tools in automated configuration tasks at the IP layer, current IP-NMS's can in no manner execute coordinated functionalities with the optical transport layer not even for relatively easy tasks, such as link provisioning. But what may be seen as a great potential of these tools is the capability of providing inputs for solving multi-layer problems, given their major automated functionalities at the IP layer.

4 Carrier Grade Management Functions

4.1 Current Transport Network Management Systems

4.2 Functional Limitations of Current Carrier Network Management Systems

4.2.1 ITU-T Telecommunications Management Network (TMN)

There are various standardization bodies in place that have released certain recommendations defining principles and concepts for the Telecommunication Network Management. One is ITU-T Telecommunications Management Network (TMN) Recommendation M.3010. Work on this recommendation started in 1985 in CCITT and defines concepts of TMN architectures (TMN functional architecture, TMN information architecture, and TMN physical architectures) and their fundamental elements. This Recommendation also describes the relationship among the three architectures and provides a framework to derive the requirements for the specification of TMN physical architectures from the TMN functional and information architectures.

The purpose of this Recommendation is to serve as an umbrella Recommendation for the development and use of TMN Recommendations within ITU-T. Figure 6. Example of relation between TMN-related Recommendations [TmnM3000]shows the relation between different TMN recommendations.

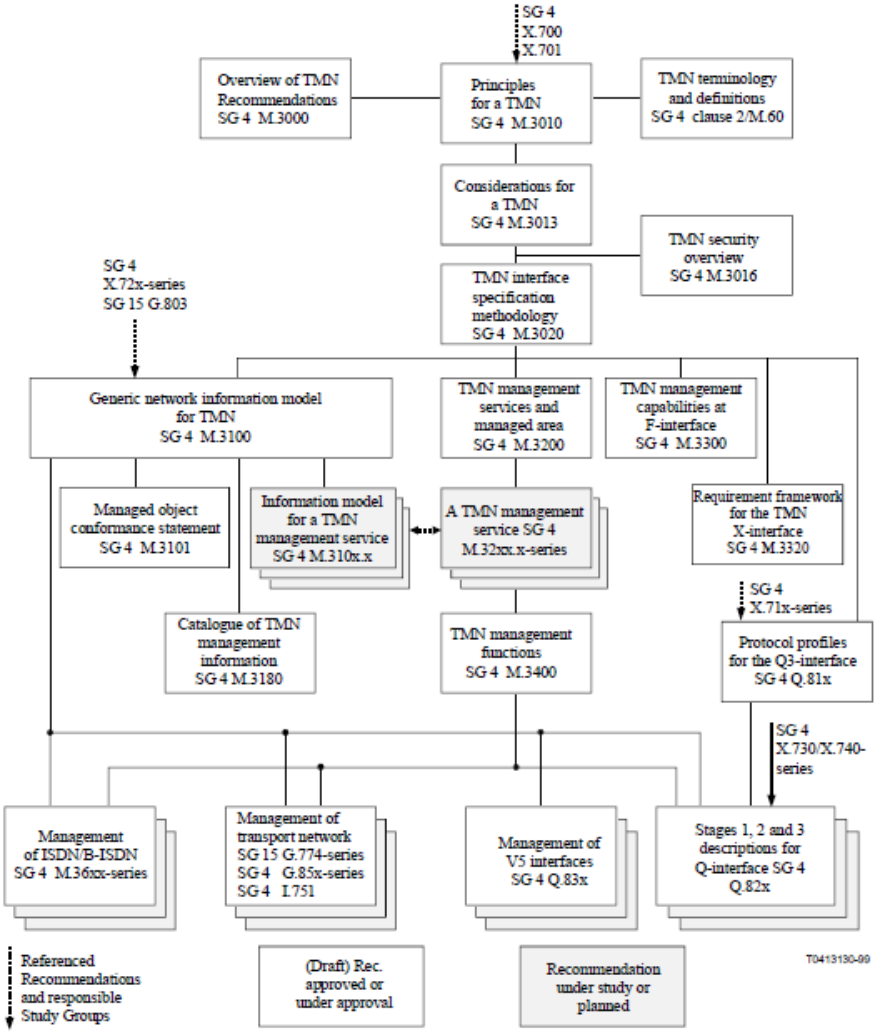

Figure 6. Example of relation between TMN-related Recommendations [TmnM3000]

One important TMN concept is the Logical Layered Architecture (LLA). This architecture distinguishes between network element, network, service and business management. While IP Management has traditionally focused on network element and network management only, the different transport management systems support all layers. The LLA can be used to identify four management system layers on top of the network elements which are managed: Element Management System (EMS), Network Management System (NMS), Operations Support System (OSS), and Business Support System (BSS). The respective architecture is shown in Figure 7. Layers in TMN with interfaces between layers, including the generic interfaces as defined in M.3010.

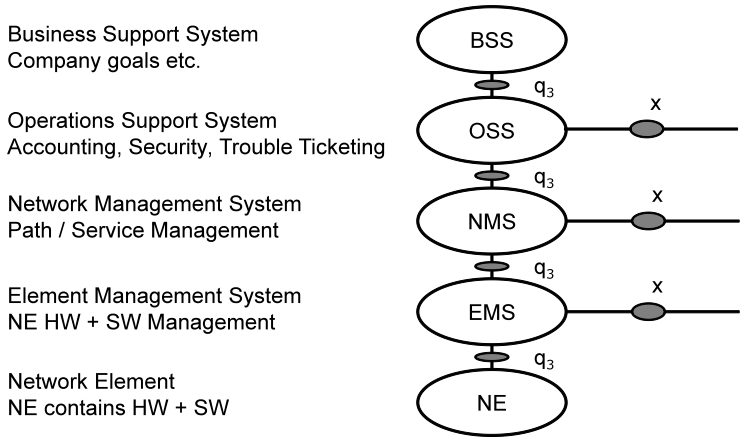

Figure 7. Layers in TMN with interfaces between layers

The most important difference between TMN and IP Management is that the first concentrates on the specification of management architectures and the second on the implementation of management protocols. The architectural concept defined by TMN is very complex compared to the SNMP driven IP architecture. As a result, there are only a limited number of TMN products on the market, whereas there are many commercial and public domain IP Management products.

However, due to the described nature of different telecommunication networks and their Management Systems, often one will find a dedicated Management System for Transport equipment, e.g. SDH and WDM while there are separate management systems purely managing other devices, e.g. Layer 2 or Layer 3 devices. The demand to merge those different layers and their technologies behind grows with the network's continually increasing complexity.

4.2.2 MTOSI:

The TM Forum's Multi-Technology Operations System Interface (MTOSI) addresses the above mentioned need for a harmonized view on the whole network and is considered the standard for implementing interfaces for different OSS's that manage different portions of a service provider network.

MTOSI is a unified open interface to be used between Operations Systems (OSs), where an OS is any management system that exhibits Element Management Layer (EML), Network Management (NML) and/or Service Management Layer (SML) functionality as defined in the ITU-T TMN model.

The Network Management System-to-Element Management System communication is a special case and is defined by the Multi-Technology Network Management (MTNM) standards.

MTOSI is defined in terms of:

- a set of business requirements and behavior specifications which define what the interface is expected to do,
- a management information model defining the objects and operations available on those objects,
- an implementation architecture leveraging web-services technology (WSDL/SOAP/HTTP/JMS), and,

- detailed specification of the solution set in WSDL, XML Schema and supporting documentation.

Standardized interfaces between many vendors, technologies, and systems allow service providers to deliver new services and products faster and at lower cost.

MTOSI covers both service and resource level interfaces. At the resource level, MTOSI includes interfaces for inventory, provisioning, fault management, and performance management. At the service level, MTOSI has interfaces for service activation and for service inventory.

MTOSI supports the management of these technologies: SONET/SDH, PDH, DWDM, Ethernet, DSL, ATM, and Frame Relay. Support is planned for T-MPLS, PBB-TE, GPON, and Control Plane management.

MTOSI uses a single interface infrastructure and applies the same patterns across multiple technologies. For example, the same basic termination point and connection models are applied across all connection-oriented technologies ranging from DWDM to ATM. A similar statement can be made about the MTOSI connectionless model.

Documents pertaining to these standards may be downloaded from the TeleManagement Forum home page at www.tmforum.org

No doubt that the above described standardization work is the right approach to enable service providers to mix OSSs of different vendors in terms of functionality, price and quality. However the standards give no answer to how the right mix of management systems could be achieved.

Coordination of mentioned different management systems will help the service providers to overcome the challenge of growing bandwidth in times of stagnating service revenues. Coordination of the differents OSSs in an easy to deploy way addresses exactly more effectiveness in the service provider's daily work and organization of the service prove.

4.2.3 MTOSI NBI in ADVA's FNM:

Some of the carrier grade management systems available on the market do not provide an MTOSI interface yet whereas others like ADVA's FSP Network Manager provides a northbound MTOSI interface using traditional web-services technologies (WSDL/SXD and SOAP/HTTP) to implement a combination of standard, pre-standard and proprietary operations.

The current north bound interface is based on the released MTOSI v1.0 and related specifications and the pre-release MTOSI v2.0/MTNM v3.5 Connectionless Technology Management work. Following FNM releases will provide "MTOSI Release 2.1" according to Telemanagement Forum standard.

4.3 Functional Limitations of Current Carrier Network Management Systems

The main functional limitation on a Transport Network Management System is certainly the level of integration of Management capabilities for devices that operate at different layers than the Transport System. That is a pure SDH or WDM System at Layer 1 may not cope with the requirements a Layer 2 or Layer 3 Network Management System has.

While in the transport Layer 1 environment the operator is typically monitoring the quality of service using standard mechanism like SDH or OTH overhead bytes to determine the performance of a service without touching any payload, at higher layers the monitoring goes beyond that point when throughput of packets and frames are evaluated. Since the Transport Network itself and its Management System never meant to be capable of handling these different demands, todays OSS landscape yet consist of various OSS for the different layer devices.

In addition, the Transport Management System and higher Layer Management System have different demands in terms of security functionalities. After all those two technologies, their planning, I&C and alarm surveillance typically run in different departments at a service provider.

The Transport Management Systems provide a big range of configuration, surveillance and monitoring. However there is no possibility to define different behaviour based on beforehand defined combination of incoming events.

5 Multilayer Management

Historically, Internet and carrier-grade transport layers have been conceived in a complete independent manner, from planning to provisioning and management. Thus, it is common in a medium-big size network operator to have within the Network Operating Center (NOC), groups specialized in each network layer, each using its own management tools, as those shown in chapters 3 and 4.

Many providers keep track of inter-dependencies of both layers throughout the use of inventory databases in-house systems or even spread sheets, but this represents a technique with numerous drawbacks. Umbrella management systems are in-house developed, and require huge development efforts and are hard and expensive to maintain, operate and upgrade. They are usually related to high-level workflows that assign orders or tickets to the different groups, assigning per-layer tasks, and querying the different databases. In many

cases, these systems are the link between the business departments, which sell the services and send the requests to the network, and the network groups, which are in charge or activating the service and upgrading the network when necessary. While the management task assigned to a specific group is subject to achieve a low dependency of manual interventions, workflows that involve several layers are full of manual steps.

This leads to an open issue around the isolation of multi-layer management and the incremental need of solutions that either integrate or coordinate functionalities between both layers, on one side to avoid redundancy of operations and to improve service provisioning in means of time and expenses.

There are several approaches to solve this isolation. On the one hand, there is the vision of integrating the different network layers, such as the IP over DWDM solution proposed by Cisco. In this vision, parts of the transport functions are integrated in the IP/MPLS routers. The main issue is that, in order to have an integrated network management and operations, both the router and the transport equipment need to be from the same vendor. Otherwise, the management turns out complex and does not solve the issue-

In the same line, there are approaches to integrate in the same equipment functionalities of the same vendor. That is, a router and a transport node are integrated, easing the management. As in the previous case, the main limitation is the inherent mono-vendor approach.

The last approach is developing a true multi-layer management system, which can provide an unified view and, coordinate the set of operations, taking into account the particularities of IP and transport layers. The transport Network itself it is usually multi-layer, with several OTN and Ethernet layers. There are approaches like, that claim to be a multilayer management. However, that only applies to transport networks, with the same philosophy of a connection oriented transport approach. Recently, Cyan Management System has appeared as an interesting framework for coordinating different layers. The main issues are that: i)it only manages networks and devices which and Cyan compliant and ii) it is a proprietary approach, with all developments in Cyan's side.

The ONE adapter aims at providing a holistic approach, giving a coordinated solution capable of suiting an evolutionary not disruptive approach for multi-layer management. The ONE adapter allows the easy creation of workflows involving several layers using the already deployed Network Management Systems. Thus, actions in the network involving several layers can be orchestrated. These actions in the network are abstracted, making them vendor-independent in the view of the workflows. Use of standards is encouraged, so as to have an easy integration with any network layer and vendor.

5.1 Benefits of Network Management Coordination

As opposed to the current network operation scenario, future networks implementing a control plane could be operated like the network shown in Figure 8. With an automated IP Network Management System, a single operator can change the virtual topology of the IP/MPLS network and perform management tasks network-wide instead of in a single element at a time. This extreme simplification leads to significantly smaller provisioning times and reduction in operational costs. Nowadays, the request of a new link between two routers involves several departments in the company, configuration in all the network equipment and takes much more time.

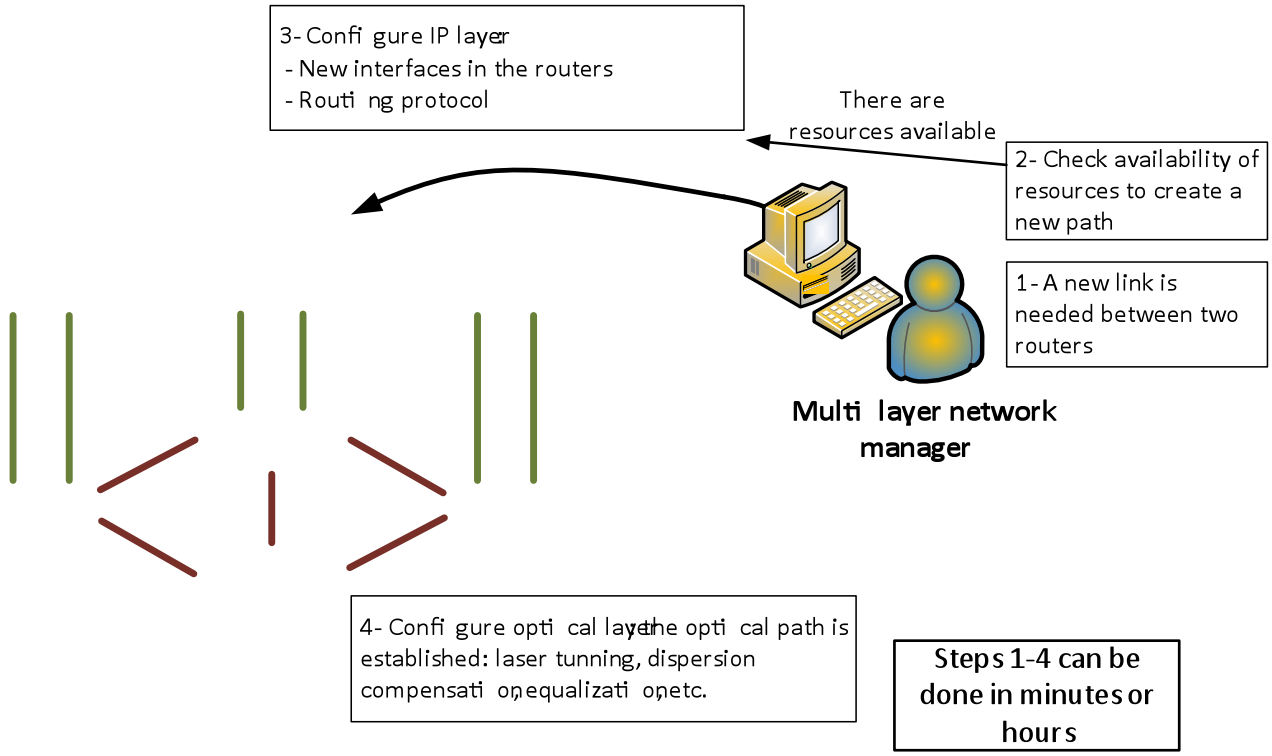

Figure 8. Future Netwok Management Process

An automated IP Network Management System with Multilayer capabilities can also help a network operator control the whole virtual topology for the IP/MPLS network, running optimisation algorithms periodically taking as inputs the network resources and traffic demands. As Internet traffic has, in principle, unpredictable distribution and grows every year, the operator can take actions based on current overall state of the network to change the topology according to costs or performance criteria.

Traditional network planning considers IP/MPLS and transport networks separately. On the one hand, IP/MPLS planning consists of the initial placement and dimensioning of routers taking as input a set of service requirements. On the other hand, transport network planning involves designing, engineering and routing of transport connections, based on the connectivity needed by the IP/MPLS layer. This two-step planning process is inefficient for network evolution. Once the IP/MPLS network nodes are fixed and initial connectivity is provided, upgrades may be limited to increasing the capacity and deploying new connections.

Alternatively, joint network planning would consider all network layers at once and would allow complementing the flexibility of IP technologies with the cost-effectiveness of optical switching, together with dynamic optical networks to optimise global costs. Such joint planning can use information about equipment costs and service requirements to jointly design the IP and optical layers through multilayer optimisation algorithms. As a result, the virtual topology would be cost-efficient, considering the traffic flows are switched in the optimal layer, depending on the global cost implications of the network traffic matrix.

Automated networks provide the flexibility and efficiency needed to beat competition, reducing time to market while getting most out of the investment and allowing rapidly launch, deliver and assure new generation of services.

Automated Transport Management simplifies the whole process of service provisioning. One would only need to connect to one single device to provision services, define the service type and transport parameters, let the SW chose the optimal route to reach the destination NE while optical constrains are considered. Computation of a new service takes place within few seconds, followed by automatic provisioning of all resources required for the desired service. The benefit is clearly less time and manual efforts it takes to setup a new service. Along with automated inventory and resource discovery, determination of best route chosen or going a preferred route from source to destination, opposed to the traditional approach where one would have to do all this task manually and eventually having deep knowledge of the entire network and its parameters. Complemented by automated tasks like data base backups, scheduled reporting and activation of new services through service activation engine, regular maintenance activities such as release upgrades leads to less requirement of resources to run the traditional daily tasks.

A flexible transport layer, which may be achieved by introducing WSS ROADM devices for directionless and colourless switching is the base for a full dynamic optical layer that no longer requires manual intervention when adding or removing new services.

On top of it, this flexible network offers a broad variety of automatic service restoration options. In addition to the data layer, the GMPLS control plane enables the automated service delivery of pure wavelength services. Since the GMPLS Control Plane is interoperable throughout different transport layers, other service types like ODUk on G.709 capable service modules or Packet flows on Ethernet service modules may also be provisioned. That multilayer traffic engineering also enables multivendor interoperability at different layers.

A common Network Management may automate multilayer traffic engineering in a multivendor environment, making Network Management Systems for the different transport domains redundant and reduce the overall workload on service provisioning activities

5.2 Economic Benefits

The shift from voice-centric to data-centric communication and the increasing demand for IP services generate new business opportunities for equipment suppliers, software developers, and network operators [Par05]. Thus, network operators are confronted with tougher competition in the market and are forced to transport an increasing amount of data at decreasing price.

As the networks grew geographically, centralized network management became troublesome. The resulting decentralization of network management and the creation of isolated islands of IP and carrier networks increased the network management cost. The cost is incurred by the duplication of network management functions, the increase in the number of human resources, the manual intervention and the lack of coordination between the two network management layers. Many manual interventions and complexity have always been considered as a main factor of network management operational cost [Cla11].

In order to ensure an adequate return on investments and to master this worldwide, highly capital-intensive business, carrier providers seek new ways to run and manage networks [Ft1999].

5.2.1 Reduction of complexity and duplication of network devices

Another factor, contributing to the high operational cost of networks, is the static nature of carrier networks and multi-vendor technologies. It causes not only interoperability issues but also increases the complexity of the network. Consequently, it forces network operators to spend more money on network management.

While the function duplication, manual operation, technology and the language differences are the main reasons of increasing operational cost of network providers, automation of network management of both layers can counteract this. Automation leads to lower operational cost through the possibility of reduction of function duplication, manual intervention and coordination between network management systems and network management functions.

5.2.2 Reduction of manual and error prone intervention

The fact that manual intervention in the process of service provisioning leads not only to inaccuracy in the network but also to a high operational cost [Par05] [Ncs02]. Manual intervention can also be blamed for the long service provisioning times, adding inefficiency in the network.

Manual operation has its origin in the historical development of the network, which was originally designed for voice delivery with circuit switching technology. When IP traffic first emerged, carriers could easily transport the traffic across their existing network. Nobody predicted a situation, in which the data traffic exceeds the voice traffic within a few years. Consequently, carriers fell into a situation, in which their network is not optimized. The enlargement of networks, which led to the separation of IP and the carrier layers, increased the number of human capital needed. As stated by Chahine [Cha04], the process of service provisioning in today's practices after the SLA setup needs to be handled by at least 6 departments in the carrier layer with the involvement of at least 6 persons in those departments. It involves the sales, administration, project management and three sub section of the network operation center. According to [Cha04], by allowing system automation, one can save as much as 51 percent of OPEX per service.

5.2.3 Increase in capacity utilization

There is consensus among scholars that carrier-to-subscriber links are mostly underutilized, except for peak hours, which exist for a brief period of time only and causes even congestion. Furthermore, regardless of the mixture of voice and IP traffic, all carriers face this problems, either congestion or network overbuilds.

Considering the best-effort nature of IP traffic, carriers always try to address congestion by increasing the network capacity. This, however, results in over-provisioning, leaving many providers link underutilized.

Furthermore, the support of IP traffic needs duplication of hardware and specific wavelengths, increasing the service cost. The traditional SONET ring configuration, which is usually leveraged by automatic protection switching (APS), is one of the main sources of network inefficiency. In terms of utilization, it leads to 100% network overbuild. Despite this high cost and inefficiency of 1+1 protection, the IP network still provides only best effort services.

IP and carrier providers can increase network utilization and prevent under-utilization through network management automation supporting coordination between the two network management layers. The coordination allows better traffic engineering and system optimization.

5.3 Current Multilayer Management Approaches

Some initiatives have been reported up to now in this field, such as Cyan's Management System - CyMS, which stands as a multi-layer management tool capable of providing an integrated three-dimensional view of the various layers of a Cyan compliant Network. This software performs as a visualization tool capable of representing physical and logical connectivity in order to allow planning, operation and verification tasks. It provides powerful tools for operators to determine dependencies between layers and how they interact. This solution represents a contribution towards multi-layer management approaches with the important limitation that current Networks are multi-vendor based, in this sense, solutions require being multi-vendor platforms capable of coordinating tasks between heterogeneous layers.

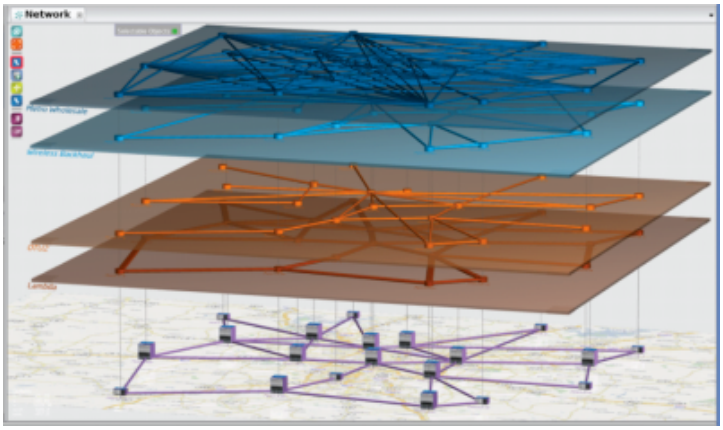

Figure 9. Multilayer CyMS 3D View [Cya11]

CyMS is deeply adapted and designed to comply with TMF MNTM and ITU G.800 principles. It also shows dynamically network evolution making possible identifying where the problem's causes located are. This tool uses "heat maps" that inform about alarm criticism performed by colour gradient representation allowing the network operator to proactively identify which network regions need evolution, changes or re-engineering.

As conclusion, we summarize CyMS advantages and disadvantages:

Advantages

- Integrated Management.
- 3D Multilayer view which allows better network behaviour comprehension.
- Heat Maps informing about alarm criticism.

Disadvantages

- Proprietary System. When high number of operators & vendors bet for it, its price will grow.
- Updates & maintenance will be on Cyan side which will add cost every change needed to be due to new technologies.
- If one vendor you have is not supported by Cyan, in operator's case, what to do?

Besides the CyMS software other initiatives from Cisco and Cyan push towards management tools based on a multi-vendor control plane, which represents a rather difficult and challenging task, since it requires the cooperation of other vendors in order to communicate in an open way to all vendor devices [Cyb11].

5.4 Integrated multilayer devices and network management

Juniper has recently pushed towards the development of a new hybrid device (unveiled on March 2011) [Jun11], which aims to combine optical and electronic technologies under the same chassis. Junipers PTX Series Packet Transport Switch aims to unify both technologies under a same system, avoiding current limitations towards isolation and interaction, whilst pointing to reducing carrier costs. Adding optical switching to a packet switch is representative of an integration approach from Juniper Networks, to such initiatives the One Adapter is able to illustrate future scenarios where no longer IP and Optical Layers are two completely isolated systems. Under this new scenario, how could the ONE solution face multi-layer management? This question raises an interesting new focus, in order to orient efforts on design and architectural premises that point on the same direction of current on-going developments.

Figure 10. Juniper PTX [JUN11]

Juniper's PTX approach up to now is simply integrate physically both IP and Transport in the same "box". The IP router still has its own management system and transport equipment also does which means no management plane integration. In the long term, this convergence may become a reality but now it is not. With current PTX status, ONE adapter is helpful to coordinate both management planes and, in the future, probably operators would not want to have all its equipment under the same vendor which also leaves to ONE adapter a place.

An arising question, taking these approaches as basis would be rather multi-layer management solutions should push towards integrated or coordinated approaches? To evaluate current trends and understand in which direction these solutions are pushing to is as important to the project as it may strengthen and empower design and architectural design premises. The One Adapter aims to a coordinated solution capable of suiting an evolutionary not disruptive approach for multi-layer management.

5.5 IP/WDM Integration

One of the approaches to reduce the complexity in the IP and transport world goes towards the integration of coloured transport interfaces in the IP layer routers. This integration will contribute by establishing optical paths while directly configuring these interfaces and using, in theory, the control plane to complete the network configuration.

The final objective consists in a complete multilayer integration that will allow the routers to establish through UNI interface the desired paths along the network. However, nowadays there are not completely integrated solutions, despite this, coloured transponders usage is restricted to scenarios where manually transport path establishments have to be done.

The main claimed advantages are OpEx and CapEx savings due to the transponder number reduction, space occupation and energy consumption. The QoS increase obtained due to the knowledge acquired by the router about the transport layer. Thanks to this, BER reduction will avoid the unnecessary usage of protection mechanisms.

However, the main disadvantages re the Interoperability and signal compatibility. Standardized work is needed to be done in order to assure a perfect match between coloured interfaces and transport equipment. The transport system architecture may be incompatible with power measuring and adaptation systems on transponders which can mean the impossibility of creating particular paths across the transport network.

Whether the management of a network with IP/WDM integration with coloured interfaces is simpler that today's network is still an open issue, as routers have never had to deal with transport specific issues.

5.6 The ONE Adapter in Management Functions Standardization

The ONE adapter is designed to be flexible so as to adapt to different mechanisms of interacting with a variety of external sub-systems such as IP and Transport NMS, network monitoring infrastructures etc. However, in the course of this project we will outline and provide contribution to different standardization efforts in order to improve multi-layer provisioning in general.

The primary contribution towards standardization will come towards developing ontology definitions to define semantic relationships between configuration processes on different router vendors and transport networks as well as standard management operations such as monitoring and path computation. Currently, an operation, for example, OSPF configuration on IP routers, requires different configurations on different vendors based on the IOS used and transformation of complex configurations between vendors is not trivial. By developing ontological definitions of configuration processes in IP routing, we can use the semantic relationship to translate a standard configuration definition to the corresponding router vendor with ease. If a standardized ontology definition for configuration is adopted by router vendors, it will also help in easy integration of hardware with new IOS versions, not only in the scope of the ONE adapter but in the IP management ecosystem in general.

The use of standardized ontology definition for IP configuration can also be applied in the upcoming (Software Defined Networking) SDN frameworks such as OpenFlow and Junos SDK [OFW1, JSD1]. SDN frameworks allow users to flexibly configure basic IP operations such as forwarding, lookup etc. and can be especially useful when testing or deploying new routing protocols in the IP network. However, there is no ubiquitous SDN approach which makes it difficult for integrating two SDN approaches in a multi-vendor network scenario. In case that SDN approaches follow a standardized ontology for their configuration operations, third-party systems can facilitate inter-operability in SDN approaches with ease.

Another challenge in multi-layer operations to be addressed by the ONE adapter is that of discovery and maintenance of multi-layer topology information. Standards for describing multi-layer topology are currently under development under the MTNM model supported by TM Forum [Confirm]. However, to date, these standards only address multi-layer topology in the transport ecosystem and are not equipped to support IP-over-transport topology information. In order to facilitate multi-layer operations, it is imperative to have a standardized topology description for the multi-layer network. Another important aspect here is that of multi-layer topology discovery, which is necessary to keep the topology description up-to-date. In order to have complete information of the multi-layer topology, the discovery mechanism must not only integrate discovery mechanisms in both IP and transport layers but also correlate the same using the inventory databases maintained by operators.

The work in the ONE project will build upon existing standards to develop mechanisms for multi-layer topology description and discovery and can contribute to standardization of the same in various standards bodies. The same mechanism can also be used to contribute to the standardization of the Traffic Engineering Database (TED) population and description models inside the IETF PCE working group. While the PCE has emerged as the de-facto architecture for path computation in single/multi-domain/multi-layer networks, currently there are no standardized mechanisms to describe or update the TED, especially in a multi-layer network scenario. The standardization of a mechanism to describe and update the multi-layer topology can significantly boost the standardization and adoption of the PCE architecture in a multi-layer network scenario.

Finally, the ONE adapter can contribute to the standardization for integrating systems such as AAA, SLA management and Billing in a multi-layer network scenario. With the emergence of dynamic circuit services in commercial networks, it is necessary to develop mechanisms for supporting dynamic service provisioning in multi-layer network scenarios. Service provisioning would not only include mechanisms for provisioning circuits in the network, but must also incorporate standards based mechanisms for AAA and billing. Mechanisms must also be developed to facilitate dynamic SLA negotiation in order to reduce the time required to provision a service, especially in a multi-domain network scenario. The ONE adapter approach will develop upon current control and management plane standards to incorporate these advanced features in the multi-layer network scenario and possibly extend them to the multi-domain network scenario.

6 Conclusions

IP Networks are typically managed though customized systems and individual tools. Some network management systems, like HP OpenView are highly used for provisioning IP and Ethernet services. To configure devices, CLI is still being the preferred approach, while SNMP is mainly used for alarm monitoring and configuration polling, failing to be used as a configuration protocol. NETCONF seems to be the IETF bet towards a true and standard configuration protocol. The data models are defined in Yang. However, specific data models for the technologies still need to be defined. On the other hand, transport networks, in which the transmission issue is complex, use vendor specific NMSs which provide all the management functions. MTOSI has aroused as the standard to intercommunicate network management systems, and is supported by the TMF.

Given the current level of management functions isolation between IP and transport networks and the different approach to the standardization of management protocols (NETCONF vs MTOSI), the ONE approach seems a good solution to facilitate the coordination among different NMS's on a complex layered network scenario, each interacting and communicating trough separate customizable interfaces.

7 References

[Aut02] A. Authenrieth and A. Kirstdter, “Engineering end-to-end IP resilience using resilience differentiated QoS,” IEEE Commun. Mag., pp. 50–57, January 2002.

[Bat06] Bates, T., Chen, E., and R. Chandra, BGP Route Reflection: An Alternative to full Mesh Internal BGP, RFC 4456, April 2006

[Cha04] Rayane Chahine, Optical Cost Reduction using ASON/ASTN, Optical society of America 2004.

[Cla11] Clavena, Scott, Optical Signaling System, Light Reading, Inc. January 28.

[Clemm06] A. Clemm, “Network Management Fundamentals”, Cisco Press, 2006.

[Cya11] CYAN CyMS Multi-Layer Management System: http://cyaninc.com/cyms/cyan-cyms (URL last checked on May 2011).

[Cyb11] CYAN CyMS Multi-Layer Management System: http://www.lightreading.com/document.asp?doc_id=181700 (URL last checked on May 2011).

[Ft1999] FT.COM (1999, July 10) http://www.ft.com/ftsurveys/q62ca.htm

[Gru05] C. Gruber, “A comparison of bandwidth requirements of path protection mechanisms,” ICN 2005, LNCS Springer, vol. 3420, pp. 133–143, 2005.

[HPJ11] HP Web Jetadmin: http://h20338.www2.hp.com/hpsub/cache/332262-0-0-225-121.html?jumpid=ex_r2845_go/webjetadmin/gc121306 (last checked on May 2011).

[IBM10] IBM White Papers. Reducing complexity and minimizing mistakes in network configuration. September 2010.

[JUN11] http://www-jnet.juniper.net/es/es/products-services/packet-transport/ptx-series/(last checked on May 2011).

[JuSch] http://osnove.tel.fer.hr/nastavnici/randic/oum/Seminar0809/Pages%20from%20D1%5B1%5D.3-2.pdf

[MIJ04] Mi-Jung Choi, Hyoun-Mi Choi, Hong J.W, Hong-Taek Ju. "XML-based configuration management for IP network devices". Communications Magazine IEEE, July 2004.

[Ncs02] NCS TIB 02-4, Technical information bulletin 02-4 May 2002.

[NETCONF] NETCONF and YANG Status, Tutorial, Demo , Jurgen Schonwalder,75th IETF 2009, Stockholm, 2009-07-30**[**

[NMS11] Comparison of Network Monitoring Systems http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems (URL last checked on May 2011).

[OIF2003.249] OIF Specification, “RSVP Extensions for User Network Unterface (UNI) 1.0 Signalling, Release 2”. February 2004.

[OIF2003.351] OIF Specification, “User Network Interface (UNI) 2.0 Signalling Specification: Common Part”, January 2006.

[Par05] W. Park, C. Choi, D. Kim, Y. Jeong, and K. Park, “IPTV-aware multiservice home gateway based on FTTH access network,” in International Symposium on Consumer Electronics, Jun. 2005, pp. 285–290

[Rfc3535]	http://www.ietf.org/rfc/rfc3535.txt
[Rfc3139]	http://tools.ietf.org/html/rfc3139
[Rfc6020]	http://wiki.tools.ietf.org/html/rfc6020
[Ric04]	Nathalie Rico and Omar Cherkaoui, A Policy plane for IP –Optical network, IEEE, ICCS 2004
[Ros06]	Rosen, E. And Y. Rekhter, BGP/MPLS IP Virtual Private Networks, RFC4364, February 2006
[Rue02]	S. Ruepp, N. Andriolli, J. Buron, L. Dittmann, and L. Ellegard, "Restoration in all-optical GMPLS networks with limited wavelength conversion," Computer Networks Special Issue on Opportunities and Challenges in Optical Networks, 2008.
[SNT07]	http://searchnetworking.techtarget.com/review/OpenNMS-2007 (URL last checked on May 2011).
[Sub10]	M. Subramanian, T. A. Gonsalves and N. U Rani, "Network Management: Principles and Practice", Pearson Education India, 2010
[Vas04]	J.-P. Vasseur, M. Pickavet, and P. Demeester, Network Recovery, Protection and Restoration of Optical, SONET-SDH, IP, and MPLS. Morgan-Kaufmann Publishers, Elsevier, 2004, ISBN: 0-12-715051-x.
[Wan02]	J. Wang, L. Sahasrabuddhe, and B. Mukherjee, "Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: Performance comparisons using GMPLS control signaling," IEEE Commun.Mag., vol. 40, no. 11, pp. 80–87, Nov. 2002.
[YuAja]	An Empirical Study of the NETCONF Protocol James Yu, and Imad Al Ajarmeh DePaul University, Chicago, IL, USA

8 Acronyms

[ASON]	Automated Switched Optical Network
[BGP]	Border Gateway Protocol
[BPSR]	Bidirectional Path Switching Ring
[CLI]	Command-line interface
[CMIP]	Common Management Information Protocol
[CyMS]	Cyan's Multi-layer Management System
[DWDM]	Dense Wavelength Division Multiplexing
[E-NNI]	External Network-Network Interface
[GMPLS]	Generalized Multiprotocol Label Switching
[GUI]	Graphic User Interface
[I-NNI]	Internal Network-Network Interface
[IP]	Internet Protocol
[IP NMS]	Internet Protocol Network Management System
[LLA]	Logical Layered Architecture
[MPLS]	Multiprotocol Label Switching
[MSP]	Multiplex Section Protection
[MTOSI]	Multi-Technology Operations System Interface
[NETCONF]	Network Configuration Protocol
[NMS]	Network Management System
[OAMP]	Operation Administration Maintenance and Provisioning
[OSI]	Open System Interconnection
[OTN]	Optical Transport Network
[OV-NNM]	OpenView Network Node Manager
[PCE]	Path Computation Element
[PMD]	Polarization Mode Dispersion
[SDH]	Synchronous Digital Hierarchy
[SLA]	Service Level Agreement
[SML]	Service Management Layer
[SNCP]	Sub-network Section Protection
[SNMP]	Simple Network Management Protocol
[TED]	Traffic Engineering Database
[TMN]	Telecommunications Management Network
[UNI]	User Network Interface
[UPSR]	Unidirectional Path Switching Ring

Management Protocols

A.1 SNMP

A.1.1 Commands

The SNMP protocol operations are the following:

- Configuration: Set
- Data Gathering: Get, Get Next, Get Bulk
- Notify Operations: Trap, Inform.

A.2 NETCONF

A.2.1 Commands

The operations that are defined yet are the following.

OPERATION	DETAILS
get-config(source, filter)	Retrieve a (filtered subset of a) configuration from the configuration datastore source.
edit-config(target, default-operation,test-option, error-option, config)	Edit the target configuration datastore by merging, replacing, creating, or deleting new config elements.
copy-config(target, source)	Copy the content of the configuration

	datastore source to the configuration datastore target.
delete-config(target)	Delete the named configuration datastore target.
lock(target)	Lock the configuration datastore target.
unlock(target) **get(filter)**	Unlock the configuration datastore target. Retrieve (a filtered subset of a) the running configuration and device state information.
close-session()	Gracefully close the current session.
kill-session(session)	Force the termination of the session session.
commit()	Commit candidate configuration datastore to the running configuration (#candidate capability).
discard-changes()	Revert the candidate configuration datastore to the running configuration (#candidate capability).
validate(source)	Validate the contents of the configuration datastore source (#validate capability)
create-subscription(stream, filter, start, stop)	Subscribe to a notification stream with a given filter and the start and stop times.

Figure 11. NETCONF Operations

A.3 YANG

YANG file example [RFC6020]

```
// Contents of "acme-system.yang"

module acme-system{
```

```
        namespace "http://acme.example.com/system";
        prefix "acme";
        organization "ACME Inc.";
        contact "joe@acme.example.com";
        description "The module for entities implementing the ACME system.";
        revision 2007-06-09 {
                description "Initial revision.";
        }
        container system {
                leaf host-name {
                        type string;
                        description "Hostname for this system";
                }
                leaf-list domain-search {
                        type string;
                        description "List of domain names to search";
                }
                container login {
                        leaf message {
                                type string;
                                description "Message given at start of login session";
                        }
                        list user {
                                key "name";
                                leaf name {
                                        type string;
                                }
                                leaf full-name {
                                        type string;
                                }
                                leaf class {
                                        type string;
                                }
                        }
                }
        }
}
```