Development of Alarm Management Tool for an Enterprise Optical Network Element

Ajay Kumar.V[1], M B Kamakshi[2], Venkatesha B V[3]

Abstract— **Network Management and Security has become a very sensitive and important topic for manufacturers and network operators. In optical networks, Alarm management deals with detection and isolation of faults based on the alarms received from the network elements. This paper describes the development of a Alarm management tool for an enterprise optical node managed by an enterprise network management system. The tool is implemented in order to reduce the manual effort in validating the alarms. Description of the same is presented. For any network management system, FCAPS is the term used to represent its functionalities like Fault, Configuration, Accounting, Performance and Security management. Alarm management aspect for an enterprise optical node is being presented in this paper.**

Index Terms— FCAPS - Fault Configuration Accounting Performance Security, NMS - Network Management System. PSS - Photonic Service Switch, SAM - Service Aware Manager, DWDM - Dense Wavelength Division Multiplexing, Alarm Management, SNMP - Simple Network Management Protocol, UDP - User Datagram protocol, Traps, Wireshark, Optical Networks, Network element, OSSI- Operations Support Systems Interface, SSH-Secure Shell, FMDH - Fault Management Defect Handler, ODU-Optical Data Unit, DCM-Dispersion Compensation Management

1 INTRODUCTION

The Internet is growing faster than ever, with traffic across the core of the network quadrupling every year. This tremendous growth in traffic demands is fueled by many factors. The explosive growth of web-related services over the Internet has resulted in millions of users using online, thus causing an explosive growth in the demand for bandwidth. Different applications ranging from multimedia transmissions, video-conferencing, online applications are being used. To fuel this ever-increasing demands of bandwidth, new technologies emerged in the form of Optical Networks.

Today's Optical Networks are capable of carrying large amounts of data. Commercial systems have been deployed with a fiber capacity of several Tera bits per second, which is equivalent to millions of simultaneous telephone conversations. As optical network technology advances and higher bandwidth is demanded, the amount of data transmitted over a single optical fiber is expected to increase further. Due to such high data rates, even a short service disruption may cause large amounts of data to be affected. Many different types of service disruptions occur frequently in practice. They include bending and cutting of fiber, loss of signal, equipment failure, and human error. Besides Alarms, optical networks are vulnerable to sophisticated attacks that are not possible in electronic networks. Therefore, it is of critical importance for such networks to have fast and effective methods or tools for identifying and locating network failures. This is especially important for the physical layer, where any physical failure should be detected, located and corrected before it is noticed by the upper layer protocols.

In optical networks, the physical layer generally consists of several basic network components. Optical components are passive or active. Passive optical components do not have monitoring equipment capable of detecting and reporting alarms. Active optical components have monitoring equipment and therefore are capable of reporting alarms to the network management system or network manager.

Network Control and Management related functions can be described and classified using the OSI management framework, which defines five functional areas.

- Fault Management is responsible for fault detection, root cause analysis, fault isolation, fault correction, and alarm/notification.
- Configuration Management is responsible for maintaining an accurate inventory of resources including hardware, software, and circuits within the network, and with the ability to change/control the inventory in a reliable and effective manner.
- Accouting Management is responsible for identifying costs assosciated with network communication resources and establishing charges for the use of resources and services.
- Performance Management is responsible for evaluating and analysing the effectiveness and efficiency of network resources and related communication activities.

- Security Management is responsible for network and system security management.

Fault detection in optical networks depends on alarms/traps generated by different types of network monitoring equipment in response to unexpected events. Depending on the placement and capabilities of the monitoring devices, the network Alarm manager or a network management system may receive a large number of redundant alarms for some network failures, while it may not receive any alarms for other network failures. In order for Alarm detection and localization mechanism to be fast and effective, it is important to reduce the number of redundant alarms. This will reduce the alarm processing time as well as ambiguity in Alarm localization.

Optical networks and all networks, in general need a Alarm management system or tool that is able to identify the Alarms that occur from the information given by the network elements. A Fault is defined as the accidental interruption of the ideal functioning of the network due to tiredness of the components. Faults produce signal degradation or complete signal interruption. The former are called *soft faults*, and the latter are called *hard faults.*

Section II deals with the introduction of the Alcatel-Lucent developed enterprise-specific optical node called Photonic Service Switch (PSS) and the enterprise-specific Network Management System called Service Aware Manager (SAM). Section III deals with the implementation procedure for Alarm management. Section IV shows the snapshots of the validated results obtained for one card supported by PSS and also the corresponding traces of traps using a network monitoring tool, Wireshark. Section V gives conclusion. The terms SAM and NMS, PSS and optical node, faults, alarms and traps, are used interchangeably.

2 . Photonic Service Switch (PSS) and Service Aware Manager (SAM).

2.1 Photonic Service Switch

The Alcatel-Lucent 1830 Photonic Service Switch (PSS) represents a new breed of photonic switch for next generation access, metro and long-haul wavelength division multiplexing (WDM). It is a multi-reach platform that spans access, metro, regional and long-haul applications and supports a wide range of data rates, enabling service delivery in a variety of environments and applications. It is used in broadband transport networks for telecommunication operators and enterprises as Telco's to provide high-bandwidth connectivity over distances up to 4000km. It also supports for the full range of network topologies, including ring, point-to-point and optical mesh topologies. Fig.1 shows the schematic of a PSS node managed by the SAM.

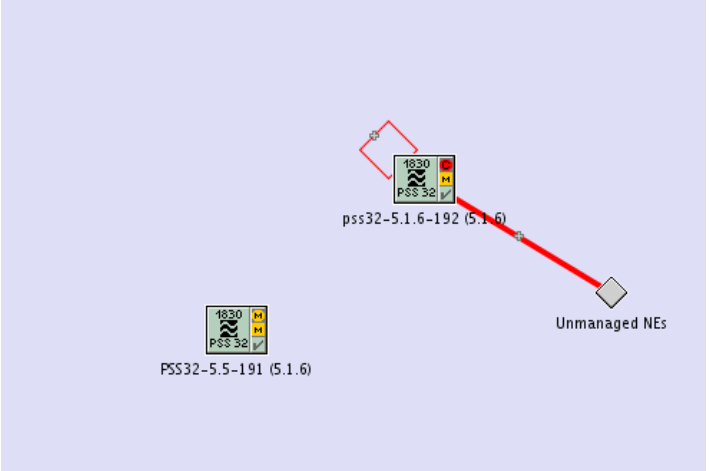

Fig.1 Graphical Representation of PSS node (simulator node)

Key Features of PSS (Optical Network Element)

- A static, tunable/reconfigurable optical add/drop multiplexer (T/ROADM) with single wavelength add/drop granularity
- Supports WDM functionality
- Colorless and any direction add/drop capabilities
- Up to 88 wavelengths and 50GHz ITU WDM per fiber
- ODU1, ODU2, ODU3 and ODU4 interfaces according to the G.709 standard
- 100 Gb/s and 40 Gb/s channel capacity, with best-in class
- Wavelength Tracker technology enables end-to-end power control, monitoring, tracing and fault localization for each individual wavelength channel
- Supporting for various cards according to the service required, i.e.., Optical Transponder Cards, Filter Cards, and Amplifier Cards.

2.2 Service Aware Manager

The Service Aware Manager (SAM) is a network management application which is designed using industry standards like Java framework, multi-tier layering, and web service, standard interfaces. The use of the industry standard interfaces allows the SAM to interoperate with other network systems. Fig.2 shows the user interface of SAM.

i) Key Features of SAM (NMS)

- Use of open standards that promote interoperation with other systems
- Distributed server processing

- Using muti-tier model that groups functions in separate, well-defined elements
- Creation of web services
- Component Redundancy
- Uses the underlying protocol as SNMP

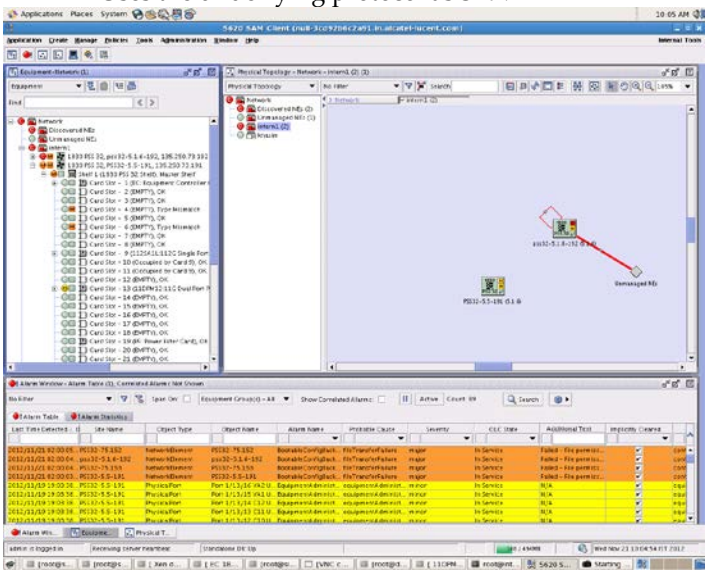

Fig.2 SAM GUI showing Alarms window and topology

ii) Key Components of SAM

- The server is a Java-based network-management processing engine
- The Database is Oracle relational database that provides persistent storage
- Java based GUI clients which provide a graphical interface for the network operators.

iii) Network Management Capabilities of SAM

- Alarm correlation up to the service level.
- service and routing provisioning
- inventory reporting at the equipment
- network performance and account data collection

3 Implementation of Alarm Management Tool.

As mentioned in the previous sections, Service Aware Manager is an NMS which manages the Photonic Service Switch, which is an optical network element. Fig.3 shows the flow in implementation of Alarm management tool for PSS managed by SAM. In Fig.3, the major elements are PSS, SAM and an OSSI, which is Alcatel-Lucent specific coding methodology. Initially, dump of Alarms supported by a card is taken from the node (PSS) by logging into the node through SSH protocol. The lists of alarms are raised on the node with the help of a binary tool, supported by the node. Since the node is managed by the SAM (NMS), all alarms raised on the node are reported to the NMS. The underlying protocol for communication between the Node and the NMS is SNMP. The alarms seen by thee NMS are extracted using the XML API client and are compared with the node alarm parameters. If the both alarm specifics match, them they are validated as Passed, else they are validated as Failed. The binary tool supported by the node is called FMDH, which stands for Fault Management Defect Handler. The tool developed has both the Frontend and Backend. Frontend includes a graphical user interface for selection of a particular card at a particular slot. Backend includes the coding in extracting all the alarms supported by the node.

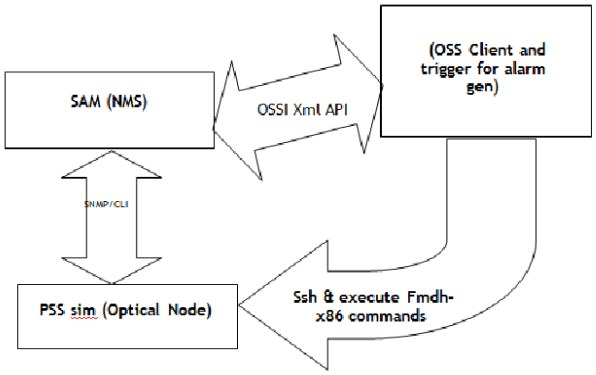

Fig.3 Method implemented in developing the alarm management tool

3.1 Back End Implementation Procedure

- A particular card supported by the node is chosen for alarms validation
- That particular card is to be configured on the node
- The dump of the alarms supported by the node are extracted by logging into the node through Secure Shell Protocol.
- The alarms need to be syntactically arranged for execution on the node, using the binary tool supported on the node.

Fig.4 shows the developed GUI, which gives options for validating a card.

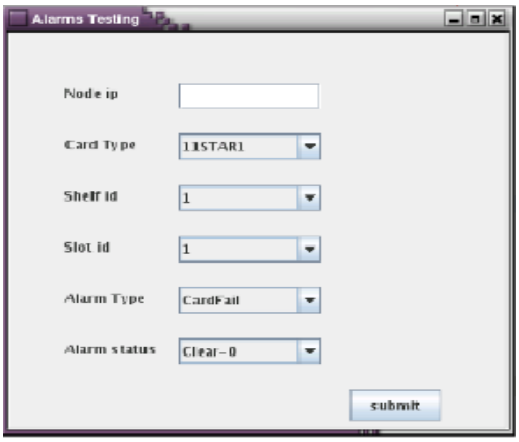

Fig.4 Developed GUI showing various fields on the Frontend

3.2 Front End Implementation Procedure

- On the frontend, which is implemented using Java, a particular card supported by the optical node can be chosen
- The front end also provides options to choose particular slot and shelf on which the card is configured
- Node IP address is also an input provided

4 Results and Discussion

As mentioned in the Section III, one particular card A2325A, supported by the node is chosen, which is an Amplifier Card, and its validated results are given in below figures. The characteristics of the card are as mentioned below.

Optical Amplification function is performed via multistage EDFA amplifiers, most with mid-stage DCM access. These amplifiers are implemented as integrated variable gain optical amplifier modules which include fast feedback for transient control. It provides a maximum gain of 25dB. Fig.5 shows the validated test results for the A2325A card.

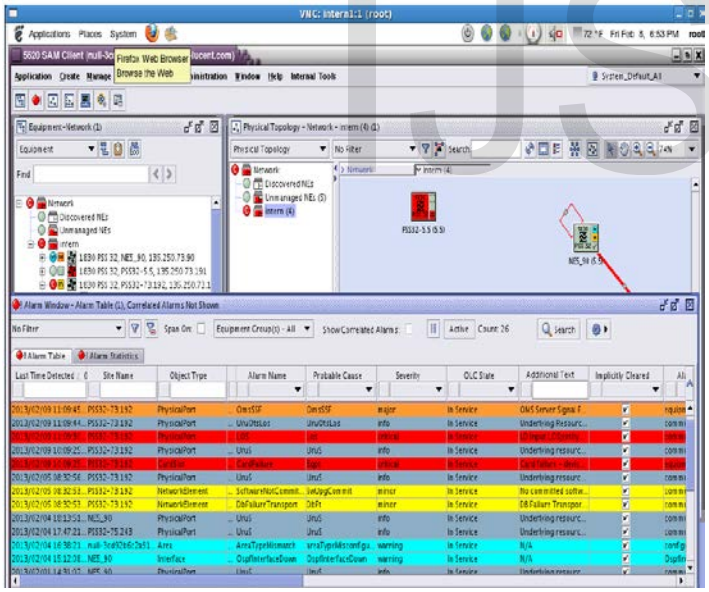

Fig.5 SAM GUI showing alarms captured for the A2325A card

Since the underlying protocol for communication between the node and the NMS is SNMP in this case, the alarms can also be referred to as traps. Fig.6 shows the recorded traps using Wireshark, which is a network monitoring tool, generated as part of tool's execution for mentioned card. The figure gives an insight of various attributes related to traps, like source from where the trap is generated, destination of the trap, underlying protocol, timestamp etc. Fig.7 shows the packet format for one particular alarm/trap, where in layer 2, layer 3, layer 4 and layer 7 information is recorded using the Wireshark tool. Fig.7 shows the layer 7 information, i.e., SNMP related information, which is of importance in this context.

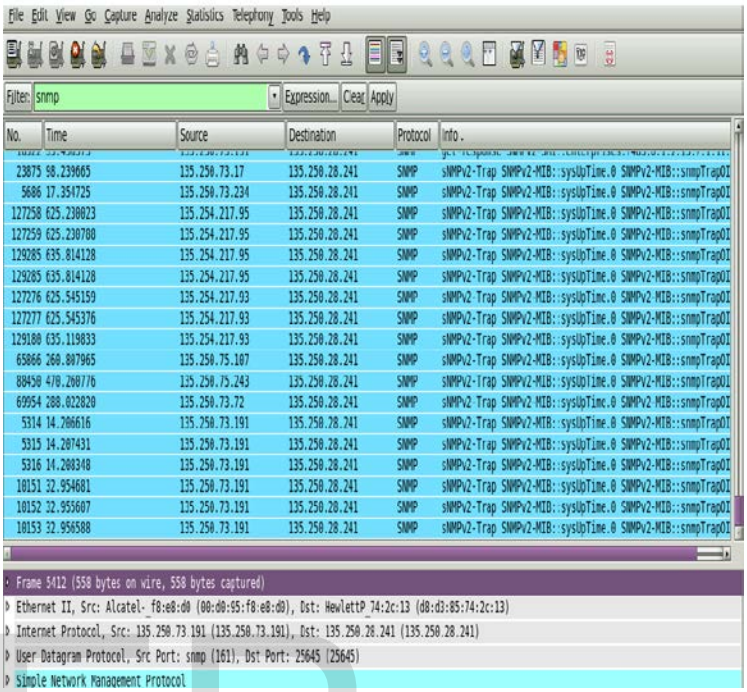

Fig.6 Screenshot of Alarms/Traps recorded from the tool using wireshark

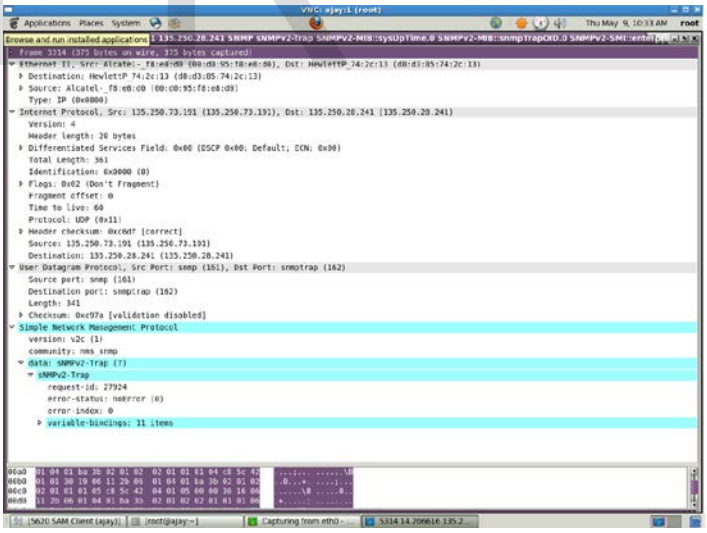

Fig.7 Screenshot of packets information recorded using wireshark

Fig. 8 shows thes user interface of wireshark network monitoring tool. Fig. 9 shows the SNMP traps traffic monitored as a part of tool's execution for the amplifier card. The blue graph in Fig.9 shows the UDP Traffic and red graph shows the SNMP Traffic. The peaks in the graphs shows the traps.

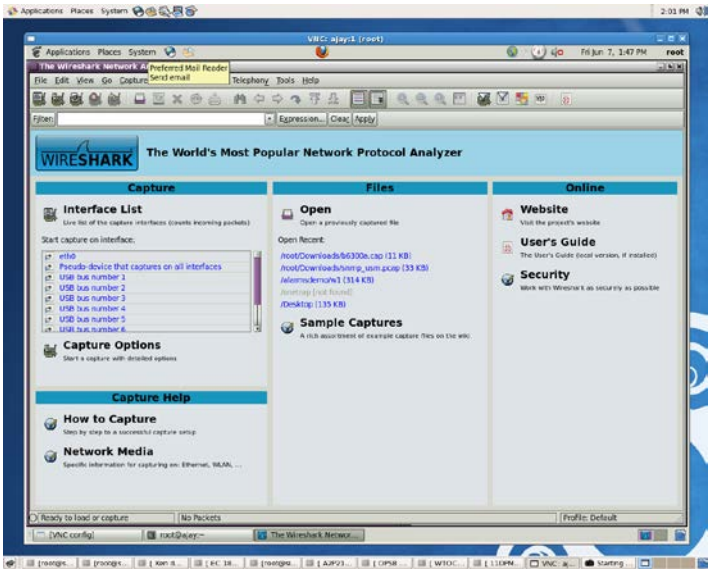

Fig.8 User Interface of wireshark

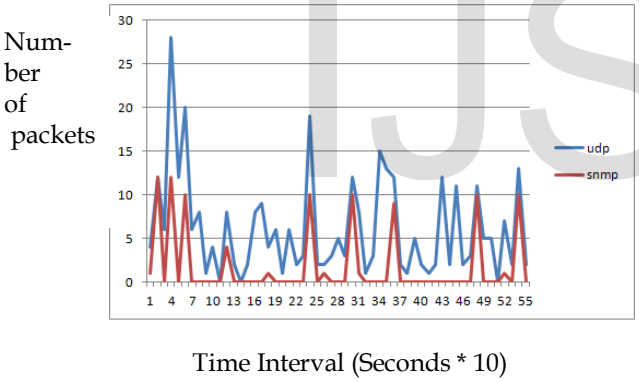

Fig.9 Graph showing the SNMP and UDP traffic

5. Conclusion

The tool discussed reduces the manual effort in validating individual alarm at a time, which is an inefficient procedure for validation. It provides for validating bulk or total number of alarms of a card, supported by the optical node. The front end developed, i.e., the user interface provides the flexibility and granularity in choosing a particular card, particular shelf and slolt etc., for the validation of the alarms.

REFERENCES

1] Ma-kun Guo, Yi-min Wang Qi Yu, "Research and Implementation of Network Management System Based on XML View", International Conference on Logistics Engineering and Intelligent Transportation Systems (LEITS), 2010, Page(s): 1 - 4

[2] Stanic, Subramaniam, S.Sahin, G.Choi, H.Choi, "Active monitoring and alarm management for Alarm localization in transparent all-optical networks", IEEE Transactions on Network and Service Man -agement, 2010, Volume: 7, Issue: 2, Page(s): 118 - 131

[3] Wang Haitao, Chang Chun Qin, "Network management system based on Java technology", 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, Page(s): V1-685 - V1-688

[4] Xiaolin Lu, "An Architecture for Web Based and Distributed Telecommunication Network Management System", 22 Nov. 2009, Third International Symposium on Intelligent Information Technology Application, 2009. IITA 2009, Volume: 1, Page(s): 152 - 155

[5] Ismail, M.N, "Network Management System Framework and Development", International Conference on Future Computer and Communication, ICFCC 2009, 3-5 April 2009, Page(s): 450 - 454

[6] Stanic, S. Subramaniam, "Distributed Hierarchical Monitoring and Alarm Management in Transparent Optical Networks", IEEE Interna -tional Conference on Communications, 2008, Page(s): 5281 - 5285

[7] Stanic Sava,Sahin, Gokhan, Hongsik Choi, Subramaniam, Suresh Hyeong-Ah Choi, "Monitoring and alarm management in transparent optical networks". Fourth International Conference on Broadband Communications, Networks and Systems, 2007, Page(s): 828 - 836

[8] Alcatel-Lucent Reference guides and Data sheets

[9] www.snmp.org

[10] www.wiresshark.org

AUTHORS

First Author – Ajay Kumar .V, M.Tech, R.V. College of Engineering, Bangalore, vajaykumar403@gmail.com.

Second Author – M B Kamakshi, Assistant Professor, R. V. College of Engineering, Bangalore, kamakshimb@rvce.edu.in.

Third Author – Venkatesha B V, Technical Manager, Alcatel-Lucent, Bangalore, venki.bv@alcatel-lucent.com