

Reusable NM Components

1.0 EXECUTIVE SUMMARY

Every equipment manufacturer requires a solution for the element management of the equipment. Traditionally, an EMS is built custom to the requirements of the network elements that it has to manage. When the equipment manufacturer builds a new product line or upgrades the existing one, the cost to port / re-engineer the existing EMS becomes a major hurdle for the change.

Reusable NM Components (RNMC) provides an easy solution to this problem. RNMC is based on basic understanding that each EMS has few generic needs along with specific requirements of network elements. These generic needs are; management protocol based messaging, handling alarms and events, logging and tracing, persistence, access-controlled GUI, and maintaining audit logs. Whereas specific needs are based on custom GUI for provisioning and statistics monitoring.

RNMC provides a set of reusable components that support these generic needs and are extensible enough to plug-in specific behaviour into them.

CONTENTS		
<u>SECTION</u>		<u>PAGE</u>
1.0	EXECUTIVE SUMMARY	1
2.0	BUSINESS CHALLENGES	1
3.0	RNMC SOLUTION	2
3.1	BENEFITS	3
3.2	FAULT MANAGEMENT	3
3.3	CONFIGURATION MANAGEMENT	4
3.4	PERFORMANCE MANAGEMENT	4
3.5	SECURITY MANAGEMENT	4
4.0	REFERENCES	5

2.0 BUSINESS CHALLENGES

The emerging technologies are resulting in the expansion of the telecom network at a fast pace. This expansion calls for a significant effort to provision, manage and monitor this network. There is always a challenge to maintain this network so as to provide uninterrupted services to the end user and stay ahead in the competition.

NMS, EMS and OSS provide the answer to these goals. But there are numerous challenges faced in the development of these solutions. Some of the challenges are:

- How to make these systems extensible so that they can be customized to cater to the need of the network expansions involving multi-technology and multi-vendor systems?
- How to make the seamless integrations of these systems with the emerging network and other existing OSS systems?
- All of the Telecom Service Providers are having some NM solution to manage their existing networks. And whenever there is a new product line in their network they need to enhance their existing NM solutions. So, which standard approach and specifications to follow to develop these systems such that if needed the components of the systems are reusable and in a short time, with a minimalist effort and inexpensive way they are ready to support multi-technology systems?

3.0 RNMC SOLUTION

Building an NM solution from scratch requires a lot of effort and basic modules present in common software applications. Moreover, the turn around time to build such a system is large and is bound to result in a loss of the prospective business for the customer.

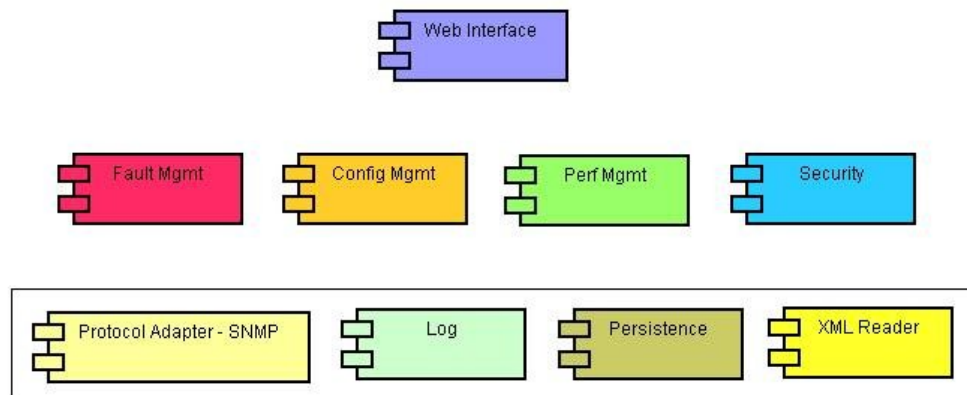


Figure 1: Reusable NM Components

The RNMC aims at providing the common components those are required to build any software application and the basic components of an NM system by strategically selecting the freeware (those are best-in-industry third party products) and building components on the top of it. Its support for Fault, Configuration, Performance and Security Management is geared to a high degree of customization and extension with minimal coding. This enables the use of the developed components to build an NM solution with FCAPS capabilities in a quick and inexpensive way.

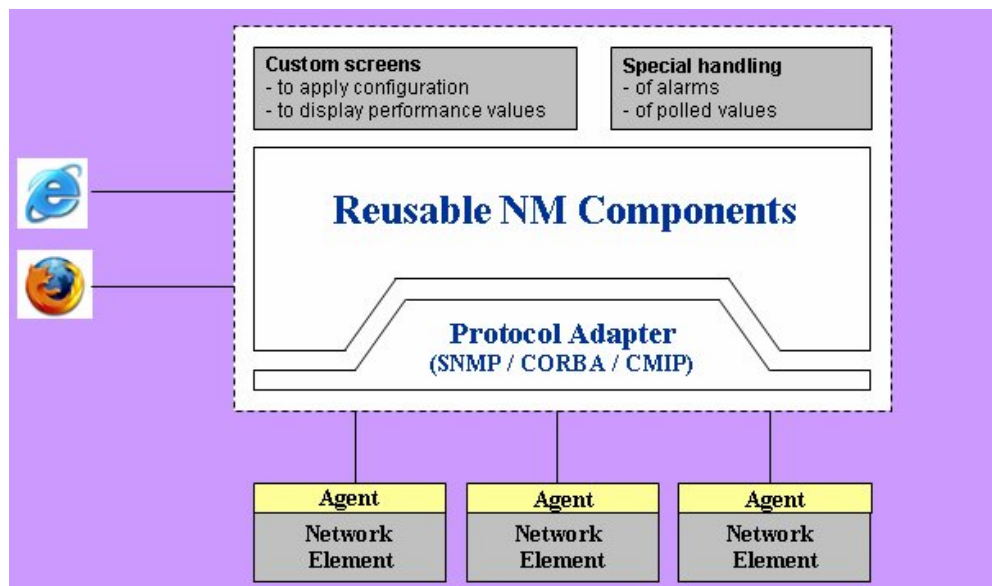


Figure 2: The big picture

In order to build a new EMS using RNMC, first an appropriate protocol adapter needs to be plugged into the components. Then few custom handlers are prepared to address specific requirements of a network. These custom handlers are plugged into the predefined hooks of RNMC, through XML files. (This is facilitated by Java reflections). Then custom screens are built for configuration & performance parameters for the network elements, and are plugged into the CM & PM components. This builds the complete EMS. RNMC facilitates a web-based interface for operators.

3.1 Benefits

Modular Design

All the best-in-practice Object Oriented Design principles and it is ensured that there is a loose coupling in the architecture layers. Thus, the developed independent client and server modules ensure that selective module can be deployed those are required in a specific NM implementation.

Platform Independent

The components have been developed using Java technologies which ensure that it runs on multiple platforms.

Multiple Database and ORM tools Support

Default Hibernate template support from Spring framework is used as an ORM interface for implementing the data access object layer ensuring that it is compatible with any RDBMS. Default Hibernate support can be replaced by any other template implementation by plugging it in Spring framework.

Customizable and Extensible

RNMC is capable to meet the requirements of any NM implementation with the support of its highly customizable and extensible features. The components are customizable using XML based configuration files. Extensions are possible as the plug-in feature for customizable hooks is also provided, i.e., if an application requires to deviate from or enhance the feature provided it can be achieved with a minimal code effort by using the Java API provided and an XML configuration for the same.

Interface for supporting multiple protocols

RNMC Protocol Adaptation Layer encapsulates all the protocol specific implementation and ensures support to any of SNMP, TL1, CLI, CMIP or CORBA protocols thus enabling the management of multi-technology and multi-vendor systems. Presently, it supports SNMP v1, v2c traps and notifications.

Client Interface

A support for HTTP based web client is provided. The latest MVC framework Struts2 has been exploited to develop this web client. HTTPS access to the application via the web client is also supported. But interface between frontend & backend components is very loosely coupled and the frontend developed using any other technology can also be plugged with the existing backend components.

3.2 Fault Management

This component is responsible for receiving the events and alarms from the managed network, logging them in the persistent storage and reporting them in a presentable format to the NOC operators.

Key features of Fault Management are:

- The alarms/events conform to the ITU-T X.733 Alarm Reporting specification.
- Highly scalable design is adaptable to handle high alarm rate scenarios.
- Provision to suppress unwanted events, enriching them with useful information.
- Support of the operator initiated actions on these events is provided.
- Configuring multiple event listeners on either criteria i.e., for the same protocol events/alarms multiple event listeners could be opened and also for different protocol events/alarms multiple event listeners could be opened.
- Configuring multiple event handlers those shall assist the specific implementation requirement while processing an event/alarm.
- Presenting the active/historical alarms and events on a web based GUI. The present implementation exploits the displayTag library to display the alarms in tabular format. Also, the support for pagination, sorting and filtering of alarms is supported. Filtering is supported on each and every displayed attribute of the alarm/event.

Business benefits those can be realized by Fault Management are:

- Real Time monitoring of alarms/events occurring in the network.

- Reduce the downtime of the network by taking appropriate actions on the reported alarms, thus preventing the service degradation and increasing the customer satisfaction.
- Analyzing the alarms/events reported and maintaining the notes added to the alarms/events. This helps in isolating the faults quickly and efficiently.
- Proactively working on the service affecting conditions and increasing the reliability of the managed network.

3.3 Configuration Management

This component is responsible for provisioning of network elements. It takes values for configurable parameters, stores it in local database, and applies them on the network element.

Key features of Configuration Management are:

- Maintaining values in the local persistent storage
- Applying scalar as well as tabular values
- Applying data in multiple datasets, if there is constraint on packet size in the network

Business benefits those can be realized by Configuration Management are:

- Provides a generic mechanism for Configuration Management irrespective to the data model specific to the managed network elements
- Facilitates extensibility of configuration management in the EMS

3.4 Performance Management

This component is responsible for providing the Authorization, Authentication and Auditing functions.

Key features of Performance Management are:

- Fetching scalar as well as tabular values
- Managing transactions in case dataset is big enough for a single network packet
- Periodically polling values from various managed network elements.

Business benefits those can be realized by Performance Management are:

- Provides a generic mechanism for Configuration Management irrespective to the data model specific to the managed network elements
- Facilitates extensibility of performance management in the EMS

3.5 Security Management

This component is responsible for providing the Authorization, Authentication and Auditing functions.

Key features of Security Management are:

- Role Management function that enables creation, modification, display and deletion of Access Based Roles in EMS.
- User management function that enables creation, modification, deletion of users and grouping of users into Access Based Roles created in EMS.
- Session management function that enables to determine the list of active user session details those are accessing the NM application and an access control based support to delete them.
- User login authentication.
- Role-based authentication on every user request.
- Audit Management function to track the operations performed by various users.
- SSL support provided to access the application via the web client.
- By XML configuration additional features being developed on the top of the components can also be ensured for authorized accesses.

Business benefits those can be realized by Security Management are:

- Access control based mechanism prevents the NM application from unauthorized accesses.
- Provision of security for all the management functions supported by the NM application.
- Enables to provide the users secured access to restricted functions of the application on the basis of domain expertise.
- No extra effort or time required to provide authorized accesses to the additional features being developed on the top of the framework.

4.0 REFERENCES

1. ITU-T M.3010 (TMN Architecture)
2. ITU-T X.733

PROPRIETARY NOTICE

All rights reserved. This publication and its contents are proprietary to Hughes Systique Corporation. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Systique Corporation, 15245 Shady Grove Road, Suite 330, Rockville, MD 20850.

Copyright © 2006 Hughes Systique Corporation

CONTACT INFORMATION:

Phone: +1.301.527.1629

Fax: +1.301.527.1690

email: whitepaper@hsc.com

Web: www.hsc.com

APPENDIX A ABOUT HUGHES SYSTIQUE CORPORATION

HUGHES Systique Corporation (HSC), part of the HUGHES group of companies, is a leading Consulting and Software company focused on Communications and Automotive Telematics. HSC is headquartered in Rockville, Maryland USA with its development centre in Gurgaon, India.

SERVICES OFFERED:

Technology Consulting & Architecture: Leverage extensive knowledge and experience of our domain experts to define product requirements, validate technology plans, and provide network level consulting services and deployment of several successful products from conceptualization to market delivery.

Development & Maintenance Services: We can help you design, develop and maintain software for diverse areas in the communication industry. We have a well-defined software development process, comprising of complete SDLC from requirement analysis to the deployment and post production support.

Testing : We have extensive experience in testing methodologies and processes and offer Performance testing (with bench marking metrics), Protocol testing, Conformance testing, Stress testing, White-box and black-box testing, Regression testing and Interoperability testing to our clients

System Integration : As system integrators of choice HSC works with global names to architect, integrate, deploy and manage their suite of OSS, BSS, VAS and IN in wireless (VoIP & IMS), wireline and hybrid networks.: NMS, Service Management & Provisioning .

DOMAIN EXPERTISE:

Terminals

- Terminal Platforms : iPhone, Android, Symbian, Windows CE/Mobile, BREW, PalmOS
- Middleware Experience & Applications : J2ME , IMS Client & OMA PoC,

Access

- Wired Access : PON & DSL, IP-DSLAM,
- Wireless Access : WLAN/WiMAX / LTE, UMTS, 2.5G, 2G ,Satellite Communication

Core Network

- IMS/3GPP , IPTV , SBC, Interworking , Switching solutions, VoIP

Applications

- Technologies : C, Java/J2ME, C++, Flash/lite, SIP, Presence, Location, AJAX/Mash
- Middleware: GlassFish, BEA, JBOSS, WebSphere, Tomcat, Apache etc.

Management & Back Office:

- Billing & OSS , Knowledge of COTS products , Mediation, CRM
- Network Management : NM Protocols, Java technologies,, Knowledge of COTS NM products, FCAPS, Security & Authentication

Platforms

- Embedded: Design, Development and Porting - RTOS, Device Drivers, Communications / Switching devices, Infrastructure components. Usage and Understanding of Debugging tools.
- FPGA & DSP : Design, System Prototyping. Re-engineering, System Verification, Testing

Automotive Telematics

- In Car unit (ECU) software design with CAN B & CAN C
- Telematics Network Design (CDMA, GSM, GPRS/UMTS)

BENEFITS:

- **Reduced Time to market :** Complement your existing skills, Experience in development-to-deployment in complex communication systems, with key resources available at all times
- **Stretch your R&D dollars :** Best Shore" strategy to outsourcing, World class processes, Insulate from resource fluctuations