CASE STUDY – PART I

Self-diagnosis and self-healing for IMS VoIP and VPN services

Abstract

This document presents a high level description of the UNIVERSELF project case study on Self-diagnosis and self-healing for IMS VoIP and VPN services, its methods, concepts and expected innovation. The specific functional, non-functional requirements and the associated problems of this case were presented in the deliverable D4.1 [3]. The prioritization of the problems and functional requirements were presented in deliverable D4.2 [4].

This case study considers self-diagnosis and self-healing features with two mains applications for a same network topology: Self-diagnosis and healing of IP networks and IMS services [5][6] and Self-diagnosis and healing of VPN networks [7].

Objectives are to enable proactive and improved reactive diagnosis and healing. Proactive diagnosis is important to prevent incident impact and it is not done today. An improved reactive diagnosis reduces the delay between incident, its detection and reparation. Then it improves customer experience.

Self-diagnosis and Self-healing must be based on reusable and flexible components to prevent the redesign from scratch of the process for new services or changes in network configuration.

Then Self-diagnosis and Self-healing must support an end to end service view facing multiple network domains and technologies which are currently managed by dedicated teams with dedicated & ossified tools. This end-to-end view is tightly related to the end-user service self-diagnosis and healing.

Date of release

17/09/2012

SEVENTH FRAMEWORK PROGRAMME

FUTURE NETWORKS

CONTENT

STORY LINE

The proliferation of networks and services (heterogeneity of networks and increasing number of services, vulnerabilities) highlights the crucial role of assurance processes. Fault and Performance Management are critical functions towards ensuring the quality of the provisioned services or network capabilities, especially in an end-to-end way. It is tightly related to the planning and configuration phases, especially when dealing with the dependencies between network element configuration and service requirements.

Present Operation Administration and Maintenance (OAM) /Operation Support System (OSS) management ecosystem (see Figure 1) is suffering from technology and vendor heterogeneity: multiple interfaces, multiple information models. Depending on the network domain and/or vendor, the management tools/interfaces/models are not the same. End to end view is enabled at the OSS level, which needs to be adapted to all vendor/technology particularities implying delays for fault or performance issue detection and mitigation. Present management is a reactive one: Following customer complaint or/and alarms, operator is then handling the problem with lot of ossified tools, isolated and dedicated teams. Operational teams are overwhelmed by the amount of data to analyse and to correlate. It implies lot of customer care, IS and human effort. The goal is to improve reactive management by reducing the delay between incident occurrence and detection reparation delay, and to enable a proactive management to prevent incident impact. It is also to enable micro-granularity management when necessary to focus on end-user issue diagnosis, facing high amount of data.

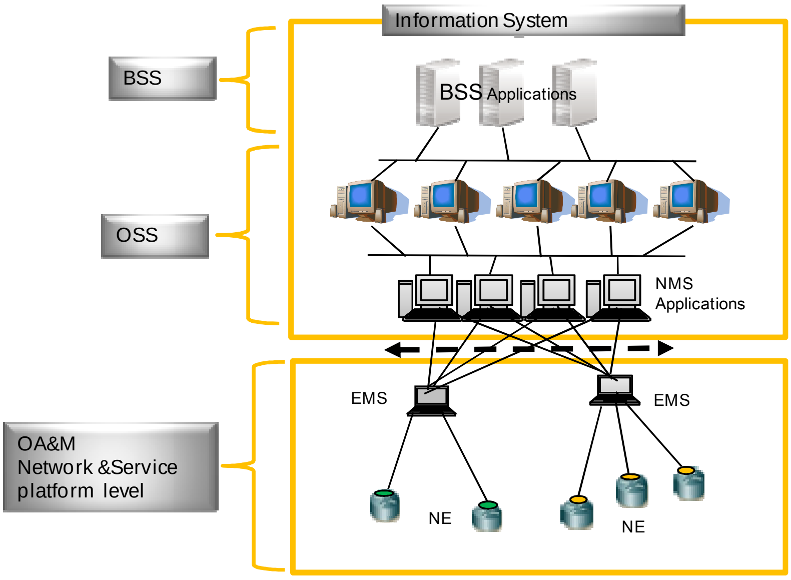

Figure 1: Example of OAM/OSS/BSS ecosystem

Objectives

This case study considers Self-diagnosis and Healing features with two mains applications for a same network topology:

- Self-diagnosis and healing of IP networks and IMS services.
- Self-diagnosis and healing of VPN networks.

Objectives are to enable proactive and improved reactive diagnosis and healing capturing the following properties:

- Proactive: to prevent incident impact (not done today).
- Improved reactive: to reduce the delay between incident, detection and reparation and then improving the customer experience.
- Reusable and flexible: to prevent the redesign of the process from scratch for new services or change in the network configuration.

- End-to-end: to face multiple network domains and technologies, which are currently managed by dedicated teams with dedicated & ossified tools, and to enable an end user diagnosis and healing.

Phases

This case study concerns Fault and Performance management processes (Operations, Assurance, see Figure 2).

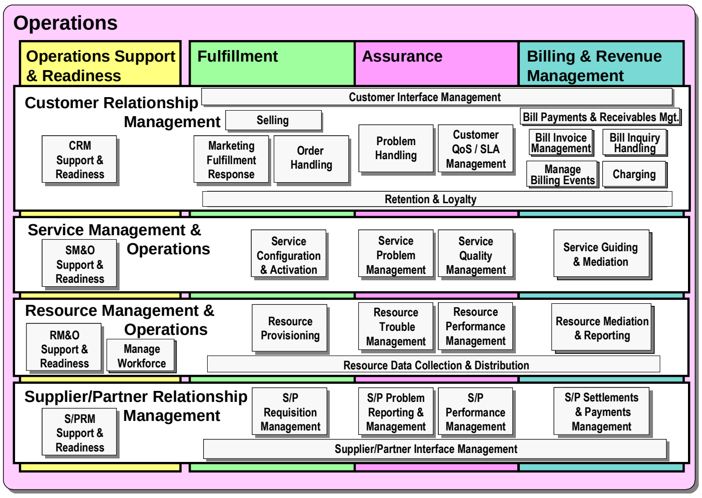
Operations
Operations Support & Readiness
Fulfillment
Assurance
Billing & Revenue Management
Customer Relationship Management
Customer Interface Management
Selling
Bill Payments & Receivables Mgt.
CRM Support & Readiness
Marketing Fulfillment Response
Order Handling
Problem Handling
Customer QoS / SLA Management
Bill Invoice Management
Bill Inquiry Handling
Manage Billing Events
Charging
Retention & Loyalty
Service Management & Operations
SM&O Support & Readiness
Service Configuration & Activation
Service Problem Management
Service Quality Management
Service Guiding & Mediation
Resource Management & Operations
RM&O Support & Readiness
Manage Workforce
Resource Provisioning
Resource Trouble Management
Resource Performance Management
Resource Mediation & Reporting
Resource Data Collection & Distribution
Supplier/Partner Relationship Management
S/PRM Support & Readiness
S/P Requisition Management
S/P Problem Reporting & Management
S/P Performance Management
S/P Settlements & Payments Management
Supplier/Partner Interface Management

Figure 2: eTOM operations processes

Customer Relationship Management, Service Management & Operations and Resource Management & Operations are concerned in this case.

It is operated on living networks and services already fulfilled (configured and provisioned) Fulfilment eTOM processes).

Topology

Figure 3 shows the network topology of the case study. Typical network topology consists in an IP/MPLS backhaul & backbone network connecting various access networks:

- Dedicated connection for VPN.
- Fixed ADSL connection with Home Gateways.
- 3G/LTE mobile connection ((e)-node B).
- WIFI/WIMAX/Femto wireless connection.

This case study addresses the technologies that are available in UNIVERSELF while keeping in mind that developed features must apply to all the elements.

Service plane is enabled with an IMS service platform mainly composed of CSCF, AS and HSS. Some of elements can be distributed over the IP/MPLS backbone nodes.

Two kinds of services are considered:

- VPN service.
- Fixed and Mobile IMS services (VoIP).

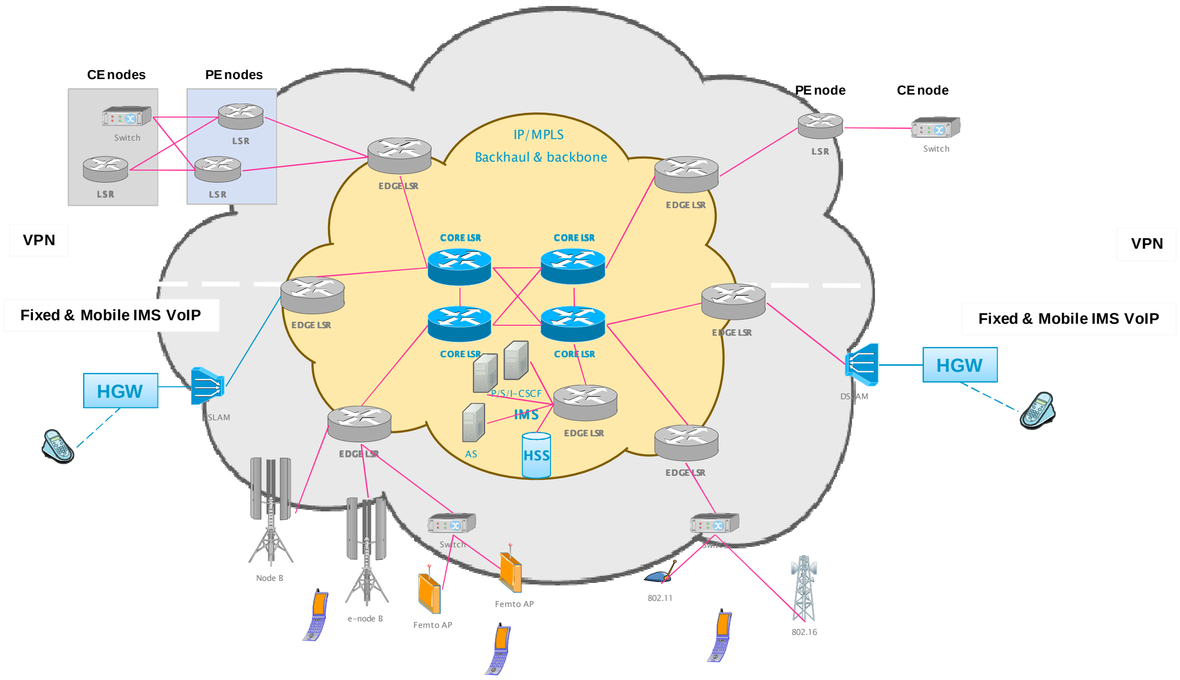

Figure 3: Case study network topology

PROBLEM STATEMENT

The elaboration of this case involves the identification of potential problems that derive from the scope of this case. The problems that can be identified are related to the different network phases that this case covers.

The main issues are:

User side:

- Experiencing service outage or degradation that implies to call customer care, several times due to customer care and management inefficiency to get end-user service & network status.

Operator side:

- Currently, network elements generate lot of alarms with various severity levels but it's practically impossible for a human operator to exploit all of them (correlation and interpretation). Generally, operators only actively monitor critical alarms if there are services impacting. Other alarms or network parameters are offline analysed if needed but often this amount of information is ignored.
- Missing of proactive analysis and action.
  - Today: only reactive actions based on alarms and customer complaints
- Deficiency of automatic anomaly detection.
  - Present tools provide mainly a view about alarms and network & service data.
  - Correlation and delay: automatic correlation is quite limited
- Service modelling:
  - Network and service representation is mostly empirical:
    - Created by human and depends on human skills.
    - Not machine readable (e.g. drawing).
    - Dedicated for each network/service.
  - Technical inventory is difficult to enable an end to end view due to:
    - Technology and network segment separation and related representation differences.
    - Cost for covering and maintaining an inventory for the last mile (boxes).
    - Lack of updates.
- Lack of micro and macro granularities:
  - Macro granularity is for global end to end and/or per network domain/technology. It gives the status for Fault and Performance management:
    - Nominal functioning (green indicator)
    - Non nominal functioning with related correlated data for reparation.
  - Micro granularity is for local and/or end user perspective for diagnosis and healing.
- Service impact analysis (End to end, OSS level)
  - Simple and limited: based on network topology in case of link or router fault and related protection.
  - Manually defined.
- Using additional probes or robots mainly does the transverse end to end management. Even if they are adapted for macroscopic service status view, they can't answer the need of microscopic analysis for end user granularity issues. Moreover, needed data may be available from network equipments themselves, but they are not considered (too much data, too much effort, need automation).
- Anomalies can be caused by network activities that deviate from the normal network usage (for example, a larger than usual number of users, or a network element outage), or by malicious activities caused by third parties.

- Management processes are static and need to be redefined for each new network or service segment. It includes service model and diagnosis process definition with maintenance of the correlation rules, data connection (with network element from various vendors).
  - For all layers including the cross layer management
  - Today processes are in silo and ossification
- Human is too much involved in every part of fault and performance management processes:
  - Defining network & service description, KPIs computation, rules for alarming.
  - Supervising the alarms and make the necessary correlations (with book of instructions) to qualify and identify incidents that can implies to be coordinated with technology and service teams.
  - Following healing actions.
  - Reporting.

MODELLING

This section briefly describes the modelling approach adopted in this case study.

Actor(s)

The main actors involved in this case study are: the end users/subscribers who are experiencing a service outage, the people involved in the management teams in charge of the network operations and customer care, the vendors in charge of providing network resources and their related management systems. Several teams of the network operator are concerned: the one in charge of the support and readiness of the service and network management infrastructure, defining the tools necessary to support fulfilment and assurance processes; the teams in charge of the fulfilment and assurance processes, and the teams in charge of the customer care.

Triggers

Triggers are related to the occurrence of an outage:

- A customer who is calling customer care for a service outage. Then customer care is responsible to find a solution and ask operation teams to find the root cause of the problem if needed.
- An outage is detected with monitoring: diagnosis and reparation are then fulfilled by operation teams.

Phases

The case study is decomposed in several phases.

Each network and service element is doted by a basic monitoring. The basic monitoring issues two types of data: alarm/events data and network and service data. For each data we distinguish a type of diagnosis, respectively Reactive and Proactive and diagnosis (see Figure 4):

- The Proactive Diagnosis is based on the network and service data and aims to detect possible incidents that can occur and have already been identified. It anticipates their occurrences by setting mitigation plans. Reparation plans should also be triggered as the mitigation plans may not definitely fixed the issue.
- The Reactive Diagnosis is based on the collected alarms and events, which are received from the network and service elements. It aims to detect alarms, analyse and qualify problems, identify their impact and select the reparation plan.

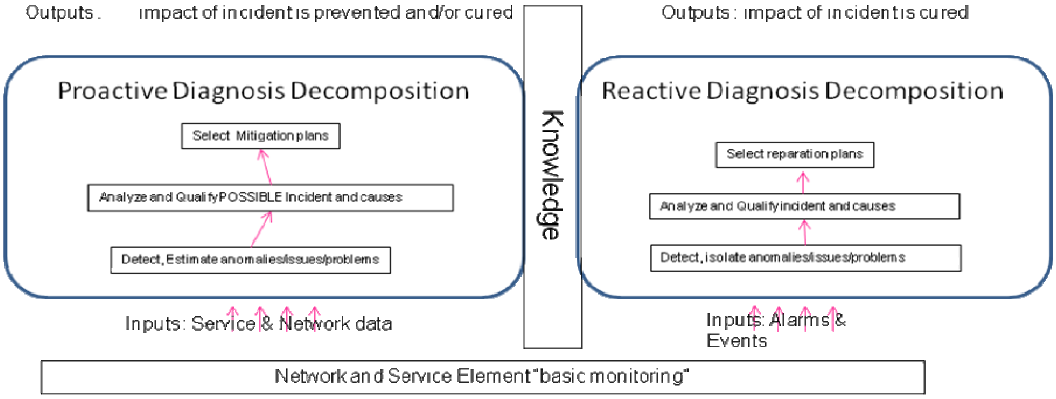
Outputs . impact of incident is prevented and/or cured
Outputs : impact of incident is cured
Proactive Diagnosis Decomposition
Select Mitigation plans
Analyze and Quali fy POSSIBLE Incident and causes
Detect, Estimate anomalies/issues/problems
Knowledge
Reactive Diagnosis Decomposition
Select reparation plans
Analyze and Qualify incident and causes
Detect, isolate anomalies/issues/problems
Inputs: Service & Network data
Inputs: Alarms & Events
Network and Service Element "basic monitoring"

Figure 4: Proactive and Reactive diagnosis

Then in terms of phases, we need to distinguish what have to be done before and after an outage even occurs (see Figure 5).

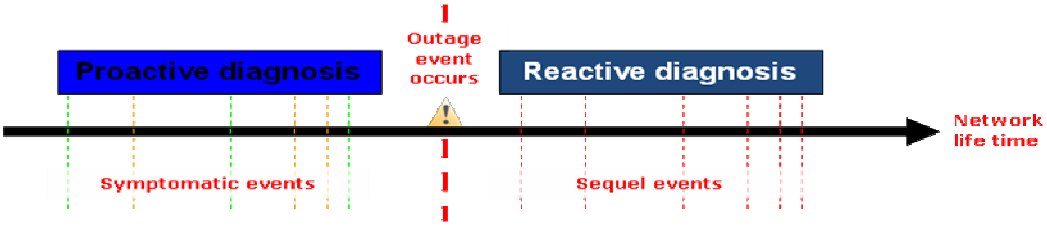

Figure 5: Phases

Before an outage event occurs:

- All diagnosis (both proactive and reactive) mechanisms should be fulfilled and ready to work: models, probes, correlation engines, etc… should be ready.
- Proactive diagnosis looks at symptomatic events, based on service and network data for qualify possible incident and causes. Mitigation plans are enforced.

After on outage event occurs:

- Reactive diagnosis looking to sequel events (alarms) to analyse and qualify the incident. Reparation plans are enforced.

INNOVATION

There are lot of techniques that are related to self-diagnosis. This case study will focus on some of the main techniques that will be integrated/instantiated/embodied thanks to the UMF.

Enabling concepts and mechanisms

Bayesian networks, case based reasoning, self-modelling, learning, pattern prediction techniques, are investigated to enable a reactive and proactive self-diagnosis for fault/congestion/anomaly detection.

Applications are:

- Self-modelling and active diagnosis for IMS services (first focus on signalling).
- Proactive Self-diagnosis for congestion detection, network by identifying the pattern that depicts the relation of congestion with variables such as link capacity, incoming to the link bytes, buffer and queue size of the node that sends traffic in the link.
- Distributed Data Mining Framework and QoS degradation identification and adaptation using Fuzzy Logic.
- Analysis of aggregated network traffic data for intrusion detection in high speed networks (SSH data).
- Proactive self-diagnosis with pattern prediction (neural networks) for networks (IMS architecture).
- Fault-diagnosis based on the combination of the Bayesian Network and Case-based reasoning (IMS architecture).

Impacts and benefits

Globally, Self-diagnosis and Healing will help to optimize the effort in operations. By enabling a proactive and reactive diagnosis taking into account the end to end and customer perspective, it will decrease customer care service and network management effort (mainly OPEX reduction).

Autonomic anomaly detection, especially if flow based, is expect to impact the cost metrics as follows:

- Flow enable component are nowadays embedded in the entire major network equipment. Therefore no additional cost is expected for the flow-exporting setup. Moreover, given the high data aggregation provided by flows, the flow collection and analysis can be performed using commodity hardware.
- Autonomic parameter tuning will allow specifying the allowed/expected rate of false positive/negatives, therefore limiting/decreasing the cost of unwanted interventions.
- OPEX is expected to decrease because of
    - A higher detection rate of anomalies,
    - A decreased number of false alerts, which generally cause extra work for the system administrators.
    - Less effort needed to tune the operational parameters of the detector.

It will also in increase the overall Quality of Experience and QoS leading the way to a churn rate decreasing.

One other aspect is reusability of the fault and performance management processes to face networks and services evolution. By defining reusable Self-diagnosis and Healing, integration and deployment costs (for both operators and vendors) will be reduced, Time To Market as well.

The migration towards these evolved processes will imply to update/change all the network and service elements. It can be considered as normal or disruptive evolution of these elements that will imply CAPEX.

REFERENCES

[1] Jacobson Ivar, Christerson M., Jonsson P., Övergaard G., Object-Oriented Software Engineering - A Case Driven Approach, Addison-Wesley, 1992

[2] Cockburn, Alistair. Writing Effective Cases. Addison-Wesley, 2001.

[3] “Synthesis of case requirements“ - Deliverable 4.1, August 2011, http://www.univerself-project.eu/technical-reports

[4] “Synthesis of case requirements – Release 2“ - Deliverable 4.2, April 2012, http://www.univerself-project.eu/technical-reports

[5] Gonzalo Camarillo, Miguel-Angel García-Martín "The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds" John Wiley & Sons, 2006, ISBN 0-470-01818-6

[6] Miikka Poikselka, Aki Niemi, Hisham Khartabil, Georg Mayer "The IMS: IP Multimedia Concepts and Services" John Wiley & Sons, 2006, ISBN 0-470-01906-9

[7] A. Valencia et al., IP Based Virtual Private Networks, RFC 2341, May 1998

CONTACT INFORMATION

For additional information, please contact: Christian Destré (christian.destre@orange.com) or Imen Grida Ben Yahia (imen.gridabenyahia@orange.com); or consult www.univerself-project.eu

UNIVERSELF CONSORTIUM

Alcatel·Lucent
THALES
NEC
orange™
TELECOM ITALIA
Telefónica
NTT
Fraunhofer FOKUS
INRIA
VTT
UCL
UNIVERSITY OF SURREY
UNIVERSITY OF TWENTE.
ΕΘΝΙΚΟΝ & ΚΑΠΟΔΙΣΤΡΙΑΚΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟΝ ΑΘΗΝΩΝ
NATIONAL & KAPODISTRIAN UNIVERSITY OF ATHENS
ibbt
Π Π