Methodology towards Integrating Scenarios and Testbeds for Demonstrating Autonomic/Self-managing Networks and Behaviors Required in Future Networks

Vassilios Kaldanis[1], Peter Benko[2], Domonkos Asztalos[2], Csaba Simon[3], Ranganai Chaparadza[4], and Giannis Katsaros[1]

[1] VELTI S.A. -Mobile Marketing & Advertising,
44 Kifissias Ave, GR 15125 Maroussi, Greece
{vkaldanis,gkatsaros}@velti.com
[2] Ericsson Hungary, Laborc u. 1, H-1037, Hungary
{peter.benko,domonkos.asztalos}@ericsson.com
[3] Budapest University of Technology and Economics, Dept. of Telecom and Media Informatics,
Magyar T. krt. 2, 1117 Budapest, Hungary
simon@tmit.bme.hu
[4] Fraunhofer FOKUS Institute for Open Communication Systems,
Kaiserin-Augusta-Allee 31, Berlin, Germany
ranganai.chaparadza@fokus.fraunhofer.de

Abstract. In this paper we report an insight of our experiences gained in devising a methodology for validating Scenarios demonstrating autonomic/self-managing network behaviors required in Future Networks—powered by IPv6 and its evolution along the path to the Self-Managing Future Internet. Autonomic networking introduces "autonomic manager components" at various levels of abstraction of functionality within device architectures and the overall network architecture, which are capable of performing autonomic management and control of their associated Managed-Entities (MEs) e.g. protocols and mechanisms, as well as co-operating with each other in driving the self-managing features of the Network(s). MEs are started, configured, constantly monitored and dynamically regulated by the autonomic managers towards optimal and reliable network services. There are some challenges involved when designing and applying a framework for integrating and validating Scenarios demonstrating autonomic behaviors we share in this paper, and show how we have addressed them. In this paper, we present the EU funded FP7 EFIPSANS Integration and Validation Framework that we designed for demonstrating a substantial selection of essential autonomic behaviors of "autonomic managers" whose implementations are based on the principles of the GANA architectural Reference Model for Autonomic Networking and Self-Management, and on the IPv6 protocols and associated extensions proposed and developed in the frame of the EC funded FP7 EFIPSANS Project.

Keywords: Autonomic behaviors of Decision-Making-Elements (DMEs/DEs), Validation of the GANA Model for Autonomic Networking and Self-Management, Testbeds Integration, Validation methodology, framework, IPv6 networks, Self-Management, Managed Entities (MEs).

R. Szabó et al. (Eds.): AccessNets 2010, LNICST 63, pp. 240–252, 2011.

1 Introduction

The main benefits of the self-management technology in systems and networks, from the operator's perspective are: to minimize operator involvement and OPEX in the deployment, provisioning and maintenance of the network, and increasing network reliability (self-adaptation and reconfiguration on the fly in response to challenges e.g. faults, errors, failures, attacks, threats, etc) [1], [2], [3], [4], [5], [6], [8], [10]. There are some challenges involved when designing and applying a framework for integrating and validating Scenarios demonstrating autonomic/self-managing network behaviors required in Future Networks. A *Scenario* must consist of a clear description of the problems/limitations with the "current network management practices" and/or "current technology that come with the devices/systems of today". The problems/limitations are with respect to either of the following needs:

a) Reducing human involvement in the management aspects considered while at the same time reducing the probability of introducing faults into any item supplied as input to the devices/network for its operation e.g. policy-specifications, configuration data, etc;
b) OR the introduction of advanced algorithms, components and mechanisms that enable the network entities to perform Self-* operations such as auto-discovery, self-configuration, self-healing, self-protection, self-diagnosis, and self-optimization operations towards guarantee reliable services, including on-demand services.

Special components called "*autonomic manager components*" (referred to as DEs in the GANA Model [2], [3]) introduced into node/device architectures and the overall network architecture are meant to address the two issues ("a" and "b"). In a *Scenario*, one must be able to talk and reason about either "current practices" and/or "current technology that come with the devices/systems of today", and that the Scenario then reflects what is being solved by Self-* technologies being introduced by the prototyped components, mechanisms and algorithms.

The integration challenges include the following:

- Interconnecting multiple testbeds environments and diverse types of testbeds required by each Scenario;
- Validating the functionality, algorithms, autonomic behaviors and architectures on which to realize the Scenario, and architectures proposed by the research and prototyping team.
- Visualization of the behaviors of "autonomic manager components" involved in a Scenario,
- How to visualize the autonomic architectural Reference Model framework in action, i.e. the framework applied to derive the implementation of the components of the Scenario architecture being demonstrated.

2 Autonomic Networking and Self-management Fundamentals

The concept of autonomicity—realized through control-loop structures embedded within node/device architectures and the overall network architecture as a whole is an enabler for advanced self-manageability of network devices and the network as a whole. The emerging GANA architectural Reference Model for Autonomic Networking and Self-Management ([1], [2], [3]) introduces "autonomic manager components" at four various levels of abstraction of functionality within device architectures and the overall network architecture, which are capable of performing autonomic management and control of their associated Managed-Entities (MEs) e.g. protocols, as well as co-operating with each other in driving the self-managing features of the Network(s). MEs are started, configured, constantly monitored and dynamically regulated by the autonomic managers towards optimal and reliable network services. The GANA Model defines a framework of hierarchical "autonomic managers" referred to as Decision Elements (DEs) in GANA, at four levels of abstraction of functionality ([1], [2], [3]).

The fundamental principles of the setup and operation of an autonomic network can be described as three cascaded phases of some automated behaviors of nodes/devices being connected together to form an autonomic network, namely:

- **[Phase-1]:** *Boot-up and Bootstrap Phase for each initializing node/device*;
- **[Phase-2]:** *Auto-Configuration Phase for each node/device and the network as a whole*;
- **[Phase-3]:** *Operation and Self-Adaptation Phase for each node/device and the network as a whole*, i.e. adaptation to challenges such as faults, errors, failures, and adverse conditions, and to policy changes by the human.

The following automated behaviors of node/devices and the network (realized as autonomic behaviors orchestrated or triggered by autonomic managers i.e. GANA DEs) apply to some phases (from the three described above):

(1) Auto-Discovery (Network-Layer-Services Discovery, Service/Application-Layer-Services Discovery): The associated behaviours apply to **Phase-1,** and some behaviors related to Auto-Discovery for more advanced service provisioning requirements beyond the minimal required at bootup/bootsrap time may still be attempted during the operation and self-adaptation time of a node/device or network.

(2) Auto-Configuration/Self-Configuration (in the Service-Layer and Network-Layer). The associated behaviours apply to **Phase-2.**

(3) Self-Diagnosing and Self-Healing, Self-Optimization, other Self-* functions. The associated behaviours apply to **Phase-3.**

Such automated behaviors must be orchestrated and regulated by specific context-aware Decision Elements (DEs) designed to detect context, start, configure, and constantly monitor and dynamically regulate the behavior of their specifically assigned (by design) Managed Entities (MEs) i.e. managed resources such as protocols, protocols

stacks and mechanisms. More details on such phases and behaviors can be found in [6], [8], [9], [10], [11], [12], [13].

What determines autonomicity for a functionality are two things: (1) the auto-discovery of items required by the functionality to perform an auto-configuration/self-configuration process; (2) the predictions/forecasting and listening for some events and reactions by the Decision Element (DE) that controls and adapts the behaviour of the functionality towards some goal, based on the events.

3 Scenarios and Demonstration Testbeds

The following key functionalities for which autonomic elements (DEs) emerged for specification and design, for the selected diverse networking environments (i.e. instantiation cases for the GANA Model) and are demonstrated in the testbeds:

- **Routing and Autonomicity.** Special DEs that implement control-loops over the "management interfaces" of routing protocols and mechanisms as their associated Managed Entities (MEs). The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted e.g. Timers and link weights in OSPF are dynamically adjusted by the Routing-Management-DEs (see [8], [10] for more details). For other general aspects related to Control Plane and Autonomicity: special DEs apart from Routing-Management-DEs have been introduced for addressing these other aspects of the control plane (signalling plane).
- **Data Plane & Forwarding and Autonomicity.** Special DEs that implement control-loops over the "management interfaces" of the Data Plane and forwarding protocols and mechanisms as their associated Managed Entities (MEs). The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted e.g. IPv6 forwarding-engine parameters, MPLS related Management Objects, and other types of Layers-1/2/2.5/3 related parameters. Parameters are dynamically adjusted by the Data Plane and Forwarding-Management-DEs (see [10] for more details).
- **Auto-Discovery, Auto-Configuration / Self-Configuration, Self-Provisioning and dynamic Re-Configuration.** Special DEs that implement control-loops over the "management interfaces" protocols and mechanisms of a node/device that is fundamental to enabling the device to advertise and update its capabilities to the network, and to discover network resources at boot-up time and during the device's operation. The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation (see [6] for more details).

- **Mobility Management and Autonomicity.** Special DEs that implement control-loops over the "management interfaces" of mobility protocols and mechanisms as their associated Managed Entities (MEs) e.g. MIPv6 and PMIPv6. The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted by the Mobility-Management-DEs (see [11] for more details).
- **QoS Management and Autonomicity.** Special DEs that implement control-loops over the "management interfaces" of QoS protocols and mechanisms as their associated Managed Entities (MEs). The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted by the QoS-Management-DEs (see [11], [13] for more details).
- **Resilience, Survivability, and/for Autonomicity.** Special DEs that implement control-loops over the "management interfaces" of resilience and survivability protocols and mechanisms as their associated Managed Entities (MEs). The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behavior of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted by the Resilience & Survivability-DEs (see [12] for more details).
- **Autonomic Fault-Management.** Special DEs that implement control-loops over the sub-interfaces of the "management interfaces" of components and modules of devices that enable the fault-management operations to be performed by Fault-Management-DEs on the components/modules (as MEs). Also, Fault-Management-DEs manage and control special MEs that handle challenges such as detection of faults, errors, failures. The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behaviour of various types of MEs of the devices to ensure optimal conditions of network operation. Parameters of the MEs are dynamically adjusted by the Fault-Management-DEs (see [12] for more details).
- **The role of Monitoring in enabling Autonomicity, and Self-Monitoring/Autonomic Monitoring as an autonomic feature.** Special DEs that implement control-loops over the "management interfaces" of Monitoring protocols and mechanisms as their associated Managed Entities (MEs). The DEs apply configuration profiles (which include policies) on this type of MEs, and then react to incidents, state changes and context changes by communicating with other DEs to enforce changes on the behaviour of various types of MEs of the devices to ensure optimal conditions of network operation. The MEs are orchestrated and parameters of the MEs are dynamically adjusted by the Monitoring-DEs (see [13] for more details).

4 Integration and Validation Framework

In this section the overall approach to Integration and Validation is described in general. We consider that the use of Templates should be applied to describing Scenarios in such a way as to show the paradigm shift brought by Autonomics and Self-Management, as well as showing the benefits brought by the various technologies conveyed by the Scenario, to key players: manufactures, Operator/network management personnel, content providers, etc. Also, some questionnaires are used answered by all project partners/developers in describing information that helps those building the testbeds. From our experience, some decisions must be made when selecting Open source tools, such as the selection of common libraries to ease the integration of Scenarios whose components emerge from multiple partner testbeds.

4.1 Integration Methodology

There are twelve (12) template-based Scenarios defined by EFIPSANS that span over heterogeneous networking environments, functionality and use-cases. In order to give a clear, uniform picture on the overall benefits of autonomic networking, the integration of some of these Scenarios in a use case trial is required. The objectives of integration are the following: Harmonize the autonomic functions to be demonstrated with regard to inter-operability and networking environment; Create a common testbed that can be used for experimentation; and Describe a high-level story-line for the Scenarios.

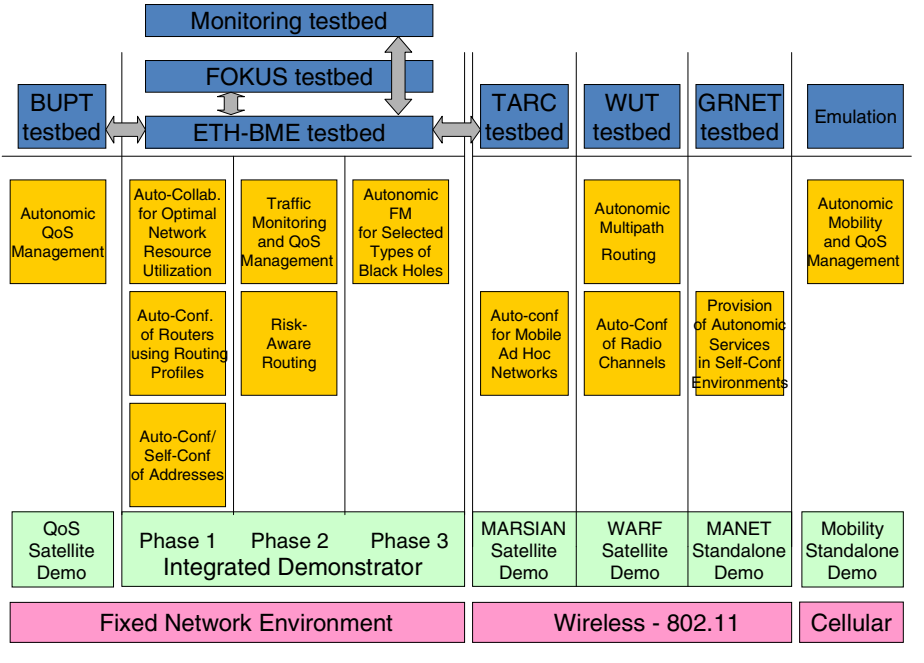

Fig. 1. EFIPSANS Scenarios and Testbeds versatility

In order to fulfill the above objectives, first we selected scenarios that can be used in a given network environment. This is necessary since most autonomic behaviors in EFIPSANS are specific to a certain network environment, such as fixed, wireless or cellular. The grouping of scenarios ensures that each scenario is demonstrated in the appropriate environment Fig. 1 next shows how different scenarios were mapped to different networking environments. The yellow boxes represent the individual scenarios while in the bottom of the figure the magenta boxes indicate the networking environment. The code names illustrated (BUPT, ETH-BME, TARC, WUT, GRNET, etc) corresponds to project partner shortcuts and therefore can be ignored.

One of the main objectives here was to create a proof-of-concept testbed that can be used to demonstrate the autonomic functions researched and developed by the project. Since the consortium members are spread practically all over Europe, it would have required considerable effort to create an integrated testbed that is installed at a single geographical location. However, the public Internet infrastructure enables a more or less straightforward interconnection of fixed networks. This motivated our decision to create a common integrated demonstrator core testbed that is composed of interconnected network segments. This core testbed will host a number of important scenarios as seen in Fig. 1 that cover all the areas of GANA-defined autonomicity and focus on the wired networks. The interconnection of the networks is based on a layer 2 tunneling solution, which enables passing both link layer and IPv6 packets (see Fig. 2). The configured tunnels transfer layer 2 packets over IPv4 packets. The tunneling choice was motivated by the fact that the connectivity provided by the current

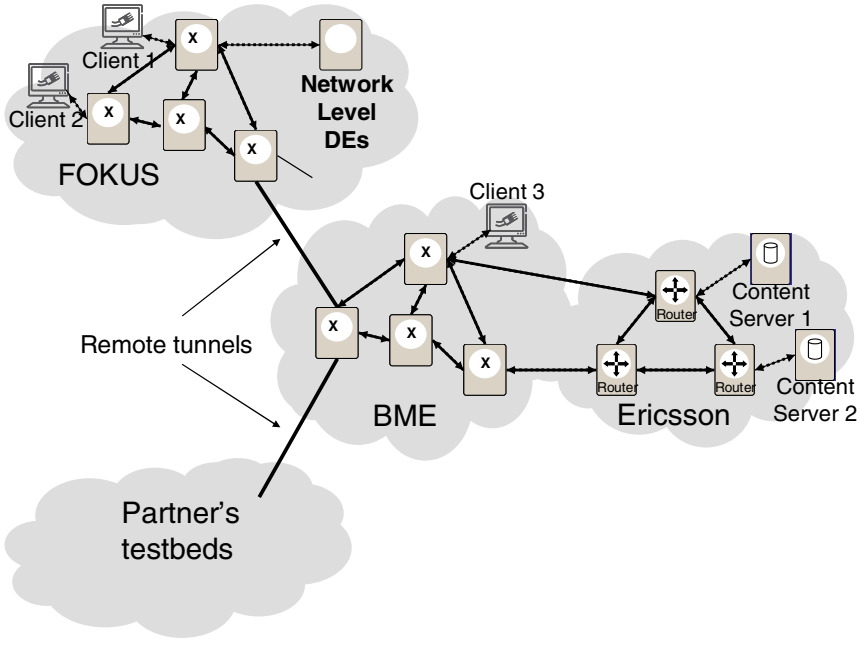

Fig. 2. Integrated Testbed overview

Internet is still based on IPv4 dominantly. We chose to tunnel layer 2 packets so that in addition to IPv6 packets, link layer packets can also be exchanged between the tunnel endpoints. This provides a totally transparent connectivity on layer 2 and on layer 3, which is necessary to demonstrate some of the EFIPSANS scenarios.

4.2 Validation Methodology

EFIPSANS validation methodology in principle aims to validate a number of fundamental (to autonomic network engineering) features of an autonomic network categorized accordingly to the project objectives per network type (fixed or mobile), functionality (layer-specific), topology (e.g. mobile ad hoc) and other (e.g. security). These features have been categorized in general under the following five key concepts:

- Auto-Discovery
- Auto/Self-Configuration
- Autonomic Routing & Self-Adaptation
- Autonomic Mobility & QoS Management
- Autonomic Network Monitoring & Fault-Management

Validation of the former key concepts is required to assess their impact on the project technology framework and evaluate to what extend the defined R&D challenges and objectives coming from those key concepts were successfully addressed and implemented within the project lifespan. In order to successfully complete such an assessment a common concept and step-based evaluation process must be specified to guarantee a smooth effective and unified evaluation.

EFIPSANS validation methodology incorporates a number of purpose-driven activities with specific expected outcomes such as:

1) Analysis of project specific documentation deemed suitable and essential in helping analyze the former key autonomic network functionalities, in terms of:

- Identification that the indentified R&D features and challenges at the project's start phase have been implemented into the underlying framework
- Identification and analysis of specific project deliverables which provide evaluations and recommendations on the adoption of key concepts in the individual work packages.
- Identification and analysis of project publications related to the key concepts to gain feedback and recommendations
- Analysis of the outcomes of the project related events (e.g. workshops) to get external insight on how the key concepts were received and anticipated by the general public.

2) Completion and distribution of specific questionnaires

Completion of specific key concept questionnaires to be distributed to various (business and technology) groups in order to obtain feedback and recommendations of issues like:

- IPv6 vs. IPv4
- Autonomic systems awareness and usability

- Anticipation of autonomic behaviors and advanced functionality
- How the key autonomic concepts improve end user experience
- Benefits for Industry players (ISPs, Operators, SPs) from deploying relevant autonomic features and functionality in existing infrastructures
- Autonomic networking: Applicability, deployment and acceptance
- Impact in higher-layer services and application deployment

3) Validation via Simulation/Emulation

Validation of the specific key concepts via simulation/emulation is used as part of the overall evaluation of the project's key concepts mainly to assess important issues around performance, stability and scalability that cannot be easily estimated in the project testbeds. Specialized satellite (to the integrated) testbeds deployed simulation/emulation approaches in order to prove and experiment with autonomic features around Mobility and QoS/QoE management in mobile/wireless environments in scenarios where real operator's core/access network mechanisms and functionality were represented successfully.

4) Analysis of the Qualitative/Quantitative Testing, Results and Reporting

Selected Qualitative / Quantitative (Q&Q) tests and results tightly dependent to the project scenarios that directly incorporate autonomic functionality related to the former key concepts have been selected for analysis and evaluation. This can work towards identifying:

- What certain innovations and advancements have been validated in each scenario
- Recommendations / lessons learnt from the integration of DEs/MEs with specific functionality implementing each key concept
- What is the impact of each scenario and relevant DEs/MEs in the respective business and technology area in the present and future systems
- Identification of any problems encountered during pilot or productive system operation

5) Analysis of key concepts to the project's Business Model

The fact that existing project scenarios already analyze the business aspects around the corresponding key concept(s) they deal with (as part of the overall business framework) creates itself a necessity to evaluate in practice the real impact of each autonomic concept in industry today. This will reveal the real value added by the project in the converged IP-based systems of today and tomorrow especially in the area of autonomic service management.

6) Analysis of the key concepts with respect to the standards

The fact that the project is tightly coupled with IPv6 technology framework and is expected to highly influence IPv6 deployment in current and future systems that are enhanced with autonomic functionality create itself the inherent need for a circumstantial analysis surrounding standardization issues. Addressing of important standardization issues around required IPv6 extensions (IPv6++) [4], [10] will allow the aforementioned key concepts to have a compatible and aligned impact in this area and particularly:

- Have the results or concepts coming from the project been taken up outside the project consortium?
- Which specific IETF drafts or standards have the key concepts contributed towards?
- How the adopted strategy achieved its purposes
- Setup the required framework for other projects to build on the top and expand further IPv6++ context [4], [10].

The formerly described validation framework aims to complements the project's demonstration environment around the key concepts in a number of scenarios implemented in specific testbeds (integrated and satellite ones). The Fig. 3 next illustrates how the developed components that realize the project key concepts are mapped within the different physical nodes per work package as software installed on these nodes in the testbeds.

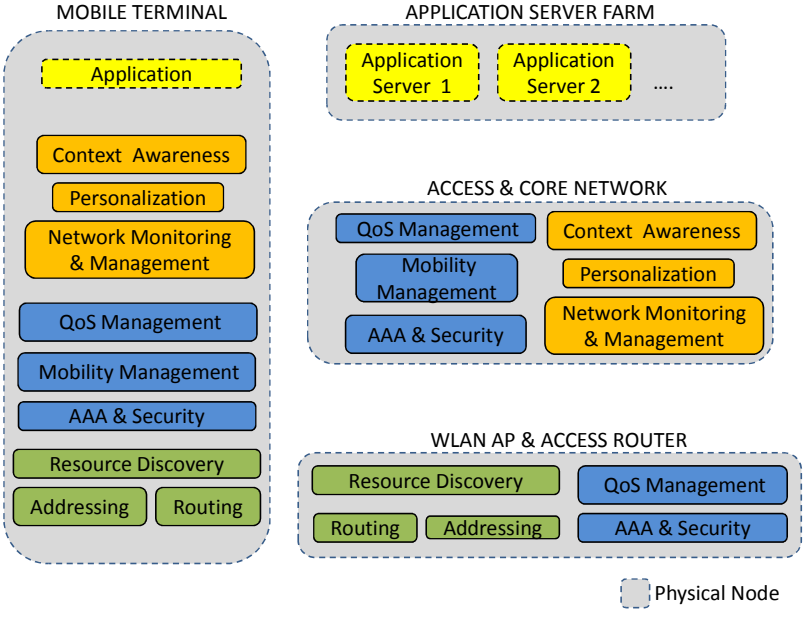

Fig. 3. EFIPSANS Validation Framework

The grey box represents a physical node (e.g. mobile terminal, router, etc) and the colored boxes within each grey box represent autonomic components or modules that implement purpose-specific autonomic functionality (in the form of DEs/DMEs) on the top of existing functionality (e.g. QoS management).

4.3 IPv6 Integration and Validation

This section reflects on the aspects related to IPv6 and the EFIPSANS proposed Extensions to (IPv6++) required for designing and building IPv6-based Autonomic Networks

and Services (we refer to the upcoming EFIPSANS deliverable D2.6 [1] for IPv6++). It also summarizes the key features of IPv6 that make the integration and validation of large scale autonomic networks in Testbeds easy to achieve.

IPv6 features such as *auto-discovery e.g. neighbor and parameter discovery, auto-configuration, advanced addressing schemes and route aggregation,* and *Support for large address space* can be considered as enablers for designing large-scale Testbeds. This is because *scalability and some automated discovery and auto-configuration features* are requirements for facilitating for more advanced autonomic/self-managing network behaviors that leverage the basic auto-discovery and auto-configuration of nodes' interfaces.

But how EFIPSANS achieves autonomic management and control of IPv6 Protocols through its mechanisms?

Here autonomic management and control of IPv6 protocols and mechanisms as so-called Managed Entities (MEs) at GANA's lowest level/layer, is based on the assignment of specific IPv6 protocols and mechanisms to specific Decision Elements (DEs) that autonomously manage and regulate/control the behavior of the different MEs. Autonomic routing involves the development of Routing-Management-DEs that are meant to be context-aware and to start, configure, monitor and dynamically regulate the behavior of IPv6 protocols and mechanisms of specific devices (as the associated MEs), such as OSFPv3 (the main routing protocol of focus in EFIPSANS). More information on how the GANA has been instantiated for realizing autonomic routing functionality in wired networks can be found in the EFIPSANS deliverables D1.7 in [1] and particularly in those from work package 1.

Regarding instantiation of GANA Mobility-Management DE(s) in an IPv6 network, the associated Managed Entities (MEs) of the Mobility-Management DE(s) are MIPv6 and PMIPv6. For Autonomic QoS Management via the QoS-Management DE(s), the associated MEs are mechanisms such as the IPv6-based DiffServ and IntServ protocols and mechanisms (see [11], [13]). The Managed Entities (MEs) associated with the GANA DEs for Auto-Discovery, Auto-Configuration/Self-Configuration i.e. NODE_MAIN_DE, are protocols and mechanisms such as Neighbor Discovery (ND), DHCPv6, NETCONF, IPv6 Stateless Address Auto configuration. For autonomicity for the Data Plane and Forwarding functionality, parameters of the Data Plane protocols and mechanisms as MEs, are dynamically adjusted e.g. IPv6 forwarding-engine parameters and Layers-1/2/2.5/3 related parameters. Parameters are dynamically adjusted by the Data Plane and Forwarding-Management DEs.

Also being validated are IPv6 protocol extensions being proposed by EFIPSANS [1], which include ICMPv6++[9], ND++ (Extensions to the ND protocol), DHCPv6++, PMIP6++.

5 Concluding Remarks

We presented our *Methodology Towards Integrating Scenarios and Testbeds* for demonstrating autonomic/self-managing networks and behaviors required in Future Networks.

The evolvable Architectural Reference Model for Autonomic Networking and Self-Management called GANA enables the design of interworking hierarchical decision-making processes at different levels of abstraction, which react to the changes in the state of the network and its environment (refer to [7] for information on the evolution of the model). The GANA has been successfully "instantiated" by EFIPSANS for autonomic management and control of different types of Managed Entities (Protocols and Mechanisms at GANA' lowest level/layer" for diverse network environments (Fixed/Mobile/Wireless Networks). Examples include: Autonomic Routing, Auto-Discovery, Auto-Configuration/Self-Configuration, Autonomic Mobility Management, Autonomic QoS Management, Autonomic Resilience, Survivability, Autonomic Fault-Management, Autonomic Monitoring, Autonomic Security Management. We have designed and implemented an integrated testbed that implements the core features of an autonomic network, based on GANA. The testbed serves as proof of concept for the applicability of the GANA model in a heterogeneous networking environment.

Since our work on validating the GANA concepts in the testbed continues, we expect to draw more lessons from running some field trials and provide a report on how GANA-based, advanced self-managing IPv6 networks can be build. We seek to show how to build diverse types of autonomic IPv6-enabled networks based on the autonomic management and control of IPv6 and lower layer protocols, and the use of EFIPSANS proposed extensions to IPv6 (IPv6++). We also aim at looking deeper into autonomic network services build on top of such networks. This will demonstrate how the Future Internet will emerge based on an evolution path that focuses on IPv6 and its Extensibility towards the Self-Managing Future Internet.

Acknowledgement

This work has been partially supported by EC FP7 EFIPSANS project (INFSO ICT-215549).

References

1. EC funded- FP7-EFIPSANS Project, `http://efipsans.org/`
2. Chaparadza, R., Papavassiliou, S., Kastrinogiannis, T., Vigoureux, M., Dotaro, E., Davy, A., Quinn, K., Wodczak, M., Toth, A.: Creating a viable Evolution Path towards Self-Managing Future Internet via a Standardizable Reference Model for Autonomic Network Engineering. Published in the book by the Future Internet Assembly (FIA) in Europe: Towards the future internet - A European research perspective. pp. 136–147. IOS Press, Amsterdam (2009)
3. Chaparadza, R.: Requirements for a Generic Autonomic Network Architecture (GANA), suitable for Standardizable Autonomic Behaviour Specifications of Decision-Making-Elements (DMEs) for Diverse Networking Environments: published in International Engineering Consortium (IEC) in the Annual Review of Communications 61 (December 2008)
4. Chaparadza, R.: Evolution of the current IPv6 towards IPv6++ (IPv6 with Autonomic Flavours). Published by the International Engineering Consortium (IEC) in the Review of Communications 60 (December 2007)

5. Greenberg, A., et al.: A clean slate 4D approach to network control and management. ACM SIGCOMM Computer Comm. Review 35(5), 41–54 (2005)
6. Prakash, A., Starschenko, A., Chaparadza, R.: Auto-Discovery and Auto-Configuration of Routers in an Autonomic Network. In: SELFMAGICNETS 2010: Proc. of the International Workshop on Autonomic Networking and Self-Management in Access Networks, ICST ACCESSNETS 2010, Budapest, Hungary (November 2010)
7. AFI_ISG: Autonomic network engineering for the self-managing Future Internet (AFI), http://portal.etsi.org/afi
8. Retvari, G., Nemeth, F., Chaparadza, R., Szabo, R.: OSPF for Implementing Self-adaptive Routing in Autonomic Networks: a Case Study. In: Strassner, J.C., Ghamri-Doudane, Y.M. (eds.) MACE 2009. LNCS, vol. 5844, pp. 72–85. Springer, Heidelberg (2009)
9. Internet Draft: ICMPv6 based Generic Control Protocol (IGCP):draft-chaparadza-6man-igcp-00.txt, https://datatracker.ietf.org/doc/draft-chaparadza-6man-igcp/
10. Chaparadza, R., et al.: IPv6 and Extended IPv6 (IPv6++) Features that enable Autonomic Network Setup and Operation. In: SELFMAGICNETS 2010: Proceedings of the International Workshop on Autonomic Networking and Self-Management in the Access Networks, ICST ACCESSNETS 2010 (November 2010)
11. Aristomenopoulos, G., et al.: Autonomic Mobility and Resource Management Over an Integrated Wireless Environment-A GANA Oriented Architecture. In: proceedings of the IEEE MENS Workshop at Globecom 2010, Miami, Florida, USA, December 6-10 (2010)
12. Tcholtchev, N., Chaparadza, R.: Autonomic Fault-Management and Resilience from the Perspective of the Network Operation Personnel. In: Proceedings of the IEEE MENS Workshop at Globecom 2010, Miami, Florida, USA, December 6-10 (2010)
13. Liakopoulos, A., et al.: Applying distributed monitoring techniques in autonomic networks. In: Proceedings of the IEEE MENS Workshop at Globecom 2010, Miami, Florida, USA, December 6-10 (2010)