Chapter 11
A Guideline for Realizing the Vision of Autonomic Networking:
Implementing Self-Adaptive Routing on Top of OSPF

Gábor Rétvári
Budapest University of Technology and Economics, Hungary

Felicián Németh
Budapest University of Technology and Economics, Hungary

Ibrahim Hokelek
Telcordia Technologies, Inc., USA

Mariusz Fecko
Telcordia Technologies, Inc., USA

Arun Prakash
Fraunhofer Institute for Open Communication Systems, Germany

Ranganai Chaparadza
Fraunhofer Institute for Open Communication Systems, Germany

Michał Wódczak
Telcordia Technologies, Inc., USA

Bruno Vidalenc
Alcatel-Lucent Bell Labs, France

ABSTRACT

Autonomicity, realized through control loop structures operating within network devices and the network as a whole, is an enabler for advanced and enriched self-manageability of communication systems. Unfortunately, very little practical knowledge is currently available that would guide a network engineer through realizing this ambitious vision. In this survey, we intend to fill this gap by providing a practical guideline for building truly autonomic systems. Our main motivation is the recognition that it is not necessary to rebuild the whole network infrastructure out of piecemeal-designed, autonomic-aware protocol components. Instead, the framework of Autonomic Networking is broad enough to accommodate many of, if not all, existing off-the-shelf network technologies. This is because sophisticated network protocol

DOI: 10.4018/978-1-60960-845-3.ch011

machinery is usually quite capable self-managing entity in itself, complete with all the basic components of an autonomic networking element, like embedded control loops, decision-making modules, distributed knowledge repositories, et cetera. What remained to be done to achieve the desired autonomic behavior is to open up of some of these intrinsic control loops and incorporate them into external decision making logics. We demonstrate this idea on the example of building advanced self-adaptive routing mechanisms on top of OSPF. First, we present a generic framework for autonomic networks, designed to integrate well-tested, legacy network technology and modern, inherently autonomic-aware functionality into a single feature-rich self-managing infrastructure. Then, we cast an illustrious legacy network technology, the Open Shortest Path First (OSPF) routing protocol, in this framework, we identify the control loops intrinsic to it, and we describe the way these can be incorporated into higher level control loops. Finally, we demonstrate this design process through two illustrative case studies, namely, adding risk-awareness and autonomic routing resilience to the OSPF routing protocol.

INTRODUCTION

To our days, networked systems, like business intranets, Web systems, cloud computing facilities, or the Internet itself, have reached a point where they are no longer just playing grounds for hackers, early adopters, network researchers, and other enthusiasts, but fundamental and omnipresent information infrastructures, indispensable for carrying on our everyday life. However, recently this ever-growing information infrastructure has become quite a challenge to operate efficiently and cost-effectively, while also ensuring that the services delivered meet the quality requirements of the users.

Some believe that it is the growing complexity, stemming from increasing host heterogeneity, mobility and diversity, that causes the recent boost in network management expenditures experimented by operators. Others believe that it is the sheer size of contemporary networks, the need for frequent system deployments, and hardware and software instabilities, that seem today to overwhelm network management staffs and skyrocket operational spending. And still others believe that the real root of the increasing burden is the changing landscape of killer applications and shifting user demands, from email and Web to peer-to-peer and real-time multimedia, all presenting unpredictable, wildly varying workload and unique quality of service requirements to the network. Whoever turns out to be right, one thing is certainly true: together, these issues make it really difficult for human operators, however skilled, to install, deploy, maintain and troubleshoot, that is, to overlook, the essential network infrastructure.

Instead of wasting expensive human resources to deal with everyday network management jobs, many of which can easily be automated, networks themselves should be better put in charge of managing themselves. A Self-managing Network, or Autonomic Network, should be engineered in such a way that traditional network management functions, and the basic network functions they act upon, like routing, forwarding, monitoring, supervision, fault-detection and fault-removal, etc, are made to autonomously respond to system failures, security threats, sudden traffic fluctuations, etc., affecting the reliable and effective operation of the network. These reactive feedback processes then would enable the network to co-operatively achieve and maintain some well-defined network goals, set by the operator. As such, even the traditional network management functions become incorporated into the overall network architecture and diffused into the very fabric of the network. This is in sharp contrast to the conventional network management school of thought, where a distinct management plane is engineered separately from the other functional planes of the network.