Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 95 (2016) 345 – 352

Procedia Computer Science

Complex Adaptive Systems, Publication 6
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2016 - Los Angeles, CA

Towards Assuring Correct Coordination of Multilayer Recovery Using Integrated Ontologies

Joseph Kroculick[a]*

[a]*Winifred Associates, Jim Thorpe PA 18229*

Abstract

Configuring automated recovery in a multilayer virtualized network presents significant architectural issues. The rules that define the interworking strategy between recovery mechanisms must be translated into technology-specific provisioning commands sent to network devices. This provisioning data is typically fragmented across many computing and networking resources. There is also a set of possible device actions that can be performed by a resource, such as forwarding traffic to a protection route, discovering a route to send traffic, adjusting security characteristics of a link, and matching sender and receiver characteristics. Consequently, multiple information models, each of which is specific to a device type and technology layer must be understood, aligned and shared. As a result, an approach is needed to verify and validate that the resulting recovery operations from the input provisioning data achieve end-to-end service requirements.

This paper presents an ontological approach to assure the correct coordination of recovery actions using an integrated knowledge model of multilayer recovery. With an ontological approach, an assurance case that proves correctness of provisioning and resulting network operations can be automated. Such an ontological model identifies the key domain elements and their relationships. Associated statements can then be retrieved from a knowledgebase so that the constraints associated with the network representation and service requirements can be tested.

Keywords: Multilayer Recovery; Provisioning

* Corresponding author. Tel.: +1-215-429-5635; fax: +0-000-000-0000 .
E-mail address: krocjoe@winifredassociates.com

doi:10.1016/j.procs.2016.09.344

1. Introduction to Multilayer Network Provisioning

As networks become virtualized and cloud-aware, it becomes increasingly important to determine whether the resilience requirements of users can be met. If the dimensions of the coordination of multilayer recovery can be aligned, it may be possible to select a particular solution approach that is optimized for a particular situation. An example of matching a solution technique to a resilience requirement is when to use restoration or protection. Restoration that efficiently discovers a new route is useful for unknown traffic demands, while protection is useful for predictable capacity demands since spare network resources are pre-allocated to working resources. For a resilience requirement of 50 ms or less, as an example, protection would be the logical choice [3, 4]. A network architecture for multilayer recovery should provide flexible technology choices to implement multilayer recovery scenarios (e.g., GMPLS RSVP-TE over DWDM with optical layer signaling or ATM recovery over SONET/SDH protection switching). The networking technology continues to evolve and similar functionality that leverages existing operations and maintenance techniques is provided by multiple layers.

Provisioning multiple distributed components to meet end- to-end resilience requirements is a challenging problem. As protocol functionality increasingly runs on network device interfaces, a framework for modeling conflicts will become necessary in order to understand what can prevent a network infrastructure service from operating correctly at one or more technology-specific layers. To achieve high availability, multiple components need to be provisioned so as to manage local behaviors to achieve the desired global behavior. The underlying constraints and assumptions that define this global behavior must be specified to prove correctness of recovery. They may include providing connectivity or continuity of service and associated temporal deadlines.

The contribution of this paper is to demonstrate how assurance-driven design can be applied to verify the correct coordination of multilayer recovery that results from device provisioning. A secondary objective is to show how this process can be automated. The paper then explores what types of information needs to be gathered, collected and transformed to manage available recovery mechanisms that are optimized for specific requirements and situations. An example situation is very fast recovery in the sub-50 ms range. A model of coordination is created from observing how the network infrastructure behaviors during a failure. This model is then related to provisioning commands which are transformed to changes on the model. This paper is organized into two parts: (1) creation of the integrated model that includes network infrastructure, service requirements and dependability requirements and (2) development of an accompanying assurance case that links service requirements to network infrastructure actions.

2. Integration Requirements for Coordination of Multilayer Recovery

Coordination of multilayer recovery presents new challenges towards integrating information from different recovery perspectives. Among these are business processes, service delivery, security, management and control. The knowledge representation of specific device properties, relationships between system elements must be aligned so as to achieve end-to-end service requirements. Achieving alignment between such concepts is difficult because the interpretation of semantics may differ at different levels within and between components. Also, recovery of failed connections has been implemented in technology-dependent ways at different layers. There is no universally accepted representation to represent device semantics. Such a representation is a data model with concepts that are interpreted and related to other concepts. A key requirement for interoperable systems is openness between component interfaces so that the implementation can differ.

2.1. Information Sharing Requirements for Coordination of Multilayer Recovery

Establishing interoperability between communication devices and components participating in automated recovery requires a shared understanding of the effect of global policy on infrastructure and protocols. The effect of policy on resources defines what happens when an event occurs. Essential information needed to manage the coordination of recovery can be exposed to a centralized controller and an inference engine. Effective reasoning over network management information depends on the availability of information that is exposed across system boundaries. As an example, in multilayer networks based on an overlay model of topologies, the recovery