European Sixth Framework Network of Excellence FP6-2004-IST-026854-NoE

Deliverable D5.5

Standardization, interaction and cooperation

The EMANICS Consortium

Caisse des Dépôts et Consignations, CDC, France
Institut National de Recherche en Informatique et Automatique, INRIA, France
University of Twente, UT, The Netherlands
Imperial College, IC, UK
Jacobs University Bremen, JUB, Germany
KTH Royal Institute of Technology, KTH, Sweden
Oslo University College, HIO, Norway
Universitat Politecnica de Catalunya, UPC, Spain
University of Federal Armed Forces Munich, CETIM, Germany
Poznan Supercomputing and Networking Center, PSNC, Poland
University of Zürich, UniZH, Switzerland
Ludwig-Maximilian University Munich, LMU, Germany
University of Surrey, UniS, UK
University of Pitesti, UniP, Romania

For more information on this document or the EMANICS Project, please contact:

Dr. Olivier Festor
Technopole de Nancy-Brabois - Campus scientifique
615, rue de Jardin Botanique - B.P. 101
F-54600 Villers Les Nancy Cedex
France
Phone: +33 383 59 30 66
Fax: +33 383 41 30 79
E-mail: <olivier.festor@loria.fr>

Document Control

Title:	Standardization, interaction and cooperation
Type:	Public
Editor(s):	Aiko Pras
E-mail:	a.pras@utwente.nl
Author(s):	WP5 Partners
Doc ID:	D5.5

AMENDMENT HISTORY

Version	Date	Author	Description/Comments
0.1	2009-09-08	H. M. Tran, J. Schönwälder	Initial version of a LaTeX template and added the NETCONF testing paper
0.2	2009-12-02	Giovane Moura	Executive summary
0.3	2009-12-04	Giovane Moura	Standardization
0.4	2009-12-17	Giovane Moura	Pre-final version
1.0	2009-12-23	Giovane Moura	Final Version

Contents

1 Executive Summary

This document is the final report of the activity undertaken in work-package 5 for training, standardization and technology transfer in the area of device, network and service management. The document covers the last full 12 months (36-48) of the EMANICS project. For the other months, please refer to the previous deliverables.

In the last phase of EMANICS, the objectives of this WP are:

- to foster active participation of EMANICS members in standardization activities (IETF, IRTF),
- to establish and maintain interactions with industry, and
- to maintain and extend cooperation with other networks and projects (within Europe and worldwide).

The most important achievement of WP5 is its contribution to Internet standardization. In this six months period, EMANICS partners contributed to 3 Request for Comments (RFCs) and 46 Internet-Drafts.

EMANICS partners have had many bilateral interactions with industry, such as meeting with Tail-f Systems in Stockholm and Nokia Siemens in Bremen concerning collaborations related to YANG data modeling language. Moreover, and multiple forms of cooperation with related EU projects, such as Euro-FGI, AGAVE project and the COST IS605 and TMA actions. EMANICS is also very active in running the key events and in organizing the top publications in our area.

Finally, EMANICS helped organizing parts of several EU Future Internet activities, such as in the FIA public events in 2009 (such as Prague and Stockholm).

2 Introduction

The title of work-package 5 is “standardization and technology transfer” for device, network and service management. The objectives of this work-package are:

- to foster active participation of EMANICS members in standardization activities, in particular within the IETF and IRTF,
- to establish and maintain interactions with industry, and
- to maintain and extend cooperation with other networks and projects (within Europe and worldwide)

To reach these objectives, three tasks have been defined:

- T5.1: Standardization,
- T5.2: Interaction with industry,
- T5.3: Cooperation with other networks and projects.

This document is the final report produced after 48 months of the EMANICS project. It shows the activities undertaken within the last 12 months of the last phase of the project. Note that the previous months have been covered in previous deliverables (5.1 - 5.4). In this deliverable, Section 3 discusses standardization, Section 4 discusses the interaction with industry and Section 5 discusses the cooperation with other networks and research projects. Section 6 provides the conclusions. In addition, Appendix A presents the NETCONF interoperability testing paper [1] published at the AIMS 2009 conference.

All meeting minutes, RFCs and Internet-Drafts can be downloaded from the EMANICS, IETF and NMRG websites; to keep the size of this deliverable reasonable, these have not been attached as annex.

3 Standardization

In the last twelve months of the EMANICS project several partners contributed to the IETF standardization process. This chapter starts with summarizing the WP5 description, as contained in the JPA. Section 3.2 discusses the EMANICS contributions to the IETF standardization process.

3.1 Description in JPA

An important goal of this NoE is to monitor and influence international standardization activities relevant to network management. Such activities take place within the IETF, IRTF, IAB, DMTF, TMF, ITU, W3C, OMG, OASIS and GGF. This work-package will actively sponsor efforts that strengthen the European presence and enhance the influence of European research on future international standards in this area. An explicit objective of EMANICS is to play a leading role in early standardization activities on Internet management, such as performed within the IRTF Network Management Research Group (NMRG). An outcome of that work will be research papers, internet-drafts and RFCs.

3.2 IETF

This section discusses the EMANICS contributions to the IETF standardization process. Section 3.2.1 gives an overview of the main IETF Working Groups to which contributions have been made; some of the text within that section is copied from the IETF WG pages (and was also already included in previous deliverables). Section 3.2.2 mentions the IETF meetings that have been attended and Section 3.2.3 lists the Internet-Drafts and RFCs to which contributions have been made.

3.2.1 Working Groups

EMANICS partners have contributed to several IETF WG, as well as a design team that most likely will become an IETF WG.

The remainder of this section will discuss the most important WGs / design teams EMANICS contributed too:

- Integrated Security Model for SNMP (ISMS)
- Network Configuration (NETCONF)
- NETCONF Data Modeling Language (NETMOD)
- Next Steps in Signaling (NSIS)
- Congestion and Pre-Congestion Notification (PCN)
- Congestion Exposure (CONEX)

In addition, Jürgen Schönwälder (JUB) is member of the IETF MIB Doctors and the IETF Security Directorate.

ISMS

The *Integrated Security Model for SNMP* (ISMS) WG is chaired by Jürgen Schönwälder (JUB). The goal of the ISMS working group is to develop a new security model for SNMP that integrates with widely deployed user and key management systems, as a supplement to the USM security model. For this integration the working group will define a standard method for mapping from AAA-provisioned authorization parameter(s) to corresponding SNMP parameters.

In order to leverage the authentication information already accessible at managed devices, the new security model will use the SSH protocol for message protection, and RADIUS for AAA-provisioned user authentication and authorization. However, the integration of a transport mapping security model into the SNMPv3 architecture should be defined such that it is open to support potential alternative transport mappings to protocols such as BEEP and TLS. The ISMS WG covers the following work items [2, 3]:

- Specify an architectural extension that describes how transport mapping security models (TMSMs) fit into the SNMPv3 architecture.
- Specify an architectural extension that describes how to perform a mapping from AAA- provisioned user-authentication and authorization parameter(s) to securityName and other corresponding SNMP parameters.
- Specify a mapping from RADIUS-provisioned authentication and authorization parameter(s) to securityName and other corresponding SNMP parameters.
- Specify a mapping from locally-provisioned authentication and authorization parameter(s) to securityName and other corresponding SNMP parameters.
- Define how to use SSH between the two SNMP engines
- Specify the SSH security model for SNMP.

NETCONF

The goal of the NETCONF working group is to produce a protocol suitable for network configuration, with the following characteristics [4]:

- Provides retrieval mechanisms which can differentiate between configuration data and non-configuration data.
- Is extensible enough that vendors will provide access to all configuration data on the device using a single protocol.
- Has a programmatic interface.

- Uses a textual data representation, that can be easily manipulated using non specialized text manipulation tools.
- Supports integration with existing user authentication methods.
- Supports integration with existing configuration database systems.
- Supports network wide configuration transactions (with features such as locking and rollback capability).
- Is as transport-independent as possible.

The NETCONF protocol uses XML for data encoding purposes, because XML is a widely deployed standard which is supported by a large number of applications. XML also supports hierarchical data structures. The NETCONF protocol should be independent of the data definition language and data models used to describe configuration and state data. It should be possible to transport the NETCONF protocol using several different protocols. The group will select at least one suitable transport mechanism, and define a mapping for the selected protocol(s).

NETMOD

YANG is a data modeling language used to model configuration and state data manipulated by the NETCONF protocol, NETCONF remote procedure calls, and NETCONF notifications. Today, the NETCONF protocol RFC 4741 lacks a standardized way to create data models. Instead, vendors are forced to use proprietary solutions. In order for NETCONF to be a interoperable protocol, models must be defined in a vendor-neutral way. YANG provides the language and rules for defining such models for use with NETCONF [5]. The YANG language is being standardized by the NETMOD working group.

NSIS

The *Next Steps in Signaling Working Group* is responsible for standardizing an IP signaling protocol with QoS signaling as the first use case. The working group concentrates on a two-layer signaling paradigm. The intention is to re-use, where appropriate, the protocol mechanisms of RSVP, while at the same time simplifying it and applying a more general signaling model [6].

The NSIS WG develops a transport layer signaling protocol for the transport of upper layer signaling. In order to support a toolbox or building block approach, a two-layer model will be used to separate the transport of the signaling from the application signaling. This allows for a more general signaling protocol to be developed to support signaling for different services or resources, such as NAT & firewall traversal and QoS resources. The initial NSIS application will be an optimized RSVP QoS signaling protocol. The second application will be a middle box traversal protocol. An informational document detailing how Differentiated Services can be signaled with the QoS Signaling protocol will be made.

Security is a very important concern for NSIS. The working group will study and analyze the threats and security requirements for signaling. Compatibility with authentication and authorization mechanisms such as those of Diameter, COPS for RSVP and RSVP Session Authorization will be addressed.

PCN

The Congestion and Pre-Congestion Notification (PCN) working group develops mechanisms to protect the quality-of-service of established inelastic flows within a DiffServ domain when congestion is imminent or existing. These mechanisms operate at the domain-boundary, based on aggregated congestion and pre-congestion information from within the domain. The focus of the WG is on developing standards for the marking behavior of the interior nodes and the encoding and transport of the congestion information. To allow for future extensions to the mechanisms and their application to new deployment scenarios, they are logically separated into several components, namely, encoding and transport along forward path from marker to egress, metering of congestion information at the egress, and transport of congestion information back to the controlling ingress. Reaction mechanisms at the boundary consist of flow admission and flow termination. Although designed to work together, flow admission and flow termination are independent mechanisms, and the use of one does not require or prevent the use of the other. The WG may produce a small number of informational documents that describe how specific quality-of-service policies for a domain can be implemented using these two mechanisms [7].

ALTO

The IETF ALTO Working Group [8] takes a different approach in dealing with congestion generated by peer-to-peer (P2P) applications, which is believed to be significant. It benenefits from the redundancy in resource availability present in P2P systems, by designing a protocol between P2P applications and Internet providers to guide peer selection. It is expected that peers, when prioritizing connections to other peers in the same provider, will be able to enjoy less congestion and, therefore, better quality of experience. The provider also has an incentive to deploy such a solution, since intradomain traffic does not have transit costs.

CONEX

The newly formed IETF CONEX Working Group is developing means of enabling congestion to be exposed along the forwarding path of the Internet. By revealing expected congestion in the IP header of every packet, congestion exposure provides a generic network capability which allows greater freedom for resource allocation. This information may in turn be used for many purposes, including congestion policing, accountability and inter-domain SLAs. It also opens new approaches to QoS and traffic engineering.

The potential implications for traffic management in general, and economic traffic management in particular, are significant. Once ISPs can see rest-of-path congestion, they

can accurately and precisely discourage users from causing large volumes of congestion, they can discourage other networks from allowing their users to cause congestion, and they can more meaningfully differentiate between the qualities of services offered from potential connectivity partners. Congestion exposure additionally provides a framework for scalable, incrementally deployable congestion pricing.

3.2.2 IETF Meetings

In Phase 2, the following IETF meetings took place:

- 75th IETF Meeting, July 2009; Stockholm, Sweden,
- 76th IETF Meeting, November 2009; Hiroshima, Japan.

The 75th IETF meeting, which was held in July 2009 in Stockholm, was attended by Georgios Karagiannis (UT), Jürgen Schönwälder (JUB) and Fabio Hecht (UniZH).

The 76th IETF meeting was organized between November 8-13, 2009, in Hishoshima, Japan. One EMANICS partners participated: Joao Araujo (UCL).

An overview of EMANICS participation to IETF meetings is provided in Table 1.

Table 1: EMANICS participation to IETF meetings

Meeting	**Name**	**Organization**	**Role**
75th IETF	Georgios Karagiannis	UT	Editor of Internet-Drafts
75th IETF	Jürgen Schönwälder	JUB	Working Group Chair Editor of Internet-Drafts
75th IETF	Fabio Hecht	UniZH	Contributor to Internet-Drafts
76th IETF	Joao Araujo	UCL	Contributor to Internet-Drafts

3.2.3 Publications

In the last 12 months of the EMANICS project, 3 RFCs and 46 Internet-Drafts were co-authored by EMANICS partners. These documents fall into the following categories:

- Transport Subsystem for SNMP
- Mapping SNMP Notifications to SYSLOG Messages
- Load Control PCN
- Common YANG Data Types
- DiffServ Resource Management

- SNMP optimizations for 6LoWPAN
- NETCONF
- COPS Usage for Policy Provisioning
- Application-Layer Traffic Optimization (ALTO)
- Session Initiation Protocol (SIP)
- Congestion Exposure (CONEX)

A short description of these drafts, which is copied from their introductory sections, can be found in the next subsections.

TRANSPORT SUBSYSTEM FOR SNMP

For the reporting period, the following RFC was produced:

- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), RFC 5590, June 2009

The following versions of the Internet-Draft "*Transport Subsystem for the Simple Network Management Protocol (SNMP)*" were produced by EMANICS partners in this phase of the EMANICS project:

- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-16, February 2009
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-17, April 2009
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-18, May 2009

This document describes a Transport Subsystem, extending the Simple Network Management Protocol (SNMP) architecture defined in RFC 3411. It describes a subsystem to contain transport models, comparable to other subsystems in the RFC3411 architecture. As work is being done to expand the transport to include secure transports such as SSH and TLS, using a subsystem will enable consistent design and modularity of such transport models. This document identifies and discusses some key aspects that need to be considered for any transport model for SNMP. It also defines a portion of the Management Information Base (MIB) for managing models in the Transport Subsystem.

MAPPING SNMP NOTIFICATIONS TO SYSLOG MESSAGES

For this phase of the project, two RFCs were produced:

- **J. Schönwälder, A. Clemm, A. Karmakar**: Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications. RFC 5676, October 2009.
- **V. Marinov, J. Schönwälder**: Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages. RFC 5675, October 2009.

Moreover, the EMANICS partners produced the following Internet-Drafts:

- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-00.txt, February 2009
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-01.txt, March 2009
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-02.txt, March 2009
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-03.txt, May 2009
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-04.txt, August 2009
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-ietf-opsawg-syslog-snmp-05.txt, August 2009
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-00, February 2009.
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-01, February 2009.
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-02, March 2009.

- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-03, May 2009.
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-04, May 2009.
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications,draft-ietf-opsawg-syslog-msg-mib-05, August 2009.
- **J. Schönwälder** : Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications, draft-ietf-opsawg-syslog-msg-mib-06, August 2009.

These drafts define mappings from Simple Network Management Protocol (SNMP) notifications to SYSLOG notifications and vice versa.

LOAD CONTROL PCN

The following Internet-Drafts have been produced for the IETF Congestion and Pre-congestion notification (PCN) working group:

- A. Charny, F. Huang, **G. Karagiannis**, M. Menth, T. Taylor: PCN Boundary Node Behaviour for the Controlled Load (CL) Mode of Operation, draft-ietf-pcn-cl-edge-behaviour-00, July 2009.
- A. Charny, F. Huang, **G. Karagiannis**, M. Menth, T. Taylor: PCN Boundary Node Behaviour for the Controlled Load (CL) Mode of Operation, draft-ietf-pcn-cl-edge-behaviour-01, October 2009.
- A. Charny, F. Huang, **G. Karagiannis**, M. Menth, T. Taylor: PCN Boundary Node Behaviour for the Single Marking (SM) Mode of Operation, draft-ietf-pcn-sm-edge-behaviour-00, July 2009.
- A. Charny, F. Huang, **G. Karagiannis**, M. Menth, T. Taylor: PCN Boundary Node Behaviour for the Single Marking (SM) Mode of Operation, draft-ietf-pcn-sm-edge-behaviour-01, October 2009.
- K. Chan, **G. Karagiannis**, T. Moncaster, P. Eardley, B. Briscoe: Pre-Congestion Notification Encoding Comparison , draft-ietf-pcn-encoding-comparison-00, July 2009.
- K. Chan, **G. Karagiannis**, T. Moncaster, P. Eardley, B. Briscoe: Pre-Congestion Notification Encoding Comparison , draft-ietf-pcn-encoding-comparison-01, October 2009.
- **G. Karagiannis**, T. Taylor, K. Chan, M. Menth: Requirements for Signaling of (Pre-) Congestion Information in a DiffServ Domain, draft-karagiannis-pcn-signaling-requirements-00, October 2009.

- K. Chan, **G. Karagiannis**, T. Moncaster, M. Menth, P. Eardley, B. Briscoe: Pre-Congestion Notification Encoding Comparison, draft-chan-pcn-encoding-comparison-04, March 2009.

There is an increased interest of simple and scalable resource provisioning solution for Diffserv network. The PCN addresses the following issues:

- Admission control for real time data flows in stateless Diffserv Domains.
- Flow termination: Termination of flows in case of exceptional events, such as severe congestion after re-routing.

Common Yang Data Types

The following Internet-Drafts on common YANG data types have been produced by EMAN-ICS partners:

- **J. Schönwälder**: Common YANG Data Types, draft-ietf-netmod-yang-types-02, March 2009
- **J. Schönwälder**: Common YANG Data Types, draft-ietf-netmod-yang-types-03, May 2009
- **J. Schönwälder**: Common YANG Data Types, draft-ietf-netmod-yang-types-04, October 2009
- **J. Schönwälder**: Common YANG Data Types, draft-ietf-netmod-yang-types-05, December 2009
- **J. Schönwälder**: Translation of SMIv2 MIB Modules to YANG Modules, January 2009

YANG is a data modeling language used to model configuration and state data manipulated by the NETCONF protocol. The YANG language supports a small set of built-in data types and provides mechanisms to derive other types from the built-in types.

DiffServ Resource Management

Within IETF NSIS working group, the following Internet-Drafts have been produced in this phase:

- A. Bader, L. Westberg, **G. Karagiannis**, C. Kappler, T. Phelan: RMD-QOSM - The Resource Management in Diffserv QOS Model, draft-ietf-nsis-rmd-14, March 2009
- A. Bader, L. Westberg, **G. Karagiannis**, C. Kappler, T. Phelan: RMD-QOSM - The Resource Management in Diffserv QOS Model, draft-ietf-nsis-rmd-15, July 2009

SNMP Optimizations for 6LoWPAN

The following Internet-Drafts have been produced in this phase:

- H. Mukhtar, S. Joo, **J. Schönwälder**: SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-00, March 2009
- H. Mukhtar, S. Joo, **J. Schönwälder**: SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-01, April 2009
- H. Mukhtar, S. Joo, **J. Schönwälder**, K. Kim: SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-02, October 2009

The Simple Network Management Protocol (SNMP) is a widely deployed application protocol for network management and data retrieval. In this document we describe the applicability of SNMP for 6LoWPANs. We discuss the implementation considerations of SNMP Agent and SNMP Manager followed by the deployment considerations of the SNMP protocol. Our discussion also covers the applicability of MIB modules for 6LoWPAN devices.

NETCONF

The following Internet-Draft have been produced in this phase:

- R. Enns, M. Bjorklund, **J. Schönwälder**: NETCONF Configuration Protocol, draft-ietf-netconf-4741bis-00, March 2009
- R. Enns, M. Bjorklund, **J. Schönwälder**, A. Bierman: NETCONF Configuration Protocol, draft-ietf-netconf-4741bis-01, July 2009

The Network Configuration Protocol (NETCONF) defined in this document provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages. The NETCONF protocol operations are realized on top of a simple Remote Procedure Call (RPC) layer.

COPS Usage for Policy Provisioning (COPS-PR)

The following Internet-Draft has been produced in this phase:

- **J. Schönwälder**: Reclassification of COPS-PR and SPPI to Historic, draft-schoenw-opsawg-copspr-historic-00, September 2009

This memo reclassifies RFC 3084, COPS Usage for Policy Provisioning, and RFC 3159, Structure of Policy Provisioning Information, to Historic status. This memo obsoletes RFC 3084, RFC 3159, RFC 3317, RFC 3318, and RFC 3571.

Application-Layer Traffic Optimization (ALTO)

The following Internet-Draft has been produced in this phase:

- **P. Racz**, Z. Despotovic: An ALTO Service based on BGP Routing Information, draft-racz-bgp-based-alto-service-00, June 2009

Session Initiation Protocol (SIP)

The following Internet-Drafts have been produced in this phase:

- V. Gurbani, E. Burger, T. Anjali, **H. Abdelnur**, **O. Festor**: The Common Log File (CLF) format for the Session Initiation Protocol , draft-gurbani-sipping-clf-00, February 2009
- V. Gurbani, E. Burger, T. Anjali, **H. Abdelnur**, **O. Festor**: The Common Log File (CLF) format for the Session Initiation Protocol , draft-gurbani-sipping-clf-01, March 2009
- R. State, **O. Festor**, **H. Abdelnur**, V. Pascual, J. Kuthan, R. Coeffic, J. Janak, J. Floroiu: SIP digest authentication relay attack, draft-state-sip-relay-attack-00, March 2009

Congestion Exposure (CONEX)

The following Internet-Drafts have been produced in this phase:

- L. Burness, M. Menth, **J. Araujo** , S. Blake, R. Woundy: The Need for Congestion Exposure in the Internet, draft-moncaster-congestion-exposure-problem-00, September 2009
- L. Krug, M. Menth, **J. Araujo** , S. Blake, R. Woundy: The Need for Congestion Exposure in the Internet, draft-moncaster-congestion-exposure-problem-01, October 2009
- L. Krug, M. Menth, **J. Araujo** , S. Blake, R. Woundy: The Need for Congestion Exposure in the Internet, draft-moncaster-congestion-exposure-problem-02, October 2009
- L. Krug, M. Menth, **J. Araujo** , S. Blake, R. Woundy: The Need for Congestion Exposure in the Internet, draft-moncaster-congestion-exposure-problem-03, October 2009

This memo sets out the motivations for congestion exposure and introduces a strawman protocol designed to achieve congestion exposure. This document was additionally significant in garnering support for the creation of a new working group, which would take form in IETF 76.

4 Interaction with industry

One of the tasks of this work-package is to interact with industry to collect network management requirements and to transfer knowledge. Interaction is organized in different ways:

- Emanics partners interact with industry within the context of the IETF
- Emanics partners interact with industry on a bilareral basis
- Emanics partners interact with industry when organizing workshops
- Emanics partners create Podcast to transfer knowledge regarding main scientific events to industry

4.1 Interaction with industry within the context of IETF

EMANICS partners have been very active in the IETF WGs, writing on Internet-Drafts and RFCs with different industry parterns. EMANICS partners (Jürgen Schönwälder (JUB), Georgios Karagiannis (UT), H. Abdelnur (INRIA), Olivier Festor (INRIA), V. Marinov (JUB), and Joao Araujo (UCL)) have collaborated with the following industry partners:

- Alcatel-Lucent
- Bell Laboratories
- British Telecom
- Cisco Systems
- Cisco Systems India Pvt Ltd
- Comcast
- DOCOMO Communications Laboratories Europe GmbH
- Ericsson
- Extreme Networks
- Huawei Technologies
- Juniper Networks
- Siemens
- Sonus
- Tail-f Systems
- Tekelec / iptel.org

4.2 Bilateral collaboration

All Emanics partners interact on a bilateral basis with industry to discuss research issues related to EMANICS. These interactions take usually place at the institutes of the partners, or at the premises of one of the industry partners. Some examples of companies Emanics partners interacted with, are presented in Table 2:

4.3 Interaction with industry organizing workhops

In this reporting period the EMANICS partners have organized two wokshops in conjunction with Cisco Systems.

The first one was the 1st EMANICS Workshop on Network Security, held on October 7th in Bremen, Germany. Jürgen Schönwälder (JUB) and Olivier Festor (INRIA) organized this workshop in JUB campus. The goal of the workshop was to provide a forum for researchers and network operators to exchange new ideas to secure networks and novel techniques to analyze security properties and security incidents in operational networks.

The other workshop organized in the report period was the 2nd EMANICS Workshop on Netflow/IPFIX Usage. Ramin Sadre (UT) and Aiko Pras (UT) were the organizes of the workshop, which took place at Bremen, Germany, in the JUB campus. The workshop addressed new applications of flows in the above mentioned and other areas, operator experiences, recent developments, as well as related activities such as flow storage and visualization.

4.4 Other forms of interaction - Podcasts

In addition to face to face meetings, EMANICS partners have also created a number of Podcasts in which the results of EMANICS research, tutorials, as well as keynotes at the world leading conferences in our field are being presented to industry and academia. The creation of these Podcast has been discussed within deliverables of WP4, and are available (amongst others) via iTunes. Below a short overview of the Podcasts that have been created in the previous phase.

IM 2009 OPENING SESSION, KEYNOTES, EXPERT PANEL AND CLOSING

The following podcasts have been recorded during theThe 11th IFIP/IEEE International Symposium on Integrated Network Management (IM 2009), which was held 1 - 5 June 2009, Long Island, New York, USA :

- Opening Session
- Keynote by Chuck Kalmanek, Vice President, AT&T, Internet and Network Systems Research, AT&T Labs

Table 2: Bilateral collaboration - Overview

EMANICS	Other Partner	Topic
HIO	Elsevier	Handbook of Network System Administration
HIO	Norsk Hydro	cfengine presentation
HIO	RIPE	Automation by cfengine
HIO	Snow	IT management challenges for the next decade
INRIA	Alcatel/Bell labs	Autonomic management
INRIA	Cisco	IPv6, Fuzzing
JUB	Amazon S3 Group	Software
JUB	BITKOM / Bundesumweltamt	Green information technology
JUB	Cisco	NETCONF, NETMOD & YANG
JUB	IsarNet	Management software
JUB	Juniper	NETCONF, NETMOD & YANG
JUB	Tail-f	NETCONF, NETMOD & YANG
JUB	DCOMBUS	SNMP technology
JUB	Nokia Siemens Networks	NETCONF, NETMOD & YANG
KTH	Cisco	Distributed monitoring
KTH	Ericsson Research, Stockholm	Auto-configuration
KTH	IBM Research	Autonomic management
LMU	DFN-Cert	Intrusion Detection Systems
LMU	Zimory	Public/Private Clouds
LMU	Platform Computing	Cloud Computing, Cluster Batch Scheduler
LMU	IBM	Virtualization, Virtual Organization Management
LMU	Stonesoft	Intrusion Detection Systems/Firewalls
LMU	NEC Lab Europe	Equinox, Cloud Management
LMU	EclipseSource	Equinox, Cloud Management
LMU	Telefonica	Equinox, Cloud Management
LMU	Deutsche Telekom	Application Virtualization
LMU	Lawrence Livermore National Laboratory	Scalable, parallel debugging
LMU	Lawrence Berkeley National Laboratory	Scalable, parallel debugging
LMU	Joint Research Centre Ispra	MPI
LMU	Atos	Open Grid Forum Europe, Grid Standards
LMU	Intellect	Open Grid Forum Europe, Grid Standards
LMU	Sun	Open Cloud Computing Interface
LMU	Fujitsu	Virtual Infrastructure Management
LMU	IT Service Management Forum	IT Service Management Education
PSNC	Cisco	Network measurements
PSNC	Geant	Network measurements
PSNC	Juniper	Network management
UCL	BT	Network management
UCL	Orange Lab UK	Network management
UCL	QinetiQ	Network management
UCL	Thales	Network management
UniBW	Cisco	IT management
UniBW	Federal Office for Information Security	Security
UniBW	General Electrics	Identity management
UniBW	German Federal Criminal Police	Security
UniBW	Giesike & Devrint	Identity management
UniBW	Hella KGaA	IT management
UniBW	Hueck & Co	IT management
UniBW	Rhode und Schwarz	Sensor management
UniBW	Secunet	Security management
UniZH	Cisco	Flow analysis
UniZH	DoCoMo	Accounting
UniZH	SWITCH	Distributed Netflow analysis
UPC	Ginkgo networks	Autonomic management
UPC	Hitachi	Autonomic management
UPC	Telefonica	Autonomic management
UPC	Ucopia Ltd	Autonomic management
UT	Brazilian Research Network	Future Internet
UT	KPMG	Network security
UT	NFI	Trace collection and analysis
UT	Pine	Trace anonymization
UT	Quarantinenet	SPAM detection
UT	Telematics Institute	Self-management of sensor networks
UT	TNO	Management of sensor networks
UT	Witteven & Bos	Intrusion detection in SCADA networks

- Keynote by Yechiam Yemini, Professor & Director, Distributed Computing Lab, Columbia University
- Keynote by Adam Drobot, CTO and President, Advanced Technology Solutions, Telcordia
- Keynote by Owen Brown, Program Manager-F6: Fractionated Spacecraft Program, Defense Advanced Research Projects Agency
- Keynote by Larry Bernstein, Distinguished Service Professor, Stevens Institute of Technology and former AT&T Executive
- Keynote by Alan Ganek, CTO and VP of Strategy and Technology, Software Group, IBM
- Distinguished expert panel on "Making Management Matters Matter", with speeches by:
  - Alexander Clemm, Cisco (panel moderator)
  - John Strassner, Waterford Institute of Technology, Ireland
  - Alan Ganek, IBM
  - Joseph L. Hellerstein, Google
  - Larry Bernstein, Stevens Institute of Technology, USA
  - George Pavlou, University College London, UK

IFIP/ACM AIMS 2008

The following podcasts have been recorded during the 2nd International Conference on Autonomous Infrastructure, Management and Security (AIMS 2008), which was held 1st-3rd July 2008, in Bremen, Germany:

- Opening Session by Jürgen Schönwälder (JUB)
- Keynote by Simon Leinen, Swiss Education and Research Network (SWITCH)
- PhD Session 1 and Main Track Session 2

NOMS 2008 OPENING SESSION, KEYNOTES AND EXPERT PANEL

The following podcasts have been recorded during the 11th IEEE/IFIP Network Operations and Management Symposium (NOMS 2008), which was held 7-11 April 2008, in Salvador, Bahia, Brazil:

- Opening Session
- Keynote by Roberto Saracco, Future Centre - Telecom Italia Lab (TILAB)

- Keynote by Prof. Ian F. Akyildiz, School of Electrical and Computer Engineering at Georgia Institute of Technology
- Keynote by Dr. Luiz Fernando Gomes Soares, TeleMidia Lab., Catholic University of Rio de Janeiro (PUC-Rio)
- Distinguished expert panel on “Ubiquitous Networks and Services: What Are the Real New Challenges Ahead?”, with speeches by:
  - George Pavlou, University College London, UK (Chair)
  - Ian Akyildiz, Georgia Tech, USA
  - Bruno Albuquerque, Google, Brazil
  - Morris Sloman, Imperial College, UK
  - Rolf Stadler, KTH Royal Institute of Technology, Sweden

5 Cooperation with other networks and projects

5.1 Description in JPA

This work-package is also responsible for the identification and liaisons establishment with professional organizations, complementary NoEs, and national and European projects in the area of network management. Information exchange will be in two directions: projects in the area of EMANICS may take advantage of the knowledge that is available within EMANICS, and EMANICS will learn from these projects new requirements and results.

5.1.1 COST-TMA Workshop in Aachen, Germany

TMA'09 was the first international workshop on traffic monitoring and analysis, sponsored by the IFIP Technical Committee on Communication Systems (TC 6). It was organized on 11 May 2009, as a full-day event on the first day of the IFIP conference Networking 2009 which will be held 11-15 May 2009, in Aachen, Germany. Aiko Pras (UT) worked there as Technical Programme Committee Co-Chair.

5.1.2 COST-TMA Workshop in Barcelona, Spain

The 5th TMA Action meeting was held in Barcelona on 5-6 October 2009 at UPC. Giovane Moura (UT) and Idilio Drago (UT) attended to these two days of workshop, in which several technical sessions took place as well as a keynotes speech and report on short term missions.

5.1.3 Dagstuhl Seminar on Management of the Future Internet

On January 27-30 Emanics members (Olivier Festor (INRIA), Aiko Pras (UT) and Burkhard Stiller (UniZH)) organized the Dagstuhl Seminar on Management of the Future Internet

The main objective of this Dagstuhl Seminar was to work together to structure research and development in the field of network management with the aim of determining the key functionality of the next generation management framework for the Future Internet. Thus, this resulting seminar aimed at:

- Collecting and synthesizing requirements towards a management framework from all application domains and network infrastructures
- Developing a possible consensus on novel paradigms and models for meeting the requirements of integrated service provisioning in the Future Internet
- Structuring and integrating the research areas in network and service management to strengthen the Future Internet innovation in this discipline

In a nutshell, the “Management of the Future Internet” Seminar shall help researchers and network operators to develop further framework mechanisms and design respective protocols and approaches for services from network operations and network business perspectives.

5.1.4 Dagstuhl Seminar on Visualization and Monitoring of Network Traffic

On May 17-20 Emanics members (Aiko Pras (UT) and Jürgen Schönwälder (JUB)) organized the Dagstuhl Seminar on Visualization and Monitoring of Network Traffic.

The aim of the seminar was to bring together for the first time people from the networking community and the visualization community in order to explore common grounds in capturing and visualizing network behaviour and to exchange upcoming requirements and novel techniques. The seminar also target network operators running large IP networks as well as companies building software products for network monitoring and visualization.

5.1.5 4th GI/ITG KuVS Workshop on The Future Internet and 2nd Workshop on Economic Traffic Management

On November 9th and 10th Burkhard Stiller (UniZH) helped to organize the 4th GI/ITG KuVS Workshop on The Future Internet and 2nd Workshop on Economic Traffic Management. The topics ”Future Internet” and ”Economic Traffic Management” have seen a wide attention of networkers and economists. Triggered by FIND/GENI activities of the NSF both the EU in the 7th Framework as well as the German BMBF in its IT strategy for 2020 have addressed this topic. Although many discussions took place in such a research environment, the application of new ideas into test-beds and possibly industry shows an emerging demand today. These two combined workshops and their topics do cover the areas of technology, infrastructure, economic theory, and operations. Furthermore, methodological and architectural topics range from the incremental improvement of today’s Internet to a complete new start (clean slate approach).

The two main goals of the 4th GI/ITG Kommunikation und Verteilte Systeme (KuVS) Workshop on Future Internet and the 2nd Workshop on Economic Traffic Management (supported by the FP6 NoE EMANICS and the FP7 STREP SmoothIT) were to give scientists, researchers, and operators the opportunity to present and discuss their ideas in these areas as well as strengthening the cooperation in the field of an economic-technology interplay.

5.1.6 Future Internet Assembly: Prague

On May 12nd and 13rd several EMANICS partners joined the Future Internet Assembly in Prague, Czech Republic. Aiko Pras (UT), Joan Serrat (UPC), George Pavlou (UCL), Alex Gallis (UCL), David Hausheer (UniZh) and Olivier Festor (INRIA) joined this assembly. One of the key activities at the FIA was MANA, which was led by (amongst others) Alix Gallis.

The Future of the Internet Conference aimed to review the strategic orientations and trends governing the future societal and economic developments of on-line Internet and Mobile societies and to present interesting ideas and projects in this area. Note that EMANICS originally had problems to join the FIA, since it is not an FP7 project.

5.1.7 Future Internet Assembly: Stockholm

On November 23th and 24th several EMANICS partners joined the Future Internet Assembly in Stockholm, Sweden. Joan Serrat (UPC) and George Pavlou (UCL) joined this assembly .Joan Serrat (UPC) has participated in all the public FIA events in 2009 (Prague and Stockholm) as speaker or co-author of presentations or demos and has also contributed with a paper for the next one to be celebrated in Valencia (Spain) in Spring 2010.

The Future Internet Assembly groups 96 projects who subscribed to the Bled Declaration. They agreed to coordinate their R&D activities to foster a strong European footprint on Future Internet. More than Euro 600 million are invested by the participants and by the European Commission to make this happen. FIA mobilises a community of some 300 experts active in shaping the European Future Internet vision

FIA'09 Stockholm broght together about 300 stakeholders in the Future Internet developments from policy makers, industry and academia, coming from mainly from EU member countries and abroad. FIA'09 is now clearly positioned as "the" European Future Internet Research and Innovation conference.

What makes it attractive is the mix of policy makers, industry and academia, debating research and innovation strategies and then best way forward for a stronger European position in Future Internet developments.

6 Conclusions

WP5 is currently structured into three tasks:

- T5.1: Standardization
- T5.2: Interaction with industry
- T5.3: Cooperation with other networks and projects

Within Internet management standardization, EMANICS partners hold strong positions within IETF WGs. In this period, 3 RFCs and 46 Internet-Drafts were (co-)authored by EMANICS partners. The chairs of the IETF-ISMS and the IRTF-NMRG are EMANICS members. EMANICS partners contributed to several IETF WGs, in particular the Integrated Security Model for SNMP (ISMS), Network Configuration (NETCONF), Next Steps in Signaling (NSIS), Congestion and Pre-Congestion Notification (PCN) as well as the YANG design team, which has turned into the new NetMod WG.

EMANICS partners have interacted with industry primarily in the form of many short meeting on a bilateral basis. In addition, most EMANICS partners have interacted with industry at various events, like conferences and workshops (for example within panels). EMANICS partners had multiple forms of cooperation with related EU projects and industries, such as:

- The COST TMA action: Traffic Measurements and Analysis.
- Dagstuhl Seminars on Management of the Future Internet and on Visualization and Monitoring of Network Traffic.
- 4th GI/ITG KuVS Workshop on The Future Internet and 2nd Workshop on Economic Traffic Management
- Future Internet Assemblies in Prague and Stockholm
- The Netflow/IPFIX usage workshop and the Network Security workshop

EMANICS helped organizing parts of several EU Future Internet activities, such as FIA public events in Prague and Stockholm. In addition, they contributed to other Future Internet initiatives, such as the 3D Internet. EMANICS members also took over the chair and co-chair positions of the IFIP WG6.6 and the Policy WG of the ACF. EMANICS members are also very active in running the key events and organizing the top publications in our area. The general conclusion is that WP5 performed well and made very strong contributions to the IETF and IRTF. In addition, Appendix A presents the NETCONF interoperability testing paper [1] published at the AIMS 2009 conference.

7 Abbreviations

AAA	Authentication, Authorization, and Accounting
ACF	Autonomic Communication Forum
BGP	Border Gateway Protocol
COPS	Common Open Policy Service
DiffServ	Differentiated Services
DSOM	Distributed Systems, Operations and Management
HIO	Oslo University College
IETF	Internet Engineering Task Force
INRIA	Institut National de Recherche en Informatique et Automat
IRTF	Internet Research Task Force
ISMS	Integrated Security Model for SNMP
JEMS	Journal and Event Management System
JUB	Jacobs University Bremen
JPA	Joint Programme of Activities
KTH	Royal Institute of Technology
LMU	Ludwig-Maximilian University Munich
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
NETCONF	Network Configuration
NGN	Next Generation Network
NMRG	Network Management Research Group
NOMS	Network Operations and management Symposium
NSIS	Next Steps in Signaling
PDB	Per Domain Behavior
PSNC	Poznan Supercomputing and Networking Center
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RMON	Remote Monitoring
RSVP	Resource Reservation Protocol
SCTP	Stream Control Transmission Protocol
SLA	Service Level Agreements
SLS	Service Level Specifications
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SSH	Secure SHell

TIC	Technologies de l'Information et de la Communication
TLS	Transport Layer Security
TMSM	Transport Mapping Security Model
TSVWG	Transport Area Working Group
UniS	University of Surrey
UniZH	University of Zrich
upc	Universidat Politecnica de Catalunya
UPI	University of Pitesti
UT	University of Twente
VoIP	Voice over IP
WG	Working Group

8 Acknowledgement

This deliverable was made possible due to the large and open help of the WP5 Partners of the EMANICS NoE. Many thanks to all of them.

References

[1] H. M. Tran, I. Tumar, and J. Schönwälder. NETCONF Interoperability Testing. In *Proc. 3rd International Conference on Autonomous Infrastructure, Management and Security (AIMS '09)*, pages 83–94. Springer-Verlag, 2009.

[2] Homepage of the IETF ISMS WG: *http://www.ietf.org/html.charters/isms-charter.html*.

[3] Wiki page of the IETF ISMS WG: *http://www.eecs.iu-bremen.de /wiki/index.php/ISMS_Working_Group*.

[4] Homepage of the IETF NETCONF WG : *http://www.ietf.org/html.charters/ netconfcharter.html*.

[5] Homepage of the YANG design team : *http://www.yang-central.org/*.

[6] Homepage of the IETF NSIS WG: *http://www.ietf.org/html.charters/nsis-charter.html*.

[7] Homepage of the IETF PCN WG: *http://www.ietf.org/html.charters/pcn-charter.html*.

[8] Homepage of the IETF ALTO WG : *http://tools.ietf.org/wg/alto/charters*.

[9] D. Harrington and J. Schoenwaelder. Transport Subsystem for the Simple Network Management Protocol (SNMP). RFC 5590 (Proposed Standard), June 2009.

[10] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-16, February 2009.

[11] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-17, April 2009.

[12] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-18, May 2009.

[13] J. Schoenwaelder, A. Clemm, and A. Karmakar. Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications. RFC 5676 (Proposed Standard), October 2009.

[14] V. Marinov and J. Schoenwaelder. Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages. RFC 5675 (Proposed Standard), October 2009.

[15] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-00, February 2009.

[16] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-01, March 2009.

[17] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-02, March 2009.

[18] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-03, May 2009.

[19] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-04, August 2009.

[20] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-ietf-opsawg-syslog-snmp-05, August 2009.

[21] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-schoenw-syslog-msg-mib-00, April 2008.

[22] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-schoenw-syslog-msg-mib-01, November 2008.

[23] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-schoenw-syslog-msg-mib-02, March 2009.

[24] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-schoenw-syslog-msg-mib-03, May 2009.

[25] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-schoenw-syslog-msg-mib-04, May 2009.

[26] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-ietf-opsawg-syslog-msg-mib-05, August 2009.

[27] J. Schönwälder. *Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications*, draft-ietf-opsawg-syslog-msg-mib-06, August 2009.

[28] A. Charny, F. Huang, G. Karagiannis, M. Menth, and T. Taylor. PCN Boundary Node Behaviour for the Controlled Load (CL) Mode of Operation,draft-ietf-pcn-cl-edge-behaviour-00, July 2009.

[29] A. Charny, F. Huang, G. Karagiannis, M. Menth, and T. Taylor. PCN Boundary Node Behaviour for the Controlled Load (CL) Mode of Operation,draft-ietf-pcn-cl-edge-behaviour-01, October 2009.

[30] A. Charny, J Zhang, G. Karagiannis, M. Menth, and T. Taylor. PCN Boundary Node Behaviour for the Single Marking (SM) Mode of Operation, draft-ietf-pcn-sm-edge-behaviour-00, July 2009.

[31] A. Charny, J Zhang, G. Karagiannis, M. Menth, and T. Taylor. PCN Boundary Node Behaviour for the Single Marking (SM) Mode of Operation, draft-ietf-pcn-sm-edge-behaviour-01, August 2009.

[32] K. Chan, G. Karagiannis, M. Menth, P. Eardley, and B. Briscoe. Pre-Congestion Notification Encoding Comparison, draft-ietf-pcn-encoding-comparison-00, July 2009.

[33] K. Chan, G. Karagiannis, M. Menth, P. Eardley, and B. Briscoe. Pre-Congestion Notification Encoding Comparison, draft-ietf-pcn-encoding-comparison-01, October 2009.

[34] G. Karagiannis and G. Apostolopoulos. Requirements for Signaling of (Pre-) Congestion Information in a Diffserv Domain, draft-karagiannis-pcn-signaling-requirements-00, October 2009.

[35] K. Chan, G. Karagiannis, T. Monaster, M. Menth, P. Eardley, and B. Briscoe. Pre-Congestion Notification Encoding Comparison, draft-chan-pcn-encoding-comparison-04, October 2009.

[36] J. Schönwälder. *Common YANG Data Types, draft-ietf-netmod-yang-types-02*, March 2009.

[37] J. Schönwälder. *Common YANG Data Types, draft-ietf-netmod-yang-types-03*, May 2009.

[38] J. Schönwälder. *Common YANG Data Types, draft-ietf-netmod-yang-types-04*, October 2009.

[39] J. Schönwälder. *Common YANG Data Types, draft-ietf-netmod-yang-types-05*, December 2009.

[40] J. Schönwälder. *Translation of SMIv2 MIB Modules to YANG Modules, draft-schoenw-netmod-smi-yang-00*, January 2009.

[41] A. Bader, L. Westberg, G. Karagiannis, C. Kappler, and T. Phelan. *RMD-QOSM - The Resource Management in Diffserv QOS Model,* draft-ietf-nsis-rmd-14, March 2009.

[42] A. Bader, L. Westberg, G. Karagiannis, C. Kappler, and T. Phelan. *RMD-QOSM - The Resource Management in Diffserv QOS Model,* draft-ietf-nsis-rmd-15, July 2009.

[43] J. Schönwälder. *SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-00*, January 2009.

[44] J. Schönwälder. *SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-01*, Abril 2009.

[45] J. Schönwälder. *SNMP optimizations for 6LoWPAN, draft-hamid-6lowpan-snmp-optimizations-02*, October 2009.

[46] J. Schönwälder. *NETCONF Configuration Protocol, draft-ietf-netconf-4741bis-00*, March 2009.

[47] J. Schönwälder. *NETCONF Configuration Protocol, draft-ietf-netconf-4741bis-01*, July 2009.

[48] J. Schönwälder. *Reclassification of COPS-PR and SPPI to Historic, draft-schoenw-opsawg-copspr-historic-00*, September 2009.

[49] Z. Despotovic P. Racz. *An ALTO Service based on BGP Routing Information, draft-racz-bgp-based-alto-service-00*, July 2009.

[50] V. Gurbani, E. Bruger, T. Anjali, H. Abdelnur, and O. Festor. *The Common Log File (CLF) format for the Session Initiation Protocol, draft-gurbani-sipping-clf-00*, February 2009.

[51] V. Gurbani, E. Bruger, T. Anjali, H. Abdelnur, and O. Festor. *The Common Log File (CLF) format for the Session Initiation Protocol, draft-gurbani-sipping-clf-01*, March 2009.

[52] R. State, O. Festor, H. Abdelnur, V. Pascual, J. Kuthan, R. Coeffic, J. Janak, and J. Floroiu. *SIP digest authentication relay attack, draft-state-sip-relay-attack-00*, March 2009.

[53] L. Burness, M. Menth, J. Araujo, S. Blake, and R. Woundy. *The Need for Congestion Exposure in the Internet*, draft-moncaster-congestion-exposure-problem-00, September 2009.

[54] L. Krug, M. Menth, J. Araujo, S. Blake, and R. Woundy. *The Need for Congestion Exposure in the Internet*, draft-moncaster-congestion-exposure-problem-01, October 2009.

[55] L. Krug, M. Menth, J. Araujo, S. Blake, and R. Woundy. *The Need for Congestion Exposure in the Internet*, draft-moncaster-congestion-exposure-problem-02, October 2009.

[56] L. Krug, M. Menth, J. Araujo, S. Blake, and R. Woundy. *The Need for Congestion Exposure in the Internet*, draft-moncaster-congestion-exposure-problem-03, October 2009.

Appendices

A NETCONF Interoperability Testing

NETCONF Interoperability Testing

Ha Manh Tran, Iyad Tumar, and Jürgen Schönwälder

Computer Science, Jacobs University Bremen, Germany
{h.tran,i.tumar,j.schoenwaelder}@jacobs-university.de

Abstract. The IETF has developed a network configuration management protocol called NETCONF which was published as proposed standard in 2006. The NETCONF protocol provides mechanisms to install, manipulate, and delete the configuration of network devices by using an Extensible Markup Language based data encoding on top of a simple Remote Procedure Call layer. This paper describes a NETCONF interoperability testing plan that is used to test whether NETCONF protocol implementations meet the NETCONF protocol specification. The test of four independent NETCONF implementations reveals bugs in several NETCONF implementations. While constructing test cases, a few shortcomings of the specifications were identified as well.

Key words: Network Management, NETCONF, Interoperability Testing

1 Introduction

The NETCONF protocol specified in RFC 4741 [1] defines a mechanism to configure and manage network devices. It allows clients to retrieve configuration from network devices or to add new configuration to these devices. The NETCONF protocol uses a remote procedure call (RPC) paradigm. A client encodes an RPC request in Extensible Markup Language (XML) [2] and sends it to a server using a secure, connection-oriented session. The server returns with an RPC-REPLY response encoded in XML.

The NETCONF protocol supports features required for configuration management that were lacking in other network management protocols, for instance SNMP [3]. NETCONF operates on so called datastores and represents the configuration of a device as a structured document. The protocol distinguishes between running configurations, startup configurations and candidate configurations. In addition, it provides primitives to assist with the coordination of concurrent configuration change requests and to support distributed configuration change transactions over several devices. Finally, NETCONF provides filtering mechanisms, validation capabilities, and event notification support [4].

The aim of this paper is twofold. First, we describe a NETCONF interoperability testing plan that is used to test whether NETCONF protocol implementations meet the NETCONF protocol specification in RFC 4741. The test plan particularly focuses on testing the correctness of NETCONF messages and

operations; it is not our current goal to measure the performance of NETCONF implementations. Second, we will discuss the observations and results that show how the test plan found some NETCONF implementation bugs, and how it revealed a few shortcomings where the specification (RFC 4741 and RFC 4742 [5]) is either somewhat ambiguous or totally silent.

In order to make the paper concise and precise, we use the word request when we refer to an `rpc` request message and the word response when we refer to an `rpc-reply` response message. We refer to NETCONF operations such as `get-config` by typesetting the operation name in teletype font. The names of test suites are typeset in small caps, e.g., VACM.

The rest of the paper is structured as follows: An overview of the NETCONF protocol is presented in Section 2. Section 3 provides information about the systems under test before the test plan is introduced in Section 4. The NETCONF interoperability tool (NIT) is described in Section 5. Preliminary observations are reported in Section 6 before the paper concludes in Section 7.

2 NETCONF Overview

The NETCONF protocol [1] uses a simple remote procedure call (RPC) layer running over secure transports to facilitate communication between a client and a server. The Secure Shell (SSH) [6] is the mandatory secure transport that all NETCONF clients and servers are required to implement as a means of promoting interoperability [5].

The NETCONF protocol can be partitioned into four layers as shown in Figure 1. The transport protocol layer provides a secure communication path between the client and server. The RPC layer provides a mechanism for encoding RPCs. The operations layer residing on top of the RPC layer defines a set of base operations invoked as RPC methods with XML-encoded parameters to manipulate configuration state. The configuration data itself forms the content layer residing above the operations layer.

The NETCONF protocol supports multiple configuration datastores. A configuration datastore is defined as the set of configuration objects required to get a device from its initial default state into a desired operational state. The `running` datastore is present in the base model and provides the currently active configuration. In addition, NETCONF supports a `candidate` datastore, which is a buffer that can be manipulated and later committed to the `running` datastore, and a `startup` configuration datastore, which is loaded by the device as part of initialization when it reboots or reloads [4].

Table 1 shows the protocol operations that have been defined so far by the NETCONF working group of the IETF. The first two operations `get-config` and `edit-config` can be used to read and manipulate the content of a datastore. The `get-config` operation can be used to read all or parts of a specified configuration. The `edit-config` operation modifies all or part of a specified configuration datastore. Special attributes embedded in the config parameter control which parts of the configuration are created, deleted, replaced or merged.

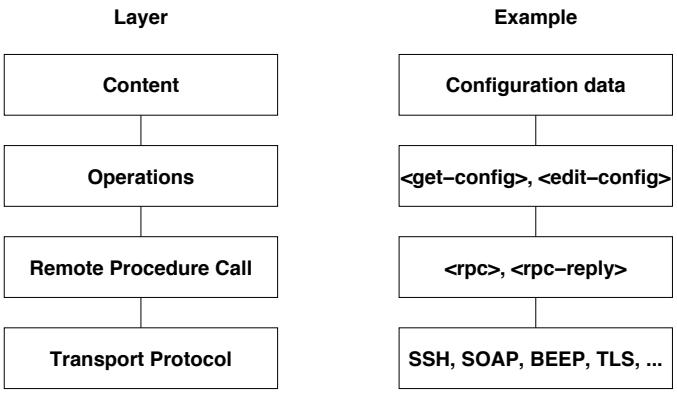

Fig. 1. NETCONF protocol layers [1].

The test-option and the error-option parameters control the validation and the handling of errors. The `copy-config` operation creates or replaces an entire configuration datastore with the contents of another complete configuration datastore and the `delete-config` operation deletes a configuration datastore (the `running` configuration datastore cannot be deleted).

The `lock` and `unlock` operations do coarse grain locking of a complete datastore and locks are intended to be short lived. More fine grained locking mechanisms are currently being defined in the IETF [4]. The `get` operation can be used to retrieve the running configuration and the current operational state of a device.

Table 1. NETCONF protocol operations (arguments in brackets are optional) [4]

Operation	**Arguments**
get-config	source [filter]
edit-config	target [default-operation] [test-option] [error-option] config
copy-config	target source
delete-config	target
lock	target
unlock	target
get	[filter]
close-session	
kill-session	session-id
discard-changes	
validate	source
commit	[confirmed confirm-timeout]
create-subscription	[stream] [filter] [start] [stop]

NETCONF sessions can be terminated using either the `close-session` operation or the `kill-session` operation. The `close-session` operation initiates a graceful close of the current session while the `kill-session` operation forces the termination of another session.

The optional `discard-changes` operation clears the candidate configuration datastore by copying the running configuration into the candidate buffer while the optional `validate` operation runs validation checks on a datastore. The optional `commit` operation is used to commit the configuration in the candidate datastore to the running datastore.

A separate specification published as RFC 5277 [7] extends the base NETCONF operations defined in RFC 4741 for notification handling. This is done by adding the `create-subscription` operation and introducing new `notification` messages carrying notification content. By using a notification stream abstraction, it is possible to receive live notifications as well as to replay recorded notifications.

NETCONF protocol introduces the notion of capabilities. A capability is some functionality that supplements the base NETCONF specification. A capability is identified by a uniform resource identifier (URI). The base capabilities are defined using URNs following the method described in RFC 3553 [8]. NETCONF peers exchange device capabilities when the session is initiated: When the NETCONF session is opened, each peer (both client and server) must send a `hello` message containing a list of that peer's capabilities. This list must include the NETCONF `:base` capability[1]. Following RFC 4741, we denote capabilities by the capability name prefixed with a colon, omitting the rest of the URI.

3 Systems Under Test

The systems used for the NETCONF interoperability testing comprise Cisco 1802 integrated services routers, Juniper J6300 routers, the Tail-f ConfD software for configuration management, and the EnSuite software [9] for configuration management. The ConfD software is an extensible development toolkit that allows users to add new components by writing a configuration specification for a data model and loading the generated object and schema files for the components. For the sake of consistency, we refer to the ConfD software as the Tail-f system. The EnSuite software contains a YencaP implementation used to test the NETCONF configuration protocol and extensible features on an experimental network management platform. It also supports web-based configuration management for NETCONF and additional modules and operations for the platform; e.g., the BGP_Module for configuring BGP routers and the Asterisk_Module for configuring VoIP servers. Table 2 briefly describes the four platforms and the SSH support of the four systems. The ConfD and EnSuite are installed and configured to run on Linux XEN virtual machines [10].

Table 3 presents the NETCONF capabilities announced by the systems under test. The Tail-f system supports all capabilities except the `:startup` ca-

[1] `urn:ietf:params:netconf:base:1.0`

Table 2. Systems under test

System	Platform	SSH Support
Juniper	JUNOS ver. 9.0	ver. 1.5/2.0
Tail-f	ConfD ver. 2.5.2	ver. 2.0
Cisco	IOS ver. 12.4	ver. 2.0
EnSuite	YencaP ver. 2.1.11	ver. 2.0

pability. The Cisco, Juniper and EnSuite systems support fewer capabilities and apparently the Cisco implementation favours a distinct `startup` datastore while the Juniper implementation favours a `candidate` datastore with commit and rollback support. The EnSuite implementation supports both `startup` and `candidate` datastores. Note that some implementations can be configured to support additional capabilities, but we used the more standard default settings in our tests. In addition to the capabilities listed in Table 3, each system announces several proprietary capabilities.

Table 3. NETCONF capabilities supported by the systems under test

Capability	Juniper	Tail-f	Cisco	EnSuite
`:base`	√	√	√	√
`:writable-running`		√	√	√
`:candidate`	√	√		√
`:confirmed-commit`	√	√		
`:rollback-on-error`		√		
`:validate`	√	√		
`:startup`			√	√
`:url`	√	√	√	√
`:xpath`		√		√

The Tail-f and Juniper implementations use an event driven parser. They do not wait for the framing character sequence to respond to a request. The Cisco and EnSuite systems do not seem to have an event driven parser or at least they do not start processing requests until the framing character sequence has been received.

The Juniper implementation is very lenient. For example, it continues processing requests even if the client does not send a `hello` message or the client does not provide suitable XML namespace and message-id attributes. The Juniper implementation supports a large number of vendor-specific operations. In addition, it renders the returned XML content in a tree-structure that is relatively easy to read and it generates XML comments in cases of fatal errors before closing the connection. As a consequence, the Juniper implementation is very easy to use interactively for people who like to learn how things work without using tools other than a scratch pad and a cut and paste device. The EnSuite im-

plementation shares the same characteristics with the Juniper implementation. Moreover, it returns an error message with an explanation of the reason and does not close the connection when the client sends illegal input. It, however, requires message-id attributes for requests.

The Tail-f and Cisco implementations are much less tolerant when processing input not closely following RFC 4741. They also return XML data in a compact encoding, minimizing the embedded white-space and thus reducing message sizes. Without proper tools, it is pretty difficult for humans to read the responses. In some cases, these two implementations close the connection when the client sends illegal input without an indication of the reason for closing the connection. In such cases, it can take some effort to investigate the wrongdoings.

Finally, we like to point out that the Cisco implementation we have tested does not support structured content; i.e., its configuration content is a block of proprietary IOS commands wrapped in an XML element. As a consequence, several of the advanced NETCONF features for retrieving and modifying structured configuration data cannot be applied. The EnSuite implementation still contains bugs and partially supports the `candidate` and `url` capabilities; e.g., several operations on the `candidate` datastore do not seem to work.

4 Test Plan

In this section we describe our NETCONF test plan. To make the execution of the tests efficient and to keep the collection of tests organized, we divided our test plan into five test suites. A test suite is a collection of test cases that are intended to be used to test and verify whether the systems under test meet the NETCONF protocol specification contained in RFC 4741 and RFC 4742.

Table 4 lists the test suites and the current number of test cases in each suite. The total number of test cases is 87. Each test case contains three parts: (i) a pre-configuration prepares the system under test for the test; (ii) a main test sends requests to, and receives responses from, the system under test, and verifies the responses; (iii) a post-configuration brings the system under test to the initial status. Our organization of test cases into test suites is not directly following the vertical layering model show in Figure 1 and the horizontal organization of operations and capabilities in the operations layer as one might expect. The reason is essentially our attempt to reduce the overhead of the pre-configuration and post-configuration parts during the execution of the test suite on the systems under test, e.g., in order to test the `edit-config` operation on a network interface, we describe a sequence of test cases for `create`, `replace`, `merge` and `delete` operations with setting up and cleaning up the interface once. This also led to a more tightly integrated organization of the test cases.

The first test suite is referred as the GENERAL test suite because it includes test cases for individual operations such as `lock`, `unlock`, `close-session`, `kill-session`, `discard-changes`, `validate`, and `commit`. The `lock` and `unlock` test cases verify that the responses do not contain an error or the responses contain a proper error, e.g., a `lock` request to the datastore already locked causes

Table 4. Test suites and current number of test cases

Test Suite	No. Test Cases
GENERAL	19
GET	11
GET-CONFIG	16
EDIT-CONFIG	15
VACM	26

an error. The `kill-session` test case contains a pre-configuration that prepares another running session before terminating it, while the `validate` test case contains a post-configuration that discards a change after validating it. This test suite also checks the format of requests and responses. Few test cases verify whether the responses contain the compulsory attributes and the attribute's value matches the value contained in the requests.

The next two test suites are the GET and GET-CONFIG suites. These suites aim to test the filter mechanism of the `get` and `get-config` operations. While `get` operates on the `running` configuration datastore and the device's state data, `get-config` operates on different sources of the configuration data such as the `running` and `candidate` datastores (depending on the support of capabilities), resulting in additional test cases for the GET-CONFIG suite. Test cases verify several types of subtree filters, e.g., a test case checks whether the system under test returns the entire content of the running configuration data plus the operational state when no filter is used, or another test case checks whether the system under test returns nothing when an empty filter is used.

The EDIT-CONFIG suite involves tests modifying the configuration data in the datastore. This suite includes test cases for the `delete-config`, `copy-config`, and `edit-config` operations. The `edit-config` operation test cases support the `create`, `replace`, `merge` and `delete` operation attributes. Several test cases in this suite are data model specific due to the lack of a common data model, thus we need to implement several tests in different ways. This extra work can be reduced if implementers volunteer to support a common data model.

The last test suite is the VACM suite verifying the NETCONF protocol operations against the VACM data model [11]. This data model is a YANG version of the `SNMP-VIEW-BASED-ACM-MIB` (View-based Access Control Model for the Simple Network Management Protocol [12]). YANG [13] is a data modelling language for NETCONF. Test cases in this suite are generated from this data model focusing on the `group`, `access`, and `view` lists.

5 Test Tool (NIT)

We have implemented a tool called NIT (NETCONF Interoperability Testing tool) to automatically execute the test suites against a system under test. Our NIT tool basically performs the following operations:

1. connecting to a system under test using the SSH

2. verifying the initial `hello` message
3. executing test cases by
   - sending a test request and receiving a response
   - verifying both the request and the response following the criteria defined by RFC 4741.
4. reporting the failure or the success of each test

The tool is equipped with an XML parser to analyze the responses for verification. The parser, upon receiving a response, provides a list of elements with quantity, a list of attributes with quantity, a list of attribute values and a list of text parts. With this information, the tool can detect possible flaws from the responses, such as whether any element or attribute is missing, whether an error must be returned. The following example presents a response without an error or a warning:

```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="1007"
           xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <ok/>
</rpc-reply>
]]>]]>
```

The parser provides the following information of the response:

```
-Element Types
    rpc-reply 1
           ok 1
-Attribute Types
   message-id 1
        xmlns 1
-Attribute Values
   message-id ['1007']
        xmlns ['urn:ietf:params:xml:ns:netconf:base:1.0']
-Text Parts
              []
```

We have used the Python unit testing framework [14]. The framework features test automation, shared configuration of setup and shutdown methods, arrangement of tests into collections, and independent reporting of the tests. The tool takes advantage of these features to maintain a single SSH connection for all tests and to group related tests into a collection; e.g., tests concerned with creation, modification and deletion operations are grouped together to reuse and clean the testing environment easily. The tool organizes test cases into several collections of test cases, namely test suites, as discussed in Section 4.

While the tool has been used successfully to test some specific devices (see next section), it possesses several limitations. Firstly, it lacks a resumption mechanism to continue the test run when it encounters connection loss due to the

misbehavior of systems under test. Secondly, while the test cases are believed to comply with RFC 4741, the test scripts, i.e., the piece of code that implements test cases, depends on the specification and configuration of components of the tested systems to produce the requests and to verify the responses. Finally, the framework requires some extra work for complicated test cases; e.g., testing the `lock` operation requires an extra session to lock the database.

6 Preliminary Observations

We have used the NIT tool to test the systems described in Section 3. Since the result of the tests are specific to the different NETCONF implementations, we present the results by referring to system X and we leave out the mapping of X to the systems described in Section 3. Note that we did manually re-check the failed test cases in order to erase bugs in the test scripts. Despite these efforts, several test cases reflect our interpretation of RFC 4741 and there might not be full agreement with our interpretation and thus the numeric results presented below should be taken with a grain of salt.

Table 5. Test result summary organized by the systems under test

System	Success	Failure	Irrelevant
A	47.2%	14.9%	37.9%
B	82.8%	9.2%	8.0%
C	17.3%	10.3%	72.4%
D	17.3%	21.8%	60.9%

Table 5 presents the result of the NIT tool for the systems under test. The "success" and "failure" columns indicate the percentage of passed and failed test cases respectively, while the "irrelevant" column indicates the percentage of test cases that cannot be applied to a specific system due to either system configuration or implementation problems (e.g., the `vacm` data model is not implemented).

We learned that the systems A and B comply reasonably well with the RFCs. The system A fails 14.9% of the test cases and most of them are related to the basic format of request and response messages or the filter mechanism of the `get` operation. The system B performs better with very few failed test cases and most of them are concerned with the validation of XML elements in request messages. The two systems A and B have very few problems with the filter mechanism of the `get-config` operation or the usage of the `edit-config` operation for creating, modifying and deleting configuration elements. The systems C and D perform poorer with 72.4% and 60.9% irrelevant test cases and 10.3% and 21.8% failed test cases, respectively. The failed test cases are related to the format of requests and responses or the filter mechanism of the `get` operation.

Table 6. Test result summary organized by the test suites

Test Suite	Success	Failure	Irrelevant
GENERAL	73.6%	13.2%	13.2%
GET	29.5%	52.3%	18.2%
GET-CONFIG	48.4%	14.1%	37.5%
EDIT-CONFIG	38.3%	1.7%	60%
VACM	19.2%	5.8%	75%

Table 6 reports the passed and failed test cases organized by the test suites over the total number of running test cases for the systems under test. There are two remarks: (i) the GET suite obtains a high percentage of failed test cases 52.3%, and (ii) the EDIT-CONFIG suites obtains low percents of failed test cases 1.7%. We found that the majority of failed test cases from the GET suite is related to the filter mechanism of the `get` operation.

With the failed test cases in mind, we have looked back into the RFCs. There are several things where the RFC is either somewhat ambiguous or totally silent. In general, the RFC should provide more detailed descriptions for error situations and it might be necessary to better constrain the currently open ended format of request and response messages since they for example allow arbitrary values for attributes. Furthermore, the RFC should be updated with clearer examples. Some particular issues are listed below:

- The RFC ignores the XML declaration

  ```
  <?xml version$="1.0" encoding="UTF-8"?>
  ```

  for requests and responses. Some systems do not execute a request without this declaration while other systems do. It seems that the IETF working group favours to have a mandatory XML declaration.
- The examples in RFC 4741 often omit namespace declarations for request and response messages. Only few systems execute a request without a proper namespace declaration and it would help interoperability if the examples would contain namespace declarations where necessary.
- RFC 4741 requires that additional attributes present in the `<rpc>` element of a request message must be returned in the `<rpc-reply>` element of the response message without any change (see section 4.1 of the RFC 4741). This requirement leads to problems when such an attribute conflicts with attributes generated by the implementation. One implementation generated duplicated attributes (and thus invalid XML) while another implementation removes a duplicated attribute resulting in violation of RFC 4741.
- RFC 4741 allows arbitrary strings for the `message-id` attribute. From the tests, we found that implementations terminate the session often without an error indication or return strange results when the `message-id` attribute in a request message contains unexpected content such as the literal string `]]>]]>` or the literal string `</rpc>`. Of course, a proper NETCONF client would not generate such request messages since they are invalid XML. But

on the other hand, one can question whether arbitrary content in request and response attributes is a feature worth to support.

Some of the items listed above are meanwhile actively discussed on the NETCONF working group mailing list and work is underway to revise RFC 4741 in order to fix bugs and to clarify the processing of NETCONF messages [15].

7 Conclusions and Future Work

We have carried out some work on NETCONF interoperability testing. This work aims at observing the compliance of NETCONF implementations with RFC 4741. It also aims at identifying inconsistencies in the RFC. We have proposed a test plan consisting of five test suites. Each test suite contains a number of test cases that involve a single operation or a group of related operations. The test cases exploit several aspects of RFC 4741 including the format of request and response messages, the filter mechanism supported by some operations, NETCONF capabilities, and so on. The test cases have been coded into the NIT tool, which automates the execution of test runs. It should be noted, however, that the test cases so far have not been reviewed and as such there might be disagreement on some test cases whether they are correct or not relative to RFC 4741.

We have used the NIT tool to test four different NETCONF implementations. Our preliminary observations indicate that the number of failed test cases is relatively high for some systems, thus raising the question of the compliance of these systems with RFC 4741. We have also noted some inconsistencies in RFC 4741 that should be addressed in a future revision of this document. It should be mentioned that some test cases are our interpretation of RFC 4741 and it needs to be worked out to what extend our interpretation meets the interpretation of the working group.

While some interesting initial results have been obtained, this work still requires several improvements. First, the coverage of RFC 4741 by the test cases needs to be evaluated and increased by adding additional test cases as needed. Furthermore, it would be nice to reduce the dependency of the test cases on different data models. Third, the NIT tool should be improved to better support more complicated test cases that involve multiple NETCONF sessions. Fourth, it would be nice to have a tool able to generate test suites out of YANG data models. And finally, it would be valuable to repeat the tests with a larger number of different NETCONF implementations and to evaluate how test results impact future software revisions and lead to more interoperability.

Acknowledgment

The work reported in this paper is supported by the EC IST-EMANICS Network of Excellence (#26854).

References

1. R. Enns. NETCONF Configuration Protocol. RFC 4741, December 2006.
2. C. Sperberg-McQueen, J. Paoli, E. Maler, and T. Bray. Extensible Markup Language (XML) 1.0 (Second Edition). http://www.w3.org/TR/2000/REC-xml-20001006, October 2000. Last access in July 2008.
3. J. Case, R. Mundy, D. Partain, and B. Stewart. Introduction and Applicability Statements for Internet Standard Management Framework. RFC 3410, December 2002.
4. J. Schönwälder, M. Björklund, and P. Shafer. Network Configuration Management using NETCONF and YANG. *IEEE Communications Magazine*, 2009.
5. M. Wasserman and T. Goddard. Using the NETCONF Configuration Protocol over Secure Shell (SSH). RFC 4742, December 2006.
6. T. Ylonen and C. Lonvick. The Secure Shell (SSH) Protocol Architecture. RFC 4251, January 2006.
7. S. Chisholm and H. Trevino. NETCONF Event Notifications. RFC 5277, July 2008.
8. M. Mealling, L. Masinter, T. Hardie, and G. Klyne. An IETF URN Sub-namespace for Registered Protocol Parameters. RFC 3553, June 2003.
9. V. Cridlig, H. J. Abdelnur, J. Bourdellon, and R. State. A NetConf Network Management Suite: ENSUITE. In *Proc. 5th IEEE International Workshop on IP Operations and Management: Operations and Management in IP-Based Networks (IPOM '05)*, volume 3751 of *LNCS*, pages 152–161. Springer, 2005.
10. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the Art of Virtualization. In *Proc. 19th ACM Symposium on Operating Systems Principles (SOSP '03)*. ACM, October 2003.
11. J. Schönwälder. VACM Yang Data Model. Jacobs University Bremen, October 2008.
12. B. Wijnen, R. Presuhn, and K. McCloghrie. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). RFC 3415, December 2002.
13. M. Björklund. YANG - A data modeling language for NETCONF. Internet draft, January 2009.
14. Python Unit Testing Framework. http://pyunit.sourceforge.net/. Last access in November 2008.
15. R. Enns, M. Björklund, and J. Schönwälder. NETCONF Configuration Protocol. Internet Draft <draft-ietf-netconf-4741bis-00.txt>, Juniper Networks, Tail-f Systems, Jacobs University, March 2009.