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

Final report on standardization, interaction and cooperation
Deliverable 5.4

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:	Final report on standardization, interaction and cooperation
Type:	Public
Editor(s):	Aiko Pras
E-mail:	a.pras@utwente.nl
Author(s):	Aiko Pras
Doc ID:	D5.4

AMENDMENT HISTORY

Version	Date	Author	Description/Comments
0.1	2008-12-15	Giovane Moura	Initial version
Final	2009-01-15	Aiko Pras	Final version

Legal Notices

The information in this document is subject to change without notice.

The Members of the EMANICS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the EMANICS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

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 is an updated version of the interim report D5.3, and covers the full first 18 months of the second phase of the EMANICS project.

In the second 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 eighteen months period, EMANICS partners contributed to 2 Request for Comments (RFCs) and 38 Internet-Drafts. This is even more than what was achieved in the previous period, and may make EMANICS one of the most successful NoEs to this respect. In addition, EMANICS partners are also very active within the “Network Management Research Group” (NMRG) of the “Internet Research Task Force” (IRTF).

EMANICS partners have had many bilateral interactions with industry 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 Management of the Future Internet (ICT Event Lyon) and the MANA activity (FIA, Madrid). In addition, they contributed to other Future Internet initiatives, such as the 3D Internet.

1 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 36 months of the EMANICS project. It shows the activities undertaken within the full first 18 months of Phase 2. Note that, to make this deliverable self-contained, some text of the previous deliverable (D5.3) has been included in this deliverable. Section 2 discusses standardization, Section 3 discusses the interaction with industry and Section 4 discusses the cooperation with other networks and research projects. Section 5 provides the conlusions. In addition, Appendix A presents a draft version of the NETCONF testing report, while Appendix B contains a report from the 73th IETF Meeting.

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.

2 Standardization

In the second phase of the EMANICS project several partners contributed to the IETF standardization process and joined the IRTF "Network Management Research Group" (NMRG) meetings. This chapter starts with summarizing the WP5 description, as contained in the JPA. Section 2.2 discusses the EMANICS contributions to the IETF standardization process and Section 2.3 gives an overview of EMANICS contributions to the IRTF-NMRG.

2.1 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.

2.2 IETF

This section discusses the EMANICS contributions to the IETF standardization process. Section 2.2.1 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 D5.2). Section 2.2.2 mentions the IETF meetings that have been attended and Section 2.2.3 lists the Internet-Drafts and RFCs to which contributions have been made.

2.2.1 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)

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

ISMS

The *Integrated Security Model for SNMP* (ISMS) WG is chaired by Jürgen Schönwälder, who works at JUB and is member of the EMANICS NoE.

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 [1, 2]:

- 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 security-Name 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 [3]:

- 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 [4]. 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 [5].

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 [6].

2.2.2 IETF Meetings

In Phase 2, the following IETF meetings took place:

- 69th IETF Meeting, July 2007; Chicago, USA,
- 70th IETF Meeting, December 2007; Vancouver, Canada,
- YANG design team Meeting; September 2007, Stockholm.
- 71th IETF Meeting, March 2008; Philadelphia, USA,
- 72th IETF Meeting, August 2008; Dublin, Ireland,
- 73th IETF Meeting, November 2008; Minneapolis, USA,
- NETMOD Workgroup Interim, October 2008; Herndon, Virginia

The 69th IETF meeting, which was held in July 2007 in Chicago, was attended by Georgios Karagiannis (UT). At that meeting he provided presentations at the PCN and NSIS WGs, and participated at the TSVWG working group.

Although no EMANICS participants attended the 70th IETF meeting (December 2007, Vancouver), slides of the IRTF-NMRG / EMANICS meeting, which was held shortly before the IETF meeting, were presented at OPSAREA meeting by the OPSAREA leader, Dan Romanescu [7].

The 71th IETF meeting was organized between March 9-14, 2008, in Philadelphia, USA. Two EMANICS partners participated: Jürgen Schönwälder (JUB) and Georgios Karagiannis (UT). JJürgen Schönwälder chaired the ISMS WG meeting, and contributed to a number of other WGs, such as OPSAWG and NETCONF. He also participated at the CANMOD BOF meeting. At the Philadelphia IETF meeting, it was decided that the NETCONF data modeling requirements discussion is over. There is now work going on to draft a charter for a NETCONF data modeling language working group, and the YANG specifications are likely becoming the basis of this IETF effort. The details need to be further discussed, and rough consensus within the IETF has to be reached.

Also Jürgen Schönwälder attended some design team meetings on a management data language for the network configuration protocol NETCONF, which is currently standardized by the IETF. This team consists of active IETF members from organizations like Ericsson Juniper, tail-f, and Jacobs University. The team is working on several Internet-Drafts defining a NETCONF data modeling language and a set of reusable data type definitions This work has been called ”YANG” [4].

The 72th IETF meeting took place in Dublin, Ireland (July 27-August 1). From Emanics, Jürgen Schönwälder (IUB) participated. He contributed, amongst others, to the ISMS WG (which he is chairing), to the OPSAWG WG (where he is document editor), as well as the newly established NETCONF Data Modeling Language (netmod) WG. The datatype draft that was prepared by Jürgen Schönwälder was accepted as starting point for the YANG datatypes.

The 73th IETF meeting took place in Minneapolis, USA (16-21 November 2008). From Emanics, Fabio Hecht (UniZH) went to this meeting, where he joined the ALTO Application Layer Traffic Optimization) and the LEDBAT Less Than Best Effort Transport) working groups. Jürgen Schönwälder (JUB) participated remotely and joined discussions of the NETCONF and NETMOD working groups. A report from Fabio Hecht with more details about this meeting can be found in Appendix B.

In addition to the IETF meeting in Minneapolis, the IETF NETMOD working group did hold an interim WG meeting on October 8-10, 2008 in Herndon, Virginia, USA. The goal of this three day meeting was to work through the open issues of the proposed YANG data modeling language and associated specifications (YANG data type collection, translation to DSDL). The meeting was hosted by Juniper Networks and had industrial partipants from Huawei USA, Ericsson, Juniper Networks, Tail-f, SNMP Research, Siemens-Nokia, and Vigil Security. Jürgen Schönwälder participated in this meeting due to his role as WG editor of the YANG data types document and his active involvement in the original YANG design team (see also: http://trac.tools.ietf.org/wg/netmod/trac/wiki/interim_oct08)

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

Table 1: EMANICS participation to IETF meetings

Meeting	Name	Organization	Role
69th IETF	Georgios Karagiannis	UT	Editor of Internet-Drafts
71th IETF	Jürgen Schönwälder	JUB	ISMS co-chair Editor of Internet-Drafts
71th IETF	Georgios Karagiannis	UT	Editor of Internet-Draft
71th IETF	Gijs van den Broek	UT	
YANG meeting	Jürgen Schönwälder	JUB	Design team member
72th IETF	Jürgen Schönwälder	JUB	ISMS co-chair Editor of Internet-Drafts
73th IETF	Fabio Hecht	UniZH	
73th IETF	Jürgen Schönwälder	JUB	ISMS co-chair Editor of Internet-Drafts

2.2.3 Publications

In the the full 18 months of the second Phase of the EMANICS project, 2 RFCs and 38 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
- SNMP Traffic Measurement and Trace Exchange Formats
- SNMP Context EngineID Discovery
- DiffServ Resource Management
- InterDomain-QOSM
- NSLP for Quality-of-Service Signaling
- Load Control PCN
- Pre-Congestion Notification Encoding Comparison
- SMIng
- SNMP Trace Analysis Definitions
- Common YANG Data Types

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

TRANSPORT SUBSYSTEM FOR SNMP

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 Mapping Security Model (TMSM) - Architectural Extension for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-09, July 2007
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-10, September 2007
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-11, November 2007
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-12, February 2008
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-13, August 2008
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-14, October 2008
- D. Harrington, **J. Schönwälder**: Transport Subsystem for the Simple Network Management Protocol (SNMP), draft-ietf-isms-tmsm-15, November 2008

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

In this phase of the project, EMANICS partners produced the following Internet-Draft:

- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-marinov-syslog-snmp-01.txt, February 2008
- **V. Marinov, J. Schönwälder** : Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages, draft-marinov-syslog-snmp-02.txt, October 2008

- **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..
- **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..

These drafts define mappings from Simple Network Management Protocol (SNMP) notifications to SYSLOG notifications and vice versa. They are currently considered for standardization within the OPSAWG.

SNMP TRAFFIC MEASUREMENT AND TRACE EXCHANGE FORMATS

The following versions of the Internet-Draft “SNMP Traffic Measurements and Trace Exchange Formats ” were produced by EMANICS partners in this period:

- **J. Schönwälder**: SNMP Traffic Measurements and Trace Exchange Formats, draft-irtf-nmrg-snmp-measure-02.txt, December 2007
- **J. Schönwälder**: SNMP Traffic Measurements and Trace Exchange Formats, draft-irtf-nmrg-snmp-measure-03.txt, February 2008
- **J. Schönwälder**: SNMP Traffic Measurements and Trace Exchange Formats, draft-irtf-nmrg-snmp-measure-04.txt, March 2008
- **J. Schönwälder**: SNMP Traffic Measurements and Trace Exchange Formats, draft-irtf-nmrg-snmp-measure-05.txt, May 2008
- **J. Schönwälder**: SNMP Traffic Measurements and Trace Exchange Formats, draft-irtf-nmrg-snmp-measure-06.txt, September 2008

In addition, a RFC was produced after these versions:

- **J. Schönwälder**, Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats, RFC 5345, October 2008.

The Simple Network Management Protocol (SNMP) is widely deployed to monitor, control and configure network elements. Even though the SNMP technology is well documented, it remains relatively unclear how SNMP is used in practice and what typical SNMP usage patterns are. This Internet-Draft proposes to carry out large scale SNMP traffic measurements in order to develop a better understanding how SNMP is used in real world production networks. It describes the motivation, the measurement approach, and the tools and data formats needed to carry out such a study.

SNMP CONTEXT ENGINEID DISCOVERY

In this phase the following versions of the Internet-Draft "*Simple Network Management Protocol (SNMP) Context EngineID Discovery*" were produced by EMANICS partners

- **J. Schönwälder**: Simple Network Management Protocol (SNMP) Context EngineID Discovery, draft-ietf-opsawg-snmp-engineid-discovery-01, January 2008
- **J. Schönwälder**: Simple Network Management Protocol (SNMP) Context EngineID Discovery, draft-ietf-opsawg-snmp-engineid-discovery-02, February 2008
- **J. Schönwälder**: Simple Network Management Protocol (SNMP) Context EngineID Discovery, draft-ietf-opsawg-snmp-engineid-discovery-03, July 2008

The Simple Network Management Protocol (SNMP) version three (SNMPv3) requires that an application knows the identifier (snmpEngineID) of the remote SNMP protocol engine in order to retrieve or manipulate objects maintained on the remote SNMP entity. This document introduces a well-known localEngineID and a discovery mechanism which can be used to learn the snmpEngineID of a remote SNMP protocol engine. The proposed mechanism is independent of the features provided by SNMP security models and may also be used by other protocol interfaces providing access to managed objects.

In addition, the following RFC was produced in this phase:

- **J. Schönwälder**, Simple Network Management Protocol (SNMP) Context EngineID Discovery, RFC 5343, September 2008.

DIFFSERV RESOURCE MANAGEMENT

The following Internet-Draft has 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-11, August 2007
- A. Bader, L. Westberg, **G. Karagiannis**, C. Kappler, T. Phelan: RMD-QOSM - The Resource Management in Diffserv QOS Model, draft-ietf-nsis-rmd-12, November 2007
- A. Bader, L. Westberg, **G. Karagiannis**, C. Kappler, T. Phelan: RMD-QOSM - The Resource Management in Diffserv QOS Model, draft-ietf-nsis-rmd-13, July 2008

This document describes an NSIS QoS Model for networks that use the Resource Management in Diffserv (RMD) concept. RMD is a technique for adding admission control and preemption function to Differentiated Services (Diffserv) networks. The RMD QoS Model allows devices external to the RMD network to signal reservation requests to edge nodes in the RMD network. The RMD Ingress edge nodes classify the incoming flows into traffic classes and signals resource requests for the corresponding traffic class along the data path to the Egress edge nodes for each flow. Egress nodes reconstitute the original requests and continue forwarding them along the data path towards the final destination. In addition, RMD defines notification functions to indicate overload situations within the domain to the edge nodes.

NSLP FOR QUALITY-OF-SERVICE SIGNALING

The following Internet-Drafts have been produced in Phase I:

- J. Manner, **G. Karagiannis**, A. McDonald: NSLP for Quality-of-Service Signaling, draft- ietf-nsis-qos-nslp-15, July 2007
- J. Manner, **G. Karagiannis**, A. McDonald: NSLP for Quality-of-Service Signaling, draft- ietf-nsis-qos-nslp-16, February 2008

This specification describes the NSIS Signaling Layer Protocol (NSLP) for signaling QoS reservations in the Internet. It is in accordance with the framework and requirements developed in NSIS. Together with GIST, it provides functionality similar to RSVP and extends it. The QoS NSLP is independent of the underlying QoS specification or architecture and provides support for different reservation models. It is simplified by the elimination of support for multicast flows. This specification explains the overall protocol approach, design decisions made and provides examples. It specifies object, message formats and processing rules.

LOAD CONTROL PCN

Three Internet-Drafts have been produced for Pre-congestion notification:

- L. Westberg, A. Bader, D. Partain, **G. Karagiannis**: LC-PCN - The Load Control PCN solution, draft-westberg-pcn-load-control-01, August 2007
- L. Westberg, A. Bader, D. Partain, **G. Karagiannis**: LC-PCN - The Load Control PCN solution, draft-westberg-pcn-load-control-02, November 2007
- L. Westberg, A. Bader, D. Partain, **G. Karagiannis**: LC-PCN - The Load Control PCN solution, draft-westberg-pcn-load-control-03, February 2008
- L. Westberg, A. Bader, D. Partain, **G. Karagiannis**: LC-PCN - The Load Control PCN solution, draft-westberg-pcn-load-control-04, July 2008
- L. Westberg, A. Bader, D. Partain, **G. Karagiannis**: LC-PCN - The Load Control PCN solution, draft-westberg-pcn-load-control-05, July 2008

There is an increased interest of simple and scalable resource provisioning solution for Diffserv network. The Load Control PCN (LC-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.

Admission control in a Diffserv stateless domain is a combination of:

- Probing, whereby a probe packet is sent along the forwarding path in a network to determine whether a flow can be admitted based upon the current congestion state of the network
- Admission control based on data marking, whereby in congestion situations the data packets are marked to notify the egress node that a congestion occurred on a particular ingress to egress path.

The scheme provides the capability of controlling the traffic load in the network without requiring signaling or any per-flow processing in the core routers. The complexity of Load Control is kept to a minimum to make implementation simple.

PRE-CONGESTION NOTIFICATION ENCODING COMPARISON

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

- K. Chan, **G. Karagiannis**: Pre-Congestion Notification Encoding Comparison, draft-chan-pcn-encoding-comparison-01, November 2007
- K. Chan, **G. Karagiannis**: Pre-Congestion Notification Encoding Comparison, draft-chan-pcn-encoding-comparison-02, February 2008
- K. Chan, **G. Karagiannis**: Pre-Congestion Notification Encoding Comparison, draft-chan-pcn-encoding-comparison-03, February 2008

A number of mechanisms have been proposed to support differential Quality of Service for packets in the Internet. DiffServ is an example of such a mechanism. However, the level of assurance that can be provided with DiffServ without substantial over-provisioning is limited. Pre-Congestion Notification (PCN) uses path congestion information across a PCN region to enable per-flow admission control to provide the required service guarantees for the admitted traffic. While admission control will protect the QoS under normal operating conditions, an additional flow termination mechanism is necessary to cope with extreme events (e.g. route changes due to link or node failure).

In order to allow the PCN mechanisms to work it is necessary for IP packets to be able to carry the pre-congestion information to the PCN egress nodes. This document explores different ways in which this information can be encoded into IP packets. This document does not choose the encoding but provide guidance and recommendation based on different criteria.

SMING

The following SMIng related Internet-Draft has been produced by EMANICS partners:

- **J. Schönwälder**: Protocol Independent Network Management Data Modeling Languages - Lessons Learned from the SMIng Project, draft-schoenw-sming-lessons-01, September 2007

A data modeling language for network management protocols called SMIng was developed within the IRTF-NMRG over a period of several years. This memo documents some of the lessons learned during the project for consideration by designers of future data modeling languages for network management protocols.

SNMP TRACE ANALYSIS DEFINITIONS

The following Internet-Drafts on SNMP trace analysis definitions have been produced by EMANICS partners. Development of these drafts took place within WP7:

- **J. van den Broek, J. Schönwälder, A. Pras, M. Harvan**: SNMP Trace Analysis Definitions, draft-schoenw-nmrg-snmp-trace-definitions-00, January 2008
- **J. van den Broek, J. Schönwälder, A. Pras, M. Harvan**:: SNMP Trace Analysis Definitions, draft-schoenw-nmrg-snmp-trace-definitions-01, February 2008
- **J. van den Broek, J. Schönwälder, A. Pras, M. Harvan**:: SNMP Trace Analysis Definitions, draft-schoenw-nmrg-snmp-trace-definitions-02, April 2008

The Network Management Research Group (NMRG) started an activity to collect traces of the Simple Network Management Protocol (SNMP) from operational networks. To analyze these traces, it is necessary to split potentially large traces into more manageable pieces that make it easier to deal with large data sets and simplify the analysis of the data.

This document provides some common definitions that have been found useful for implementing tools to support trace analysis. This document mainly serves as a reference for the definitions underlying these tools and it is not meant to explain all the motivation and reasoning behind the definitions. Some of this background information can be found in other research papers.

Common Yang Data Types

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

- **J. Schönwälder**: Common YANG Data Types, draft-schoenw-netmod-yang-types-00, May 2008
- **J. Schönwälder**: Common YANG Data Types, draft-schoenw-netmod-yang-types-01, November 2008

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.

2.3 IRFT

In the first full 18 months of the second phase of the EMANICS project two Internet Research Task Force (IRTF) Network Management Research Group (NMRG) [48] meetings were organized. The IRTF-NMRG is chaired by Jürgen Schönwälder (JUB). Table 2 gives an overview of the EMANICS participation to these IRTF-NMRG meetings.

Table 2: EMANICS participation to IRTF-NMRG meetings

Meeting	Name	Organization	Role
Enschede	Aiko Pras	UT	Organizer
Enschede	Jürgen Schönwälder	JUB	NRMG Chair
Enschede	Lisandro Granville	UT	
Enschede	Krzysztof Nowak	PSNC	
Enschede	Gijs van den Broek	UT	
Enschede	Olivier Festor	INRIA	
Enschede	Sameh Bel Haj Saad	INRIA	
Enschede	Jürgen Schönwälder	JUB	NRMG Chair
Enschede	Georgios Karagiannis	UT	
Enschede	Gijs van den Broek	UT	

2.3.1 23th NMRG meeting - Enschede

The 23th NMRG meeting took place November 8-9, 2007 at the campus of the University of Twente, Enschede, Netherlands. The following text, which is partially copied from the original meeting minutes and which can be found on the NMRG website, summarizes the meeting results. The results of this meeting were also presented by the area director at the OPSAREA meeting of the 70th IETF meeting, which took place in Vancouver, Canada, from December 2-7. The slides of this presentation can be downloaded from [7].

PERFORMANCE OF SNMP OVER SSH/TLS/DTLS

Jürgen Schönwälder gave a brief introduction into the motivation behind SNMP over secure transports and the ISMS work done in this space. He then discussed some technical aspects of running SNMP over SSH, TLS, and DTLS and finally showed some measurements done with a prototype implementation. Since there are some inconsistencies and shortcomings in the data set, the measurements need to be repeated. Once that has happened, a detailed paper about this work will be submitted.

A VISUALIZATION TOOL FOR SNMP TRACES

Lisandro Zambenedetti Granville presented a tool being developed by one of his students which (a) provides a Web-based front-end to the functionality provided by the snmpdump tool and (b) creates visualizations such as topology graphs, MIB object usage graphs, and traffic intensity graphs. It is unclear whether this work continues once the student involved has finished his assignment.

SNMP TRACE ANALYSIS AT PSNC

Krzysztof Nowak reported about some SNMP traces they have collected and analyzed. His presentation was based on the material that can also be found in EMANICS deliverable D7.2. There were some discussions concerning the nature of the data sets.

Poznan is collecting more traces and creating ideas to do further analysis, for example concerning reaction time to network events detected by SNMP management systems.

DETECTING PERIODIC AND APERIODIC SNMP TRAFFIC

Gijs van den Broek briefly explained the problem of separating periodic from aperiodic traffic. After a discussion how people would approach the problem, the work done in Twente was presented by Gijs. This lead to a detailed discussion about assumptions made by several definitions. It became clear that some assumptions are unavoidable.

DEFINITIONS

The second day focusses solely on the discussion of common definitions for SNMP trace analysis work. First, it was recognized that the flow definition used in the IM paper (although not spelled out well in the paper) is consistent with the session definition introduced by Gijs.

Next, it was recognized that the term session using by Gijs can be misleading since for example ISMS uses the term session to refer to SSH or TLS connections. Since the term sequence can also be misleading, it was decided to use the term ”slice” since this term nicely fits that model that we split flows into slices and has no other meaning in the SNMP context.

After some extensive discussion concerning potential definitions of these terms, an initial set of definitions was drafted by JS and GB and presented at the end of the meeting.

It was agreed to continue work towards a consistent set of definitions that are needed for the trace analysis work done at the University of Twente (periodic/aperiodic traffic) and at the Jacobs University Bremen (table retrieval algorithms). The definitions will be put into an ID with the final goal to progress them in the NMRG towards RFC publication. The research groups will then use these definitions in the research papers they are working on.

2.3.2 24th NMRG meeting - Philadelphia

The 24th NMRG meeting was held in Philadelphia, USA on March 14, 2008, in conjunction with the 71th IETF meeting. Two EMANICS partners participated: Jürgen Schönwälder

(JUB) and Georgios Karagiannis (UT). In addition, Gijs van den Broek, who is a M.Sc. student at the UT, also participated. In total there were about 20 participants to this meeting and interestingly several agenda items were closely related to EMANICS work (see also the meeting minutes).

One of these items was the work on SNMP trace analysis definitions, which was introduced by Gijs van den Broek. This work is directly related to EMANICS WP7, and is thus a good example of collaboration between the EMANICS research WPs and WP5. After his presentation, there were several questions about how the definitions would work with some of the less common things that have been seen in management traffic, such as responses appearing on a different interface from the corresponding request, interleaved table walks, and how the slice definition excludes event-directed polling.

Another item was the ”network management research classification”, which was presented by Georgios Karagiannis. This classification is currently under development within EMANICS WP1, and is therefore another good example of EMANICS work being presented to (pre-)standardization groups. The goal of the work is to define a taxonomy for organizing network and systems management research topics. The plan is to incorporate this taxonomy into the JEMS system (https://submissoes.sbc.org.br/), and use it for future conferences (such as NOMS, IM, DSOM) and to classify research efforts in IRTF. The meeting observed that taxonomies are rarely perfect, but can be useful nonetheless.

Although there were several questions and comments, the general conclusion was that this work is being useful, and that the challenge is to limit its size. At the NMRG meeting also the status of the ”SNMP Traffic Measurements” draft was summarized (by Bert Wijnen). Also this work is a direct outcome of previous EMANICS WP7 work. Since the previous round of comments has been responded to, the next step is to formally ask the IRTF chair to ask for review in the IRSG, before moving to RFC.

Finally Jürgen Schönwälder presented a report on the IAB review. He noted that there is a desire to increase participation by operators. To that end, co-location of meetings with nanog might help. Another concern of the IAB is that some of the NMRG's work is showing up in academic publications rather than RFCs, limiting the visibility of the work. Consequently there is a desire to consider republication of some papers as RFCs. Finally, Jürgen noted that he hopes to step down as chair, and that consequently there is a need for new co-chairs.

2.3.3 25th NMRG meeting - Munich

To exchange experiences with and discuss ideas on the usage of Netflow/IPFIX in network management, the Network Management Research Group (NMRG) of the Internet Research Task Force (IRTF), together with the European EMANICS Network of Excellence, organized a one day workshop on October 30th, 2008, at the Leibniz Rechenzentrum (LRZ) in Munich. The workshop, which was organized by Ramin Sadre and Aiko Pras (UT) and hosted by Heinz-Gerd Hegering and Helmut Reiser (LMU / LRZ), was attended by about 40 people from industry and academia. The workshop was opened by Benoit Claise, who gave an overview of Netflow/IPFIX. The remainder of the day was structured according to the following questions:

- What technologies are developed to capture flows?
- What technologies are available to analyze flow data?
- How do sampling and aggregation affect the volume and accuracy of data collection and analysis?
- For what kind of applications can Netflow/IPFIX be used?
- Should we have a standard format for the annotation of Netflow/IPFIX traces?

A report of this meeting is currently being written and will be submitted to JNSM. Detailed minutes can be found in [49]. As a result of this meetings, their have been a series of interactions between Cisco, IsarNet and the UT on further collaboration in the area of flow analysis.

3 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 and IRTF-NMRG
- Emanics partners interact with industry on a bilareral basis
- Emanics partners organize special theta days. Two kinds of theta days exist: national and international
- Emanics partners create Podcast to transfer knowledge regarding main scientific events to industry

3.1 Interaction with industry within the context of IETF & IRTF-NMRG

Emanics partners have been very active in the IETF and IRTF-NMRG. Within the IETF, for example, within the context of the YANG design team and the NETMOD working group, there is strong collaboration between Emanics partners, Juniper Networks, Huawei USA, Ericsson, Juniper Networks, Tail-f, SNMP Research, Siemens-Nokia as well as Vigil Security. The joint Emanics / IRTF-NMRG workshop on Netflow/IPFIX usage, was attended by participants from rh-tec Business GmbH, NECLAB Europe, Verizon Business, IP Exchange GmbH, Fluke Networks, IsarNet AG, CESNET, Cisco, ntop, IP Exchange GmbH, Blue Coat Systems, Inc., NetDescribe GmbH and SWITCH. As a result of these industrial interactions, Emanics partners have received equipment to test NetConf Interoperability (See Annex A). Further details on industrial interaction within the context of IETF & IRTF-NMRG can be found in Section 2.

3.2 Bilateral collaboration

All Emanics partners interact on a bilareral basis with industry to discuss research issues related to EMANICS. These interactions take usually place at the institutes of the partners, or at the premisses of one of the industry partners. Some examples of companies Emanics partners interacted with, are presented in Table 3:

3.3 Theta days

In the second phase of the project several EMANICS partners organized theta days where certain topics related to Emanics research are discussed with multiple industrial pertners. Below is a selection of these meetings. Note that this selection is just a small subset of the interactions EMANICS partners had with industry, since it is not always possible to

Table 3: 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
KTH	Cisco	Distributed monitoring
KTH	Ericsson Research, Stockholm	Auto-configuration
KTH	IBM Research	Autonomic management
LMU	Fujitsu	Virtualization & IT management
LMU	HP Labs Bristol	AI-based automated planning to assist fault recovery
LMU	IBM	IT Management
LMU	LRZ	Virtualization
LMU	Siemens AG	Management of virtual IT solutions
LMU	TUV	IT Management
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

distinguish between EMANICS research results and other results. In addition, interaction with industry sometimes sometimes is confidential, such as in cases project plans are discussed or traces are shared.

One theta day was organized on October 1, 2007, at the FSC in Muenchen-Perlach. There were 10 participants from FSC, and about 10 from LRZ and LMU. There were presentations on topics like (in German): "Virtualisierung der Infrastruktur im SecP", "Technisches und organisches Service Management fr virtualisierte Umgebungen", "Virtualisierung als Grundlage fr Automatisierung im IT management", "Storage Virtualisierung", "Software-un Hardware-Aspekte bei Betriebskonzepten", " Server management im Blade Servers" and Virtual I/O Management.

Another meeting was organized on October 22, 2007, at the LRZ in Garching. This meeting was attended by 25 participants. Discussion took place on the following topics: 1) Business Service oriented Resource Management, 2) Model based resource mgt. strategies 3) IO Virtualization Concepts 4) Role based access control concepts for service and infrastructure management 5) Lifecycle mgt for a system mgt station Derived from these topics, about 10 topics for diploma theses and student practical work have been announced by LMU and LRZ.

Starting from October 2007 LMU had also monthly meetings with TUM and Siemens AG, Corporate Technology. Discussion topics included: 1) Trend Analysis for virtual IT solutions 2) Virtualization in Embedded Systems 3) Management of virtual IT solutions 4) Security of virtual IT solutions

On April 18th, 2008 a half day theta day on biometrics was organized in Munich. It was attended by Gabi Dreo Rodosek (UniBwM), Peter Breuer (DERMALOG), Martin Ditscherlein (TST Biometrics), Casimir Graf von Maltzan (TST Biometrics), Michael von Foerster (Bosch Sicherheitssysteme GmbH), Torsten Hope (Certego GmbH), Dr. Wolfgang Uebel (primion Technology AG), Steffen Gpel (Dimension Data) and Lutz Neugebauer (BITKOM). Three presentations from TST Biometrics, UniBwM, and Bitkom provided an insight into research activities in the area of biometrics and lively discussions on possible collaboration. As a first immediate result, UniBwM was included in the biometrics brochure of BITKOM (German Association for Information Technology, Telecommunications and New Media).

On Monday 28th April 2008, a theta day took place at the University of Federal Armed Forces Munich (UniBwM). In the morning, the topic "Applied security research" was discussed among the following participants: Gabi Dreo Rodosek (UniBwM), Gerhard Schabhser (Bundesamt fr Sicherheit in der Informationtechnik (BSI), German Federal Office for Information Security), Udo Helmbrecht (President of the BSI), Rainer Baumgart (secunet), Kai Martius (secunet), Christoph Hampe (Bosch Sicherheitssysteme GmbH, Bosch Security Systems), and Wolfgang Effing (Giesecke & Devrient). The workshop in the afternoon was open to a broader audience including also interested students and faculty from UniBwM. After introductions from the president of UniBwM Merith Niehuss and Gabi Dreo, Udo Helmbrecht (BSI) talked about "IT security research within the high-tech initiative of the German Federal Government". His presentation included an overview of security research clusters in Germany that showed a lack of representation in southern Germany. Kai Martius then gave a talk on "High security research - exotic or cutting edge", that comprised customer requirements, producer interests and research opportunities within different industries. The day was closed by a lively panel discussion with all workshop participants. This theta day promoted the objective of founding a security research group at UniBwM with the collaboration of the above mentioned companies.

In May 2008 LMU had a one week exchange of researchers with HP Labs, Bristol, UK. The subject of cooperation was: AI-based automated planning to assist fault recovery, and planning processes for networked IT services

In May 2008 UniBW had a series of meetings with TST, Primion and Dermalog. The topic was biometrics: use cases and cooperation possibilities. In June 2008 Idencom joined these meetings

On June 19, 2008 a half day theta day took place on SPAM detection. The meeting was organized at the University of Twente, and attended by representatives of Quarantainenet, which is a company that specialises in the development of network security and network management tools. The meeting discussed two new approaches to detect SPAM, based on IP addresses and netflow traces. Further research and interaction in this area has been agreed upon.

In June, July and September, 2008, several theta days were organized on the topic Intrusion Detection in Supervisory Control And Data Acquisition (Scada) networks. Meetings were in general attended by 10 people, coming from UT, Witteveen & Bos, ABB and Waternet. As a result, a joint project proposal was developed and the UT performs security measurements on several of such networks.

Starting in August, 2008, several meetings were organized by the UT on the topic of Phishing detection. In the discussions several companies participated, including SURFnet (the dutch NREN), Tiscali/Telfort (an ISP), Quarantainenet (a SME that specialises in the development of network security and network management tools), ING/Direct (Internet bank) and Hives (most popular social network in the Netherlands). As a result, a proposal on this topic has been submitted for the dutch Sentinels programme.

On September 4, 2008 Mark Burgess (HIO) attended a meeting on ”IT management challenges for the next decade”, This meeting took place at Snow’s headquarters in the NL. There were about 150 people there (120 from snow and 30 of their customers who came to listen).

Between September 8-12, 2008 Mark Burgess (HIO) visited RIPE’s network centre in Amsterdam. Mark discussed there ”Automation by cfengine” (see WP6). There were 10 people present and detailed discussions.

LMU, UT and IUB started preparing a joint Emanics / IRTF-NMRG Workshop on Netflow/IPFIX Usage in Network Management. This meeting will be held on October 30, 2008 at the LRZ in Munich. Participants from several industries will attend, such as Cisco, NEC, rh-tec Business GmbH, IsarNet AG and Switch. For details see: http://www.simpleweb.org/netflow/

On November 20, 2008 Rolf Velthuys (KPN, the Netherlands) visited the UT to talk about research and developments.

3.4 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.

REPORT OF THE IRTF-NMRG

A first podcast summarizes the results of the joint IRTF-NMRG and EMANICS Workshop on Challenges in Network Management research. The podcast has been recorded at the plenary IETF meeting on March 22, 2007, in Prague. The title is: Key challenges in Network Management research, the presenter is Aiko Pras (UT).

IM 2007 OPENING SESSION

The following podcasts have been recorded at the opening session of the 10th IFIP/IEEE Integrated Management Symposium (IM 2007), which was held May 21-25, 2007, in Munich, Germany:

- Opening by Prof. Faerber, member of the academic senate of the University of Federal Armed Forces, Munich
- Opening by Alexander Keller, IBM T.J. Watson Research Center, USA
- Opening by Prof. Heinz-Gerd Hegering, Leibniz Supercomputing Center, Germany
- Opening by Hans Spitzner, Bavarian Vice-Minister of Economic Affairs, Infrastructure, Transport and Technology
- Keynote by Ulrich Pfeiffer, Regional CTO, Software Global Business Unit, HP

NOMS 2006 DISTINGUISHED EXPERT PANEL ON VOIP MANAGEMENT

The following podcasts have been recorded at the 2006 IEEE/IFIP Network Operations and Management Symposium on April 6, 2006, in Vancouver, Canada.

- VoIP Management - Does the Emperor have any clothes on?. Intro by Aiko Pras (University of Twente)
- Provider challenges in VoIP?. By Magda Nassar (AT&T).
- Applications and Trends in Wireless Consumer Networking. By Alexander Gelman (Panasonic).

- VoIP Management. By Amy Pendleton (Nortel).
- VoIP Management - The Emperor Has No Clothes On. By Henry Sinnreich (Pulver.Com).
- Closing discussion between panelists and audience.

SNMP RELATED PODCASTS

The following SNMP related podcasts are now available for industry and academia:

- Management standards:Overview and history of the ISO, ITU-T, IETF and DMTF management standards. It resents CMIP/CMIS, TMN and SNMP, and discusses the main differences between these approaches.
- Introduction to SNMP: Goals, principle operation, structure and standards.
- Structure of Management Information: SMI Versions 1 and 2. After an introduction it discusses scalar objects (naming,instances, definition) and table objects (definition). Textual conventions and notificationtypes are introduced too.
- Introduction to MIBs: This tutorial starts with an example, discusses the difference between MIB definition and instance, and the modular structure of MIBs. It gives the list of current IETF hardware MIBs, transmission MIBs, network MIBs, transport MIBs, application MIBs and vendor specific MIBs. It concludes with naming of MIB modules.
- MIB-II: The standard Management Information Base: MIB-II. After an introduction it discusses the status of the MIB-II, the original design goals, its basic structure and relationship to the TCP/IP layers, and the various groups (system, IF, AT, IP, ICMP, TCP, UDP, EGP, Transmission and SNMP).

3.5 Other interactions

Several EMANICS partners investigated the possibilities to collaborate within the CELTIC context. The problem with CELTIC, however, is that acceptance is a two phase process. In the first phase a project plan must be submitted and accepted at a European level. Once the project is accepted, funding must be requested at national level. Several EMANICS partners have experienced that, after acceptance at EUropean level, funding could not be obtained at national level. As a consequence, partners had to withdraw from the CELTIC proposal.

4 Cooperation with other networks and projects

4.1 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. Cooperation with professional organizations will focus on IFIP WG6.6 (Management of Networks and Distributed Systems) and IEEE CNOM. In the next period collaboration with other European projects will focus on the COST 605 (Econ@Tel) project; such collaboration could take the form of a joint workshop.

4.1.1 Joint EMANICS/EuroFGI - EUNICE 2007 Summer School

As a joint activity, EMANICS and EuroFGI organized the 13th EUNICE Open European Summer School and IFIP TC6.6 Workshop on Dependable and Adaptable Networks and Services. This workshop took place between July 18-20, 2007 at the University of Twente, the Netherlands. This Summer School is sponsored by IFIP TC6.6, IEEE ComSoc and the Netherlands Organization for Scientific Research (NWO). Proceedings are published as part of the Springer LNCS series. The number of participants was 64.

The main goal of the EUNICE Summer School is to give young researchers, and particularly Ph.D. students, the opportunity to present their work at an international level. The EUNICE Summer School also seeks to offer comprehensive and inspiring invited talks from experienced experts in the field, providing a context for discussions on ongoing research and new challenges. The EUNICE Summer School is an initiative of the European University Network of Information and Communication Engineering, or EUNICE Network for short. Although the summer school events are organized by the member institutions taking turns, submission to and participation in the events are open to researchers outside the EUNICE Network.

The 13th EUNICE Summer School returned to Enschede, The Netherlands, where it was hosted earlier in 2000. Back in 2000, the theme of the summer school was ‘Innovative Internet Applications.’ Much has changed since then: wireless network technologies have become a constantly growing part of the Internet infrastructure, and increasingly smaller and more powerful computing devices with flexible connectivity open the possibility of new services and applications. The EUNICE 2007 theme, ‘Dependable and Adaptable Networks and Services,’ linked to this change and how it affects and is affected by research in the field of information and communication technology. One of the main challenges in the next decade will be to make the Internet and the services that are provided on top of it more dependable and adaptable. Research on this theme is needed for fixed, wireless and adhoc networking, ubiquitous communication and computing, sensor networks, and context-awareness. While individual mobile applications with context-aware and personalized features emerged, at the same time many challenges for network and service architectures were imposed concerning integration, interoperability, management, provisioning, reliability and security. On the one hand research has to make available a sound understanding of these applications and their supporting service and network architectures. On the other hand, research should produce service and network infrastructure solutions to be able to provide the necessary quality of service for the envisioned applications [50].

4.1.2 Joint EMANICS/AGAVE Workshop on Management of Network Virtualisation

As a joint activity, EMANICS and AGAVE organized a joint workshop on Management of Network Virtualisation. This very successful workshop took place on November 6th, 2007, in Brussels. Speakers from both projects, as well as a number of invited speakers, presented their work.

The workshop focussed on discussing the latest developments in network virtualisation: an increasingly important topic for today's networks as well as the future Internet.

Network virtualisation serves several goals. On the one hand service differentiation may be achieved through the provisioning and management of virtual network resources. Virtual networks may support certain service features/requirements in terms of packet transfer characteristics, robustness and resilience to failures and congestion. On the other hand, the network provider may use virtual networks to facilitate network management, e.g. through load balancing of traffic, or partitioning of network resources. Virtual networks may span a single provider domain but may also extend across multiple providers to provide end-to-end virtual Internets. The workshop addressed architectures, business models and network management solutions for network virtualisation as well as specific mechanisms to implement and operate virtual networks.

The slides of the presentations can be downloaded from [51].

4.1.3 Joint EMANICS/COST IS605 Dagstuhl Seminar

In January 2008 UniZH organized a Dagstuhl Perspectives Seminar on “Telecommunication Economics”. This seminar can be seen as a joint interaction between EMANICS WP8 and the COST Action IS605.

The goal of this Perspectives Workshop on ”Telecommunication Economics” was to discuss and develop a strategic research and training outline among key people/organizations in order to enhance the competence in the field of telecommunication economics and respective network management tasks for integrated Internet and telecommunication networks. The view on respective guidelines and recommendations to relevant players (end-users, enterprises, operators, regulators, policy makers, and content providers), especially focusing on the provision of new converged broadband, wireless, content delivery networks to people and enterprises was the core.

The main objective of this Workshop was to allow business partnering to drive networking services and their sustainable provisioning for consumers and enterprises alike. This included in more specific detail the following four areas:

- The support of engineering leadership gained in mobile, broadband, digital TV, and wire-line communications, and selected media fields, by new sustainable business models in a fully deregulated and diversified demand framework.
- The study and identification of business opportunities throughout the value chain, especially for enterprises, content, and specialized services.
- The contribution to a strategy relative to socio-economic needs by increasing the motivation for deployment of cost effective and flexible solutions using networks and content.
- The provisioning of guidelines and recommendations for utilizing different types of technologies and quantify necessary actions. These results will potentially supply regulators and standardization bodies with analysis and guidelines for creating conditions for fast growing competitive mobile, broadband, and content markets while speeding up business.

4.1.4 Joint ACF, AUTOI, EMANICS Workshop on Autonomic Management in the Future Internet

On May 14, 2008 a joint ACF, AUTOI and EMANICS Workshop on Autonomic Management in the Future Internet was organized at the Universitat Politcnica de Catalunya, Barcelona, Spain. The workshop brought together researchers from three communities the ACF, the AUTOI FP7 programme, and the EMANICS NoE to discuss their respective challenges and the potential solutions for them, regarding realizing the vision of the Future Internet. It is believed that this meeting has been highly beneficial for all three. The ACF has been able to present part of its current objectives and attract researchers to participate in its experts and working groups. AUTOI has have the opportunity to share its views on building a new architecture for the Future Internet and how this architecture can relate to and drive the standardization process. Finally, it helped EMANICS to fulfill its objective of disseminating and giving visibility to its work, as well as enabling it to integrate with a wider community. Subjects of interest for discussion included:

- Self-Managing Frameworks and Architectures
- Knowledge Engineering, including Information Modelling and Ontology Design
- Policy Analysis and Modeling
- Service Composability
- Service Deployment
- Semantic Analysis and Reasoning Technologies
- Virtualization of Resources
- Self-Managed Networks
- Orchestration Techniques

- Context and Context-Awareness
- Adaptive Management

The workshop was organized by Joan Serrat (UPC), Spyros Denazis, Joel Fleck and John Strassner. More information about the workshop can be found here [52].

4.1.5 NAVS November 2007 concertation meeting

EMANICS members also participated at the 9th Networked Media (NAVS) Concertation Meeting, which took place in Brussels on 13-14 November 2007. On the first day EMANICS members organized the Standards and Interoperability session, for which they invited Vic Hayes, who has been chairman of the IEEE 802.11 (WLAN) standardization efforts for more than 10 years. His message was that, to be successful, researchers should actively participate for many years within standardization organizations; it is not sufficient to just bring an idea to a standardization organization and hope that they will standardize it within 1 or 2 years. On the second day of the NAVS meeting, together with members from AGAVE, a report was presented of our joint workshop on Management of Network Virtualisation.

4.1.6 EU FutureInternet meetings

On November 25, 2008, Olivier Festor (INRIA) and Aiko Pras (UT) joined the Future Media 3D Internet task force meeting in Lyon, France. Between November 25-27 Olivier Festor (INRIA), David Hausheer (UniZH), Christian Morariu (UniZH), Iris Hochstatter (UniBW), Gabi Dreo (UniBW) and Aiko Pras (UT) joined the ICT event in Lyon. At that event, Emanics members organized a special meeting on management of the future Internet.

Between December 9-12 Olivier Festor (INRIA), David Hausheer (UniZH), George Pavlou (UCL), Alex Gallis (UCL) and Aiko Pras (UT) joint the FIA in Madrid. AT that meeting, the MANA activities were organized by Alex Gallis.

4.1.7 IFIP TC6-WG6.6

In September 2007, at the Borovez, Bulgaria meeting of IFIP TC6, Aiko Pras (UT) and Olivier Festor (INRIA) took over the chair / vice-chair positions of IFIP WG6.6. The aims of IFIP WG6.6 is to facilitate cooperation between different organizations and individuals internationally in the areas of distributed operations and management, integrated network management, systems management, and service engineering. To be an effective conduit in the technology transfer between the academic and research communities, industry and the standard bodies. The scope of WG 6.6 is Operations and Management paradigms and technologies for novel and complex systems and networks continuously evolving over different levels of abstraction such as element, network, service, and business level. The Operations and Management encompass different function areas such as configuration, fault, accounting, performance and security. This includes new technologies such as autonomic computing, distributed and policy based management as well as already established management protocols and information models. The scope of the working group encompass the operation and management of existing networked systems including enterprise networks and multi-provider networks as well as emerging ad-hoc and sensor networks, Grids, peer-to-peer networks and interplanetary networks.

4.1.8 Autonomic Communication Forum

In 2007 Joan Serrat (UPC) became co-chair of the Policies Experts Group of the Autonomic Communication Forum (ACG). The ACF organizes teleconference meetings on a monthly basis and at least twice a year phase-to-phase meetings. Phase-to-phase meetings are open to companies and individuals and the aim is to present the evolution of activities of the different Experts Groups and Working Groups within the ACF. Among the participants up to now there are representatives from Telefonica, Whitestein Technologies, Hitachi, IBM, HP, Motorola and Intel. The first phase-to-phase meeting where Joan Serrat participated took place in March 2007 at the EU premises with the attendance of at least the above company representatives and two EU officers. The second took place in San Jose (CA) in November 2007. As co-chair of the Policies Experts Group Joan Serrat had the opportunity to present in these meetings his current projects in the field of policy based management, which are part of EMANICS WP9. As the most tangible result of this activity a joint paper with Motorola and others has been presented at the EASe 2008 workshop in Belfast, April 2008.

4.1.9 Additional forms of cooperation

EMANICS partners have established strong contacts with the main universities and industries world-wide, and play a leading role in the world of network and service management. This becomes apparent by the fact that EMANICS partners became member of the IM/NOMS Steering Committee, have organized some of the main conferences in our field (like IM'07) and hold positions in the top journals in our field:

- IEEE Communications Magazine: editors
- Transactions on Network and Service Management: editorial board members
- Journal on Network and Systems Management,: editorial (advisory) board members
- International Journal on Network management: associate editor and editorial board members.

Also in this period Joan Serrat (UPC) continued collaborating within the ACF. Between September 22 and 26, 2008 Manweek was organized at Samos Island, Greece. Emanics members were there responsible for various activities, such as general manweek submissions (UT), chairing MMNS (UCL) and organizing the IFIP WG6.6 meeting. Emanics members interacted with COST TMA, and will help organizing the COST-TMA workshop in May 2009 (Aachen). Emanics members (UT) joint the two-day IFIP TC 6 meeting.

5 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 and the IRTF-NMRG. In this period, 2 RFCs and 38 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 members have organized three IRTF-NMRG meetings, are members of the IETF MIB Doctors and the IETF Security Directorate.

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, such as:

- the Euro-FGI NoE: joint organization of the EUNICE 2007 Summerschool,
- the AGAVE project: joint workshop on the management of virtual networks,
- the COST IS605 action: joint Dagstuhl Seminar on “Telecommunication Economics”.
- the COST TMA action: Traffic Measurements and Analysis.

EMANICS helped organizing parts of several EU Future Internet activities, such as Management of the Future Internet (ICT Event Lyon) and the MANA activity (FIA, Madrid). 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 is running well and made very strong contributions to the IETF and IRTF.

6 Abbreviations

AAA	Authentication, Authorization, and Accounting
ACF	Autonomic Communication Forum
BGP	Border Gateway Protocol
CETIM	University of Federal Armed Forces Munich
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

References

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

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

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

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

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

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

[7] as presented at the IETF OPSAREA meeting of the 70th IETF meeting: http://www3.ietf.org/proceedings/07dec/slides/opsarea-0.pdf Slides of the 23th NMRG meeting.

[8] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-10, July 2007.

[9] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-10, September 2007.

[10] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-11, November 2007.

[11] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-12, February 2008.

[12] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-13, August 2008.

[13] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-14, October 2008.

[14] D. Harrington and J. Schönwälder. *Transport Subsystem for the Simple Network Management Protocol (SNMP)*, draft-ietf-isms-tmsm-15, November 2008.

[15] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-marinov-syslog-snmp-01, February 2008.

[16] V. Marinov and J. Schönwälder. *Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG* , draft-marinov-syslog-snmp-02, November 2008.

[17] 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.

[18] 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.

[19] J. Schönwälder. *SNMP Traffic Measurements and Trace Exchange Formats*, draft-irtf-nmrg-snmp-measure-02, December 2007.

[20] J. Schönwälder. *SNMP Traffic Measurements and Trace Exchange Formats*, draft-irtf-nmrg-snmp-measure-03, February 2008.

[21] J. Schönwälder. *SNMP Traffic Measurements and Trace Exchange Formats*, draft-irtf-nmrg-snmp-measure-04, March 2008.

[22] J. Schönwälder. *SNMP Traffic Measurements and Trace Exchange Formats*, draft-irtf-nmrg-snmp-measure-05, May 2008.

[23] J. Schönwälder. *SNMP Traffic Measurements and Trace Exchange Formats*, draft-irtf-nmrg-snmp-measure-06, September 2008.

[24] J. Schönwälder. *Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats*, RFC 5345, October 2008.

[25] J. Schönwälder. *Simple Network Management Protocol (SNMP) Context EngineID Discovery*, draft-ietf-opsawg-snmp-engineid-discovery-01, January 2008.

[26] J. Schönwälder. *Simple Network Management Protocol (SNMP) Context EngineID Discovery*, draft-ietf-opsawg-snmp-engineid-discovery-02, February 2008.

[27] J. Schönwälder. *Simple Network Management Protocol (SNMP) Context EngineID Discovery*, draft-ietf-opsawg-snmp-engineid-discovery-03, July 2008.

[28] J. Schönwälder. *Simple Network Management Protocol (SNMP) Context EngineID Discovery*, RFC 5343, September 2008.

[29] A. Bader, L. Westberg, G. Karagiannis, C. Kappler, and T. Phelan. *RMD-QOSM - The Resource Management in Diffserv QOS Model,* draft-ietf-nsis-rmd-11, August 2007.

[30] A. Bader, L. Westberg, G. Karagiannis, C. Kappler, and T. Phelan. *RMD-QOSM - The Resource Management in Diffserv QOS Model,* draft-ietf-nsis-rmd-12, November 2007.

[31] A. Bader, L. Westberg, G. Karagiannis, C. Kappler, and T. Phelan. *RMD-QOSM - The Resource Management in Diffserv QOS Model,* draft-ietf-nsis-rmd-13, July 2008.

[32] J. Manner, G. Karagiannis, and A. McDonald. *NSLP for Quality-of-Service Signaling,* draft-ietf-nsis-qos-nslp-15, July 2007.

[33] J. Manner, G. Karagiannis, and A. McDonald. *NSLP for Quality-of-Service Signaling,* draft-ietf-nsis-qos-nslp-16, February 2008.

[34] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *LC-PCN - The Load Control PCN Solution*, draft-westberg-pcn-load-control-01, August 2007.

[35] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *LC-PCN - The Load Control PCN Solution*, draft-westberg-pcn-load-control-02, November 2007.

[36] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *LC-PCN - The Load Control PCN Solution*, draft-westberg-pcn-load-control-03, February 2008.

[37] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *LC-PCN - The Load Control PCN Solution*, draft-westberg-pcn-load-control-04, July 2008.

[38] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *LC-PCN - The Load Control PCN Solution*, draft-westberg-pcn-load-control-05, November 2008.

[39] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *Pre-Congestion Notification Encoding Comparison*, draft-chan-pcn-encoding-comparison-01, November 2008.

[40] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *Pre-Congestion Notification Encoding Comparison*, draft-chan-pcn-encoding-comparison-02, February 2008.

[41] L. Westberg, A. Bhargava, A. Bader, and G. Karagiannis. *Pre-Congestion Notification Encoding Comparison*, draft-chan-pcn-encoding-comparison-03, February 2008.

[42] J. Schönwälder. *Protocol Independent Network Management Data Modeling Languages - Lessons Learned from the SMIng P]roject, draft-schoenw-sming-lessons-01*, September 2007.

[43] J. van den Broek, J. Schönwälder, A. Pras, and M. Harvan. *SNMP Trace Analysis Definitions ,* draft-schoenw-nmrg-snmp-trace-definitions-00, January 2008.

[44] J. van den Broek, J. Schönwälder, A. Pras, and M. Harvan. *SNMP Trace Analysis Definitions,* draft-schoenw-nmrg-snmp-trace-definitions-01, January 2008.

[45] J. van den Broek, J. Schönwälder, A. Pras, and M. Harvan. *SNMP Trace Analysis Definitions,* draft-schoenw-nmrg-snmp-trace-definitions-02, April 2008.

[46] J. Schönwälder. *Common YANG Data Types, draft-schoenw-netmod-yang-types-00*, May 2008.

[47] J. Schönwälder. *Common YANG Data Types, draft-schoenw-netmod-yang-types-01*, November 2008.

[48] Homepage of the IRTF-NMRG: *http://www.ibr.cs.tu-bs.de/projects/nmrg/*.

[49] Minutes of the IRTF/NMRG Emanics workshop on Netflow/IPFIX usage : *http://www.ibr.cs.tu-bs.de/projects/nmrg/minutes/minutes-025.txt*.

[50] A. Pras and M. J. van Sinderen, editors. *Dependable and Adaptable Networks and Services, Proceedings of the 13th Open European Summer School and IFIP TC6.6 Workshop, EUNICE 2007*, Enschede, The Netherlands, July 2007. LNCS.

[51] Slides presented at the joint AGAVE/EMANICS workshop on Network Virtualisation: http://www.ist agave.org/events/index.html.

[52] Home page of the Joint ACF AUTOI EMANICS Workshop on Autonomic Management in the Future Internet Workshop: *http://www.autonomic-communication-forum.org/node/62*.

Appendices

A NETCONF Interoperability Testing

NETCONF Interoperability Testing

Iyad Tumar, Ha Manh Tran, Jürgen Schönwälder
Computer Science, Jacobs University Bremen, Germany
{i.tumar, h.tran, 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 (XML) based data encoding on top of a simple Remote Procedure Call (RPC) layer.

This report describes a NETCONF interoperability testing plan that is used to test whether NETCONF protocol implementations meet the NETCONF protocol specification. The test of three independent NETCONF implementations reveals bugs in several NETCONF implementations. While constructing test cases, a few shortcomings of the specifications were identified as well.

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 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 many features required for configuration management that were lacking in other network management protocols, like for example 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 report is twofold. First, we describe a NETCONF interoperability testing plan that is used to test whether the NETCONF protocol implementations meet the NETCONF protocol specification in RFC 4741. 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) 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 (NOT) 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) [5] is the mandatory secure transport that all NETCONF clients and servers are required to implement as a means of promoting interoperability [6].

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].

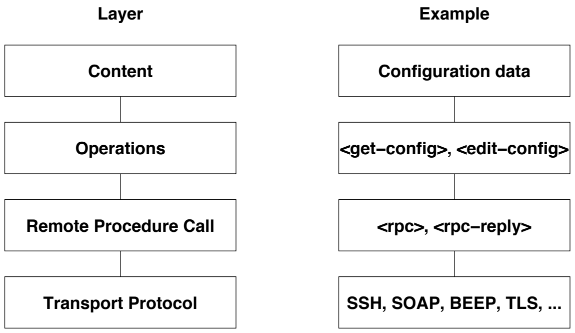

Figure 1. NETCONF protocol layers [1].

Figure 2 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 is created, deleted, replaced or merged. 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.

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

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]

Figure 2. NETCONF protocol operations (arguments in brackets are optional) [4]

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 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.

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

3 Systems Under Test

The systems used for the NETCONF interoperability testing comprise Cisco 1802 integrated services routers, Juniper J6300 routers, and the Tail-f ConfD software 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. Table 1 briefly describes the three platform and the SSH support of the three systems. The ConfD is installed and configured to run on a Linux XEN virtual machine [9].

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

Table 1. Systems under test

Table 2 presents the NETCONF capabilities announced by the systems under test. The Tail-f system supports all capabilities except the `:startup` capability. The Cisco and Juniper 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. In addition to the capabilities listed in Table 2, each system announces several proprietary capabilities.

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

Table 2. NETCONF capabilities supported by the systems under test

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 system does not seem to have the event driven parser or at least it does 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 get use for users who like to learn how things work without using tools other than a scratch pad and a cut and paste device.

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 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.

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 [1] and RFC 4742 [6].

Table 3 lists the test suites and the number of test cases in each suite. The total number of test cases is currently 87. 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 during the execution of the test suite on the systems under test. This led to a more tightly integrated organization of the test cases.

The most basic test suite is the GENERAL test suite. It includes test cases for general operations such as `lock`, `unlock`, `close-session`, `kill-session`, `discard-changes`, `validate`, and `commit`. To test the behavior of the system under test, a client sends `lock` requests and checks the reaction of the server. For exam-

Test Suite	Number of Test Cases
GENERAL	19
GET	11
GET-CONFIG	16
EDIT-CONFIG	15
VACM	26

Table 3. Test Suites

ple, a test case might send a `lock` requests to an already locked datastore and then verify that the server reacts with a proper error message. The GENERAL test suite also tests the general format of requests and responses. For example, test cases check whether response messages contain the `message-id` attribute and that it matches the value contained in the request message.

The second test suite is the GET suite. It contains a collection of test cases that are intended to be used to test the filter mechanism of the `get` operation. For example, a test case checks whether the systems under test returns the entire content of the contents of the entire running configuration data plus the operational state when no filter is used. The third suite is the GET-CONFIG suite. It contains test cases related to the filter mechanism of the `get-config` operation.

The fourth suite is the EDIT-CONFIG suite. It includes test cases for the `edit-config`, `copy-config`, and the `delete-config` operations. Several of the test cases contained in the EDIT-CONFIG suite are data model specific and we had to implement several tests in different ways due to a lack of common data models. This extra work can be reduced if implementers volunteer to implement a common data model. A proposal for such a data model, a YANG version of the `SNMP-VIEW-BASED-ACM-MIB`, is contained in the appendix of this paper.

The last test suite is the `vacm` suite. It includes a collection of test cases to test the NETCONF protocol operations against the VACM data model (see appendix).

5 Test Tool (NOT)

We have implemented a tool called NOT (NETCONF interOperability Testing tool) to automatically execute the test suites against a system under test. Our NOT tool basically performs the following operations:

- connecting to a system under test using the SSH
- verifying the initial `hello` message
- 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 [1].
- reporting the failure or the success of each test

The tool is equipped with an XML parser to analyze the responses for verification; i.e., 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 is missing or any error is returned. The following example shows the information of a response without errors or warnings:

```
---ELEMENT TYPES
  rpc-reply 1
         ok 1
---ATTRIBUTE TYPES
 message-id 1
      xmlns 1
---ATTRIBUTE VALUES
 message-id [u'1007']
      xmlns [u'urn:ietf:params:xml:\
               ns:netconf:base:1.0']
---TEXT PARTS
            []
```

We have used the Python unit testing framework [10]. 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 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 re-use and clean the testing environment easily. The tool organizes test cases into several collections of test cases, namely test suites, that have been 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 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.

This page was intentionally removed as requested by vendors.

7 Conclusion

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 NOT tool, which automates the execution of test runs.

We have used the NOT tool to test three 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.

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 NOT 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, Juniper Networks, December 2006.

[2] C. Sperberg-McQueen, J. Paoli, E. Maler, and T. Bray. *Extensible Markup Language (XML) 1.0.* CERT, Second edition, October 2000.

[3] J. Case, R. Mundy, D. Partain, and B. Stewart. Introduction and Applicability Statements for Internet Standard Management Framework. RFC 3410, SNMP Research, Network Associates Laboratories, Ericsson, December 2002.

[4] J. Schönwälder, M. Björklund, and P. Shafer. Network Configuration Management using NETCONF and YANG. *(under review)*, 2008.

[5] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Protocol Architecture. RFC 4251, SSH Communications Security Corp, Cisco Systems, December 2006.

[6] M. Wasserman and T. Goddard. Using the NETCONF Configuration Protocol over Secure Shell (SSH). RFC 4742, ICEsoft Technologies, Inc., December 2006.

[7] S. Chisholm and H. Trevino. NETCONF Event Notifications. RFC 5277, Nortel, Cisco, July 2008.

[8] M. Mealling. An IETF URN Sub-namespace for Registered Protocol Parameters. RFC 3553, SSH Communications Security Corp, Cisco Systems, June 2003.

[9] 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 *Proceedings of the 19th ACM Symposium on Operating Systems Principles*, October 2003.

[10] Python unit testing framework. http://pyunit.sourceforge.net/. Last access in November 2008.

A SNMP Yang Module

```
module snmp {

  /* $Id: snmp.yang 3001 2008-10-14 14:56:23Z schoenw $ */

  /*
   * Q1: What to do about permanent or readonly table entries?
   */

  namespace "urn:ietf:params:xml:ns:yang:snmp";
  prefix "snmp";

  include "snmp-common";
  include "snmp-vacm";

  organization
   "IETF NETMOD (NETCONF Data Modeling Language) Working Group";

  contact
   "Editor:   Juergen Schoenwaelder
              <mailto:j.schoenwaelder@jacobs-university.de>";

  description
   "This module contains a collection of YANG definitions for
    configuring SNMP engines via NETCONF.

    Copyright (C) The IETF Trust (2008).  This version of this
    YANG module is part of RFC XXXX; see the RFC itself for full
    legal notices.";
  // RFC Ed.: replace XXXX with actual RFC number and remove this note

  revision 2008-10-11 {
    description
      "Initial revision, published as RFC XXXX.";
  }
  // RFC Ed.: replace XXXX with actual RFC number and remove this note

}
```

B SNMP Common Yang Submodule

```
submodule snmp-common {

  /* $Id: snmp-common.yang 3016 2008-11-03 08:56:59Z mbj@tail-f.com $ */

  belongs-to snmp {
    prefix snmp;
  }

  organization
   "IETF NETMOD (NETCONF Data Modeling Language) Working Group";

  contact
   "Editor:   Juergen Schoenwaelder
              <mailto:j.schoenwaelder@jacobs-university.de>";
```

```
description
 "This submodule contains a collection of common YANG definitions
  for configuring SNMP engines via NETCONF.

  Copyright (C) The IETF Trust (2008).  This version of this
  YANG module is part of RFC XXXX; see the RFC itself for full
  legal notices.";
// RFC Ed.: replace XXXX with actual RFC number and remove this note

revision 2008-10-14 {
  description
    "Initial revision, published as RFC XXXX.";
}
// RFC Ed.: replace XXXX with actual RFC number and remove this note

/*** collection of SNMP specific data types ***/

typedef admin-string {
  type string {
    length "0..255";
  }
  description
   "Represents and SnmpAdminString as defined in RFC 3411.";
  reference
   "RFC 3411: An Architecture for Describing SNMP Management Frameworks";
}

typedef identifier {
  type admin-string {
    length "1..32";
  }
  description
   "Identifiers are used to name items in the SNMP configuration
    data store.";
}

typedef context {
  type admin-string {
    length "0..32";
  }
  description
   "The context type represents an SNMP context name.";
}

typedef sec-name {
  type admin-string;
  description
    "The sec-name type represents an SNMP security name.";
}

typedef mp-model {
  type union {
    type enumeration {
      enum any     { value 0; }
      enum SNMPv1  { value 1; }
      enum SNMPv2c { value 2; }
      enum SNMPv3  { value 3; }
    }
```

```
      type int32 {
        range "0..2147483647";
      }
    }
    reference
     "RFC3411: An Architecture for Describing SNMP Management Frameworks";
  }

  typedef sec-model {
    type union {
      type enumeration {
        enum any     { value 0; }
        enum SNMPv1  { value 1; }
        enum SNMPv2c { value 2; }
        enum USM     { value 3; }
      }
      type int32 {
        range "0..2147483647";
      }
    }
    reference
     "RFC3411: An Architecture for Describing SNMP Management Frameworks";
  }

  typedef sec-level {
    type enumeration {
      enum no-auth-no-priv { value 1; }
      enum auth-no-priv    { value 2; }
      enum auth-priv       { value 3; }
    }
    reference
     "RFC3411: An Architecture for Describing SNMP Management Frameworks";
  }

  typedef engineid {
    type binary {
      length "5..32";
    }
    reference
     "RFC3411: An Architecture for Describing SNMP Management Frameworks";
  }

  container snmp {
    description
      "Top-level container for SNMP related configuration and
       status objects.";
  }

}
```

C SNMP VACM Yang Submodule

```
submodule snmp-vacm {

  /* $Id: snmp-vacm.yang 3016 2008-11-03 08:56:59Z mbj@tail-f.com $ */

  belongs-to snmp {
```

```
  prefix snmp;
}

include "snmp-common";

organization
 "IETF NETMOD (NETCONF Data Modeling Language) Working Group";

contact
 "Editor:   Juergen Schoenwaelder
            <mailto:j.schoenwaelder@jacobs-university.de>";

description
 "This submodule contains a collection of YANG definitions for
  configuring the View-based Access Control Model (VACM) of
  SNMP via NETCONF.

  Copyright (C) The IETF Trust (2008).  This version of this
  YANG module is part of RFC XXXX; see the RFC itself for full
  legal notices.";
// RFC Ed.: replace XXXX with actual RFC number and remove this note

revision 2008-10-11 {
  description
    "Initial revision, published as RFC XXXX.";
}
// RFC Ed.: replace XXXX with actual RFC number and remove this note

/*** collection of VACM specific data types ***/

typedef view-name {
  type snmp:identifier;
  description
   "The view-name type represents an SNMP VACM view name.";
  reference
   "RFC3415: View-based Access Control Model (VACM) for the
             Simple Network Management Protocol (SNMP)";
}

typedef group-name {
  type snmp:identifier;
  description
   "The view-name type represents an SNMP VACM group name.";
  reference
   "RFC3415: View-based Access Control Model (VACM) for the
             Simple Network Management Protocol (SNMP)";
}

typedef wildcard-object-identifier {
  type string {
    pattern ’((([0-1]|\*)(\.(([1-3]?[0-9])|\*)))’
          + ’|((2|\*)\.((0|([1-9]\d*))|\*)))’
          + ’(\.((0|([1-9]\d*))|\*))*’;
  }
  description
   "The wildcard-object-identifier type represents an SNMP
    object identifier where subidentifiers can be a wildcard,
    represented by a *.";
```

```
}

augment /snmp:snmp {

  container vacm {
    config true;
    description
     "Configuration of the View-based Access Control Model (VACM).";

    /*** group definition (vacmSecurityToGroupTable) ***/

    list group {
      key name;
      description
       "Mapping of securityName and securityModel pairs into
        groups according to the vacmSecurityToGroupTable of
        the SNMP-VIEW-BASED-ACM-MIB.";

      leaf name {
        type group-name;
        description
         "The name of this VACM group.";
      }

      list member {
        key "sec-name";
        min-elements 1;
        description
         "A member of this VACM group. According to VACM, every
          group must have at least one member.";

        leaf sec-name {
          type snmp:sec-name;
          description
            "The securityName of a group member.";
        }

        leaf-list sec-model {
          min-elements 1;
          type snmp:sec-model;
          description
           "The securityModels under which this securityName
            is a member of this group.";
        }
      }
    }

    /*** access definition (vacmAccessTable) ***/

    list access {
      key "group context sec-model sec-level";
      description
       "Definition of access right for groups according to the
        vacmAccessTable of the SNMP-VIEW-BASED-ACM-MIB.";

      leaf group {
        type keyref {
          path "../../group/name";
        }
        description
         "The group to which the access rights apply.";
      }

      leaf context {
        type snmp:context;
        description
         "The context (prefix) under which the access rights apply.";
      }

      leaf sec-model {
        type snmp:sec-model;
        description
         "The security model under which the access rights apply.";
      }

      leaf sec-level {
        type snmp:sec-level;
        description
         "The minimum security level under which the access rights
          apply.";
      }

      leaf prefix-match {
        type empty;
        description
         "If present, the context must only match the prefix of
          a request. If absent, an exact match is required.";
      }

      leaf read-view {
        type view-name;
        description
         "The name of the MIB view of the SNMP context authorizing
          read access.";
      }

      leaf write-view {
        type view-name;
        description
         "The name of the MIB view of the SNMP context authorizing
          write access.";
      }

      leaf notify-view {
        type view-name;
        description
         "The name of the MIB view of the SNMP context authorizing
          notify access.";
      }
    }

    /*** view definition (vacmViewTreeFamilyTable) ***/

    list view {
      key name;
      description
```

```
         "Definition of MIB views according to the
          vacmViewTreeFamilyTable of the SNMP-VIEW-BASED-ACM-MIB.";

        leaf name {
          type view-name;
          description
           "The name of this VACM MIB view.";
        }

        list subtree {
          key "oids";

          leaf oids {
            type wildcard-object-identifier;
            description
            "A family of subtrees included in this MIB view.";
          }

          choice type {
            mandatory true;
            leaf included {
              type empty;
              description
               "The family of subtrees is included in the MIB view";
            }
            leaf excluded {
              type empty;
              description
               "The family of subtrees is excluded from the MIB view";
            }
          }
        }
      }
    }
  }
}
```

B 73th IETF Meeting Report

IETF 73

73rd Internet Engineering Task Force

Fabio Hecht

Facts

Date: 16th-21st November 2008

Location: Hilton Hotel, Minneapolis, MN, USA

Participants: 1115 registered

Participant from UZH: Fabio Hecht

ALTO – Application-Layer Traffic Optimization WG

The newly created ALTO WG is attracting great interest from the IETF. An estimated number of 240 persons attended the meeting.
The first talk was a short introduction, by the chairs, that presented the last important modifications in the charter, stressing important changes. The most important ones are the following:

- focus is peer selection only;
- goal is to perform better than random peer selection – not optimal.

After this talk, Aaron Falk talked about the IRTF p2prg (Peer-to-Peer Research Group). They are creating a new charter and are looking for chairs.

The next talk, by Enrico Marocco (chair, Telecom Italia), presented the latest updates in the problem statement draft, reviewing discussions since Dublin. The document already points the solution: "a topology information (...) will allow applications to improve their performance and will help ISPs make a better use of their network resources". It is very clear that the objective of the WG is to improve performance and reduce inter-domain traffic, focusing on localization of traffic. They say it can also be something other than localization, but it is not clear what can that be. The original document contained the word "oracle", referring to the solution of Feldmann et al., but due to requests the term has been changed. The first comment from the audience was that solutions should not be part of the problem statement – an analysis of the solution space must be done in the first place. Another concern regards privacy. The document states that "the application does not have to disclose information it may consider sensible", but it is actually very difficult to say the least to determine what is private and what is acceptable.

Sebastian Kiesel (USTUTT) presented his draft on requirements. He showed changes in the document since the Dublin meeting, the most important ones being the following:

- not seeking the optimal solution, just better than random one;
- removed the suggestion of a sorting oracle, that would be not appropriate for requirements ;

- define core set of attributes for expressing preference, extensible to other ones.

The document reads much like the one on problem statement, and a long discussion about this was started, including the theme of why a requirements document is useful after all. In the end, it was more or less agreed that the requirements should be revisited after the problem statement document is refined.

The next talk, by Richard Yang (P4P), was entitled “P4P Design and Implementation”. They are working with two services: location and pDistance. Location is stable and returns a PID for each peer. One PID groups peers that are close together, and the granularity can be played with (AS level is suggested). The pDistance service returns a distance between two peers. PIDs can be interdomain or interdomain, and the return value can be ordinal, or numeric (he prefers the latter). Types of metrics can be: hopcount, air-mile, cost (which is the default). A person in the audience asked why then not use one of the existing Internet maps (“looking glasses”) that are available, and how different would it be to just use them. This is a point that is still controversial.

Richard Woundy presented then the talk Comcast's Experiences In a P4P Technical Trial, in which he showed some details about the draft with same title. They are working directly with P4P and ran a test with their customers. The results were improved download speed, and localization (less interdomain traffic). The experiment involved a single, 21MB, file. It was a Pando client update, so users were forced to download it. Criticism to this experiment are:

- the file is small in comparison to what people have been trading in file sharing applications;
- it was a forced download, so the gains are maximized due to a large swarm, which is not always the case.

The next presentation was about the draft “ALTO Information Export Service”, which suggests that the clients download a table containing full preference information from the ISP so they do not have to keep on constantly querying the ALTO service. He argues that the P2P applications can already do a pretty good job figuring out routing information. What is missing is only the ISP preference, which can be described in a small enough table to be downloaded completely. The presentation included the format of the file, as contained in the draft, with three fields per record: designator (“asn” or “cidr”), AS number or IP prefix (CIDR), and a priority. In his example, the application would sort the peers in three sets: preferred, default, and to be avoided. The size of the table in the tests were 1.5Mbytes (compressed). Possible issues recognized by the author are the redistribution of information by peers (could produce outdated information) and, service discovery. This work is being carried on by BitTorrent.

Stefano Previdi (Cisco) presented the next talk, entitled Routing Proximity. His goal is to establish metrics to be classify peers with regard to proximity. Routing databases (ISIS/OSPF/BGP) have already proximity metrics, so they can be used for the purpose of calculating the distance between peers. He believes everything needed to achieve localization is already available. ALTO should be just an interface to support routing (e.g. BGP) information to overlay. An important question is the addition of other metrics, such as cost, link capacity, and congestion – term that appears as a prominent motivation in the charter text.

The last presentation, “A Multi Dimensional Peer Selection Problem”, by Saumitra Das, discussed the fact that many different factors influence peer selection. Some information might come from ISPs and but ultimately the peers make the selection using information such as reputation. He suggests that different types of ALTO servers (e.g. P4P) can coexist.

The meeting ended with a word from the chairs to keep up current work and discussion on the mailing list.

LEDBAT – LEss Than Best Effort Transport WG

LEDBAT is the newly created WG that stems from the TANA BoF. The name was changed since some people considered the term "Advanced Network Applications" too unspecific. Just like ALTO, it aims at coping with P2P traffic, but works at the transport layer. The idea is to design a protocol that does not interfere with regular (best-effort) traffic, utilizing unused bandwidth. Moreover, the protocol would be able to "scavenge" network resources that would otherwise be unused.

Stanislaw Shalunov (BitTorrent) opened the session with a charter recapitulation. The objective is "to standardize a congestion control mechanism that should saturate the bottleneck, mantain low delay, and yield to standard TCP". It originated at the P2PI workshop at MIT in May/2008, creating the ALTO and TANA BoFs in Dublin, which lead to the ALTO and LEDBAT WGs in Minneapolis. The problem being solved is that TCP fills router buffers if congested, and the buffer can be large, the likely worst case are home uplinks. Since most traffic on home uplink is P2P-related, it leads to a delay in other applications that users might be using. There are two work items: experimental congestion control and current practices of applications (using multiple connections). Applications (BitTorrent, web browsers, mail servers) create multiple connections to try and maximize throughput and add stability. The practice is common, but considered more a poorly documented hack. The idea is to research and document how applications use multiple connections. Bob Briscoe mentioned that they should take into consideration how to respond to the congestion. Another person asked whether the protocol should "yield to TCP" or to be something better, more modern than TCP.

Satish Raghunath (Juniper.net) presented the next talk, entitled "LEDBAT - App Practices and Recommendations". He mostly talked about why current P2P applications open multiple connections. Mentions reliability that comes with diversity, but comes with overhead, and impact delay-sensitive traffic, due to more state needed within TCP termination devices and middleboxes. The applications try and find a "right" number of connections – too few or too many can cause problems – the objective is to maximize download speed, for example, in BitTorrent. The objective is to elaborate a document with recommendations to the number of connections. The audience asked whether he will/did look also at UDP or only TCP? At the moment, only TCP, someone (!) could contribute with a draft. Another person pointed out that Firefox opens up to 16 connections to each host, is that a good or a bad number? People also pointed out that is not true that opening multiple connections always makes downloads faster. They experimented with the iPhone over 3G and stated that handshake and congestion control don't work, especially for small images it may not be worth to open another connection. Next step: do the research!

Murari Sridharan (Microsoft) presented next "Low priority TCP: Receive-Window Control". It was a paper presentation about BATS (background transfer service). They adapt the receiver window to create a low priority service, and he explains how. The algorithm has 2 modes: rate limiting mode (1) and window scaling mode (2). Mode 1: gets accurate RTT samples, mode 2: uses binary search to drive towards target window, assuming the value lies between Wmin and Wmax; depending on whether there is congestion, window size is adjusted. Bottom line: it maintains low delay and yields to TCP. It requires no support from the network, although additional information helps it adapt quicker. He suggests this work as a starting point of how LED could look like. Question 1: has he analyzed if it works with competition between several connections? The presented answered he is working on getting these numbers. Other important questions regarded RTT independence and whether the background flow should be starved if necessary, and respective answers are that it “tries” to be independent from RTT (whatever this means) and that starvation can be controlled.

The next presentation was very short – only 5 minutes – by Nick Weaver (Berkeley), entitled “A Couple Academic Thoughts on LEDBAT”. He affirmed that there are two separate problems without use of packet marking or AQM (active queue management): detect buffer occupancy problems and detect and yield in common congestion to other types of traffic. In his opinion, LEDBAT should be defined as a TCP operating mode. Only one side should need to use the defined congestion control policy (à la 4CP) in order to ease deployment issues. He raises the question on whether DiffServ marking should be used. Bob Briscoe thinks that marking would not work, because it doesn't matter what they put there the operator won't believe. The point is that they would be marking them to be low priority, not to get higher priority.

Stanislaw Shalunov (BitTorrent, chair) presented “Low Extra-Delay Background Transport”, his idea of what could be standardized by LEDBAT. In his view, the main problem is that TCP fills the buffer and it can be large, introducing high delay in case of congestion. This delay breaks real-time applications like VoIP when a P2P application (like BitTorrent) is running. It also slows down considerably traffic that is not real time, like web browsing. He raises the question of how large should the buffer be, but does not have the answer. This raises a long discussion, and Stanislaw mentions measuring one-way delay, which is deemed impossible by at least some of the audience. He presents details of his approach, which includes using smaller packets and estimating queue delay in order to reduce window size before packet loss occurs. The presenter states though that he has done it and tested in BitTorrent DNA by 7M active users. The audience asks whether he has any numbers to show and confirm his statements, but he has not. Part of the audience did not really agree that using small packets should help, the reality is that packets are of a small size for a long time. The author says that he uses smaller packets in order to minimize serialization time and be able to obtain faster speed in a slow link.

The meeting ended with a word from the chairs pointing the WG to future work. They envision researching how applications use multiple connections in order to maximize their download speed and plan to further refine current studied approaches.