F

A complete system integration of stream-based IP flow-record querier

VAIBHAV BAJPAI

Masters Thesis

School of Engineering and Science
Jacobs University Bremen
Bremen, Germany

June 2012

[January 10, 2012 at 19:44]

ABSTRACT

Short summary of the contents in English...

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

Part I

INTRODUCTION

You can put some informational part preamble text here

1 TRAFFIC MEASUREMENT APPROACHES

2 FLOW EXPORT PROTOCOLS

2.1 NETFLOW

2.2 IPFIX

2.3 SFLOW

3 LANGUAGES AND TOOLS

4

LEGAL CONSIDERATION

Part II

STATE OF THE ART

You can put some informational part preamble text here

5 FLOWY

Flowy [1][2] is the first prototype implementation of a stream-based flow record query language [3][4][5]. The query language allows to describe patterns in flow-records in a declarative and orthogonal fashion, making it easy to read and understand.

5.1 PROCESSING PIPELINE

5.1.1 *Splitter*

5.1.2 *Filter*

5.1.3 *Grouper*

5.1.4 *Group-Filter*

5.1.5 *Merger*

5.1.6 *Ungrouper*

5.2 PYTHON FRAMEWORK

5.2.1 *PyTables and PLY*

5.2.2 *Records*

5.2.3 *Filters and Rules*

5.2.4 *Branches and Branch Masks*

6 FLOWY IMPROVEMENTS USING MAP/REDUCE

7 FLOWY 2.0

8

FLOWY: APPLICATIONS

Part III

MOTIVATION

Part IV

WORK PLAN

You can put some informational part preamble text here

9 DESIGN

10 IMPLEMENTATION

11

PERFORMANCE EVALUATION

12

CONCLUSION

Part V

IMPLEMENTATION AND EVALUATION

You can put some informational part preamble text here

13

DESIGN

14 IMPLEMENTATION

15

PERFORMANCE EVALUATION

16 FUTURE WORK

17

CONCLUSION

Part VI

APPENDIX

APPENDIX

Put your appendix here.

BIBLIOGRAPHY

[1] Kaloyan Kanev. Flowy - Network Flow Analysis Application. Master's thesis, Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany, 2009.

[2] Kaloyan Kanev, Nikolay Melnikov, and Jürgen Schönwälder. Implementation of a stream-based IP flow record query language. In *Proceedings of the Mechanisms for autonomous management of networks and services, and 4th international conference on Autonomous infrastructure, management and security*, AIMS'10, pages 147–158, Berlin, Heidelberg, 2010. Springer-Verlag.

[3] Vladislav Marinov. Design of an IP Flow Record Query Language. Master's thesis, Jacobs University Bremen, Campus Ring 1, 28759 Bremen, Germany, 2009.

[4] Vladislav Marinov and Jürgen Schönwälder. Design of a Stream-Based IP Flow Record Query Language. In *Proceedings of the 20th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management: Integrated Management of Systems, Services, Processes and People in IT*, DSOM '09, pages 15–28, Berlin, Heidelberg, 2009. Springer-Verlag.

[5] Vladislav Marinov and Jürgen Schönwälder. Design of an IP Flow Record Query Language. In *Proceedings of the 2nd international conference on Autonomous Infrastructure, Management and Security: Resilient Networks and Services*, AIMS '08, pages 205–210, Berlin, Heidelberg, 2008. Springer-Verlag.

DECLARATION

Put your declaration here.

Bremen, Germany, June 2012

Vaibhav Bajpai