

NETCONF – Secure FlowMon Probe Remote Configuration

Radek Krejčí
CESNET, z.s.p.o.
Zikova 4, 160 00 Prague
Czech Republic
krejci@liberouter.org

Pavel Čeleda
CESNET, z.s.p.o.
Zikova 4, 160 00 Prague
Czech Republic
celeda@liberouter.org

Keywords: NETCONF, network configuration, FlowMon.

Abstract

Secure remote configuration of the network devices is necessary feature in today's highly interoperable networks. After two decades of using SNMP, and (unfortunately) many vendor specific mechanisms to network device configuration, the IETF have developed new network management protocol - NETCONF [3]. This paper describes experiences of implementing NETCONF (*NETwork CONFiguration*) protocol for remote configuration of the FlowMon probe. The FlowMon probe is a passive network monitoring device based on the COMBO6X technology [1]. It is able to collect statistics about IP flows and export them in Net-Flow v5, v9 and IPFIX protocols to external collectors. The probe serves as a solid source of data for security-related applications. The presented system was developed within the Liberouter project [2].

Introduction

The NETCONF is XML based protocol using simple RPC (*Remote Procedure Call*) mechanism. XML is used for RPC messages formatting as well as for configuration data encoding. XML formatting is one of the protocol advantages and the configuration data can be processed in many ways. The NETCONF is fully independent of used configuration data model or data definition language.

The extensibility is another important feature of the NETCONF protocol. It allows to specify new capabilities (modifications of basic operations or definitions of entirely new operations) for accessing vendor or device specific functions. NETCONF protocol specifies only basic set of operations suitable for all devices (respectively for its configuration data). The list of supported capabilities is advertised in messages sent by client to server (and vice versa) during NETCONF session establishment.

System Architecture

The FlowMon probe remote configuration is divided into three separated parts:

- Configuration daemon *flowmond* used for setting up configuration changes in the FlowMon probe appliance.
- NETCONF subsystem providing operations to create modify or delete configuration data.
- Web configuration frontend with simple and intuitive user-friendly interface for changing FlowMon probe configuration data.

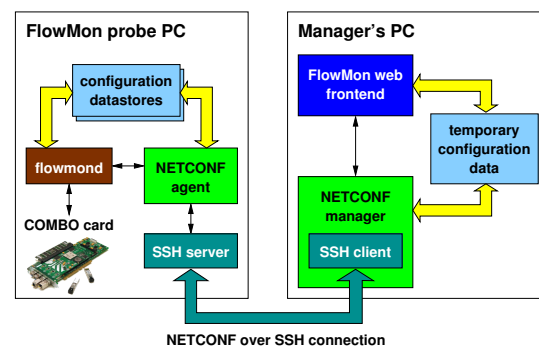


Figure 1. FlowMon probe remote configuration system architecture.

The NETCONF subsystem is designed as a core of the whole configuration system. It is able to interact with the configuration daemon on the server side as well as with the web configuration frontend on the client side.

NETCONF Subsystem

The NETCONF subsystem is an implementation of the NETCONF protocol. It cover up NETCONF manager pro-

gram (client) and NETCONF agent program (server). Both parts are connected through the SSH (*Secure SHell*) connection [4]. The connection is invoked by the NETCONF manager program. It forks a SSH program and redirects its standard output (stdout) and standard input (stdin) file's descriptors to prepared pipes. Therefore NETCONF manager program is able to write data to and read data from SSH program directly.

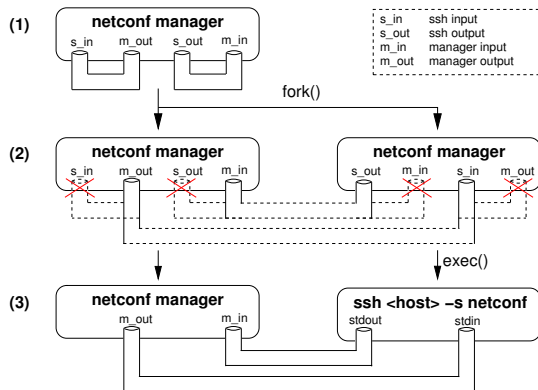


Figure 2. SSH's stdin and stdout redirection.

SSH program is invoked with `'-s netconf'` option which specifies that SSH server should start SSH subsystem called `'netconf'`. The SSH subsystem mechanism is available since SSHv2. The subsystems available on the machine are described in the `sshd's` configuration file (`/etc/ssh/sshd.config`). For the `'netconf'` subsystem it has to be specified that NETCONF agent program should be started.

As soon as `sshd` starts NETCONF agent program, the NETCONF session is established. As the first operation both sides send a `'hello'` message with a list of supported capabilities. If NETCONF agent as well as NETCONF manager receives hello message correctly, the synchronous message exchange can start. NETCONF manager program sends its requests through the SSH session to the NETCONF agent. Then the agent processes the request, performs necessary changes in configuration data or cooperates with configuration daemon to satisfy the request. When all necessary operations are performed, NETCONF agent program creates a response for processed request and sends it again through the SSH connection to the manager. Then the agent's response is displayed to user by NETCONF manager program.

NETCONF manager program includes simple interactive command line interface similar to `sftp's` user interface. Furthermore it provides non-interactive `batch mode` as an interface for automated tasks. In such case the list of required operation calls is stored into the text file. This file

is read by the program and performed automatically. The `batch mode` is useful as well as in communication with the FlowMon web configuration frontend. Frontend only prepares files with the list of required operations and then runs NETCONF manager in `batch mode`.

Conclusions

The presented NETCONF subsystem implementation preserves NETCONF protocol's independence on configuration data model. Therefore this part of the FlowMon probe remote configuration system can be easily used by other projects. Only the configuration daemon need to be modified to be able to understand configuration data and to apply configuration changes to new appliance. The presented system is successfully used for remote configuration of FlowMon probes deployed on CESNET's backbone network.

Acknowledgement

This work is supported by the GN2 project (FP6-IST 511082) and by the Research Intent of the Czech Ministry of Education MSM6383917201.

References

- [1] CESNET, z.s.p.o. *Description of COMBO Cards*. www.liberouter.org/hardware.php.
- [2] CESNET, z.s.p.o. *FlowMon Probe Project Web Page*. www.liberouter.org/flowmon/index.php.
- [3] R. Enns. *NETCONF Configuration Protocol – RFC 4741*. IETF, Network Working Group, 2006. www.ietf.org/rfc/rfc4741.txt.
- [4] M. Wasserman and T. Goddard. *Using the NETCONF Configuration Protocol over Secure SHell (SSH) – RFC 4742*. IETF, Network Working Group, 2006. www.ietf.org/rfc/rfc4742.txt.

Curriculum Vitae

Radek Krejčí is a master student at the Faculty of Informatics, Masaryk University, Brno, where he got his bachelor degree. He is a member of the software group in the Liberouter project since 2005.

Pavel Čeleda works as a researcher at the CESNET and Masaryk University. He has a Ph.D. in informatics from University of Defence, Brno. His current research area include monitoring of high-speed networks.