University of Tübingen, Germany
WSI - Computer Networks & Internet

Gerhard Münz, Albert Antony,
Falko Dressler, and Georg Carle

# Using Netconf for Configuring Monitoring Probes

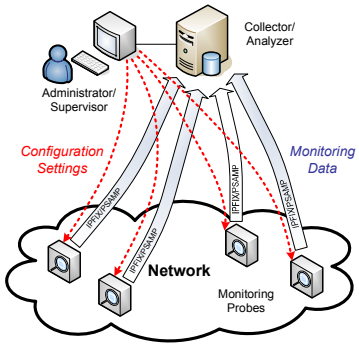
## Motivation

**Network monitoring is used by a growing number of applications.**

- Example applications are: Accounting, QoS measurements, attack detection,…
- Necessary separation between monitoring and analysis in order to cope with high traffic volumes
- Reducing the amount of monitoring data using ***flow accounting/aggregation*** and ***packet sampling***
- Distribution of the monitoring load on multiple monitoring probes in the network
- Deployment of standard export protocols ***Cisco Netflow*** and ***IETF IPFIX/PSAMP***

**Many applications require/benefit from dynamic adaptation of configurable parameters**

- to ***respond to changing traffic conditions*** and
- to ***adapt to the varying needs of the application.***
- Examples: - reconfiguration of sampling and filtering parameters
  - update of flow aggregation rules to increase/decrease aggregation level




## Configuration of Monitoring Probes

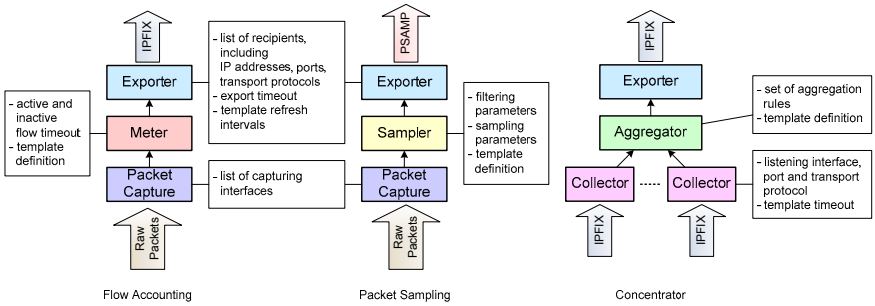
**Common practice:**

- Configuration mostly static via CLI
- Available MIBs cover only a small part of the configurable parameters:
  - CISCO-NETFLOW-MIB (read-only)
  - CISCO-NDE-MIB: configuration of export destinations (=collectors)
  - PSAMP-MIB: sampling and filtering parameters

**Our approach:**

- Usage of the ***Netconf Protocol*** for remote configuration of monitoring probes
- Definition of an XML Schema for device-independent specification of configurable parameters for:
  - packet sampling
  - flow metering and flow aggregation
  - collection and export of monitoring data

**Overview on configurable parameters:**




```
<monitorConfig>
  <sampler Id="1" operation="create">
    <interface Id="1">eth0</interface>
    <interface Id="2">eth1</interface>
    <packetProcessor Id="1">
      <ipFilter>
        <dstAddress>10.0.2.66</dstAddress>
      </ipFilter>
    </packetProcessor>
    <packetProcessor Id="2">
      <randOutOfN>
        <population>5</population>
        <size>3</size>
      </randOutOfN>
    </packetProcessor>
    <template>
      <templateId>1025</templateId>
      <field>
        <name>sourceIPv4Address</name>
      </field>
      <field>
        <name>sourceTransportPort</name>
      </field>
      <field>
        <name>destinationIPv4Address</name>
      </field>
      <field>
        <name>destinationTransportPort</name>
      </field>
    </template>
    <exporter>
      <sourceId>4712</sourceId>
      <exportTimeout>500</exportTimeout>
      <exportTo Id="1">
        <address>10.0.2.5</address>
        <port>1200</port>
        <protocol>udp</protocol>
      </exportTo>
    </exporter>
  </sampler>
</monitorConfig>
```

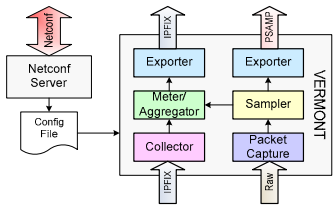
Example Configuration

**Implementation:**

- Decision to use SOAP as transport protocol for Netconf
- Usage of the light-weight *gSOAP* Toolkit
- Implementation of all mandatory and most optional protocol capabilities such as *rollback on error*, *candidate configuration*, *validate*
- Authentication and encryption based on SSL

**Integration:**

- Integration with IPFIX/PSAMP monitoring probe *VERMONT* (VERsatile MONitoring Toolkit)
- Netconf server converts device-independent configuration data into VERMONT-specific configuration file and triggers reconfiguration
- Netconf client offers UI to human administrator or API for integration into applications




Configurable Monitoring Probe VERMONT

## Conclusion

**Key benefits:**

- Usage of XML:
  - ➔ easily extensible configuration data models
  - ➔ human-readable configurations and messages
  - ➔ availability of many libraries and tools for XML processing
- Usage of Netconf:
  - ➔ reliability and flexibility
  - ➔ optional features like parameter validation, rollback on error, etc.
  - ➔ very promising standardization efforts
- Usage of SOAP as transport protocol:
  - ➔ RPC based (just like Netconf)
  - ➔ SOAP/Web Services widely deployed and supported
  - ➔ existing tools facilitate development of WS applications
  - ➔ authentication and encryption through SSL

**Open Issues:**

- Interoperability depends on agreement on a common XML-based configuration data model
- Netconf community mainly focuses on SOAP-over-SSH implementations although SOAP and Web Services technology offer many advantages

Selected References:

- B. Claise, "IPFIX Protocol Specifications," Internet-Draft, draft-ietf-ipfix-protocol-19, September 2005.
- T. Zseby, M. Molina, N. Duffield, S. Niccolini, and F. Raspall, "Sampling and Filtering Techniques for IP Packet Selection," Internet-Draft, draft-ietf-psamp-sample-tech-07, July 2005.
- F. Dressler, C. Sommer, and G. Münz, "IPFIX Aggregation," Internet-Draft, draft-dressler-ipix-aggregation-02, December 2005.
- R. Enns, "NETCONF Configuration Protocol," Internet-Draft, draft-ietf-netconf-prot-10, December 2005.
- T. Goddard, "Using the Network Configuration Protocol (NETCONF) over the Simple Object Access Protocol (SOAP)," Internet-Draft, draft-ietf-netconf-soap-07, December 2005.
- R. v. Engelen and K. A. Gallivany, "The gSOAP Toolkit for Web Services and Peer-To-Peer Computing Networks," in IEEE Cluster Computing and the GRID 2002, May 2002, pp. 128-135.

This work has been performed within the European project ***DIADEM Firewall*** (FP6 IST-2002-002154, Web: http://www.diadem-firewall.org).