Autonomic Networking Use Case for Distributed Detection of SLA Violations

draft-irtf-nmrg-autonomic-sla-violation-detection-04

Jéferson C. Nobre (University of Vale do Rio dos Sinos)
Lisandro Z. Granville (Federal University of Rio Grande do Sul)
Alexander Clemm (Sympotech)
Alberto Gonzales P. (Cisco Systems)

41st NMRG meeting, November 2016

Outline

1. Introduction
2. Problem Statement
3. Benefits of an Autonomic Solution
4. Intended User and Administrator Experience
5. Analysis of Parameters and Information Involved
6. Comparison with current solutions
7. Related IETF Work
8. Security Considerations
9. Outlook

Introduction

- Critical networked services expected to operate respecting associated Service Level Agreements (SLAs)
  - To ensure that SLAs are not being violated → constantly monitoring of service levels at the network layer
- Active measurement mechanisms
  - Better accuracy and privacy than passive ones
  - Detection of end-to-end network performance problems
- IP Performance Metrics (IPPM) WG active mechanisms
  - One-Way Active Measurement Protocol (OWAMP) [RFC4656]
  - Two-Way Active Measurement Protocol (TWAMP) [RFC5357]
  - Cisco Service Level Assurance Protocol (SLA) [RFC6812]
- Measurement probes distributed along the network to inject synthetic traffic and deliver the SLA metrics

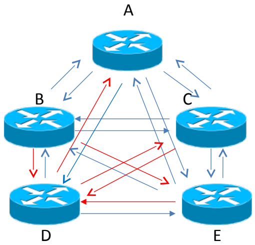
Problem Statement

- Activation of active measurement sessions → expensive in terms of resource consumption
- Required resources → function of the # of measured destinations
- Better monitoring coverage → more sessions
  - Monitor all connections is too expensive → combinatorial explosion
  - Fast reactions required to reconfigure sessions if critical flows are too short in time and dynamic in terms of traversing network paths

Problem Statement

Best practice

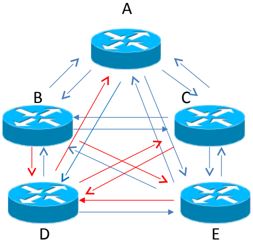
- Distribution of the available measurement sessions along the network considering human administrator expertise
- Collection of measurement and traffic information to infer which are the best destinations to activate sessions



	A	B	C	D	E
A		5	6	4	7
B	5		7	12	10
C	6	7		13	7
D	15	12	13		8
E	1	3	5	14	

Problem Statement

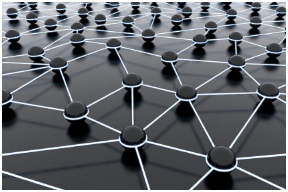
- Too difficult and labor intensive
- Inefficient considering fast changing network environments
- # of detections constrained by the # of available sessions



	A	B	C	D	E
A		5	6	4	7
B	5		7	12	10
C	6	7		13	7
D	15	12	13		8
E	1	3	5	14	

Problem Statement

- Embedded management SW → deployment control of active measurement mechanisms
    - Network device vendors → utilization to avoid devices starvation (e.g., due to configuration errors and lack of experience from human administrators)
- Lack of enhancements in scalability and efficiency
- Resources and knowledge about the network infrastructure not shared by network devices



Benefits of an Autonomic Solution

- Focus → complete solution to steer the process of measurement probe activation
- Design goals
  - Efficient
  - Reliable
  - Secure
  - Minimal human intervention
- Components for the implementation of measurement probe activation
  - Algorithms
  - Protocols
  - Metrics
  - Technologies

Benefits of an Autonomic Solution

Features

1. Optimization of resource consumption and avoidance of resource starvation on the network devices
   - Better efficiency in the measurement session activation decisions
   - Sharing of measurement results
2. Increase on the # of detected SLA violations
   - Better network coverage
3. Decrease on the time necessary to detect SLA violations
   - Adaptivity features of an autonomic loop → capturing network dynamics faster than an human administrator
4. Reduction on the workload of human administrators
   - At least to avoid their need to perform operational tasks

Intended User and Administrator Experience

- AN solution → to avoid the human intervention in the distributed detection of SLA violations
- SLA monitoring performed by less experienced human administrators
- Some information necessary from the human administrator
  - E.g., SLOs (regarding the SLA being monitored) provided by the human administrator
- Configuration and bootstrapping of network devices → minimal for the human administrator
  - E.g., information about the address of a solution-enabled device
  - Exchange of configuration data among the devices themselves

Analysis of Parameters and Information Involved

Device Based Self-Knowledge and Decision

- Each device → self-knowledge about local SLA monitoring
  - E.g., SLOs, historical measurement data
- AN decision on devices about the measurement session activation algorithm

Interaction with other devices

- Network devices → info sharing about SL results
  - Increase the # of detected SLA violations and their speed
- Definition of network devices that exchange measurement data → creation of a new topology
- Different approaches for topology definition
  - E.g., correlated peers (local relevancy of remote results)
  - Bootstrapping → known endpoints neighbours as initial seed

Comparison with current solutions

- No standardized solution for distributed autonomic detection of SLA violations
- Current solutions usually restricted to ad hoc scripts running on a per node fashion to automate some administrator's actions
- Some proposals for passive probe activation (e.g., DECON and CSAMP), but without the focus on autonomic features
- Barford *et al.* (INFOCOM 2009) → Detection and localization of links which cause anomalies along a network path
- Nobre *et al.* (CNSM 2012, ICC 2013, AINA 2014) → Utilization of P2P technology embedded in network devices to improve probe activation decisions using autonomic loops

Related IETF Work

Large-Scale Measurement of Broadband Performance (LMAP) WG

- AN solution relevant for LMAP → SLA violation screening
- Solution to decrease the workload of human administrators in service providers → probably highly desirable

IP Flow Information Export (IPFIX) WG

- AN solution extension for passive measurement probes (i.e., metering exporters)
- Flow information used in the decision making of probe activation

Application Layer Traffic Optimization (ALTO) Working Group

- Definition of the topology regarding the network devices which exchange measurement data

Security Considerations

Possible Approaches

- Bootstrapping of a new device → homenet approach [draft-behringer-homenet-trust-bootstrap]
- Measurement data exchange → signed and encrypted among devices
  - Sensible information about network infrastructures

Possible Attacks

- Denial of service (DoS) attacks → activation of more local probe than the available resources allow
- Results could be forged by a device (attacker) in order to this device be considered peer of a specific device (target) → to gain information about a network infrastructure

Updates and Outlook

Revision 04

- Minor revisions
  - Mostly updates on references

Outlook

- Minor revisions
  - Bootstrapping of a new device → anima approach

WGLC?

Autonomic Networking Use Case for Distributed Detection of SLA Violations

draft-irtf-nmrg-autonomic-sla-violation-detection-04

Jéferson C. Nobre (University of Vale do Rio dos Sinos)
Lisandro Z. Granville (Federal University of Rio Grande do Sul)
Alexander Clemm (Sympotech)
Alberto Gonzales P. (Cisco Systems)

Thanks for your attention! Questions?