# Autonomic Networking Use Case for Distributed Detection of SLA Violations

**Jeferson C. Nobre**, Lisandro Z. Granville, Alexander Clemm, Alberto Gonzales P.
Federal University of Rio Grande do Sul (UFRGS)
Cisco Systems

**34th NMRG meeting (Toronto, CA), July 2013**



# 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 $\rightarrow$ 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

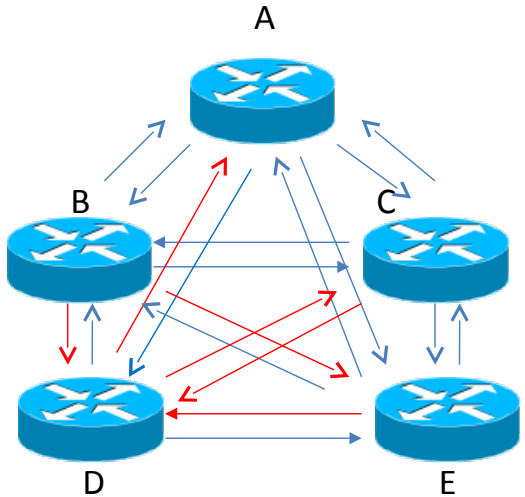
# Problem Statement

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

# Problem Statement

## Best practice

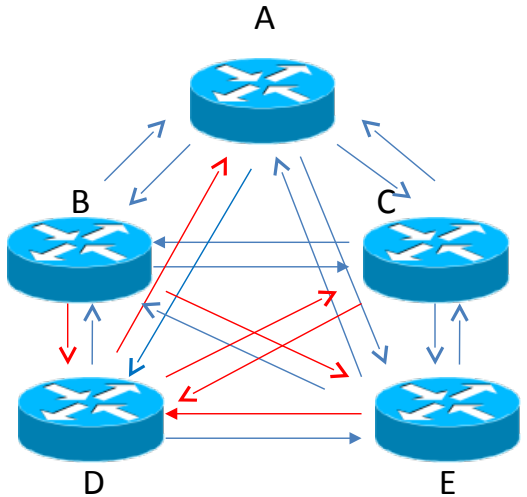
- Distribution of the available measurement probes along the network considering human administrator expertise
- Collection of measurement and traffic information to infer which are the best locations to activate probes




| | 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

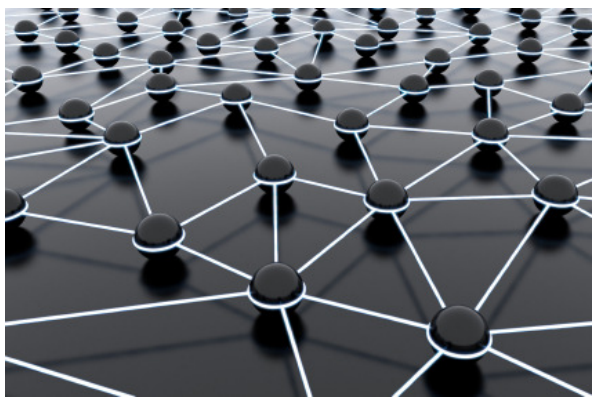
- Too difficult and labor intensive
- Inefficient considering fast changing network environments
- # of detections constrained by the # of available probes




| | 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 $\rightarrow$ deployment control of active measurement mechanisms
  - Network device vendors $\rightarrow$ 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

- Goal $\rightarrow$ complete solution to steer the process of measurement probe activation
- Settings of necessary parameters for this activation
  - Efficiently
  - Reliably
  - securely
  - Minimal human intervention
- Autonomic solution should include and/or reference specific algorithms, protocols, metrics and technologies for the implementation of measurement probe activation

# Benefits of an Autonomic Solution

## Features

1. Optimization of resource consumption and avoidance of resource starvation on the network devices
   - Better efficiency in the probe 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 $\rightarrow$ 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 $\rightarrow$ 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 $\rightarrow$ 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 $\rightarrow$ self-knowledge about local SLA monitoring
  - E.g., SLOs, historical measurement data
- AN decision on devices about the probe activation algorithm

## Interaction with other devices

- Network devices $\rightarrow$ info sharing about SL results
  - Increase the # of detected SLA violations and their speed
- Definition of network devices that exchange measurement data $\rightarrow$ creation of a new topology
- Different approaches for topology definition
  - E.g., correlated peers (local relevancy of remote results)
  - Bootstrapping $\rightarrow$ 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) $\rightarrow$ Detection and localization of links which cause anomalies along a network path
- Nobre *et al.* (CNSM 2012) $\rightarrow$ 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 $\rightarrow$ SLA violation screening
- Solution to decrease the workload of human administrators in service providers $\rightarrow$ 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

# Outlook

## Revision 01

- IETF 91
- Minor text corrections
- Examples of SLA specifications

## Proposed solution I-D

- IETF 91
- AN P2P solution (architecture?)

# Autonomic Networking Use Case for Distributed Detection of SLA Violations

**Jeferson C. Nobre**, Lisandro Z. Granville, Alexander Clemm,
Alberto Gonzales P.
Federal University of Rio Grande do Sul (UFRGS)
Cisco Systems

**Thanks for your attention! Questions?**