Network Management Research Group
Internet-Draft
Intended status: Informational
Expires: May 14, 2015

J. Nobre
L. Granville
Federal University of Rio Grande do Sul
A. Clemm
A. Prieto
Cisco Systems

November 10, 2014

Autonomic Networking Use Case for Distributed Detection of SLA Violations
draft-irtf-nmrg-autonomic-sla-violation-detection-01

Abstract

This document describes a use case for autonomic networking in distributed detection of Service Level Agreement (SLA) violations. It is one of a series of use cases intended to illustrate requirements for autonomic networking.

Table of Contents

1. Introduction

The Internet has been growing dramatically in terms of size and capacity, and accessibility in the last years. Besides that, the communication requirements of distributed services and applications running on top of the Internet have become increasingly strict. That is the case due to the impact of disrespecting such requirements (e.g., latency in trading can have a high cost). Thus, those requirements are included in SLA specifications (examples of service fulfillment clauses can be found on [RFC7297]). Violations on these requirements usually present significant financial loss, which can by divided in two types. First, there is the loss incurred by the service users (e.g., the trader) and the loss incurred by the service provider in terms of penalties for not meeting the service. Thus, the service level requirements of critical network services have become a key concern for network administrators. To ensure that SLAs are not being violated, service levels need to be constantly monitored at the network infrastructure layer. To that end, network measurements must take place.

Network measurement mechanisms are performed through either active or passive measurement techniques. In passive measurement, network conditions are checked in a non intrusive way because no monitoring traffic is created by the measurement process itself. In the context

of IP Flow Information EXport (IPFIX) WG, several documents were produced to define passive measurement mechanisms (e.g., flow records specification [RFC3954]). Active measurement, on the other hand, is intrusive because it injects synthetic traffic into the network to measure the network performance. The IP Performance Metrics (IPPM) WG produced documents that describe active measurement mechanisms, such as: One-Way Active Measurement Protocol (OWAMP) [RFC4656], Two-Way Active Measurement Protocol (TWAMP) [RFC5357], and Cisco Service Level Assurance Protocol (SLA) [RFC6812]. Besides that, there are some mechanisms that do not fit into either active or passive categories, such as Performance and Diagnostic Metrics Destination Option (PDM) techniques [draft-elkins-ippm-pdm-option].

Active measurement mechanisms usually offer better accuracy and privacy than passive measurement mechanisms. Furthermore, active measurement mechanisms are able to detect end-to-end network performance problems in a fine-grained way (e.g., simulating the traffic that must be handled considering specific Service Level Objectives - SLOs). As a result, active is preferred over passive measurement for SLA monitoring. Measurement probes must be hosted in network devices and measurement sessions must be activated to compute the current network metrics (e.g., considering those described in [RFC4148]). This activation should be dynamic in order to follow changes in network conditions, such as those related with routes being added or new customer demands.

The activation of active measurement sessions (hosted in senders and responders considering the architecture described by Cisco [RFC6812]) is expensive in terms of the resource consumption, e.g., CPU cycle and memory footprint, and monitoring functions compete for resources with other functions, including routing and switching. Besides that, the activated sessions also increase the network load because of the injected traffic. The resources required and traffic generated by the active measurement sessions are a function of the number of measured network destinations, i.e., with more destinations the larger will be the resources and the traffic needed to deploy the sessions. Thus, to have a better monitoring coverage it is necessary to deploy more sessions what consequently turns increases consumed resources. Otherwise, enabling the observation of just a small subset of all network flows can lead to an insufficient coverage.

2. Current Approaches

The current best practice in feasible deployments of active measurement solutions to distribute the available measurement sessions along the network consists in relying entirely on the human administrator expertise to infer which would be the best location to activate such sessions. This is done through several steps. First,

it is necessary to collect traffic information in order to grasp the traffic matrix. Then, the administrator uses this information to infer which are the best destinations for measurement sessions. After that, the administrator activates sessions on the chosen subset of destinations considering the available resources. This practice, however, does not scale well because it is still labor intensive and error-prone for the administrator to compute which sessions should be activated given the set of critical flows that needs to be measured. Even worse, this practice completely fails in networks whose critical flows are too short in time and dynamic in terms of traversing network path, like in modern cloud environments. That is so because fast reactions are necessary to reconfigure the sessions and administrators are not just enough in computing and activating the new set of required sessions every time the network traffic pattern changes. Finally, the current active measurements practice usually covers only a fraction of the network flows that should be observed, which invariably leads to the damaging consequence of undetected SLA violations.

3. Problem Statement

Management software can be embedded inside network devices to control the deployment of active measurement mechanisms. In fact, this is done by some network equipment vendors, specially to avoid the starvation of the network devices (e.g., due to configuration errors and lack of experience from human administrators). However, the current approach do not enhance the active measurement capabilities in important terms, such as scalability and efficiency. For example, the number of local available measurements (and, consequently, detected SLA violations) is still bounded by the number of activated sessions. Thus, if the number of SLA violation is greater than the number of available sessions, only a fraction of the violations will be observed. Also, devices cannot share resources and knowledge about the networking infrastructures in order to take advantage of remote management information (e.g., measurement results).

4. Benefits of an Autonomic Solution

The use case considered here is the distributed autonomic detection of SLA violations. The use of Autonomic Netowrking (AN) properties can help the activation of measurement sessions [P2PBNM-Nobre-2012]. We advocate for embedding Peer-to-Peer (P2P) technology in network devices in order to improve the measurement session activation decisions using autonomic loops. Thus, it would be possible to coordinate the measurement session activation and to share measurement results among different network devices.

The problem to be solved by AN in the present use case is how to steer the process of measurement session activation by a complete solution that sets all necessary parameters for this activation to operate efficiently, reliably and securely, with no required human intervention, while allowing for their input.

An autonomic solution for the distributed detection of SLA violations can provide several benefits. First, efficiency: this solution could optimize the resource consumption and avoid resource starvation on the network devices. This optimization comes from different sources: sharing of measurement results, better efficiency in the probe activation decisions, etc. Second, effectiveness: the number of detected SLA violations could be increased. This increase is related with a better coverage of the network. Third, the solution could decrease the time necessary to detect SLA violations. Adaptivity features of an autonomic loop could capture faster the network dynamics than an human administrator. Finally, the solution could help to reduce the workload of human administrator, or, at least, to avoid their need to perform operational tasks.

5. Intended User and Administrator Experience

The autonomic solution should not require the human intervention in the distributed detection of SLA violations. Besides that, it could enable the control of SLA monitoring by less experienced human administrators. However, some information may be provided from the human administrator. For example, the human administrator may provide the SLOs regarding the SLA being monitored. The configuration and bootstrapping of network devices using the autonomic solution should be minimal for the human administrator. Probably it would be necessary just to inform the address of a device which is already using the solution and the devices themselves could exchange configuration data.

6. Analysis of Parameters and Information Involved

The active measurement model assumes that a typical infrastructure will have multiple network segments and Autonomous Systems (ASs), and a reasonably large number of several of routers and hosts. It also considers that multiple SLOs can be in place in a given time. Since interoperability in a heterogenous network is a goal, features found on different active measurement mechanisms (e.g. OWAMP, TWAMP, and IPSLA) and programability interfaces (e.g., Cisco's EEM and onePK) could be used for the implementation. The autonomic solution should include and/or reference specific algorithms, protocols, metrics and technologies for the implementation of distributed detection of SLA violations as a whole.

6.1. Device Based Self-Knowledge and Decisions

Each device has self-knowledge about the local SLA monitoring. This could be in the form of historical measurement data and SLOs. Besides that, the devices would have algorithms that could decide which probes should be activated in a given time. The choice of which algorithm is better for a specific situation would be also autonomic.

6.2. Interaction with other devices

Network devices should share information about service level measurement results. This information can speed up the detection of SLA violations and increase the number of detected SLA violations. In any case, it is necessary to assure that the results from remote devices have local relevancy. The definition of network devices that exchange measurement data, i.e., management peers, creates a new topology. Different approaches could be used to define this topology (e.g., correlated peers [P2PBNM-Nobre-2012]). To bootstrap peer selection, each device should use its known endpoints neighbors (e.g., FIB and RIB tables) as the initial seed to get possible peers.

7. Comparison with current solutions

There is no standartized solution for distributed autonomic detection of SLA violations. Current solutions are restricted to ad hoc scripts running on a per node fashion to automate some administrator's actions. There some proposals for passive probe activation (e.g., DECON and CSAMP), but without the focus on autonomic features. It is also mentioning a proposal from Barford et al. to detect and localize links which cause anomalies along a network path.

8. Related IETF Work

The following paragraphs discuss related IETF work and are provided for reference. This section is not exhaustive, rather it provides an overview of the various initiatives and how they relate to autonomic distributed detection of SLA violations. 1. [LMAP]: The Large-Scale Measurement of Broadband Performance Working Group aims at the standards for performance management. Since their mechanisms also consist in deploying measurement probes the autonomic solution could be relevant for LMAP specially considering SLA violation screening. Besides that, a solution to decrease the workload of human administrators in service providers is probably highly desirable. 2. [IPFIX]: IP Flow Information EXport (IPFIX) aims at the process of standardization of IP flows (i.e., netflows). IPFIX uses measurement probes (i.e., metering exporters) to gather flow data. In this

context, the autonomic solution for the activation of active measurement probes could be possibly extended to address also passive measurement probes. Besides that, flow information could be used in the decision making of probe activation. 3. [ALTO]: The Application Layer Traffic Optimization Working Group aims to provide topological information at a higher abstraction layer, which can be based upon network policy, and with application-relevant service functions located in it. Their work could be leveraged for the definition of the topology regarding the network devices which exchange measurement data.

9. Acknowledgements

We wish to acknowledge the helpful contributions, comments, and suggestions that were received from Mohamed Boucadair, Bruno Klauser, Eric Voit, and Hanlin Fang.

10. IANA Considerations

This memo includes no request to IANA.

11. Security Considerations

The bootstrapping of a new device follows the approach of homenet [draft-autonomic-homenet], thus in order to exchange data a device should register first. This registration could be performed by a "Registrar" device or a cloud service provided by the organization to facilitate autonomic mechanisms. The new device sends its own credentials to the Registrar, and after successful authentication, receives domain information, to enable subsequent enrolment to the domain. The Registrar sends all required information: a device name, domain name, plus some parameters for the operation. Measurement data should be exchanged signed and encripted among devices since these data could carry sensible information about network infrastructures. Some attacks should be considering when analyzing the security of the autonomic solution Denial of service (DoS) attacks could be performed if the solution be tempered to active more local probe than the available resources allow. Besides that, results could be forged by a device (attacker) in order to this device be considered peer of a specific device (target). This could be done to gain information about a network.

12. References

12.1. Normative References

[P2PBNM-Nobre-2012]

Nobre, J., Granville, L., Clemm, A., and A. Prieto, "Decentralized Detection of SLA Violations Using P2P Technology, 8th International Conference Network and Service Management (CNSM)", 2012, <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6379997>.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

[RFC6812] Chiba, M., Clemm, A., Medley, S., Salowey, J., Thombare, S., and E. Yedavalli, "Cisco Service-Level Assurance Protocol", RFC 6812, January 2013.

[RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, July 2014.

[draft-autonomic-homenet] Behringer, M., Pritikin, M., and S. Bjarnason, "draft-behringer-homenet-trust-bootstrap", draft-behringer-homenet-trust-bootstrap-02 (work in progress), February 2014.

[draft-elkins-ippm-pdm-option] Elkins, N., Hamilton, R., and M. Ackermann, "draft-elkins-ippm-pdm-option", draft-elkins-ippm-pdm-option-02 (work in progress), September 2014.

12.2. Informative References

[RFC3954] Claise, B., "Cisco Systems NetFlow Services Export Version 9", RFC 3954, October 2004.

[RFC4148] Stephan, E., "IP Performance Metrics (IPPM) Metrics Registry", BCP 108, RFC 4148, August 2005.

Authors' Addresses

Jeferson Campos Nobre
Federal University of Rio Grande do Sul
Porto Alegre
Brazil

Email: jcnobre@inf.ufrgs.br

Lisandro Zambenedetti Granville
Federal University of Rio Grande do Sul
Porto Alegre
Brazil

Email: granville@inf.ufrgs.br

Alexander Clemm
Cisco Systems
San Jose
USA

Email: alex@cisco.com

Alberto Gonzalez Prieto
Cisco Systems
San Jose
USA

Email: albertgo@cisco.com