Distributed Detection of SLA Violations

draft-irtf-nmrg-autonomic-sla-violation-detection-01

Jéferson Campos Nobre

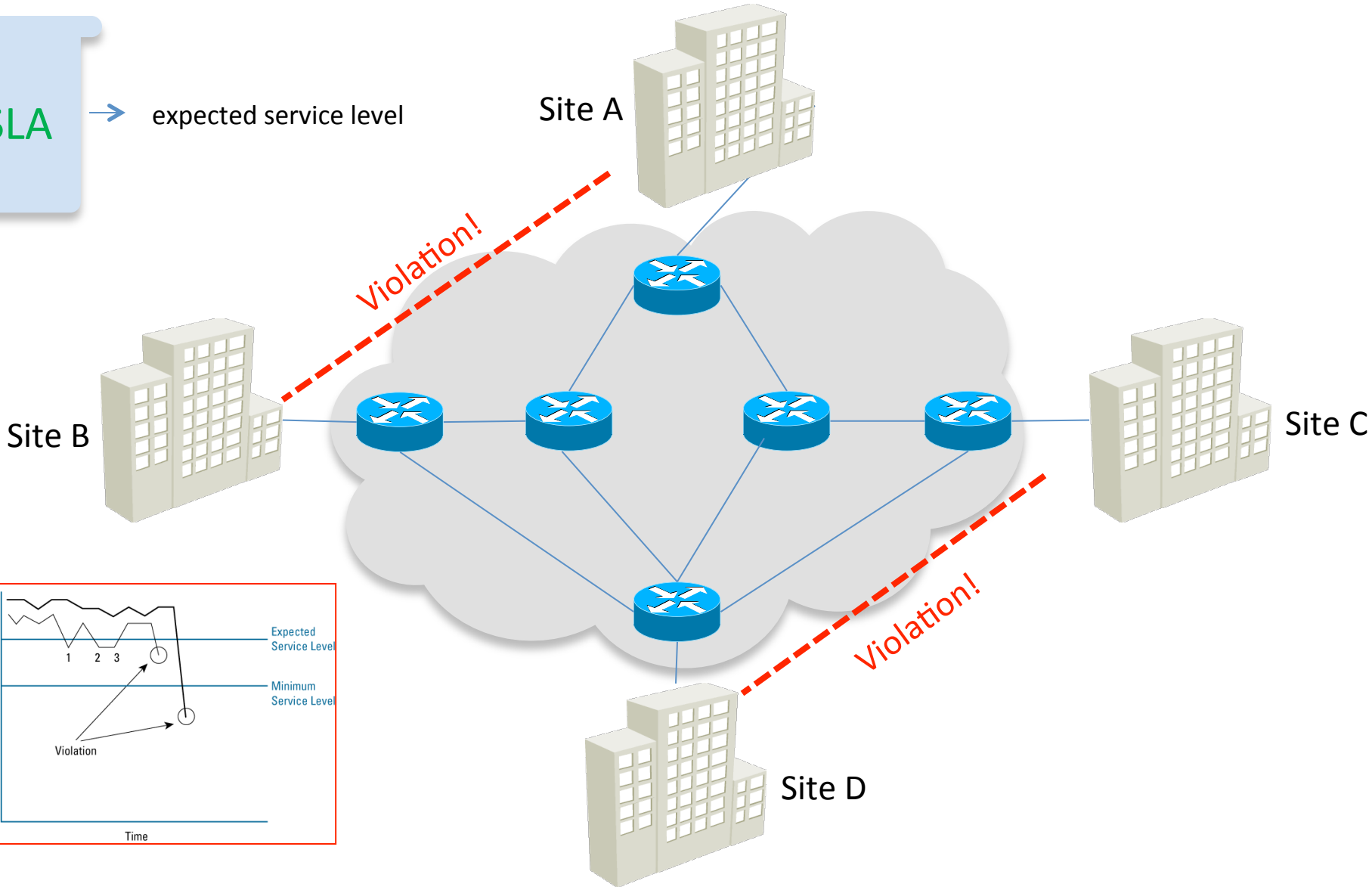
Lisandro Zambenedetti

Alexander Clemm

Alberto Gonzalez Prieto

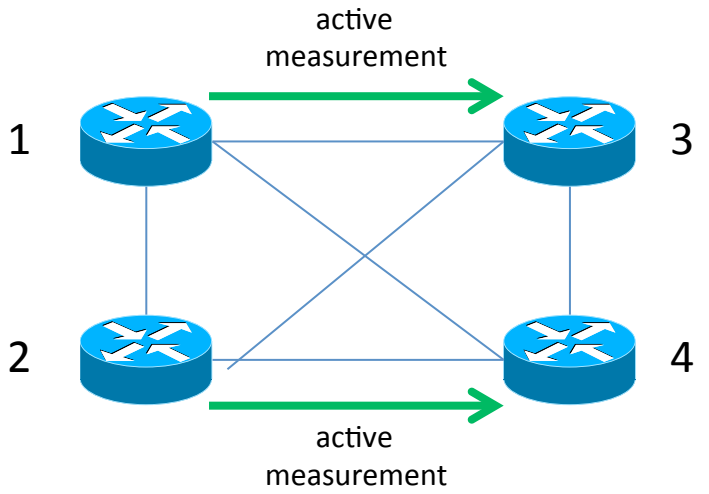
Problem definition

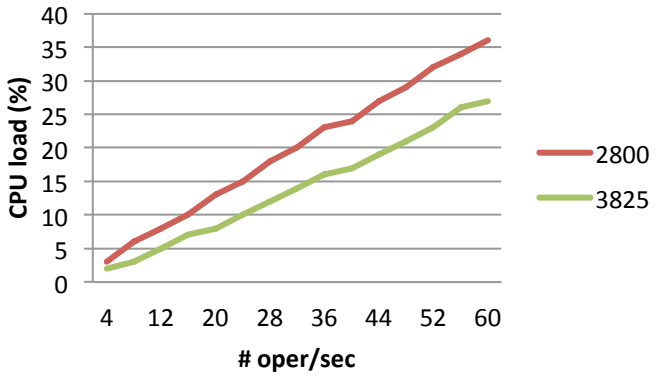
SLA → expected service level



Basic Problem

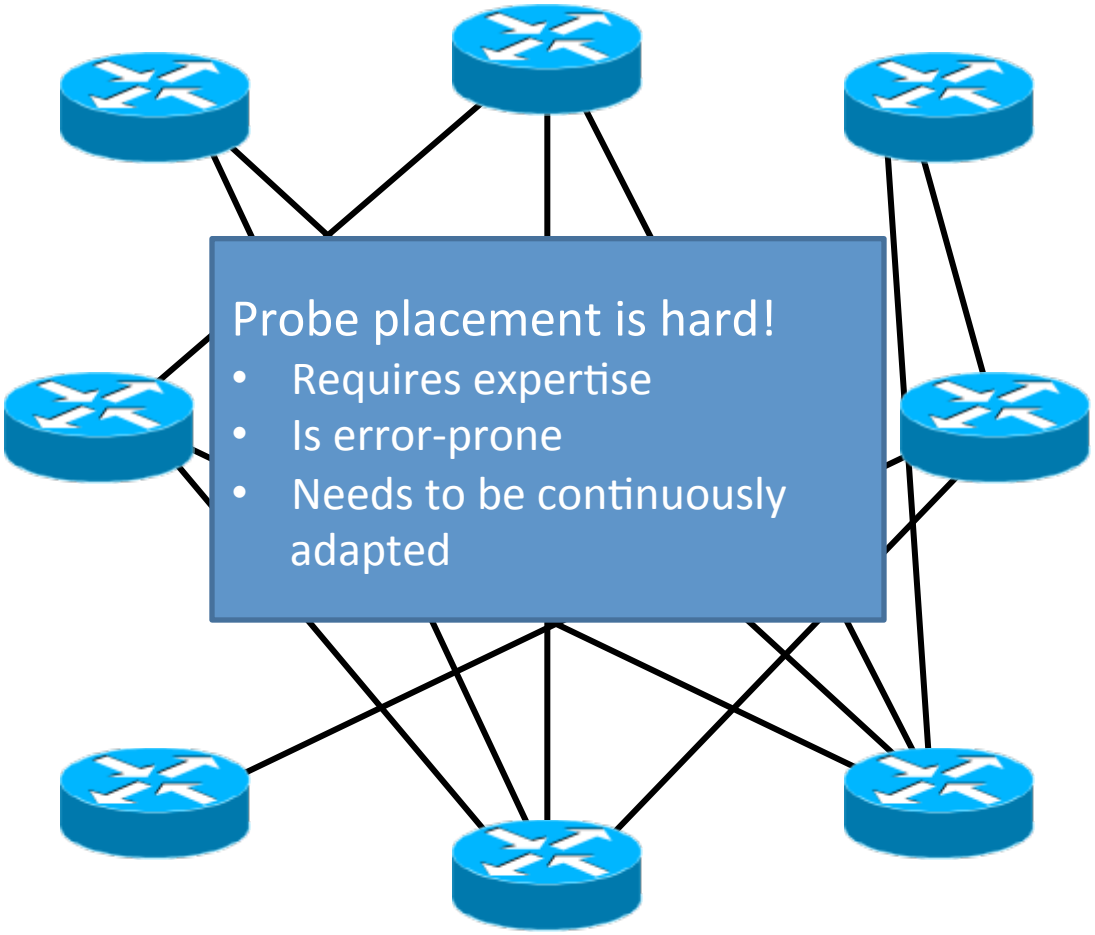
- Maximize the number of detective violations
  - Active measurement is an effective way to detect SLA violations (RFC 6812, RFC 5357)
  - However, active measurement is expensive – CPU etc
  - Cannot measure everything → need to determine probes





(Jitter Probe Running Eng 2+—2000 Active Jitter Oper—Cisco IOS 12.4(PI3)T)

“Partial mesh” manual placement



- **Determine a coverage objective, ie: 30%.**
- **Build a traffic matrix to identify the “hottest” points (hint: use NetFlow).**
- **Take the top 30% and evenly distribute operations**

A	B	C	D	E	F
B		5	6	7	5
C	1		7	12	12
D	7	5		5	11
E	4	4	12		2
F	3	8	4	18	

Slide from “Advanced Performance Measurement for Critical IP Traffic with Cisco IOS IP SLAs”

Benefits of an Autonomic Solution

Enable a service-level aware, self-monitoring network

- Autonomic solution determines what / when / how to probe without human intervention such that violations are detected with high probability
- Better coverage, violation awareness with less resources
- No dependence on hard-to-obtain human expertise
- Adaptive to dynamic network conditions
- Easy to use

Autonomic Problem formulation

- Given a set of service level objectives (“intent”)
- In the context of a network, consisting of
  - n nodes
  - s connections
  - v connections with service level violations
- Maximize v = #detected violations / (#total violations+1)
- Place a set p of probes such that v is covered
  - In the quickest possible time
  - With the least amount of resources

  #probes ≤ α (upper bound on total probes in network)

  #probes(i) ≤ β(i) (upper bound on probes per node)
- Various extensions/variations:
  - Discover the “least good”
  - Tradeoff accuracy of probes – number of probes

Placement approaches

- Random
- Decision based on local information
- Decision based on local and remote information
- Coordinated decision

Decision based on local information

- Resource constraints analysis and path ranking are performed using local information
- Place probes in iterations
  - Identify set of candidate probes
  - Initial iteration: random placement or based on top destinations
  - Subsequent iterations: time since last observation, closeness to violation determine selection probability
  - Balance coverage over time (round robin) vs scrutiny for likely offenders
- Input:
  - SLO
  - Local observations (measurements, flow)

Algorithm 2 LocalInfoPlace($\alpha, \beta, staticweigh[], path[]$)

$N \leftarrow GetNumberEdges(path[])$
$Rc \leftarrow min(\beta, \alpha/N)$
$M \leftarrow min((Rc-\text{GetNumberActiveProbes}()),\text{SizeOf}(\text{path}[]))$
for $t = 1 \rightarrow Sizeof(path[])$ **do**
  $path[t][Wu] \leftarrow GetUser(path[t])$
  $path[t][Wtl] \leftarrow GetTrafLocal(path[t])$
  $path[t][Wll] \leftarrow GetLabelLocal(path[t])$
  $t \leftarrow t + 1$
end for
$\text{SortDesc}(path[], key \leftarrow (staticweigh[Wu] * path[][Wu]/\Sigma path[][Wu]) + (staticweigh[Wtl] * path[][Wtl]/\Sigma path[][Wtl]) + (staticweigh[Wll] * path[][Wll]/\Sigma path[][Wll])/(\Sigma staticweight[]))$
for $i = 1 \rightarrow M$ **do**
  $\text{DeployProbe}(path[i])$
  $i \leftarrow i + 1$
end for

Extensions

- Decision based on local + remote information
  - Take into account results obtained from peers in previous cycle
  - Destinations for which violations are detected from one node may be strutinized more closely by others
- Coordinate probing
  - Avoid duplicate routine probing of same destinations for greater coverage in same cycle
  - Nodes exchange what they measure (best effort, gossiping)
- Identify correlated peers for better coordination
  - Weigh information from nodes that are “similar” to you
    - In terms of observations – similar PIN and other characteristics
  - Assess, discover, validate if a peer is correlated
- Note: Inter-peer communication leverages Autonomic Control Plane

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

Outlook

- Revision 02