Passively Detecting Remote Connectivity Issues Using Flow Accounting

2nd EMANICS Workshop on Netflow/IPFIX usage in network management

08.10.2009
Jacobs University Bremen, Germany

Tim Kleefass*⋆, Simon Leinen*
Jochen Kögel⋆, Dominik Schatzmann°

* SWITCH, ⋆ University of Stuttgart, ° ETH Zurich

Overview

1. Motivation
2. Methodology to detect remote connectivity issues
3. Evaluation with selected events
4. Conclusion and Outlook

Introduction

We want to find:

Remote connectivity issue

A network outage outside the own network

⇒ Caused by BGP depeering/hardware/software/... failures

⇒ Network operator wants to know that *before* his customers call

Examples:

"YouTube vs. Pakistan" (2008)

Pakistan Telecom "hijacked" a /24 prefix

⇒ All traffic to YouTube was lost

Level(3)–Cogent depeering (2005)

Depeering of two Tier-1 ISPs

⇒ Single homed customer were not reachable

Basic idea

Network properties

SWITCHlan: Swiss research and educational network

- Partial and hot potato routing
- Default route to (two) global transit ISPs

  ⇒ Looking at BGP routing table is not enough
- Unsampled NetFlow export at border routers

  ⇒ Basis for our approach

Basic idea

In case of *remote connectivity issue*:

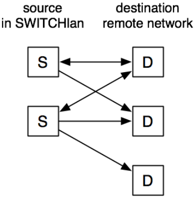
- A lot of *forward* flows, but no *reverse* flows
- E.g., failed TCP connection setup

False positives

- Scanning (port scans, Skype, ...)
- Shut down services, stale DNS records, ...

Definitions

Our interest: Can **our** users reach the entire Internet?



Forward flow (“request”)

Leaving the **own** network to well known services/ports

Reverse flow (“answers”)

Corresponding to forward flows, with *inverse key*

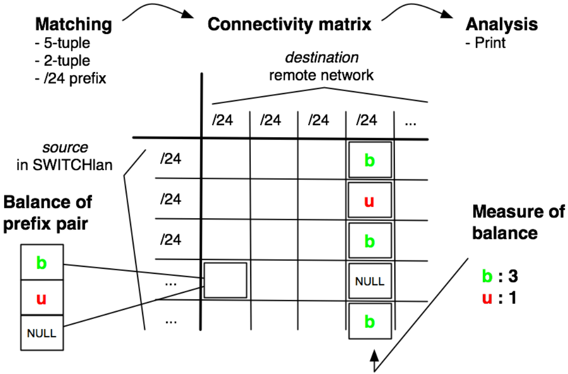
Balanced flow

If there is a reverse flow to a forward flow (within Δt)

Balance of a /24 prefix pair *(binary)*

$$(src,\ dst) \text{ is } \begin{cases} \textit{balanced} & \text{if there is } \textbf{at least one} \text{ balanced flow} \\ \textit{unbalanced} & \text{else} \end{cases}$$

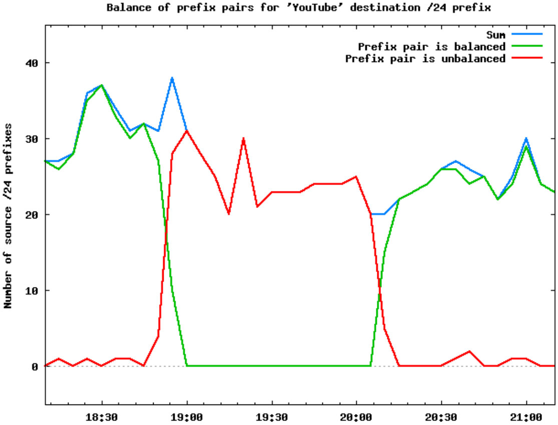
Connectivity Matrix

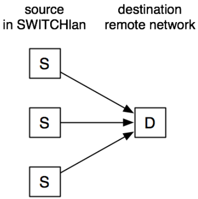


- Collecting connectivity information between prefix pairs
- Fill and clear connectivity matrix every 5 minutes

Measure of Balance Sum of prefix pairs per destination /24 prefix

Single /24 outage (“YouTube vs. Pakistan”, HTTP traffic)



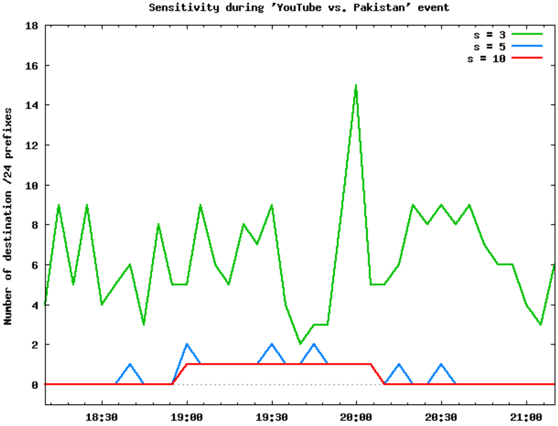


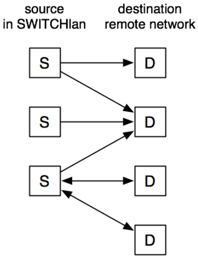
Measure of balance

b == 0
u >= 10

⇒ High number of unbalanced prefix pairs

Sensitivity during “YouTube vs. Pakistan” event





source
in SWITCHlan

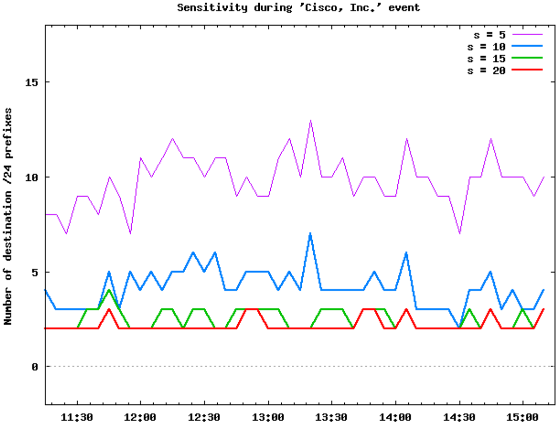
destination
remote network

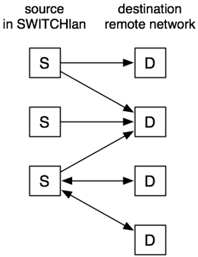
S S S

D D D D

Parameter *s* for sensitivity setting: number of source prefixes

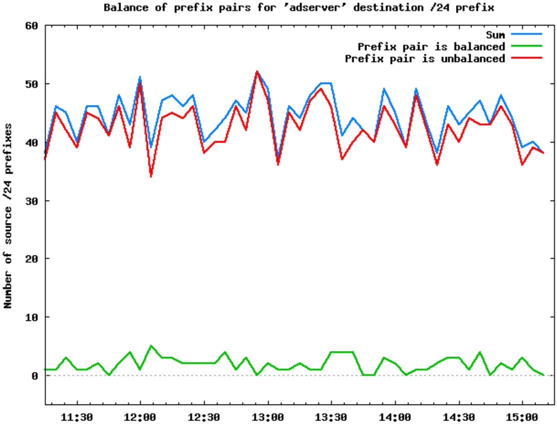
Sensitivity during another single /24 outage

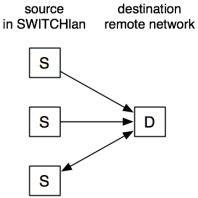




≥ 2 destination prefixes with ≥ 20 "unbalanced" source prefixes

Blacklisting destination prefixes: Example



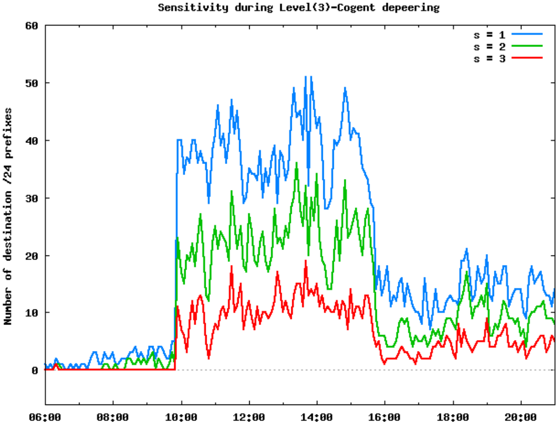


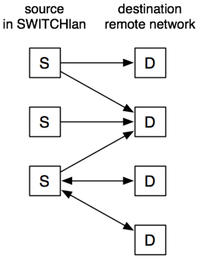
Measure of balance

b <= 5
u >= 10

An adserver which was shut down, but people still try to use it

Sensitivity during Level(3)-Cogent depeering (DNS traffic)





Only one border router, only Cogent single homed users!

Towards a tool for network administrators

- Present a list of /24 prefixes with issues (e.g., on a website)
- Display last/changes in BGP path (e.g., route views project)
  ⇒ Tier-1 outage could be seen fast
- Link to BGP play and other useful tools
- Link to blacklist IP addresses/prefixes/...
  ⇒ Network administrator can blacklist known issues or false positives

⇒ Network administrator has to decide about each issue

Conclusion and Outlook

Summary

- Method to find remote connectivity issues
- Passive approach using unsampled NetFlow from border routers
- Method based on aggregated prefixes
- Resistant against scanning
- Efficient processing and real-time capable
- Also works with IPv6

Outlook

- Better display for Tier-1/ISP failures
- Live-display
- Integrate in pmacct (from Paolo Lucente) ?

The end.

Thanks for your attention! – Questions?

Tim Kleefass SWITCH/University of Stuttgart

Simon Leinen SWITCH

Jochen Kögel IKR, University of Stuttgart

Dominik Schatzmann CSG, ETH Zurich