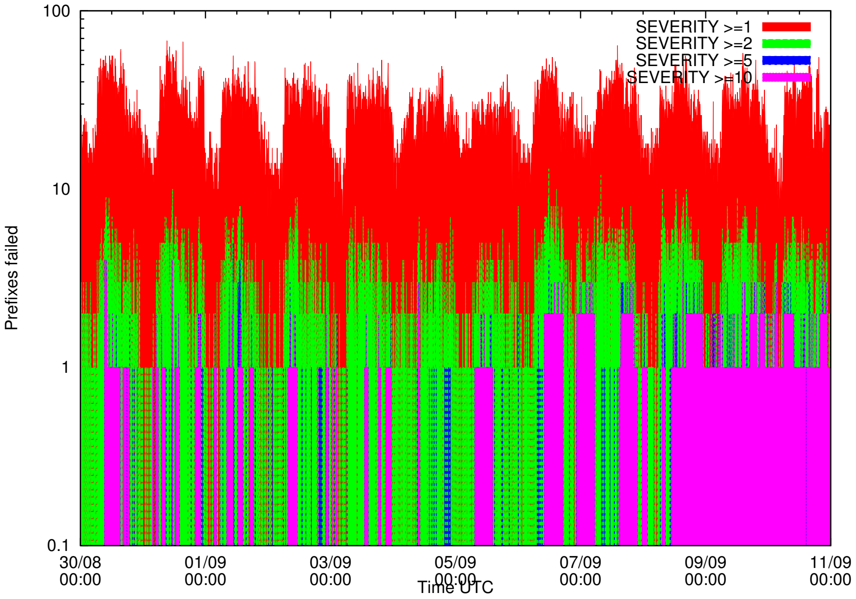
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für
Technische Informatik und
Kommunikationsnetze

Daniel Aschwanden
asdaniel@ee.ethz.ch
07-907-769

Who turned off the Internet?

Mining Temporary Unreachability of the Internet



Semester Thesis MA-2012-11
April 2012 through October 2012

Advisors:
Dominik Schatzmann

Supervisor:
Prof. Dr. Bernhard Plattner

Communication Systems Group – CSG
Computer Engineering and Networks Laboratory – TIK
Department of Information Technology and Electrical Engineering – ITET
Swiss Federal Institute of Technology – ETH

Abstract

Keywords

Acknowledgments

Daniel Aschwanden

Contents

CHAPTER 1

Introduction

1.1 Motivation

The Internet is interconnecting networks all over the world since more than 40 years by 2012. The end-to-end reachability of hosts has always been a basic service of the Internet. However, this reachability is sometimes disrupted for various reasons, such as link or router collapses[], natural disasters[], political revolutions[] and human errors[]. There is a real need for methods to systematically detect and locate Internet outages of remote autonomous systems, subnets, and even single hosts if they are of importance. This is particularly true for Internet service providers (ISP), as for example costumers are generating costs for time intensive debugging and support by complaining at the ISP for unreachable networks or the ISP is contractually liable for unreachable networks. An automated, ongoing detection and tracking of connectivity issues of the Internet may generate transparent outage information for customers and enables the ISP to react adequately on a detected reachability problems if possible, for example by changing routes in case of a failure of a transit provider. As outlined in section 1.2 in detail, researches and industrial vendors have proposed various approaches for systematically detect, locate and troubleshoot Internet outages and loss of end-to-end reachability. However, most of these approaches rely on control-plane information as BGP routing messages or data-plane information achieved by active probing. For this reason, FACT was introduced by **?** as a flow-based approach of connectivity tracking. This is a fully passive approach for identifying remote connectivity problems and relies solely on flow-level information of cross-border network traffic. This The detection of a outage is consolidated by aggregating the unresponsive hosts to network and AS level and rating the severity of the events by affected users.

An obvious caveat of this approach lies in the misinterpretation of service failures to host failures in case no other service is running on the observed host. This problem also exists on higher aggregation level, i.e. if a single host fails the entire network / AS is wrongly detected as down. This is even worse if this service or host is very popular with regard to internal network users. Depending on the kind of service, this may be a real problem, i.e. if this host is a web server providing important content, or may be negligible because the service or application connecting to this service is already handling this service outtage as in the case of a Skype super-node. However, from a flow-point of view the connections to a Skype super-node or to a web server looks very similar and are often indistinguishable. For this reason, services have to be views at a longer time scale in order to detect services which can be characterized as stable and thus relevant for outage analysis.

1.2 Related Work