The NorNet Project: A Research Platform for Robust and Secure Networks

Thomas Dreibholz
Simula Research Laboratory
Martin Linges vei 17, 1364 Fornebu, Norway
dreibh@simula.no

***Abstract*—This talk gives an overview of the NorNet project, the new Internet testbed for multi-homed systems, and its research objectives.**[1][2]

Keywords: NorNet, Testbed, Multi-Homing, Setup, Research

I. Introduction

Having stable and uninterrupted Internet connectivity is becoming increasingly important, particularly with regard to applications like cloud computing, service as a platform and many others. Connectivity problems could e.g. be caused by a hardware failure or a natural disaster. In order to improve the robustness of Internet connectivity, it is obvious to connect endpoints to multiple Internet service providers (ISP) simultaneously. This property is denoted as multi-homing. For example, Transport Layer protocols like the Stream Control Transmission Protocol (SCTP, RFC 4960 [1]) or Session Layer frameworks like Reliable Server Pooling (RSerPool, RFC 5351 [2]) make use of multi-homing to support availability-critical applications.

However, while in theory a failure of one ISP should be independent of other ISPs, it is not really known what happens in practise in today's commercial networks. It is evident that there are hidden dependencies among ISPs. Also, what about connectivity problems due to intentional malicious behaviour, i.e. targeted attacks on such systems? Research in realistic Internet setups is clearly necessary, in order to answer these open questions. For that purpose, the NorNet project is building up a multi-homed testbed distributed all over the country of Norway. This talk gives some basic ideas on NorNet as well as an overview of its intended research objectives.

II. Setup

The NorNet testbed consists of two separate parts:

1) NorNet Core: the wired part, and
2) NorNet Edge: the wireless part.

A. NorNet Core

For NorNet Core, there is a hardware setup as shown in Subfigure 2(a) at – in the near future – 10 different sites distributed over Norway. Figure 1 depicts these sites on the mainland of Norway as well as the islands of Svalbard, with the central site containing the management infrastructure at the Simula Research Laboratory [3] in Fornebu (nearby Oslo). Each site setup consists of a switch, a router (the first server) and three research nodes (the lower three servers). The research nodes run virtual machines for experiments. In the usual case, the research systems run PlanetLab-based software [4]. However, it is also possible to add custom system images as well (e.g. to boot special operating systems or adapted kernels).

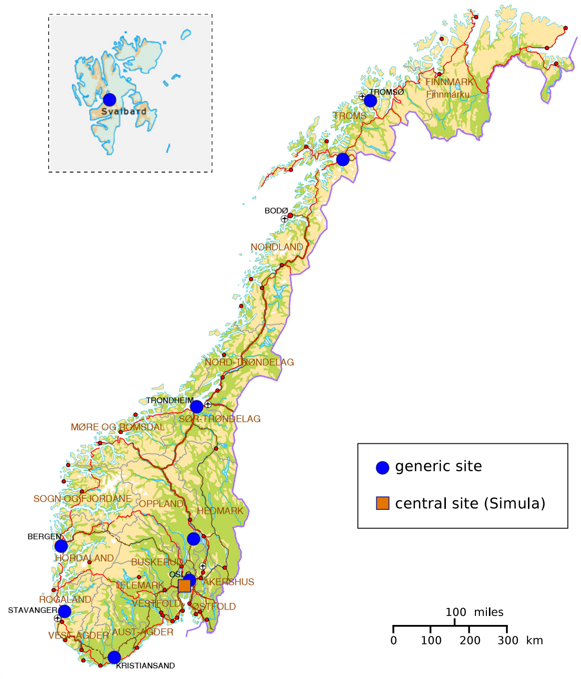
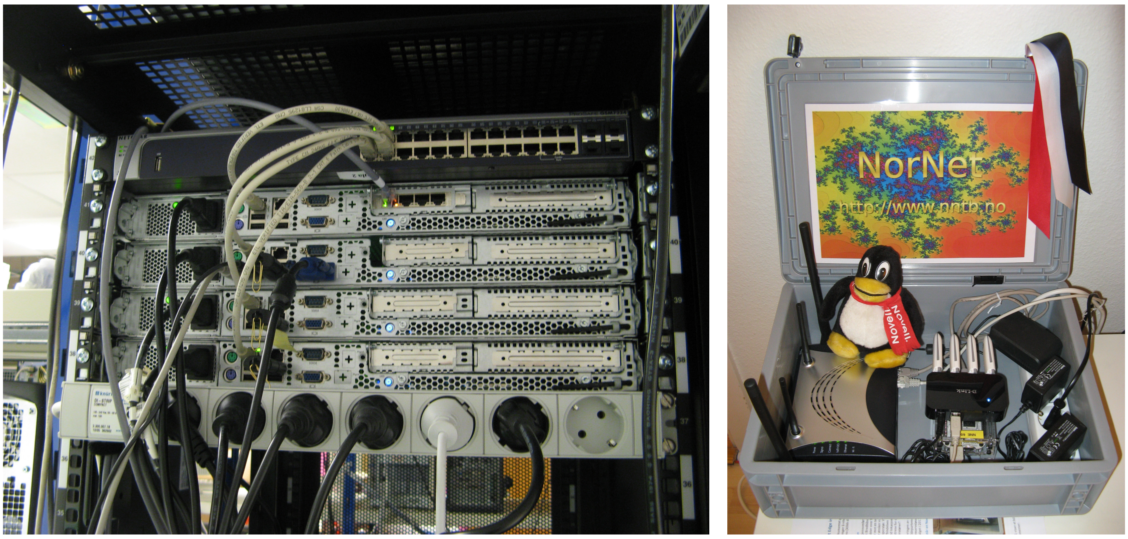


Figure 1. The NorNet Core Sites Map

The router connects the research setup to the different ISPs at the corresponding site (in the picture: currently only one). It is based on Linux and utilises IP-rules [5] to realise routing via different ISPs. That is, based on the source address of an IP packet, a per-ISP routing table is chosen. For example, if the source address of a packet is within the IP range of the ISP Versatel, it should be routed via the Versatel ISP connection. On the other hand, if it has a DFN source address, it should go out via the DFN interface. By setting the *Type of Service* (TOS) field of IPv4 packets/Traffic Class of IPv6 packets to certain values, a researcher may also explicitly select the outgoing interface, i.e. he could e.g. send a packet from a DFN IP address out over the Versatel interface. The connectivity between sites is realised via GRE and IPv6-over-IPv6-based static tunnels, i.e. there is full control over the

[1] Parts of this work have been funded by the Research Council of Norway (Forskingsrådet), prosjektnummer 208798/F50.

[2] The author would like to thank Hakim Adhari for his friendly support.



(a) A NORNET CORE Site

(b) A NORNET EDGE Node

Figure 2. The NORNET Hardware

outgoing local interface/ISP as well as the incoming remote interface/ISP. A more detailed introduction to NORNET CORE can be found in [6].

B. NORNET EDGE

For research on wireless networks, it is clearly necessary to have a much more fine-granular view of the networks than it is necessary for wired networks. Therefore, NORNET EDGE needs significantly more sites. For that purpose, each NORNET EDGE site consists of a NORNET EDGE node, as depicted in Subfigure 2(b). It is a small, Linux-based embedded system, equipped with up to four USB-stick-based UMTS modems (for the four UMTS providers in Norway: TELENOR, NETCOM, NETWORK NORWAY, TELE2) and an ICE modem (CDMA-based mobile broadband). Optionally, the node can also be connected via Ethernet to a wired network for administrative purposes. So far, around 300 of these nodes have been distributed; in addition, 200 are planned in the future.

III. RESEARCH

Clearly, the main research objectives of the NORNET testbed are subjects related to robustness and multi-homing, i.e. how to make the connectivity more robust for availability-critical applications as well as how to simultaneously utilise multiple ISP connections to improve application payload throughput and quality of service by using load sharing and appropriate data scheduling. Of particular interest in this context is current research on multi-path transport, e.g. based on Concurrent Multipath Transfer with SCTP (CMT-SCTP [7], [8]) as in [9], as well as congestion control strategies for multi-path transport as in [10]. Real-world Internet experience with such new approaches is also highly relevant in the context of IETF standardisation, as it is necessary for e.g. CMT-SCTP [11].

Research on robustness is clearly related to discovery and handling of currently hidden dependencies among different ISPs. However, while most research in this context currently focusses on "unintended" service interruptions like natural disasters or hardware issues, it is clearly necessary to also take maliciously intended denial of service into consideration. That is, how can an attacker exploit the existence of multiple ISP connections to cause service interruptions – and, of course, how can this be prevented? Particularly, are there already attacks on multi-homed system ongoing in the Internet of today? These topics are highly new and should be answered right *before* attackers actually get able to successfully run large-scale exploits.

REFERENCES

[1] R. R. Stewart, "Stream Control Transmission Protocol," IETF, Standards Track RFC 4960, Sept. 2007, ISSN 2070-1721.

[2] P. Lei, L. Ong, M. Tüxen, and T. Dreibholz, "An Overview of Reliable Server Pooling Protocols," IETF, Informational RFC 5351, Sept. 2008, ISSN 2070-1721.

[3] A. Tveito, A. M. Bruaset, and O. Lysne, *Simula Research Laboratory – by thinking constantly about it*. Heidelberg, Baden-Württemberg/Germany: Springer, Nov. 2009, ISBN 978-3642011559.

[4] M. Huang, *MyPLC User's Guide*, Aug. 2006.

[5] M. A. Brown, *Guide to IP Layer Network Administration with Linux*, Apr. 2003.

[6] T. Dreibholz and E. G. Gran, "Design and Implementation of the NorNet Core Research Testbed for Multi-Homed Systems," in *Proceedings of the 3nd International Workshop on Protocols and Applications with Multi-Homing Support (PAMS)*, Barcelona, Catalonia/Spain, Mar. 2013.

[7] T. Dreibholz, "Evaluation and Optimisation of Multi-Path Transport using the Stream Control Transmission Protocol," Habilitation Treatise, University of Duisburg-Essen, Faculty of Economics, Institute for Computer Science and Business Information Systems, Mar. 2012.

[8] J. R. Iyengar, P. D. Amer, and R. Stewart, "Concurrent Multipath Transfer using SCTP Multihoming over Independent End-to-End Paths," *IEEE/ACM Transactions on Networking*, vol. 14, no. 5, pp. 951–964, Oct. 2006, ISSN 1063-6692.

[9] T. Volkert, M. Becke, M. Osdoba, and A. Mitschele-Thiel, "Multipath Video Streaming based on Hierarchical Routing Management," in *Proceedings of the 3nd International Workshop on Protocols and Applications with Multi-Homing Support (PAMS)*, Barcelona, Catalonia/Spain, Mar. 2013.

[10] M. Becke, T. Dreibholz, H. Adhari, and E. P. Rathgeb, "On the Fairness of Transport Protocols in a Multi-Path Environment," in *Proceedings of the IEEE International Conference on Communications (ICC)*, Ottawa, Ontario/Canada, June 2012, pp. 2666–2672.

[11] P. D. Amer, M. Becke, T. Dreibholz, N. Ekiz, J. R. Iyengar, P. Natarajan, R. R. Stewart, and M. Tüxen, "Load Sharing for the Stream Control Transmission Protocol (SCTP)," IETF, Network Working Group, Internet Draft Version 06, Mar. 2013, draft-tuexen-tsvwg-sctp-multipath-06.txt, work in progress.