Section 1:
Network monitoring based on flow measurement techniques

This research is performed within the scope of the SURFnet Research on Networking (RON) project (Activity 1.2 - Measurement Scenarios).

Authors

Michiel Uithol	University of Twente
Vincent van Kooten	University of Twente

Supervisors

Aiko Pras	University of Twente
Pieter-Tjerk de Boer	University of Twente

Keywords: SURFnet, Flow measurement, Tools

Table of contents: Section one

Table of contents: Section two

Introduction

For our bachelor assignment at the University of Twente, research into tools for IP flow measurement was performed. The research is restricted to open source software for collecting, processing and displaying the results of these flow measurements. In this document we will focus on the application of these flow measurements within SURFnet. More detailed descriptions of SURFnet and this assignment are provided below.

The contribution of this report consists of providing the reader an overview in the current broad range of open source tools to perform and present traffic measurement. Choices have to be made in order to choose a tool that fits a certain situation.

The report consists of two sections. Section one describes the research questions, the approach and the general conclusions of this bachelor assignment. This section is primarily intended for internal use within the University of Twente. Section two describes measurement techniques, flow standards, open source tools for flow measurement, actual testing of these tools and scenarios for possible implementation options. This section is primarily intended for use and distribution within SURFnet.

SURFnet

SURFnet is an innovative computer network specially used for higher education and research in the Netherlands. The network is being maintained by the SURF foundation. Ongoing innovation has made SURFnet5 one of the world's most advanced networks with congestion-free connections to the major Dutch, European and transatlantic networks. Speed, reliability and security of the network are key issues. If everything goes according to the planning, SURFnet5 will be completely replaced by SURFnet6 at January 1st 2006.

SURFnet6 is heading in a new direction, as far as the technique and architecture of the network are concerned. The reason for this change is both technical and economical.

A new type of usage has arisen: extremely large data streams between two fixed points in the network. In order to route this traffic in such a way that the normal internet traffic is not hampered, another type of network is needed.

Above all, routers are very expensive, while the price of transmissions on links between these routers has decreased considerably. Because of these advances the idea has risen for a hybrid network, which is a combination of a traditional IP-network with revolutionary optical techniques. The optical techniques include lambda switching for the large data streams, so the routers will not be bothered with an extra load.

Advantage of this new architecture is that fewer routers are needed. SURFnet6 will completely be built out of fibre links owned and managed by SURFnet.

Research questions

The research network in the Netherlands is called SURFnet. The next generation of that network, SURFnet6, will be a managed dark fibre network that supports lambda-switching. For this network an improved monitoring service might be required, which provides usage and performance figures to its users. In order to design such a service, research is needed on the following topics:

- Determine which standards are available for exporting network information.
- Investigate existing open source tools that can be used to present network usage figures.
- Investigate different scenarios where monitoring is appropriate.

Approach

In order to answer research question one, the different user groups in the SURFnet situation have to be determined. The users will be specified together with their demands and wishes. Next background research on the field of traffic measurement has to be performed. By investigating the possibilities of the traffic measurement techniques the main focus of research will become clear. An in depth view of the selected measurement technique has to be provided.

To answer the second research question, a search for usage measurement programs that are distributed under an open source license should be performed. Next phase consists of creating a list of requirements for the tools. Only the most promising tools will be selected for further testing. These tools will be described in individual reports.

The last research question requires an investigation into scenarios. These example scenarios have to point out how tools can be used in practice and how the tools can fulfil SURFnet users' needs.

Conclusions

To answer the first research question, we determined the different users of SURFnet. With their wishes for measurement information in mind an overview was created of the possibilities to display throughput information. Our research shows that this can be displayed well using flow techniques. Flow measurements have different advantages over the current measurements based on the Simple Network Protocol (SNMP). Advantages include better insight into the network by showing traffic between specific points in the network. This is valuable information for the possible introduction of lambda paths. For this traffic a distinction can be made among the used services. Flow measurement also provides data mining possibilities e.g. how large the percentage of IPv6 usage is. More advantages are named in *section two, chapter 4*.

Other techniques do not suffice because they do not provide enough detail in network traffic or demand too many resources. For the named advantages over other the standards we have chosen flow techniques to collect network information.

After research into the different standards to export flow information, our final preference goes out to IP Flow Information Export (IPFIX). IPFIX is an initiative from the Internet Engineering Task Force (IETF)[1], an attempt at creating one standard for flow output. Although IPFIX is currently not widely available, we believe it will become a standard in the industry.

In order to answer the second research question, an investigation into the currently available open source tools was performed. Requirements were made to select the most promising tools among the 33 found to process flow information. Tools surviving this selection were tested.

For every tested tool a report was made, these can be found in section 2. The tools were tested on the various aspects that are required to install and run a tool in a network environment. Testing also revealed that not all tools surviving the primary selection are good enough to deploy in an actual network.

To answer the third research question we engineered different possible scenarios. A selection was made among the tested tools, which should be able to present this data to the users. Sample scenarios display possibilities to perform traffic measurements in SURFnet. These scenarios also provide multiple possibilities for administrators to fulfil their own and the networks user's needs.

An environment where such scenario's can be deployed is the new SURFnet6 where innovations in network statistics might be required. Currently only output figures for individual routers are available together with latency measurements. The flow extensions as suggested would be an improvement and gives the user more insight into the network.

[1] The Internet Engineering Task Force is charged with developing and promoting Internet standards. It is an open, all-volunteer organization, with no formal membership or membership requirements.