DEGREE PROJECT IN COMPUTER ENGINEERING, FIRST CYCLE
STOCKHOLM, SWEDEN 2016

Analysis and Evaluation of Network Management Solutions

A Comparison of Network Management Solutions Suitable for Networks with 2,500+ Devices

MURAT GABDURAHMANOV and SIMON TRYGG

KTH ROYAL INSTITUTE OF TECHNOLOGY
INFORMATION AND COMMUNICATION TECHNOLOGY

Analysis and Evaluation of Network Management Solutions

A Comparison of Network Management Solutions Suitable for Networks with 2,500+ Devices

Murat Gabdurahmanov and Simon Trygg

2016-06-16

Bachelor of Science Thesis

Examiner
Gerald Q. Maguire Jr.

Academic adviser
Anders Västberg

KTH Royal Institute of Technology
School of Information and Communication Technology (ICT)
Department of Communication Systems
SE-100 44 Stockholm, Sweden

Abstract

Some companies today are using sub-optimal and nearly obsolete management systems for their networks. Given the large number of different services that are demanded by users, there is a need to adapt the network structure to support the current and potential future demands. As a result, there is a need for new Network Management Solutions (NMSs).

The aim of this thesis project is to help a company who uses a NMS called Local Area Network (LAN) Management Solution (LMS). LMS was designed by Cisco for managing LAN networks. However, the company's demands are growing and they need to expand their network more than expected. Moreover, LMS is designed to only support devices by Cisco, whereas the company wants a universal solution with wide device support from many manufacturers.

This thesis presents an analysis of their current system and suggests potential solutions for an upgrade that will meet all of the company's demands and will have a long operating life. To help find reasonable solutions a thorough evaluation of their existing NMS and network monitoring and management needs was made. This evaluation gave good insights into different aspects of their system. A reasonable solution was found by following a three-step approach, beginning with 82 possible solutions, filtering out and breaking down with each step, until only the most suitable NMS was left.

Two NMSs has been proposed as equally suitable replacements: IBM Tivoli Netcool/OMNIbus and ManageEngine OpManager. Regardless of which one is chosen, they both have the following advantages over the company's existing NMS: they are very stable solutions which can handle a large number of managed devices; they are universal solutions with wide device support, and the company can add custom support if needed; they are user-friendly with the ability to add custom interfaces; and they both have a professional first-line technical support department locally located.

Keywords. Analysis, evaluation, Network Management Solution (NMS), monitoring, management, Cisco, LAN Management Solution (LMS), Tivoli, Netcool, OMNIbus, OpManager.

Sammanfattning

Vissa företag använder idag suboptimala och föråldrade övervakningsssystem för sina nätverk. Med tanke på det stora antalet olika tjänster som efterfrågas av användare finns det ett stort behov av att anpassa nätverksstrukturen för att stödja de nuvarande och potentiellt framtida kraven. Som ett resultat finns det ett behov av nya övervakningssystem (Network Management Solutions (NMSs)) för nätverken.

Syftet med detta examensarbete är att hjälpa ett företag som använder NMS:en Local Area Network (LAN) Management Solution (LMS). LMS utecklades av Cisco för att hantera lokala nätverk (LANs). Men med tiden har företagets krav förändrats och de har därför behövt expandera sitt nätverk mer än väntat. Dessutom är LMS endast utformad för att hantera enheter tillverkade av Cisco, medan företaget vill ha en universal lösning med stöd för enheter från många olika tillverkare.

Denna rapport presenterar en analys av deras nuvarande system, samt föreslår möjliga lösningar som kan ersätta detta. Den nya lösningen ska vara långvarig samt ska uppfylla alla krav företaget ställt. För att hitta lämpliga lösningar har en grundlig utvärdering av den befintliga NMS:en samt en analys av de ställda kraven utförts. Denna analys gav goda insikter i olika aspekter av deras nuvarande system. En lämplig lösning hittades genom att följa en trestegsmetod. Metoden utgick från 82 möjliga lösningar, som efter flera steg av filtrering resulterade i de mest lämpade ersättningssystemen.

Två NMS:er har föreslagits som lika lämpliga ersättare: IBM Tivoli Netcool/OMNIbus och ManageEngine OpManager. Oavsett vilken som väljs, har de båda följande fördelar jämfört med den nuvarande NMS:en: de är båda väldigt stabila lösningar som klarar av en stor mängd hanterade enheter; de är universella lösningar med stöd för en stor mängd olika enheter, dessutom går det även att lägga till eget stöd för enheter vid behov; de är användarvänliga och har möjlighet till att anpassa egna gränssnitt; samt att de båda har en professionell first-line teknisk support placerad lokalt i landet.

Nyckelord. Analys, utvärdering, övervakningssystem, nätverk, hantering, Cisco, LAN Management Solution (LMS), Tivoli, Netcool, OMNIbus, OpManager.

Acknowledgements

We would like to thank our examiner Gerald Q. "Chip" Maguire Jr. for his great support throughout the writing of this report by providing us with excellent feedback and constructive criticism.

We would also like to thank everyone at "Netcorp" who assisted us throughout the work we did. This thesis project would not have been possible without their help and the access to their resources.

Stockholm, June 2016
Murat Gabdurahmanov and Simon Trygg

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

3DES	Triple DES. 9
a.k.a.	also known as. 19, 20
AIX	Advanced Interactive eXecutive. 45
API	Application Programming Interface. 44, 48, 50
ASR	Aggregation Services Routers. 27, 28
BTO	Business Technology Optimization. 19
CA	Computer Associates International. viii, 18, 21, 33, 36–39, 73, 75
CLI	Command Line Interface. vii, 9, 21
CMDB	Configuration Management Database. 50
CPE	Customer-provided Equipment. 16
CPU	Central Processing Unit. 44, 50, 51, 63
CSV	Comma-Separated Values. 50
DES	Data Encryption Standard. xv, 9
EMC^2	Egan, Marino, Connolly, and Curley. 39, 73, 75
ESXi	Elastic Sky X Integrated. 42
EUR	Euro. 38, 39
f.k.a.	formerly known as. 18, 38, 73–76
FCAPS	Fault, Configuration, Accounting, Performance, and Security. vii, 2, 6, 21, 24, 55, 61
FMS	Flexible Monitoring System. 74, 76
FreeNATS	Free Network Automatic Testing System. 73, 75
GB	Gigabyte. 27
Gbps	Gigabit per second. 8

GUI	Graphical User Interface. 1, 11, 17, 32, 36, 37, 39–41, 43, 44, 46–49, 51–55
HP	Hewlett Packard. viii, ix, xvi, 19, 27, 33, 34, 39–45, 52, 73, 75
HPE	HP Enterprise. ix, 33, 34, 39, 41–43, 52, 53, 57, 75
HTML	Hypertext Markup Language. xvi, 10, 11, 40, 46
HTML5	HTML version 5. 40
HTTP	Hypertext Transfer Protocol. vii, xvi, 9, 10, 21, 37
HTTPS	Hypertext Transfer Protocol Secure. vii, 10, 11, 21, 36
IBM	International Business Machines. i, iii, ix, x, 18, 33, 34, 43–45, 53, 54, 57, 73, 75, 83
ICMP	Internet Control Message Protocol. 50
ICT	Information and Communication Technology. 48
IDEA	International Data Encryption Algorithm. 9
IETF	Internet Engineering Task Force. 10, 26
IMAP	Internet Message Access Protocol. 9
IMC	Intelligent Management Center. viii, ix, 33, 34, 39–41, 43, 52, 53, 57, 75
IP	Internet Protocol. 1, 40, 41, 46, 48, 49, 51, 54, 58
ISO	International Organization for Standardization. 6, 21
ISP	Internet Service Provider. 59
IT	Information Technology. 47, 48
JSON	JavaScript Object Notation. 47
KPI	Key Performance Indicator. 50
LAN	Local Area Network. i, iii, vii, xvi, 1, 2, 11, 13, 21
LDAP	Lightweight Directory Access Protocol. 45, 48, 51, 55
LMS	LAN Management Solution. i, iii, vii, xi, xiii, 1–3, 5, 11–18, 21, 25, 28, 37, 39, 61, 75

ME	Metro Ethernet. 27, 28
MIB	Management Information Base. 8, 11, 14, 45, 53, 54
MPLS	Multiprotocol Label Switching. 15, 16, 41
NCM	Network Configuration Manager. 45, 46
NID	Network Interface Device. 27
NMIS	Network Management Information System. ix, 33, 34, 48, 49, 53, 54, 74, 75
NMS	Network Management Solution. i, iii, vii–ix, 1–6, 15–21, 24–39, 41–43, 45, 46, 48–59, 61–66, 74, 76, 78
NNMi	Network Node Manager i. ix, 33, 34, 41–43, 52, 53, 73, 75
NNTP	Network News Transfer Protocol. 9
NOC	Network Operations Centre. 44, 45
NOI	Netcool Operations Insight. 43–45, 56
NPM	Network Performance Monitor. 19, 20, 59, 76
OID	Object Identifier. 7, 8
OpenKBM	Open Knowledge Based Management. 74, 76
OpenNMS	Open Network Management System. 18, 74, 75
OPNET	Optimized Network Engineering Tools. 74, 76
OSI	Open Systems Interconnection. 16
OSI$_2$	Objective Systems Integrators. 74, 75
PA	Power Admin. 74, 75
PDU	Protocol Data Unit. 8, 9
POP3	Post Office Protocol version 3. 9
PRTG	Paessler Router Traffic Grapher. 19, 76
PSIRT	Product Security Incident Response Team. 13
RADIUS	Remote Authentication Dial-In User Services. 46, 51, 55
RANCID	Really Awesome New Cisco conflg Differ. 18, 19, 21, 59, 76
RFC	Request for Comments. 7, 10, 26, 28
RSA	Rivest, Shamir, Adleman. 9
SCADA	Supervisory Control And Data Acquisition. 44
SECSH	Secure Shell. 10

SEK	Swedish krona. 41, 45, 46, 77
SFTP	Secure File Transfer Protocol. vii, 10, 16, 21
SMTP	Simple Mail Transfer Protocol. 9
SNMP	Simple Network Management Protocol. vii, xi, xviii, 1, 7–9, 11–13, 19–21, 30, 32, 37, 45, 47, 50
SNMPv1	SNMP version 1. 8, 37, 38, 40
SNMPv2	SNMP version 2. 8, 9
SNMPv2c	SNMP version 2 community. 9, 37, 38, 40
SNMPv2p	SNMP version 2 party-based. 9
SNMPv2u	SNMP version 2 user-based. 9
SNMPv3	SNMP version 3. 9, 16, 30, 31, 36–38, 40, 43, 55
SSH	Secure Shell. vii, xviii, 9, 10, 16, 21, 40, 45, 48
SSH-1	SSH version 1. 9, 40
SSH-2	SSH version 2. 9, 10, 40
SSL	Secure Socket Layer. 10
TACACS	Terminal Access Controller Access-Control System. 51
TCP	Transmission Control Protocol. 1, 10, 47, 58
TLS	Transport Layer Security. 10
UDP	User Datagram Protocol. 8
UI	User Interface. 10, 40
UIM	Unified Infrastructure Management. viii, 18, 21, 33, 37–39, 73, 75
US	United States. 49, 51, 59
UX	Unix. 45
VM	Virtual Machine. 27, 39, 42
VPFM	Visualization Performance and Fault Manager. 73, 75
VPN	Virtual Private Network. 10
WDM	Wavelength-division Multiplexing. 16
XML	Extensible Markup Language. 40

Chapter 1

Introduction

This chapter describes the background and problems that led to this bachelor's thesis project, as well as a description of the purpose and goals that are to be fulfilled as a result of this project. Lastly, it gives a short summary of the research methodology used and delimitations that set the scope of this thesis project.

As described further in Section 1.6 on page 3, the company where we performed this thesis project has requested the name of the company not to be named in this thesis, hence we will simply refer to the company as "Netcorp".

1.1 Background

It is hard for companies to keep track of and support the demands of their rapidly growing customer base. This is especially true when it comes to networks. Many companies choose to maintain their current network systems (both hardware and software), if they do the job "well enough", as the employees are familiar with this system. Furthermore, the introduction of new hardware and software most likely requires a learning process. In some cases, it may be worth the time-consuming learning process if the new system is sufficiently better that it would result in more effective work in the long term. This inertia of existing systems is especially common for Network Management Solutions (NMSs) as these systems are complete and it is hard to stop managing the network with the existing system in order to transition to a new NMS.

Cisco Prime Local Area Network (LAN) Management Solution (LMS) is a powerful tool for managing and monitoring smaller networks, meaning it is a suitable tool for LANs. LMS uses the Simple Network Management Protocol (SNMP), a well-known protocol for managing network devices over Transmission Control Protocol (TCP)/Internet Protocol (IP), to communicate with its managed devices. Via its Graphical User Interface (GUI), LMS gives administrator(s) the ability to monitor, manage, administer, troubleshoot, keeping track of inventory, etc., of all the networked devices via a single platform.

1.2 Problem Definition

Cisco LMS is a widely used NMS by many companies for network management. However, as mentioned in Section 1.1 on the previous page, LMS is intended for smaller LANs, hence as the networks in these companies grow, LMS becomes insufficient and sub-optimal. The current situation with more than 2,500 devices results in a unstable NMS where frequently occurring bugs and system suspensions are common. Cisco claims that LMS supports up to 10,000 devices, while in the case of Netcorp, it seems that it can barely handle their 2,500 devices. Moreover, LMS lacks new device support, resulting in unsupervised hardware in Netcorp's network, which is not ideal.

Netcorp's network has grown substantially and is expected to continue to grow. Furthermore, with Netcorp's current NMS they are constrained to Cisco products, which limits their expansion capabilities. Hence there is a need for new network management software that can be used with the company's current hardware and meet their needs. Alternatively, there is a need to replace the existing software and hardware in order to meet the company's networking needs. The expected number of network devices that will need to be managed over the lifetime of this new NMS is 5,000 devices.

1.3 Purpose

The purpose of this degree project is to identify a NMS that supports all of Netcorp's current hardware and can fulfil all their near term network management needs. This hardware and their needs are described in detail in Section 2.3 on page 15.

1.4 Goals

The goal of this thesis project is to find a solution that can handle Netcorp's current network, as well as being future-proof and support their upcoming needs for at least five years. The solution should manage all the aspects of the Fault, Configuration, Accounting, Performance, and Security (FCAPS) framework* via a single NMS, and be flexible enough to support plausible future network implementations.

* Described in Section 2.1.2 on page 6.

A secondary goal is for us to gain experience and knowledge in this area, this should facilitate our future professional work. The goal of the written thesis is to facilitate Netcorp's transition to their new system, to demonstrate our knowledge of this subject, and so that others facing the problem of managing networks of 2,500 or more network devices can also benefit from what we have learned.

1.5 Research Methodology

The research methods that were used began with interviews with the network managers inside Netcorp in order to define the requirements for a new NMS. These interviews were expected to give us better insight into their existing systems and problems with LMS. We conducted a literature search (including web search) to learn about available NMSs. We analysed both the advantages and disadvantages of each of these systems, as well as their price performance in the context of Netcorp's requirements. We also performed real-world testing of a subset of these systems to see how they perform. This project followed a three-step approach, described in Section 3.1 on page 23, using both qualitative and quantitative research methods and following the realistic philosophical research paradigm.

1.6 Delimitations

The focus of this thesis project will be network management and monitoring, specifically those aspects that must be upgraded with respect to the existing NMS in order to meet Netcorp's current and near future needs. This thesis will not consider any network topology changes, changes in traffic handling, or network engineering. If there is sufficient time and resources, a small prototype environment will be set up to facilitate our presentation and evaluation of the solution or solutions that we will propose.

The research done in this thesis project is about, and based on, Cisco's LMS version 4.2, which is the version Netcorp uses.

As described earlier, the name of the company where we conducted our thesis project will not be disclosed. The company will therefore be referenced to as "Netcorp" throughout the thesis, a name chosen due to the fact that the focus of this project is on network management for companies/corporations. The existence of any company or companies named Netcorp or similar name is purely coincidental, and has no relation to this thesis project.

1.7 Structure of the Thesis

Chapter 1 gives an introduction into the research area that the thesis will consist of. Chapter 2 presents basic background information about NMSs, protocols, and tools for network management. Related work is also described in Chapter 2. Chapter 3 provides an overview of the research method used in this thesis. Chapter 4 presents what was done and how it was done, different decisions that was made, and how these decisions helped us to meet the project's goals. Chapter 5 presents an analysis and discussion of our results. Finally, Chapter 6 provides a conclusion to our research and reflections about the project.

Chapter 2

Background

This chapter provides basic background information about Network Management Solutions (NMSs), as well as relevant protocols and tools used in NMSs. Additionally, this chapter describes information about Netcorp's current NMS, LMS. The chapter also describes related work which was used to facilitate this thesis project.

2.1 Network Management

This thesis project is concerned with network management. Network management includes the complete range of tools and protocols used to configure, monitor, and manage a network. In this section, network management is described in general terms, along with some tools and protocols that are of importance in this thesis project.

2.1.1 Background

In larger networks, such as corporate or university networks, there are not only a large number of computers connected to the network, but there is also a lot of network infrastructure, such as routers, switches, servers, etc. In these networks, network management can often become quite difficult and resource consuming. It is important to keep track of every device in order to be able to detect and predict network faults and to maintain a stable network environment. However, the main question is: How do you effectively manage large networks?

Of course, this management could be done manually given sufficient manpower to directly configure, monitor, and manage each device. However, this is not a scalable solution in networks with thousands of devices. Instead, it is more appropriate to use tools to automate configuration, monitoring, and management of all these network connected devices. One approach is to collect all the relevant data at a central point in the network. This central point can then be accessed either directly or remotely to configure, monitor, and manage the entire network. The software used at this central point is often called a NMS.

Network management includes activities such as monitoring devices for crashes, monitoring current load versus capacity, identifying faulty components, and notifying network administrator(s) about changes in the network's status. NMS also implies communication with each of the devices, for example performing queries of the device or to update the device's configuration. A further description can be found in Section 2.1.2.

2.1.2 Fault, Configuration, Accounting, Performance, and Security (FCAPS)

To standardise and simplify the structure of network management, the International Organization for Standardization (ISO) has standardised a framework and divided the ISO-model for network management into smaller groups: Fault, Configuration, Accounting, Performance, and Security (FCAPS).

A **fault** is defined as an event that has a negative impact. The purpose of fault management is to recognise, isolate, correct, and log all faults in the network. In more advanced systems, fault management can be used to predict faults by inspecting current and previous events and searching for patterns that are associated with faults. The assumption is that if the pattern reoccurs, then the fault will occur. In addition to logging every fault, a notification is often sent to the network administrator(s), either via the management system itself, email, a text message, or another form of communication.

Configuration management is, amongst other uses, used to poll configurations from the network devices and store them for backup purposes, track changes made in configurations, and to simplify configuration of devices (for example by implementing functionality to configure or update many devices at the same time). Configuration management is an important part of network management, since faults can occur in a network when a device is configured incorrectly or buggy updates are installed. Being able to rollback to an earlier working configuration can simplify network management and save a lot of resources.

The goal of **accounting** (which in the ISO model also includes user administration) is to manage the different users of the network and to collect information about their resource usage. Users are often divided into groups, departments, etc., each of which have different permissions to access the network's resources, different priorities, and different levels of importance to the organisation's operations. User activity, resource usage, etc. can be tracked for various purposes, such as charging for service(s), investigating abuse, predicting future capacity requirements, etc.

Performance management is done to ensure that the network's performance levels remain within acceptable values. This may involve monitoring many different variables, such as throughput, response time, packet loss rate, error rates, percentage utilisation, and more. Performance management is often based on collecting information via SNMP, as described in Section 2.1.3.

Security management is both the process of ensuring that unauthorised users do not have access and to ensure that data remains intact. Ensuring that no unauthorised users have access is done by authentication, encryption, firewalls, security policies, intrusion detection systems, etc. Ensuring that data remains intact (for example despite hard drive failure, active attack, or any other event that could cause data loss) is done by incremental backups, redundancy, cryptographic check sums, etc.

2.1.3 Simple Network Management Protocol

Perhaps the most popular and wide-spread protocol for network monitoring and management is SNMP. As is described in Request for Comments (RFC) 1157 [1], SNMP is a protocol used in a network of network management stations and network elements, such as workstations, routers, switches, servers, printers, and more. Each network element has management agents responsible for performing the tasks requested by the network management station. SNMP provides communication between these nodes.

There are two types of SNMP messages: manager-to-agent and agent-to-manager. Manager-to-agent messages are requests sent from a network management station to a network element, for instance `GetRequest`, to retrieve the value of a variable or a list of values, and `SetRequest` to change the value of a variable or a list of values. Agent-to-manager messages are usually responses to the network management station from a network element, such as responses to the `GetRequest` and `SetRequest` messages, but can also be asynchronous trap messages.

Trap messages, as shown in Figure 2.1 on the next page, are *unsolicited* messages sent from a management agent on a network element to a network management station to indicate to the network management station the occurrence of significant events, for instance `linkDown` to notify the network management station that a network link is down. To reduce the bandwidth used by traps, only a Object Identifier (OID) is sent to the network management station. The network management station then matches this OID with a OID in a Management Information Base (MIB) which has a detailed description of this trap OID.

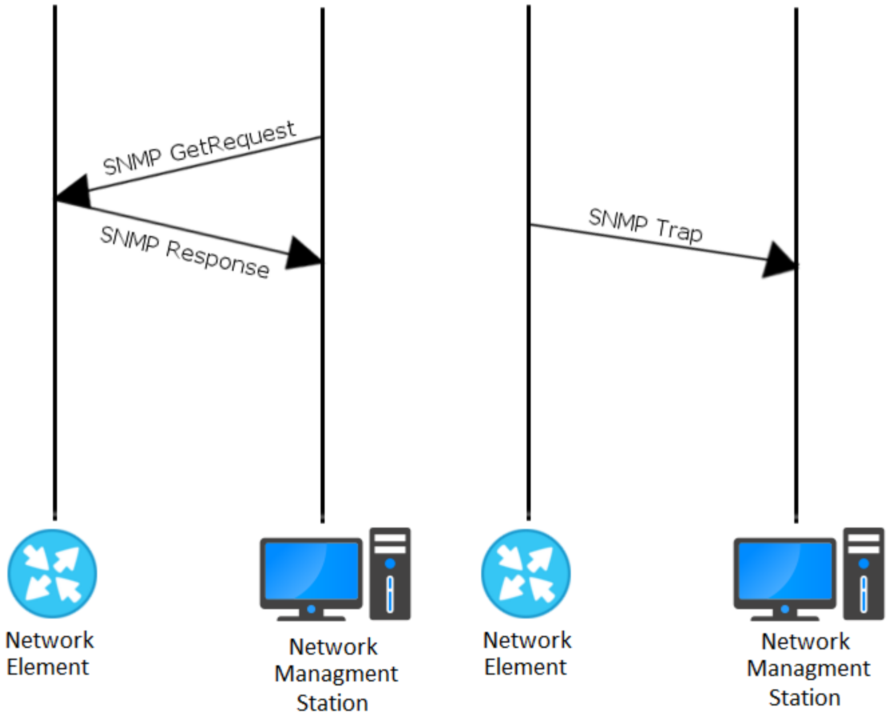


Figure 2.1: A SNMP request/response example to the left, and a trap example to the right.

SNMP version 1 (SNMPv1) lacks some important features, mainly some missing functionality and a near complete lack of security. Counters for tracking activity are only 32 bits long, which limits some of the functions. For instance, a 1 Gigabit per second (Gbps) ethernet interface can wrap a 32-bit `ifInOctets`* counter in 34 seconds [2], thus if the counter is being polled at one minute intervals, it will show misleading data. SNMPv1 is not reliable when operating over User Datagram Protocol (UDP), as delivery is not assured and dropped packets are not reported, hence there is no guarantee that traps arrive at their destination, nor that requested information is returned. Additionally, all SNMP Protocol Data Units (PDUs) between nodes are sent in clear text, which in practice provides no security at all.

SNMP version 2 (SNMPv2) addresses the problem of 32 bit counters by implementing 64-bit counters. It also addresses the problem of poor reliability

* A counter storing the number of octets received by a interface.

by implementing a new type of message: inform requests. Inform requests are identical to traps, but the network management station acknowledges to the network element receipt of the inform request, which assures the source that this PDU has arrived, otherwise the device will attempt to transmit the inform request again.

SNMPv2 was later on divided into several subprotocols: SNMP version 2 community (SNMPv2c), SNMP version 2 party-based (SNMPv2p), and SNMP version 2 user-based (SNMPv2u), where each focuses on a different approach.

Lastly, a "reunited" SNMP version 3 (SNMPv3) was released which merges the previous subprotocols' functions into one protocol, and improves security by adding encryption and authentication [3].

2.1.4 Command Line Interfaces

A Command Line Interface (CLI) enables users to interact with and operate software (including operating systems) via a text-based interface. There are several very convenient tools for CLI based network management: Secure Shell (SSH) and Telnet.

2.1.4.1 Telnet

Telnet is mostly intended for text based login to computers, but can also be used for example for communication between automated processes. Because many of the application protocols on the Internet are text based (request and reply), Telnet applications can be used to communicate with many servers. Examples of such protocols are Simple Mail Transfer Protocol (SMTP), Post Office Protocol version 3 (POP3), and Internet Message Access Protocol (IMAP) for email; Hypertext Transfer Protocol (HTTP) for web access; and Network News Transfer Protocol (NNTP) for Usenet access [4].

2.1.4.2 Secure Shell

SSH is a protocol for secure connections with computers/devices over the Internet. It is a secure substitute for Telnet as all traffic is encrypted. SSH has two versions, named SSH version 1 (SSH-1) and SSH version 2 (SSH-2), with the latter being the improved version. When initiating a secure connection, a packet encrypted with a 128-bit key is sent from the client to an SSH server. After the connection is established each data segment is encrypted using encryption algorithms, such as Rivest, Shamir, Adleman (RSA), Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption Algorithm (IDEA), and Blowfish, among others [5].

SSH can be used for remote logins, tunnelling, X11 connectivity, Secure File Transfer Protocol (SFTP), and TCP port forwarding.

2.1.5 Secure File Transfer Protocol

According to the Internet Engineering Task Force (IETF) draft *draft-ietf-secsh-filexfer-13* [6] SFTP was designed as an extension for SSH-2, but can interoperate with a number of other applications, such as Transport Layer Security (TLS) and information transfer via Virtual Private Networks (VPNs). SFTP provides secure file access, transfer, and management; it does not provide authentication and security; instead it depends on the underlying protocols to handle these. SFTP should not be confused with the "Simple File Transfer Protocol" [7], as this does not run over SSH, while SFTP was designed from the ground up by the IETF Secure Shell (SECSH) working group.

SFTP not only supports file transfers, but it also provide a range of operations on remote systems files. In combination with a User Interface (UI), SFTP offers additional capabilities, such as resuming interrupted transfers, directory listings, and remote file removal. SFTP is platform independent and is commonly available on most platforms.

2.1.6 Hypertext Transfer Protocol Secure

HTTP is a communication protocol used to transfer hypermedia on the Internet. Hypertext Transfer Protocol Secure (HTTPS)[8] is a further development of HTTP and offers encrypted transport of data, to and from web servers. HTTPS connections are often used for e-commerce and for transferring sensitive data, for authentication and management of private information, and more importantly to secure the user's integrity. Using HTTPS users should be able to trust the web server and that a third party should not be able to listen in on the connection. Given an appropriate certificate it is possible for a user to verify his own identity to the server, and for the user to verify the identity of the server.

HTTPS was developed by Netscape [9] for secure transactions and was initially known as "HTTP over Secure Socket Layer (SSL)". As stated in RFC 2818 [8], HTTPS can also run with TLS instead of SSL, thus it is commonly known simply as HTTP *Secure*.

Both HTTP and HTTPS are generally utilised together with Hypertext Markup Language (HTML), where HTTP/HTTPS deals with *transferring* the data and HTML *encodes* the contents.

2.1.7 NetFlow

NetFlow is a tool developed by Cisco [10]. It provides the ability to collect information about traffic as it enters or exits an interface on an router. That information can be exported and analysed by the network administrator(s) to find out the source and destination of each traffic flow, class of service, and if congestion was caused - what caused it. When NetFlow is used, flow monitoring typically consists of three main components [11]:

Flow exporter aggregates packets into flows and exports flow records to one or more flow collectors.

Flow collector receives data from a flow exporter. The flow collector is responsible for reception, storage, and pre-processing of that data.

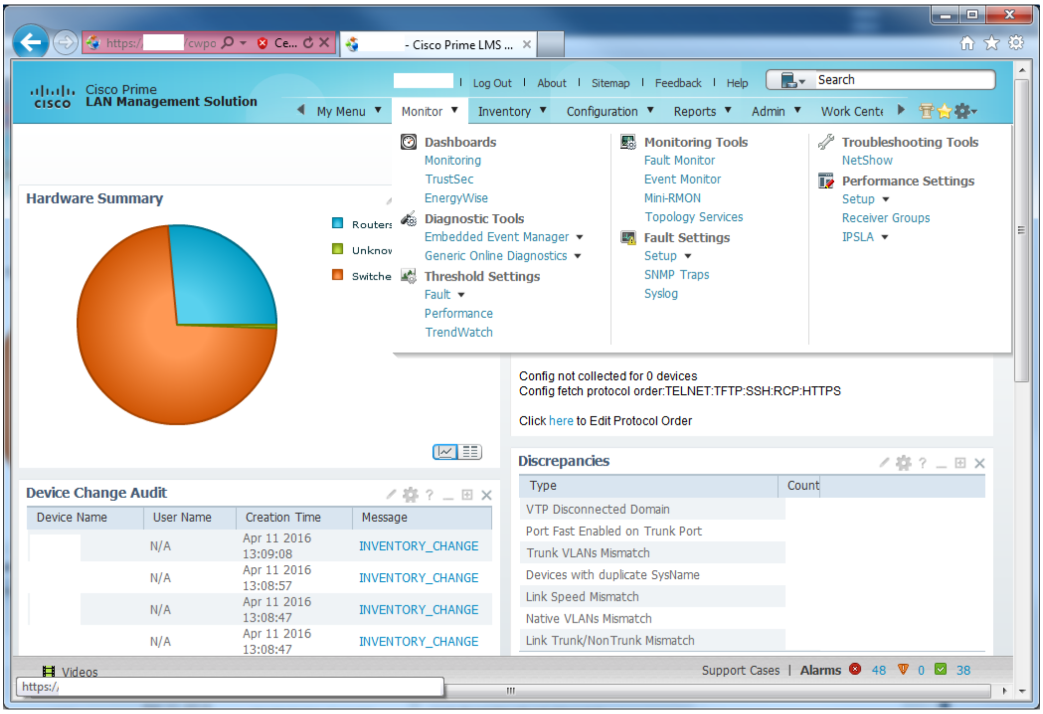
Analysis application analyses flow data in the context of intrusion detection, traffic profiling, or for some other purpose.

2.2 Cisco Prime LAN Management Solution

As stated earlier, Netcorp is currently using Cisco Prime LMS. LMS is designed to manage a network of Cisco products. It provides a broad set of management functions, such as configuration, compliance, monitoring, troubleshooting, and administration of the network.

LMS utilises many protocols to provide powerful features to optimise small-to-medium-sized Cisco networks. Using HTTPS and HTML, LMS collects and presents all the tools that are needed to manage such networks via a relatively simple GUI, as shown in Figure 2.2 on the following page.

While the presentation of the network is “simple”, compared to how it would be without an GUI, it is still rather complex as there are many different tabs and options. When LMS receives information via SNMP and presents it via the GUI, this is done with the help of the relevant MIB. Each specific MIB describes the variables that can be managed through SNMP. These variables are defined with the regard to the variable’s data type, access rights, etc. [12].



Config not collected for 0 devices
Config fetch protocol order:TELNET:TFTP:SSH:RCP:HTTPS

Click here to Edit Protocol Order

Device Change Audit

Device Name	User Name	Creation Time	Message
	N/A	Apr 11 2016 13:09:08	INVENTORY_CHANGE
	N/A	Apr 11 2016 13:08:57	INVENTORY_CHANGE
	N/A	Apr 11 2016 13:08:47	INVENTORY_CHANGE
	N/A	Apr 11 2016 13:08:47	INVENTORY_CHANGE

Discrepancies

Type	Count
VTP Disconnected Domain	
Port Fast Enabled on Trunk Port	
Trunk VLANs Mismatch	
Devices with duplicate SysName	
Link Speed Mismatch	
Native VLANs Mismatch	
Link Trunk/NonTrunk Mismatch	

Figure 2.2: The main view of LMS

2.2.1 Functions

LMS provides many different functions for many different purposes. These functions co-exist and work together to provide optimal utilisation for network management. These functions provide support for the following functional categories: administration, management, monitoring, alerts, reporting, and even inventory information. Each category of functions consists of a number of functions that utilise various protocols, mostly SNMP, to provide relevant information for the network administrator(s). To give more insight into what each category consists of, we give the following brief explanation [13]:

Administration functions simplify and centralise setup and configuration of the LMS.

Management functions provides configuration backup, software image management, and the ability to send out mass configurations and updates to network devices. With dynamically guided work flows for managing events and tasks, LMS reduces the chance for errors.

Monitoring functions help to quickly identify and fix problems that occur. The goal is to fix problems as quickly as possible - before they have any negative affect on end users or services. An alert is always sent to the event browser by the LMS when a fault occurs. SNMP polling helps to identify device availability and performance issues, as well as giving the possibility to collect statistics about endpoints and devices. Troubleshooting is embedded into LMS to quickly isolate problems.

Reporting functions are very important as they contain valuable information about inventory, configurations, regulatory compliance, services, capabilities of the network, user tracking, life cycle reports (such as End-of-sale, Contract Management, Cisco Product Security Incident Response Team (PSIRT)), and other Cisco Prime LMS reports. These potential reports are presented in a single menu for simple navigation and access. Generating reports can be done manually or scheduled to run during any preferred time period and can be generated periodically.

Inventory information is useful as LMS supports more than 600 different Cisco device types, thus LMS can keep detailed information about every device in the network, such as chassis, module, interfaces, and so on. This information is very valuable to network administrator(s), for example when identifying old hardware for possible upgrading. There is a single menu for discovery and device status, user tracking, and inventory dashboards.

2.2.2 Licences and Limitations

Cisco sells LMS under several different licences depending on the number of devices that require management. The maximum number of devices that can be handled is 10,000. Depending on the number of devices the company has, there are certain scaling limitations on the LMS servers. Some examples of these limitations from [14, Chapter 3] are shown in Table 2.1 on the next page.

Table 2.1: The limitations of various features in LMS, for the all licenses [14, Chapter 3].

Feature	**Limitation**	**License**
Fault Management	Maximum of 80,000 ports or interfaces.	All licenses.
Inventory, Configuration and Image management	10,000 devices. 200 port and module configuration groups with 90% port groups and 10% module groups. Maximum of 500,000 ports with an average of 50 ports per device. Maximum of 100,000 ports in a port and module configuration group. Maximum of 250,000 ports for each LMS job.	All licenses.
Device Performance Management	MIB objects scaling limit is 6,000.	For up to 500 LMS devices.
	MIB objects scaling limit is 30,000.	For up to 1,000 LMS devices.
	MIB objects scaling limit is 50,000.	For up to 2,500 LMS devices.
	MIB objects scaling limit is 100,000.	For up to 5,000 LMS devices.

2.3 Netcorp

This section provides information about Netcorp's current network and the requirements they have for their new NMS.

2.3.1 Infractructure

Netcorp's infrastructure is built up mostly out of Cisco equipment and is composed of three major networks and many smaller networks for their services. Today, there are about a total of 2,500 devices in the network, where a majority of these devices are switches. As seen in Figure 2.3, the three major networks are the Customer Network (running Multiprotocol Label Switching (MPLS)), the Internal Network, and the Management Network. The Management Network manages the many smaller networks for television and radio communication.

Of the three major networks, the Management Network is the smallest as it uses the Customer Network as a data carrier. This makes the Customer Network and the Internal network the main networks that need monitoring, which is done with LMS.

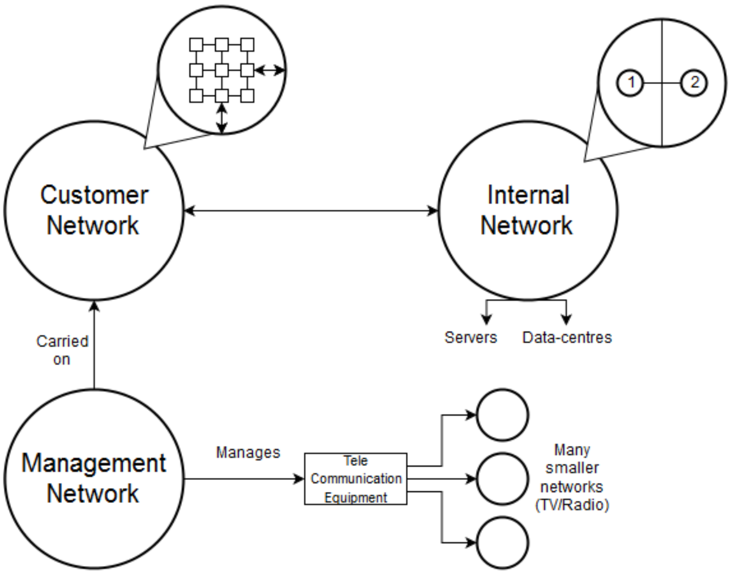


Figure 2.3: An overview of Netcorp's network infrastructure.

2.3.1.1 Customer Network

The Customer Network consist of nine provider nodes interconnected with each other. These provider nodes are mainly located in major cities, as high-capacity connectivity is available between major cities. From each of these provider nodes, smaller nodes responsible for sending out data and services span out towards Customer-provided Equipment (CPE) terminals located at a subscriber's premises. These smaller nodes also span out towards telecommunication masts and transfer data between cities via radio signals.

Netcorp's Customer Network consists of switches operating at Layer 2*. However, by using MPLS the switches can achieve functionalities of a router, making routing decisions at similar speeds to traditional Level 3 routing [15]. Thus, MPLS nodes are often called routers, even though they are physically switches.

2.3.1.2 Internal Network

Located at two geographical locations, the Internal Network consists of servers and data centres. These networks consist mostly of 10 connections. Between the two locations all traffic is multiplexed via Wavelength-division Multiplexing (WDM) into optical fibres to traverse at high speed, and later be demultiplexed by another WDM demultiplexer on the receiver side and directed to the correct destination. Note that the Customer Network is connected to the WDM network as well.

By using SSH and Telnet, network administrator(s) access servers, data centres, routers, and switches to manage them remotely. By setting up SFTP servers on the Internal Network, the configuration of servers can be simplified, as configuration files can be transmitted to all nodes in the network, and if SFTP is used, then the file transfer would be secure as well.

2.3.2 NMS Requirements

There are certain requirements the new NMS must meet in order to be a suitable replacement for LMS. The requirements can be split into two different categories: required and preferred.

2.3.2.1 Required features

The features listed below are required of the new NMS, and must be met in order for it to be a suitable replacement for LMS.

- Monitoring, management, and configuration of network devices,
- Support for communication to managed devices via SNMPv3,

* Layer 2 of the Open Systems Interconnection (OSI)-model - the data link layer.

- Polling and storing backups of configuration files of managed devices,
- Alarm tracking of important events on managed devices,
- Management of user accounts on the NMS,
- System reports (network inventory, topology, alarms, performance, etc.),
- Inventory over all managed devices,
- History of alarms, system reports, etc.,
- Send queries to managed devices,
- Troubleshooting,
- Ability to manually turn off monitoring of a specific device or interface,
- Automatic device discovery, and
- Support for a wide variety of devices, including devices from Cisco.

2.3.2.2 Preferred features

Listed below are features that Netcorp is unsatisfied with in LMS, and thus a better implementation is preferred in the new NMS.

- Less complex GUI than LMS,
- A clear definition of what causes an alarm,
- Graphical visualisation of system reports,
- An easy-to-understand dashboard/front page, and
- Forwarding of alarms to other systems.

2.4 Related Work

This section discusses related work concerning analysis and evaluation of NMSs. Four different works are described as these have helped us greatly by providing ideas, facts, and other relevant information.

2.4.1 Survey of Network Performance Monitoring Tools

In 2006, Travis Keshav wrote a survey of network performance monitoring tools [16] which analyses different network performance monitoring tools. Due to the age of this report, some of the information is obviously outdated, and cannot be used today - ten years later. However, the report provides a lot of useful information that is still valuable. Although technology has changed a lot in ten years and solutions used at that time might not even work today (for example due to software end-of-life, system incompatibility, and more), the general structure of networks and the needs for monitoring are still more or less the same.

His report gives useful insights into what aspects to focus on when analysing network monitoring tools. This lead to a lot of questions which were very useful for our thesis project, such as “Is it of interest to monitor network flows?” or “Is it only network infrastructure that should be monitored or should workstations also be monitored?”.

In his survey, many different types of network monitoring are described, including: application and host-based monitoring, flow monitoring, packet sniffing, bandwidth analysis, and wireless network monitoring. Most interesting is the analysis of NMSs (referred to as network monitoring platforms in the report). This analysis is of the same type as we need to perform in our thesis project, therefore his survey was very helpful.

Excluding Cisco LMS, the following three NMSs were discussed:

- VitalSuite [17],
- Computer Associates International (CA) Unified Infrastructure Management (UIM) (formerly known as (f.k.a.) NimBUS by Nimsoft, as it is referred to in the report) [18], and
- International Business Machines (IBM) Tivoli Netcool/OMNIbus [19].

2.4.2 Open Source Networking Tools

In 2010, Cynthia Harvey described 55 replacements for various networking tools, all available as open source [20]. Many interesting tools are discussed with regard to backup solutions, network simulation, and anti-spam filters amongst other applications. Three of these tools are particularly relevant as they are described as NMSs:

- Open Network Management System (OpenNMS) [21],
- Really Awesome New Cisco confIg Differ (RANCID) [22], and
- Zenoss [23].

Furthermore, RANCID is described as a replacement for Cisco LMS, making it very relevant to our analysis. Unfortunately, RANCID turns out to be unsuitable for Netcorp, as described in Section 5.4.3 on page 58.

2.4.3 Large Scale Network Monitoring

Reddit - sometimes referred to as “the front page of the Internet” - is a popular Internet forum where users can converse about various topics. In the subreddit* /r/networking, a thread created by the user “Clayd0n” asks for advice on large scale network monitoring [24].

A great benefit of forums is that everyone can join the discussion, thus opinions from many different sources are available at a single place. This is especially true in this thread, where many users agree that having two or more NMSs is often much better than trying to find a single (NMS) system that supports every function. The argument is that most NMSs can not do everything right, while smaller, more focused solutions, often are better at a specific task.

One NMS, Orion [25] (also known as (a.k.a.) SolarWind Network Performance Monitor (NPM)), is even referred to as a “Frankenstein experiment” by the user “nof”, since it does “everything”, but all the components feel as if they are kludged together and it ends up doing a mediocre (at best) job of them all.

In the thread there are several recommended tools for network management. These are, as of March 8^{th} 2016:

- RANCID [22] is recommended for monitoring, configuration polling, and deployment. RANCID supports multiple systems, such as Cisco routers, Juniper routers, Catalyst switches, Foundry switches, Alteon switches, Hewlett Packard (HP) Procurve switches, and more.
- NetBrain [26] for automation.
- Paessler Router Traffic Grapher (PRTG) [27] for network monitoring via SNMP and Netflow.
- Cacti [28] for accounting and performance monitoring.
- CactiEZ [29], as a simpler version of Cacti.
- Network weathermap [30] for creating live network maps from statistics.
- Observium [31] as a fairly broad solution that monitors a lot of aspects of the network.
- Zabbix [32] as a free monitoring system for Linux.

The following complete NMSs are frequently recommended:

- HP OpenView [33] (a.k.a. HP Business Technology Optimization (BTO)) is a very widely recommended NMS that includes nearly every function needed for network management.

[*] A subreddit is a part of the forum focusing on a specific subject.

- Zenoss [23], which can either be very basic or very complex, depending on how you customise it. It offers map building via SNMP, with responsive monitoring and high refresh rate even under load. However, it seems to have trouble in larger networks.

- Orion (a.k.a. SolarWind NPM) [25], although it is disliked by some users and some users feel that it costs a bit more than it should, is described as a good, single console that scales, is multi-vendor and provides a reliable NMS.

In the thread, a discussion about open source software is persistent. Different benefits are listed, for example that it in the majority of cases in addition to being free of charge, open source software is seen as more secure, since anyone can inspect the code and thus detect security (and other) flaws. On the other hand, open source software is sometimes disliked since often there is no customer support. Many feel that customer support is required in most enterprise environments. The user "snowbirdie" also raises a very valid point that many open source projects often consists of "just a couple of developers who have no time for patches, quality control, or even just stops developing because they don't care anymore". This is indeed a very important aspect to consider when evaluating monitoring solutions. However, there are companies that offer commercial support for open source software. Additionally, even company supported software often reaches a point that the company no longer wants to support it.

2.4.4 Comparison of Network Monitoring Systems

Although Wikipedia is not usually seen as a valid source in scientific reports, Wikipedia does contain a list of network monitoring systems [34] (which is also regularly updated). This list is also accompanied with some information about each network monitoring system. For this thesis project, the *list of names* is used, but the information about each system is acquired from a first-hand source, typically its own website or documentation. Thus, Wikipedia provided a valid source, by providing the names of different network monitoring systems. This greatly facilitated the process of identifying potential network monitoring systems for further exploration in this thesis project.

The list of network monitoring systems is quite long and can be found in Appendix A.1 on page 73.

2.5 Summary

Network management is a very broad subject, and has therefore, for simplicity, been divided into several groups following the ISO-standardised FCAPS framework. There are many tools on the market which realise one or more parts of FCAPS, as well as a couple of “complete packages” that include all the aspects of the FCAPS framework in a single solution, typically called Network Management Solutions (NMSs).

Tools for network management make use of many different protocols, with SNMP usually being the most prominent one. Other protocols, such as HTTP/HTTPS are used for displaying management interfaces; SSH (and Telnet) for secure (and less secure) connections via CLI; and SFTP for secure file transfers.

LMS is a NMS developed by Cisco for their products. With many useful functions for administration, management, monitoring, reporting, and providing inventory information, it includes all of the aspects of the FCAPS framework and provides good support for LANs. LMS comes with different licenses, but 10,000 devices is the maximum number of devices supported.

The related work provided a lot of useful information in the form of both ideas and facts. We gained different perspectives on the advantages and disadvantages of open source software, whether a single NMS or several tools are more suitable, and some questions that should be asked, such as “Should we monitor just the infrastructure, or should we monitor workstations and other nodes as well?”.

From the related work, we discovered many recommended tools and NMSs, such as CA UIM, RANCID, Zenoss, and NetBrain. We will explore these in the following chapters.

Chapter 3

Method

The purpose of this chapter is to provide an overview of the research method used in this thesis. Section 3.1 describes the research process. Section 3.2 details the research paradigm. Section 3.3 focuses on the data collection techniques used for this research. Section 3.4 describes the planned measurements. Section 3.5 explains the techniques used to evaluate the reliability and validity of the data collected. Finally, Section 3.6 describes our planned data analysis.

3.1 Research Process

The research process utilised both quantitative and qualitative research methods. More specifically, the process is divided into three steps: *quantitative*, *quantitative & qualitative*, and *qualitative*, as is shown in Figure 3.1. This will be referred to as the *three-step approach*.

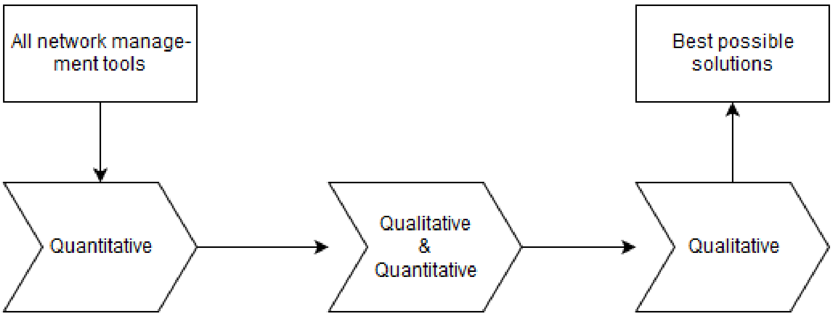


Figure 3.1: A flowchart of the research process, referred to as the three-step approach.

3.1.1 Step 1: Gathering and Filtering

First a quantitative gathering and filtering process was performed. The goal was to learn about as many network management tools as possible.

A lot of data was gathered for each network management tool, then we filtered out those tools that did not fulfil the company's specifications and kept those which did. This filtering was done by setting specific, concrete requirements that each tool has to fulfil in order to be approved. The requirements we set for this step can be seen in Section 3.6.1 on page 29.

Objective data in form of Boolean values, numerical values, and specific strings were collected in this step. The goal was to easily filter out those alternatives which obviously do not meet the requirements, in order to facilitate the next step.

3.1.2 Step 2: Theoretical In-Depth Analysis

The next step is a mixture of both quantitative and qualitative research. Of the alternatives remaining from step 1, a more in-depth, theoretical analysis is performed. A lot of subjective, text-based, in-depth information was processed in this step, to gain a deeper knowledge of each tool.

While some tools are incomplete, together with another tool they may create a complete solution. For example, tool A might fulfil the needs for *fault*, *performance*, and *security* requirements, while tool B fulfils the needs for *configuration*, *accounting*, and *security*, thus they complement each other and together they create a complete NMS that fulfils every requirement in the FCAPS model.

Tools that do not fulfil all the needs, and cannot be complemented by another tool, were filtered out in order to facilitate the next step. Note that we only considered combinations of two tools, hence there might be additional combinations of three or more tools that could be considered in future work, as described in Section 6.2.1.4 on page 63.

3.1.3 Step 3: Practical In-Depth Analysis

Lastly, when only those alternatives which fulfil all the required specifications remain, a more qualitative research process based upon additional practical in-depth analysis was performed. Each network management tool (or combination of tools) was tested in a real-world network environment to carefully test stability, user-friendliness, support, etc., to ensure it works as expected. If not, the problem might be solved or worked around, in which case the solution may be acceptable, otherwise it was filtered out.

When the practical in-depth testing was complete, it should only be a matter of personal preference and financial budget as to which solution is most suitable for Netcorp to implement.

3.2 Research Paradigm

Given the problem definition in Section 1.2 on page 2, it is only logical that this thesis project embraces the realistic philosophical paradigm. This paradigm is appropriate because the thesis is heavily based on credible data and facts, from which we seek to understand the data and develop knowledge about existing solutions in the market.

Positivism might be applied upon the implementation of the possible solutions to test if the assumptions correspond with current systems (presumably in simulated environments). This also works well when testing the performance of the alternative solutions [35].

3.3 Data Collection

This section describes the methods used to collect relevant data for this thesis project. Data collection from interviews and web-based research were collected in parallel during the first and second steps of the three-step approach, while data collection from testing was provided by the third step.

The target population for this data collection is Netcorp's network operators and administrators.

3.3.1 Interviewing

We began by collecting data by interviewing Netcorp's network specialists. From this we learned about the basic system requirements and delimitations for the new NMS, information about the current network infrastructure and its devices, issues with the current NMS (LMS), and personal suggestions for NMSs that might be relevant for the company.

3.3.2 Web-Based Research

Via web-based research we found related work. These related works were analysed to get opinions and suggestions about NMSs and suggestions of approaches for analysing NMSs. Data was also retrieved from first-hand sources, such as a product's website, data sheets, and IETF RFCs.

3.3.3 Direct Contact

In many cases, detailed information was not available via web-based research. In these cases, data was collected via direct contact with technical support and/or the sales department of the company/organisation providing the solution. Contact was made either via email, live chat, phone calls, or a physical meeting.

3.3.4 Testing

By testing the NMSs in a real-world network environment, data is collected about supported devices by testing each NMS against a selection of routers, switches, and other network devices in a lab environment. If we come across any stability issues during testing, such as bugs or system hangups, they are documented. We also test user-friendliness by navigating through menus, testing functions, and analysing the overall user experience of the NMS. Lastly, interworking between networking tools was tested (if applicable). This was done by verifying that communication between the paired tools work correctly.

3.4 Planned Measurements

In our three-step approach, neither the first or the second step requires any measurements. The third step, however, requires planning measurements before commencing testing. The test environment and the hardware/software used for this testing are described in this section.

The tests are made to collect data about the following metrics for each of the NMSs (or parts there of):

- Stability,
- Device support,
- Functionalities, and
- User-friendliness.

3.4.1 Test Environment

The test environment for the third step requires a (presumably emulated) real-world network environment similar to Netcorps' current network. The relevant parts of Netcorp's network will be replicated in the test environment, to create a scenario as identical to the actual network as possible within this projects limits.

3.4.2 Hardware/Software to be Used

During the last step in the three-step approach, we test the NMSs in a real network environment to get a proof-of-concept and to see how they each perform in a real-world scenario.

The NMS itself was installed on a system in a virtual environment. The host running the Virtual Machines (VMs) is a HP Blade server generation 9, containing two Intel Xeon E5-2600 v4 processors and 256 Gigabyte (GB) of memory. The software used for the virtual environment is VMware 6.0.

The physical host is running two VMs, where each have access to 12 GB memory and two processor cores. One machine's operating system is Microsoft's Windows Server 2008 R2 64-bit and the other's is CentOS 7 64-bit. The two different environment was used since some NMSs runs in a Microsoft Windows environment, while other runs in a Linux/Unix environment.

To test the NMSs we use actual hardware in a lab environment, connected to the same network as the VMs. Because of obvious limitations in the amount of time, hardware, space, and money, we could not construct a lab environment with all 2,500 devices, making a complete replicate of Netcorp's actual network. Hence, a handful of representative devices were chosen for the lab environment to replicate the most relevant parts of the network. The hardware consists of five switches, six routers, and one Network Interface Device (NID). Each device is listed below:

- Accedian MetroNID
- Cisco 1720 Router
- Cisco 2600 Router
- Cisco 2900 XL Switch
- Cisco 3550 Switch
- Cisco Aggregation Services Routers (ASR) 9001 Router
- Cisco ASR 901 Router
- Cisco ASR 920 Router
- Cisco Metro Ethernet (ME) 3400E Switch
- Cisco ME 3750 Switch

Some devices listed above are chosen for a specific reason: The Accedian MetroNID was chosen since it is a rather uncommon device, which will assure the new NMS supports uncommon devices and has a wide device support. The Cisco 1720 router is tested since it is one of the oldest devices in Netcorp's network, and support for this device will be tested to assure the new NMS supports older devices. The same principle applies to the Cisco 2000 series routers. The Cisco ASR 9001 routers are the core devices that builds up the Customer Network, hence, support for these devices are essential. Cisco ASR 901 and Cisco ASR 920 routers are at the centre of the Customer Network, therefore it must be ensured that the new NMS supports these devices. Note that the Cisco 920 is one of the devices in Netcorp's current network that is not supported by Cisco LMS. It is important to test that the new NMS supports this device, since Netcorp wants to manage all their network devices. Lastly, the outskirts of the Customer Network consists mostly of Cisco ME 3400E switches. The new NMS must also support these devices. The other devices listed above are simply chosen for sample testing - to test that the new NMS has wide device support.

3.5 Assessing Reliability and Validity of the Data Collected

In this section reliability and validity of the collected data is described.

3.5.1 Reliability

The data received from interviewing Netcorp's network specialists was seen as reliable data as these specialists have years of experience with the subject, and they are both familiar with the current NMS and know the requirements for the new NMS.

Data received from web-based research is seen as reliable if retrieved from a first-hand source (a product's website, data sheets, RFCs, etc.). However, even when data is not received from a first-hand source, it can sometimes be seen as reliable, depending on the perceived source's credibility.

Data based upon testing is seen as mostly reliable, since we are our own first-hand source, but due to our limited time-frame in the testing process we can not assure that aspects such as stability is tested properly.

3.5.2 Validity

Results gathered when conducting research should be repeatable. If a test is performed several times, and the resulting data is similar, then the data is seen as valid. In general the data should be authentic and originate from a reliable source. The validity of data received from interviewing Netcorp's network specialists is assumed to be valid, since we ourselves do not have access to the required systems to independently validate this data. However, we can compare the data provided by Netcorp's network specialists with data from other first-hand sources, and if they conflict (which does happen, as seen in for example Section 1.2 on page 2), then data from Netcorp's network specialists was prioritised.

3.6 Planned Data Analysis

It is good to plan and state what questions should be answered *before* research is done. This section describes the questions we set for analysis before hand, and describes why they were important.

3.6.1 First-Level Filtering

Considering the number of available NMSs in the market, and due to our limited time-frame for this thesis project, there is no room for an in-depth analysis of each and every one of them. Therefore an abstract, objective point of view is required to filter out and eliminate irrelevant NMSs. Based upon Netcorp's network infrastructure and their functionality requirements, the flowchart shown in Figure 3.2 on the following page was created as a guideline for the first step in the three-step approach, to filter out irrelevant NMSs. The functional requirements are described below, in a more detailed manner.

Device support Obviously the new NMS is required to support the devices currently in Netcorp's network. This means both that the candidate NMSs has to technically support all the devices, i.e. be able to communicate correctly with the devices; and also that this NMS supports the current *number* of devices in the network without becoming unstable, buggy, or slow. Since Netcorp only uses Cisco devices in their network infrastructure today, this implies that the new NMS should only be required to support Cisco devices. However, due to Netcorp's plans for future expansion of their network, and since they do not wish to be restricted to Cisco devices in the future, the new NMS is required to support other vendor's devices, in addition to Cisco devices.

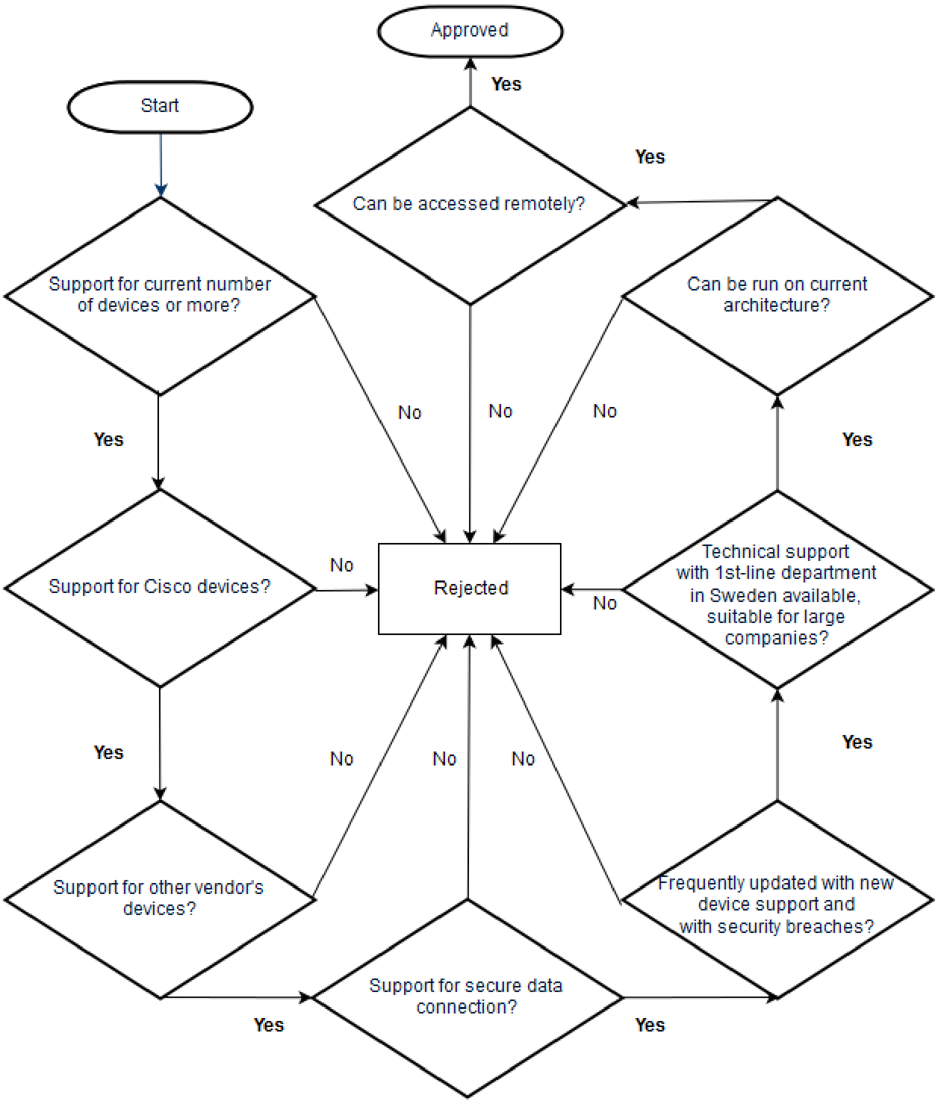

Approved
Yes
Start
Yes
Can be accessed remotely?
Support for current number of devices or more?
Can be run on current architecture?
No
No
No
Yes
Yes
Support for Cisco devices?
No
Rejected
No
Technical support with 1st-line department in Sweden available, suitable for large companies?
Yes
Yes
No
No
No
Support for other vendor's devices?
Frequently updated with new device support and with security breaches?
Support for secure data connection?
Yes
Yes

Figure 3.2: A flowchart of the filtering process in step one of the research process.

Security The new NMS is also required to support secure data communication when possible. For example, a switch in the network supporting SNMPv3 should be able to make use of the security functionalities provided by SNMPv3, i.e. authentication and encryption. Meanwhile, a switch in the network only supporting older versions of SNMP should also be supported, although the data communications is not secure.

Updates The NMS should not have reached its end-of-life, i.e. it should receive frequent software updates adding new device support and patches to fix possible security breaches or other problems. This retirement arises from the fact that the new NMS is supposed to be a long-lasting solution for Netcorp, hence a solution without support for new devices or with patches to correct security breaches will not last very long.

Technical support Netcorp does not want to have a separate department specialised in NMS administration, as this would be resource consuming. Therefore, one of the key requirements that Netcorp is looking for, is to have first-line support for the NMS located in Sweden, in order to get fast and reliable support in case of urgent matters.

Architecture As it is time and resource consuming to upgrade or replace Netcorp's current network architecture, a new NMS that can be implemented and run smoothly on their current architecture is very desirable.

Remote access Lastly, since Netcorp's servers are located in a different geographic location than their headquarters, it is a requirement to remotely access the NMS and to manage the network from the headquarters.

3.6.2 Second-Level Filtering

The second-level filtering, according to step two in the three-step approach, focuses on more in-depth research of the NMSs remaining from the first step. Below is a description of each aspect we research in this step.

In addition to these fairly abstract aspects, we use common sense and take into consideration our own (and Netcorp's) opinions of whether the NMS seems like a suitable solution for Netcorp.

Functionalities The functionalities of the new NMS must fulfil all of Netcorp's requirements, which can be seen in the list of required features in Section 2.3.2.1 on page 16 and the list of preferred features in Section 2.3.2.2 on page 17.

Security In this step we will do an overall in-depth analysis of the security aspects that were analysed in the first step, according to the three-step approach. Examples of what will be looked into are: Is SNMPv3 available to use when possible; the security of the authentication process for the system; how backup solutions are implemented; and what can be done to provide a secure data connection.

Price Lastly, the price point of the product will be analysed. If the product is not free, a subjective judgement will be made to decide if the product is worth the price, considering aspects such as Netcorp's budget, functionalities of the product, etc.

3.6.3 Real-World Testing

Following the three-step approach, real-world testing is performed in the last step. A NMS might look suitable on paper, but this test will see if it performs well in reality. Below is a description of each aspect tested in this step:

Stability The NMS should be stable. This implies that there should be no crashes of the system, even when exposed to heavy loads. The GUI should not be slow when navigating through menus and options.

Security Security is an aspect that should be tested. However, it is both difficult and time consuming to test properly. Therefore the analysis done in the second step, according to the three-step approach, together with basic testing, should be sufficient for the purposes of this thesis project.

User-friendliness In general, seamless workflow for network administrator(s) helps save time and reduces frustration. Network operators should have a clear presentation of problems/alarms that occur in the network. Therefore an easy to handle, low complexity GUI, and possibly graphical visualisation of network aspects is relevant when analysing the user-friendliness. The navigation system should follow basic user-friendliness, such as reaching every function with three or less mouse clicks [36], and having logically structured menus.

Device support We will confirm that the NMS supports the devices described in Section 3.4.2 on page 27. This is done by verifying that the NMS can detect all devices, communicate with them via SNMP, and perform all other functionalities it should be able to perform.

Chapter 4

Finding the Best Network Management Solution

The purpose of this chapter is to concisely present the results from each of the steps in the three-step approach.

4.1 Step 1: Gathering and Filtering

Following the research process described in Section 3.1.1 on page 24, a list of network management tools was gathered. The result is a list of 82 tools, shown in Appendix A.2 on page 75.

After completing this list, which has many tools, it was necessary to shorten this list. This reduction was done by eliminating tools that did not meet the criteria described in Section 3.6.1 on page 29.

The resulting list after this filtering process consists of ten NMSs:

- CA Spectrum,
- CA Unified Infrastructure Management (UIM),
- Cisco Prime Infrastructure,
- HP Intelligent Management Center (IMC),
- HP Enterprise (HPE) Network Node Manager i (NNMi),
- HPE Network Automation,
- IBM Tivoli Netcool/OMNIbus,
- ManageEngine OpManager,
- Opmantek Network Management Information System (NMIS), and

- SevOne.

4.2 Step 2: Theoretical In-Depth Analysis

Next, we performed the second step of the three-step approach according to Section 3.1.2 on page 24. Using the criteria described in Section 3.6.1 on page 29, five of the ten NMSs were considered for practical testing in the last step:

- HP Intelligent Management Center (IMC),
- HPE Network Node Manager i (NNMi),
- IBM Tivoli Netcool/OMNIbus,
- ManageEngine OpManager, and
- Opmantek Network Management Information System (NMIS).

4.3 Step 3: Practical In-Depth Analysis

Lastly, in the third step of the three-step approach according to Section 3.1.3 on page 24, we resulted with the following two final NMS solutions as recommended solutions for Netcorp:

- IBM Tivoli Netcool/OMNIbus, and
- ManageEngine OpManager.

Chapter 5

Analysis

The purpose of this chapter is to provide deeper insight and analysis of the minor and major results given in Sections 5.1 and 5.2. Sections 5.3 and 5.4 analyse the reliability and validity of our results. The chapter is concluded in Section 5.5 with a discussion, which also presents NMSs which did not make the cut, but are still worth mentioning.

5.1 Minor Results

This section describes and analyses the results from the theoretical and practical analyses.

5.1.1 Results From Theoretical Analysis

This section analyses the results from the theoretical research. Following the three-step approach, information is only given about the second step, in-depth theoretical analysis, since results from the first step were completely objective and cannot be further analysed.

A description of every NMS, as per the set of requirements in Section 3.6.2 on page 31, is given, followed by a concluding decision as to whether the NMS deserves to be tested practically in the last step, or if it seems unsuitable for Netcorp and should be rejected from further evaluation.

To reduce redundancy and clutter in the report, a description of functionalities that *all* NMSs have in common, unless explicitly stated otherwise in the NMS's corresponding section, is described below. Functionalities that are unique to one or a few NMSs will be described in the corresponding NMS's section.

Alarms The NMS notifies the network administrator(s) of important events by sending an alarm via the web interface. Alarms are categorised into different levels of criticality to allow the administrator(s) to focus on the most important events. An alarm can be suppressed if it is insignificant.

Backup The NMS polls configuration files from managed devices and stores them for backup purposes. These stored configuration files can then be used to rollback a device to an earlier configuration if configured incorrectly, and to track changes of a device's configuration.

The NMS also performs regular backups of its own file system, stored data, and configuration files, to make disaster recovery easier.

Device discovery The NMS has the ability to automatically detect devices in the network, for easy first-time setup of the system and to simplify the process of adding new devices to the network.

Reports The NMS collects network information and data from various events, such as network inventory, topology, alarms, performance, etc., and presents it to the administrator(s) either graphically or in text. This gives a real-time and historical overview of events occurring in the network, and the ability to analyse the network statistically.

Security SNMPv3 can be used for secure and encrypted communication between the NMS and its managed devices. HTTPS is used for the web-based GUI, providing a secure connection between the browser and the NMS server.

Trouble-shooting The NMS provides fault isolation and root cause analysis, which helps locate the root cause of faults, facilitating troubleshooting. It can also analyse faults to classify them for different levels of criticality, suppressing less important or symptomatic faults while prioritising critical faults to the administrator(s).

User control NMS users can be given permissions and access rights to network resources, or be assigned to groups with such properties. Users can have NMS-local accounts or be authenticated via a third-party authentication system.

5.1.1.1 CA Spectrum

At first glance, CA Spectrum [37] seems to be a suitable NMS for Netcorp. In general it provides all the basic functionalities required. Extra functionalities are described below:

Alarms CA Spectrum detects event correlations in alarms. It can correlate multiple events and suppress symptomatic alarms in order to focus on the important alarms.

Device support Spectrum has a self-certification toolkit [38] that enables support for new devices. This speeds up the process of installing new devices in the network that may not yet be officially supported by Spectrum, as the administrators themselves can certify the device. For communication between Spectrum and network devices, SNMP and other protocols are used. Support for SNMPv1, SNMPv2c, and SNMPv3 exists, so it is, in practice, possible to monitor almost every possible device.

Extensions Spectrum can be combined with other CA products to further expand its functionalities, such as with eHealth [39] or even with UIM (as described in Section 5.1.1.2 on the next page). When combined with eHealth, new capabilities emerge, such as presentation of stored historical data and automated reporting capabilities to automate the tasks of calculating long-term trends, providing a baseline for network resources, and providing performance reports for network devices. This is something that might be of interest to Netcorp, as their current system, LMS, provides similar features.

GUI There is a GUI available both through a web browser via HTTP and through a native mobile application for iPhone[40] and Android[41]. The mobile applications allows for easy access and receipt of critical alarms, even when on the move. The GUI on the web application is customisable on a per-user basis, it can provide different views for each user accessing the system and it supports an appropriate way of simplifying user rights for both users and administrator(s).

Troubleshooting Spectrum provides a feature unique among NMSs. It can compare settings on network devices to those set by a network administrator, and generate a notification when different settings than the recommended settings are used. By using smart algorithms, it can then take these non-standard configurations into account when it detects a problem in how the network is running, thus helping the administrator(s) during troubleshooting and facilitating the location of the root of the fault [42].

Price The price for monitoring 2,500 devices with CA Spectrum is around 240,000 Euro (EUR). The final price can vary, though - *J. Morling, Digital Sales Development Representative, CA Technologies, May 30, 2016.*

CA Spectrum is a good NMS which provides the required functionalities. With that said, it is not an excellent NMS, and there are better alternatives available. Spectrum seems that it could be "good enough", but since other, better solutions are available, Spectrum will not continue into the last step of testing.

5.1.1.2 CA Unified Infrastructure Management (UIM)

CA Unified Infrastructure Management (UIM) [18] (f.k.a. Nimsoft Monitor) is a system designed to bring everything into a single, unified architecture, and it supports both traditional and cloud environments. This NMS supports:

Alarms When an alarm from a device appears, it is possible for a user to take ownership of the alarm, to clarify for other users that this alarm is being taken care of by someone, thus preventing several administrator(s) from attempting to solve the same problem unknowingly.

Device support Much like CA Spectrum, CA UIM also provides a self-certification toolkit to enable support for new devices which are not yet officially supported. Also, much like Spectrum, UIM supports SNMPv1, SNMPv2c, and SNMPv3, so it is, in practice, possible to monitor almost every possible device.

Extensions CA has a "Marketplace" where various "probes" can be downloaded to extend the functionalities of their products. For example, the Configuration archive probe is available for UIM. With this Configuration archive probe, it is possible to archive configuration files of every node in the UIM environment. The interval at when this archiving occurs is customisable, and it automatically computes configuration differentials between the current and previous configurations files, to allow administrator(s) to track configuration changes.

GUI The GUI is simple to understand with straightforward menus, overviews, system report graphs, and detailed views. Compared to Cisco LMS, UIM has a considerably better GUI. UIM provides a simple, customisable dashboard consisting of "high-level badges", each of which represents the status of a managed application, a business-service, a location, or simply a group of devices. In addition, UIM also has a number of "unified dashboards", which provide important overview information of various types of technology. The unified dashboards include views of technologies from Cisco, Citrix, EMC^2, Microsoft, and more. These dashboards also provides views of datacenters, flow analysis, power units, servers, storage, VMs, etc.

Price The price for CA UIM starts at 25,000 EUR. This price, however, is most likely flexible and is not the final price - *J. Morling, Digital Sales Development Representative, CA Technologies, May 13, 2016.*

Overall, CA UIM seems like a fairly regular NMS. The only protruding feature is that users can take ownership of alarms - a very good feature that might be of use for Netcorp. However, this feature alone does not make the NMS interesting enough to test further in the last step.

5.1.1.3 Cisco Prime Infrastructure

Cisco Prime Infrastructure [43] is the successor to Cisco Prime LMS - Netcorp's current NMS. It provides many similar functionalities, but with upgraded capacity, with for example support for up to 18,000 devices, and plans to support over 100,000 devices [44].

However, Cisco Prime Infrastructure can immediately be rejected as an unsuitable solution for Netcorp. Although it was considered in the first step, as it does have support for other devices than Cisco's own devices. However, it still has very limited device support. For example, Rockwell Stratix Switches and Aruba controllers are supported, but these devices are not of interest for Netcorp. Furthermore, we seek a universal solution, which can support any device that is likely to be used by Netcorp in the near future. Unfortunately, Cisco Prime Infrastructure is unsuitable, because of its very limited device support.

5.1.1.4 HP Intelligent Management Center (IMC)

HP Intelligent Management Center (IMC) [45] is one of several NMSs from HP/HP Enterprise (HPE). IMC focuses on a highly flexible and scalable system, with powerful administration control, and detailed performance monitoring. It supports:

Alarms IMC notifies the network administrator(s) of important events by sending an alarm with both a visual and audible notification via the web interface. Alarms can also be sent via email and text message to ensure an important event is never missed, and that the attention needed is attracted.

Device support IMC provides comprehensive management of all network devices, including those from HP, Cisco, and other vendors. Additionally, IMC communicates via SNMPv1, SNMPv2c, and SNMPv3, which enables it to support basically any device with an IP address.

GUI IMC's GUI runs on HTML version 5 (HTML5), supports a wide variety of devices, including mobile devices such as smartphones and tablets. The interface is scalable to focus on the most relevant information regardless of the device's screen size.

Licences IMC comes in three different licences: Basic, Standard, and Enterprise. The main difference is the number of supported devices, where the basic license supports 50 devices. Both standard and enterprise licenses support 15,000 devices. Additionally, the basic and standard license support a single server network, while the enterprise license is scalable to support additional servers.

Extensions IMC provides customised functions and third-party device support allowing users to either extend an existing function to support third-party devices or to customise a function by compiling interactive scripts, Extensible Markup Language (XML)-files, and UI configuration files.

Telnet/SSH Via a Telnet/SSH proxy administrator(s) can remotely access and manage devices directly via their web browser. This promotes secure and controlled access via both SSH-1 and SSH-2 to devices, while providing auditing of changes on any device.

Virtualisation HP IMC is, according to HP themselves, *"one of the first management tools to integrate management and monitoring of both virtual and physical networks"* [46]. This allows for insight and management of virtual networks, and reduces migration complexity by aligning and automating network policies with virtual images.

Price The price for implementing IMC in a network with 2,500 devices is around 1,000,000 Swedish krona (SEK), but this can change depending on other factors - *M. Dikvall, Sales Specialist, Aruba, a HPE company, May 30, 2016*.

Overall, HP IMC seems like a fairly standard NMS with all the expected functionalities. It does not lack any features, but at the same time there does not seem to be anything special that makes it superior to other NMSs. However, while reading and listening to other's experience of IMC, the reviews are very good. It seems to be a very stable NMS without any problems or bugs whatsoever, and with excellent device support. This certainly sounds promising, hence IMC will be tested further in the last step.

5.1.1.5 HPE Network Node Manager i (NNMi)

HPE Network Node Manager i (NNMi) [47] is a NMS designed to bring everything into one single solution and to facilitate work with intelligent automation. It is a very scalable system, supporting very large environments with up to 25,000 nodes and 500,000 performance-polled interfaces on a single server [48]. It features:

Device support NNMi supports basically every network device from any vendor, both physical and virtual.

GUI The GUI can be a bit cluttered, which definitively can be seen as a downside. Although, because NNMi provides such a broad range of functionalities, this clutter is to be expected.

Licenses/ Extensions NNMi comes in a Premium and Ultimate edition, where each edition comes with a set of plug-ins to provide additional functionality. Examples of plug-ins for the Ultimate version are *"NNMi Smart Plug-in for MPLS"* and *"NNMi Smart Plug-in for IP Multicast"*, where the first plug-in is especially interesting for Netcorp, as their Customer Network is completely based on MPLS.

Trouble-shooting NNMi supports a definitive root cause analysis, meaning that it confirms each fault by two methods, not just one, to eliminate any false positives. Troubleshooting automates on-demand diagnostics, thus pushing one button runs a series of diagnostic actions to help determine the problem. According to HPE, this enables Level 1 operators to have suitable tools to solve many incidents that were previously passed on to Level 2 support administrator(s), increasing the efficiency of troubleshooting.

Virtualisation A lot of focus in NNMi is on managing a virtual infrastructure. For example, all machines running on VMware's Elastic Sky X Integrated (ESXi) hypervisor are fully monitorable and manageable in the same ways as physical devices. Virtualised environments are much more dynamic than traditional ones, as connections can go up and down quickly; therefore, they need to be managed closely. When VMs are done executing, they are gracefully removed. Further, as described earlier, VMs can move from host to host, which requires dynamic device discovery. NNMi has a unique way of representing virtual environments, with views called the *hypervisor wheel* and *loom*.

Price The price for implementing NNMi was unfortunately not acquired.

To conclude, HP NNMi focuses on managing both VMs and physical network devices, where both is something that Netcorp is using. Thus, this is an interesting solution, and it will be tested further in the last step.

5.1.1.6 HPE Network Automation

HPE Network Automation [47] is a smaller tool from HPE, primarily designed to be combined with another NMS from HP/HPE, such as NNMi. When combined with NNMi, the result is an integrated solution that unifies network fault, availability, and performance activities with change, configuration, compliance, and automated diagnostics. This NMS features:

Alarms HPE Network Automation does *not* provide any alarms, thus the general description for alarms does not apply to this NMS.

Automation As is clear from its name, HPE Network Automation's main task is to automate procedures. It helps track configuration changes on devices, both for finding the root of a problem and to rollback to earlier versions of a configuration. It also helps automate peer reviews and approval processes of configuration changes to speed up the process from changing a configuration to implementing the change. Network Automation makes disaster recovery easier; for example, replacing faulty devices is as easy as installing the new device and deploying the original configurations.

Device support HPE Network Automation has extensive support for devices from over 130 manufacturers, including virtual devices [49]. A function called Network Driver Studio is available to allow administrator(s) to self-develop device drivers if a device is not officially supported. HPE Network Automation operates over SNMPv3 when possible, for maximum security and wide device support.

GUI HPE Network Automation is, as said, designed to be used together with another NMS. It is not, however, a plug-in, and thus has its own independent GUI. The dashboard shows the tasks that Network Automation is capable of performing, as well as all the recent changes that have occurred to managed devices.

Licenses HPE Network Automation comes in two different editions: Premium and Ultimate. Both editions includes the functions *Network Automation Server*, *Network Automation Satellites* (smaller servers for managing devices at remote locations), and *distributed architecture options*. The Ultimate edition also includes *policy compliant features*.

Troubleshooting HPE Network Automation does *not* provide any troubleshooting, thus the general description for troubleshooting does not apply to this NMS.

Price The price for implementing Network Automation was unfortunately not acquired.

HPE Network Automation is not designed to be used alone, and will therefore not be tested further in step three. However, if used together with HPE NNMi, HP IMC, or another NMS from HP/HPE, HPE Network Automation is a great tool if the functionalities provided by it are needed by the network managers. Hence, if Netcorp selects one of these NMSs, HPE Network Automation is very much recommended if its functionalities are needed.

5.1.1.7 IBM Tivoli Netcool/OMNIbus

IBM provide many solutions for managing networks and many are part of the Netcool Operations Insight (NOI) [50] package. NOI consists of numerous components (e.g. Tivoli Netcool/OMNIbus [19]), each of which has many special advantages in terms of monitoring, discovering, centralisation, normalisation, enrichment/processing, integration, automation, visualisation, and reporting. This NMS features:

Alarms The alarms can be sent via text message or email, to notify the network administrator(s) about the current problem. The administrator, if not at work, can easily open an application on either a smartphone or a tablet to work out the issue or forward it to another administrator. It is also possible to forward alarms to other systems (e.g. Network Operations Centres (NOCs)). Further, the solution alone can act as the central platform for the underlying systems.

Device support In addition to supporting IBM's own hardware, NOI supports an extensive number of other vendors, such as HP, Juniper, Cisco, and many more. The support for different devices expands regularly together with the development of new technologies. However, switches that are not supported today will be in future. Also, in this solution there is a possibility to implement own support for devices.

Extensions The platform is designed for scalability with open Application Programming Interfaces (APIs) enabling third party integrations, such as NOC system integration, Supervisory Control And Data Acquisition (SCADA) system integrations, and offers various possibilities to automate processes. In partnership with system integrator Compose IT [51], IBM offers a customised solution with good example frameworks.

GUI NOI's GUI can look a bit cluttered at first glance, but it is quite simple to navigate through and includes many features that help to guide the administrator(s). For example, facilitating troubleshooting to find the root cause of the problem as fast as possible.

Data in the dashboard can be displayed in real time or from a historical perspective, or a mixture of both depending on needs. The presentation can be both at a detailed and on an abstract level.

Licenses NOI is licensed per monitored object. An object is, for example, an interface, Central Processing Unit (CPU), storage drive, etc.

Reports Reports can be developed and presented according to the administrator's own taste and what is needed. There is no limit on how long data can be stored. The only limit for storage is how much disk space is available for the historical database. For inventorying, everything is stored in accessible databases, which includes everything from operating system version to full configuration and how the devices are connected.

Security The solution can be connected to a custom repository or an existing repository (e.g. Lightweight Directory Access Protocol (LDAP), Active Directory, etc.).

Price The price varies from object to object, so a concrete price is hard to set until Netcorp's whole network is analysed in detail. However, as an approximation the solution would cost 30 SEK per month and switch (resulting in 900,000 SEK per year for 2,500 devices) - *J. Sigemo, CEO, Compose IT, May 25, 2016.*

To conclude, IBM's NOI is a powerful NMS that can replace Netcorp's whole networking system, as well as separate the network into different sections, such as NOC. This entails that there are many features in NOI, maybe too many for Netcorp. However, with collaboration with Compose IT, who are resellers and specialist in both NOI and SevOne, the solution can be adapted to Netcorp's requirements for a reasonable price. In addition, NOI is used by Försvarsmakten (The Swedish Armed Forces) which entails that the security aspect is trustworthy [52, Page 10]. Thus, this solution proceeds to step three in the three-step approach.

5.1.1.8 ManageEngine OpManager

ManageEngine OpManager [53] is a modular NMS, giving flexibility to enterprises to choose which functions to keep and which to discard in order to get better price performance. For example, the module Network Configuration Manager (NCM) [54] can be used to discover devices and manage their configurations. Telnet or SSH can be used to save these configurations as templates and execute them to the devices in bulk. Also commands can be sent to network devices in order to configure or group them as desired. This NMS features:

Alarms SNMP traps or system logs can be forwarded to other NMS solutions.

Backup OpManager can notify and automatically roll back to a previous configuration if an unauthorised configuration has occurred.

Device support OpManager supports out-of-the-box over 100 vendors. To list a few: 3Com, Cisco, Dell, HP, D-Link, Extreme, Fortigate, Foundry, Juniper, Netgear, Netscreen, Nortel, Linux, Solaris, HP-Unix (UX), IBM-Advanced Interactive eXecutive (AIX), Microsoft Windows, and Libert. However, if there is a certain device that is not supported by OpManager; as long as one can supply a MIB file for that specific device, Netcorp can create a template for that device, or by professional help from the Swedish reseller of OpManager, Inuit.

GUI OpManager's GUI follows a modern design of HTML making it rather clean and simple to follow. The various tabs are easily understandable. Additionally, administrator(s) can create a custom dashboard to access relevant information about the network without having to navigate via other tabs.

Licenses The licences are split into two categories, one being a rental license for a 12 month period and the other being a purchased license (one time fee) with maintenance and support for a 12 month period.

Security For security purposes, as default, no one can make any changes other than administrator(s) for OpManager's NCM itself, but this NMS can be configured such that other users can also make changes. The authentication in OpManager can be NMS-local or done by using a Remote Authentication Dial-In User Services (RADIUS) server.

Price Assuming the complete package is purchased, the price for implementing OpManager to manage a network of 2,500 devices is 820,750 SEK per year if a renting license is used, and 678,245 SEK the first year if a purchase license with 12 months maintenance and support is used (thereafter 113,040 SEK per year) - *J. Lidman, Account Manager, Inuit AB, May 17, 2016.* More detailed price information can be seen in Appendix B.1 on page 77.

Some of the advantages of this NMS is its broad scope of monitoring options, from network/server monitoring to network configuration management, Netflow traffic flow analysis, firewall analysis, IP address and switch port mapper management, and deep application inspection and monitoring. Moreover, customers do not need to pay for features they do not require, but can start using the solution to handle their current needs and at any time they can change their license (given that they have purchased the additional features) and these features become visible to users without any additional installation. Because of this, we have decided to let OpManager move onto step three in the three-step approach.

5.1.1.9 op5 Monitor Enterprise+

The NMS called op5 provides an enhanced network monitoring tool called op5 Monitor Enterprise$^+$ [55]. This tool gives the administrator(s) the ability to gain control over network performance and health using one tool with visualised dependencies, automatic alarms, alarm escalation, notifications and reports. This NMS supports:

Alarms The alarms can be sent via text message or email. Also, notifications can be custom configured to send information, for an example, via JavaScript Object Notation (JSON). The op5 monitor can implement scripts that are executable on Linux systems. The most used queries send out queries to different nodes in the network via SNMP (all versions are supported), JSON, TCP, Ping, and more.

If there is a larger network disruption, the op5 Monitor will not send alerts concerning all of the underlying devices, but instead, will say that there is a network outage and it will tell how many devices is affected by this outage.

Backup The built-in backup solution will only keep information that is entered into the system manually (i.e., which is stored in configuration files and a database).

Device support With extensive device support for various vendors, op5 Monitor Enterprise^{+} handles all Information Technology (IT) infrastructure, from network hardware, software and services, all the way to virtual or cloud based services.

GUI At first glance the GUI is cluttered with various information, requiring some deeper inspection to understand some of the information. However, the GUI is still straight forward and with time administrator(s) should be able to easily navigate without any inconvenience.

The dashboard can be manually configured to show data that is relevant for the administrator(s). The dashboard can contain the following features:

- different visualisations (via NagVis [56]),
- host/service listings with filter capabilities to show problems on a type of hosts or service basis,
- geographical map of the network,
- overall network health and monitoring overview,

- status of other op5 Monitor nodes, and
- business services - a feature where administrator(s) can, instead of focusing on the status of server monitoring, printer monitoring, network monitoring, or other technical components they can focus on the health and performance of critical business processes such as email, a web shop, production, and payroll, and how these processes are connected to the underlying Information and Communication Technology (ICT) infrastructure.

Licenses op5 Monitor is licensed per monitored IP address.

Security op5 Monitor Enterprise^{+} is, for security reasons, penetration-tested several times per year to ensure that it is not possible to gain access to sensitive information from the outside. Also, all web traffic is encrypted. Configurations of peers and pollers are sent via SSH. Besides NMS-local authentication, it is also possible to use LDAP and/or Active Directory for authentication.

Price The price for implementing op5 Monitor was unfortunately not acquired.

In overall op5 Monitor is flexible, as it allows users to do custom modifications, write custom script/checks, etc. It has an open Application Programming Interface (API) that allows making configuration changes, send in passive results, fetch information to use on other systems, get reports, and historical data. Additionally, op5 Monitor has email and phone support with deep technical competence about both the product and IT operations located in Sweden.

Although other op5 products are already being used in other systems at Netcorp, this did not affect analysis in favour of op5 Monitor. Only due to more complex GUI, compared to other solutions, op5 Monitor will not go forward to the third step in the three-step approach. However, it is still a very reasonable solution that Netcorp can keep in mind.

5.1.1.10 Opmantek Network Management Information System (NMIS)

Opmantek's Network Management Information System (NMIS) [57] is an open source NMS. With a focus on real-time aspects, NMIS provides live alerting and performance monitoring, and live summary of the entire managed environment as a single metric, which indicates reachability, availability, health, and response time of all devices being managed. NMIS provides detailed inventory management that lists all managed devices by location, type, and software revisions. The information about devices can be collected into a summary which contains health graphs. This NMS features:

Device support NMIS provides an extensive device support for many different (if not all) devices. Opmantek proudly says that *"If it has an IP address, NMIS can manage it and it will leverage the key IP of NMIS. If it doesn't have an IP address NMIS can probably manage it too!"* [58].

GUI NMIS's GUI has a simple design without any unnecessary animations or redundant features. The design provides easy to understand tabs, which makes navigation though the system simple and fast.

NMIS provides a dashboard for a quick overview of the most important parts of the system (e.g. monitored services overview, customer status and health, network metrics and health, and logging of events) without the need to search through different tabs to find them.

Troubleshooting A search function is included to quickly find interface information by node name, interface name, description, type, IP address, and for matching interfaces.

Price While NMIS itself is free of charge, Opmantek does charge for the support and modules that can extend the functionalities of NMIS. The starting price for support is at approximately United States (US) $13,000 per year for 5,000 devices. However, the price can be reduced if Netcorp were to buy a subscription for a couple of years, rather than a single year - *N. Day, Senior Engineer, Opmantek Europe, April 28, 2016.*

Opmantek does not have a first-line support for NMIS located in Sweden, but they do have partners in Sweden that can assist if necessary for an extra fee. Although they do point out that there is no need for local support, as they can provide the required support remotely and that this is more cost effective. Without the first-line support, Netcorp would have to go through the trouble of installing the whole system on their own, which will cost resources (i.e. time, manpower, etc.). However, compared to the total cost of other NMSs, NMIS is still the cheapest one and deserves to move on to the practical analysis.

5.1.1.11 SevOne

SevOne [59] collects and analyses data from all of the network nodes, and monitors the uptime of the network. SevOne sells their solution as a physical or virtual appliance, meaning it is possible to buy either the hardware with pre-installed software, or simply buy the software and run it on your own hardware. If implemented on your own hardware, it requires a server with a virtual environment based on VMware. However, when buying only the software, everything is pre-installed and pre-configured into a virtual image, so there is no need to set up the operating system, database, or web server.

SevOne nodes, often referred to as appliances or peers in a SevOne cluster, can monitor up to 200,000 objects from a single physical appliance, or 100,000 objects from a single virtual appliance [60]. This NMS features:

Alarms SevOne automatically detects, alerts, and notifies the administrator(s) of service degradations in close to real time. In SevOne both static and/or dynamic thresholds can be used on all metrics including combined metrics as Key Performance Indicators (KPIs). Dynamic thresholds automatically detect deviations from normal by comparing against baseline values of the various metrics.
SevOne can be used for both polling and receiving performance metrics. The most common polling methods are SNMP and Internet Control Message Protocol (ICMP), but it supports 20 different collection methods by default and additional customised methods are supported by using the API.

Backup In cases of misconfiguration, as a backup feature, rollbacks can be sent out as a mass configuration to SevOne nodes. If there are multiple SevOne peers on the network, this will be done automatically since all SevOne peers talk to each other and replicate configuration data.

Device discovery Devices, objects (e.g. an interface, CPU, storage drive, etc.), as well as Layer 2 and Layer 3 relations will be automatically discovered. Other ways of adding devices and objects to be monitored are entering a Comma-Separated Values (CSV) file and via API integrations with Configuration Management Databases (CMDBs), inventory systems or similar.

Device support SevOne handles an extensive number of device types from various vendors. By looking at the objects in the network instead of nodes, SevOne does not seem to be constrained by device types. Also, if there is any device type that is not supported, up on contacting SevOne, SevOne will add support for it within ten days.

GUI SevOne's GUI is simple and easy to navigate. The design seems professional, with good presentation of all available features.
The typical dashboard is for operations with current and historical status per customer and/or per service. The dashboard consists of: capacity planning to find areas which need to be upgraded, reports, graphs, alert views, status maps, etc.

Licenses SevOne is licensed per monitored object. An object is, for example, an interface, CPU, storage drive, etc.

Reports By default SevOne stores all polled data for up to one year, with the default polling with five minute granularity. This granularity can be increased or decreased depending upon the desired level of detail.
At a minimum, SevOne stores a device's name and its IP address. It can also store topology relationships and any additional kinds of information by using meta data fields, typically these are used for customer information, location, service parameters, etc.

User control For security purposes all user actions are logged. Users can have NMS-local accounts or be authenticated using a third party authentication service, such as LDAP, RADIUS or Terminal Access Controller Access-Control System (TACACS).

Price The default price is US $5 per monitored object, but it can be negotiable depending on how many objects are to be monitored - *U. Blomström, Business Development Representative, SevOne, May 16, 2016.*

As mentioned in Section 5.1.1.7 on page 43, Compose IT are Swedish resellers of SevOne. SevOne is more of a performance manager than a fault manager, as compared with other solutions. Although it fulfils all of Netcorp's needs, it is still focused on performance and data collection. Data with fine granularity gives network administrator(s) better statistics and overview over the whole network, enabling them to try to prevent future network outages. However, what Netcorp needs is a NMS that has management as the main feature and Netcorp are not interested in spending resources on analysing and comparing that fine granular data. Thus, this solution, even though it is a very suitable solution, will not go forward to the step three in the three-step approach.

5.1.2 Results From Practical Analysis

This section describes the results from the third step of the three-step approach, practical in-depth analysis, as per the requirements set in Section 3.6.3 on page 32.

There are three notes the reader should be aware of in this section: Firstly, we were unable to test all the NMSs due to various reasons, which is described in each NMS's respective section below. Secondly, as described further in Section 6.2.1.1 on page 62, we were unable to test the stability of any NMS when exposed to the heavy load of 2,500 devices. So, unfortunately, we cannot state the stability of any NMS in this scenario. Lastly, we were unable to test the Accedian MetroNID in the lab environment, as is described further in Section 5.4.2 on page 57.

5.1.2.1 HPE Intelligent Management Center

HPE IMC is one of the NMSs we unfortunately could not test since we were unable to acquire a trial-version of the NMS.

5.1.2.2 HP Network Node Manager i

This NMS gained the following results in the practical analysis:

Stability NNMi's GUI was rather slow when navigating. Not so much that it is unusable, but still enough to frustrate the user. This is probably something that can be fixed with better hardware, though. Other than this, we discovered no stability issues.

User-friendliness NNMi's GUI and the structure of the menus was rather easy to understand. It took a while to understand where some settings were located, but after a while you get a hang of it. NNMi does *not*, however, follow the rule that every function should be reached in three mouse clicks or less - far from it actually. Some functions were as deep as eight navigation steps deep, which can be rather frustrating for the user, especially in combination with the long loading sequences.

Device support NNMi supported all of the devices we tested (as listed in Section 3.4.2 on page 27) excellently, except from the Accedian MetroNID, which we were unable to test.

Overall, HP NNMi felt like a slightly outdated NMS. The interface was both slow and had a bad structure for fast navigation. Again, the long loading sequences can probably be fixed with better hardware, but the GUI itself can not. The experience of NNMi was not the best, thus, we cannot recommend it to Netcorp.

5.1.2.3 IBM Tivoli Netcool/OMNIbus

Just like HPE IMC, we were unable to test IBM Tivoli Netcool/OMNIbus since we could not acquire a trial-version of the NMS. This NMS is quite extensive and has many features that needs to be installed, thus even though if the trial-version was acquired, it would be difficult to implement in the lab environment so that it would work in the most optimal way. Nonetheless, we see this solution as the most suitable NMS for Netcorp since it is perfect on paper and has a great response from both companies and other individuals world wide (received from interviewing employees at companies running these solutions and private individuals as mentioned in Appendix C on page 83). Thus, this solution is presented as one of the two final solutions.

5.1.2.4 ManageEngine OpManager

OpManager delivered the following results during the practical analysis:

Stability OpManager performed very well in stability. The GUI was very responsive when navigating through menus and functions. We did not discover any stability issues during our testing.

User-friendliness OpManager was in our personal opinion the best performer in user-friendliness. It has a very simple and clean GUI, with easy-to-navigate and logically structured menus. It did not always follow the rule of navigating to every function in at most three mouse clicks, but in most cases it did, and even when it did not, it was far better than for example NNMi. The deepest function we had to navigate to in our testing was four mouse clicks.

Device support OpManager did not officially support all devices we tested, but since you can add support for devices yourself, we were able to successfully support all the devices after creating own profiles with data from MIB's. This excludes the MetroNID, of course.

This NMS was the overall best (together with Netcool/OMNIbus) in stability, user-friendliness and device support. Thus, this NMS is also recommended to Netcorp.

5.1.2.5 Opmantek Network Management Information System

The following results from the practical analysis were acquired:

Stability No stability issues were discovered.

User-friendliness NMIS's GUI has, as mentioned in Section 5.1.1.10 on page 48, a simple design. With accordingly named tabs the navigation though the NMS is easy. However, in some cases some information was hard to reach in the NMIS and it took more than the recommended rule of three mouse clicks. Also, the installation process was far from user-friendly. The installation guide did not provide near enough information, and in some cases it even provided incorrect information.

Device support As mentioned in Section 5.1.1.10 on page 48, Opmantek were true to their words in saying that their solution can handle everything that has an IP address. It was successful in communicating with and auto-discovering all of the devices we tested in the lab network, except from the MetroNID, of course, since we were unable to test it.

Considering NMIS has no first-line support in Sweden that can help with installation and configuration, Netcorp will depend heavily on user-friendliness at the installation process, which is lacking a bit and may lead to some frustration. Although, this might be a minor setback for this solution, compared to other solutions it is enough for not being recommended. Thus, NMIS is not recommended to Netcorp.

5.2 Major Results: The Final NMSs

This section describes the final NMSs, seen as appropriate replacements for Netcorp. We have concluded that there are two equally suitable solutions that can replace Netcorp's current NMS: IBM Tivoli Netcool/OMNIbus or ManageEngine OpManager. They have both been selected since they are very similar solutions both in terms of performance and features. Hereafter is a description of what they have in common, and those aspects which uniquely separates them from each other.

Both IBM Tivoli Netcool/OMNIbus and ManageEngine OpManager are very universal solutions, meaning they have a very wide device support for many devices from many different vendors, and even if they do not officially support a device, it is usually very easy to add custom support for a device by using data from that device's MIB. Adding custom device support can either be done yourself or by a professional. In this specific case the Swedish resellers Inuit can help Netcorp adding custom support to OpManager for no extra charge if the product is bought through them, and on the same conditions the Swedish reseller

Compose IT can help adding custom support for Netcool/OMNIbus.

Both solutions are very stable, both according to our own tests and according to professional reviews by companies and private individuals. Stability for Netcool/OMNIbus was of course not tested by us due to the lack of a trial-version, but as is also described in Section 5.3 on the next page, stability is an aspect our testing does not reliably represent, so this should not affect the outcome. According to Compose IT, Netcool/OMNIbus has never had any stability issues, even when under the heavy load of hundreds of thousands managed devices. No such bold statement has been mentioned about OpManager, but it has still gotten excellent reviews from professionals in terms of stability. It seems as if both solutions are well-developed, and in those rare cases a problem appears, an update is quickly released to correct it.

With a clean and easy-to-navigate GUI, both solutions are user-friendly. The properly named tabs and menus, enables the administrator(s) to easily find the sought information or root-cause of alarms. There are also features that help with troubleshooting, in case administrator(s) need help finding the cause of a problem, or simply want to automate procedures. Both solutions give the ability for administrator(s) to customise the dashboard, so that all relevant information is shown at the prompt.

The local resellers in Sweden helps with installing/configuring the NMSs and educates the employees about the system. In cases when administrator(s) need help with the NMS, there is a round-the-clock, any day of the week support available. The support helps out with troubleshooting, makings scripts for functions that may be relevant for the company, and creates custom support for devices that require it.

The last and most important aspect these solutions have in common is that they both fulfil all the requirements set throughout the analysis. Besides that, both solutions fulfilled all of the aspects in the FCAPS framework. For *fault* management, they both are able to recognise, isolate, correct and log all faults in the network. Both of the solutions can poll configurations from the network devices and store them for backup purposes, track changes and other functions in *configuration* management. Both of the solutions have support for multiple users and they both manage information about the users, which fulfils the *accounting* requirement of the FCAPS. The *performance* management ensures that network's performance levels remain within acceptable values for both solutions. *Security* is ensured by both solutions as they provide the ability use secure communication protocols, such as SNMPv3, and third-party authentication applications, such as LDAP and RADIUS, and are able to back up configuration files, etc.

The unique feature of Netcool/OMNIbus is “Run Diagnostics”, which runs a self-heal run book that fixes some of the basic faults in the network (i.e. Device unreachable with Ping, routing misconfiguration, etc.). This self-heal process is based on trivial knowledge and historical data. Normally an engineer would need to run these manual steps in order to resolve the issue, but NOI enables the engineers to be more efficient rather than spending time on manual steps.

One of the main differences between Netcool/OMNIbus and OpManager is that Netcool/OMNIbus cost more. However, it brings more features and possibilities to the table if Netcorp wishes to expand in the future. OpManager, on the other hand, is cheaper and is more specialised in a smaller area, which fits Netcorp today.

5.3 Reliability and Validity Analysis

There was a certain aspect in this thesis project that was not performed in a fully reliable way. This aspect was the stability testing during the third step. The original thought was to (over)load the NMSs with virtual network devices in some kind of emulation software, and see how the NMSs performs in such situation. However, due to our limited time frame and resources, we had to abandon this idea early on in the project.

The stability testing instead ended up consisting of documenting any bugs or stability issues (such as system hangups or crashes) that occurred during the short time period when we tested other aspects such as device support and user-friendliness, which was, not unexpectedly, none. Hence, the stability testing did not provide much information at all - and not necessarily because the solutions were fully stable, rather because the testing was poorly executed. Thus, the results from the stability testing are valid, but not necessarily reliable.

5.4 Discussion

This section discusses some of the aspects throughout the thesis work, such as why it was so hard to make the right decisions when choosing a NMS. It also describes the limitations which restricted our work. Lastly, it brings up the NMSs that did not make it past the first step, but are still worth mentioning.

5.4.1 Choosing the Right NMS

The hardest part with this thesis work was definitely picking out the NMSs - both choosing which NMSs to proceed with to the next step throughout the analysis, but also (mostly) choosing which NMS(s) to finally select as the recommended solution for Netcorp. In many cases, especially during the last step of the three-step approach, many solutions provided almost the exact same results, which made the selection of which NMSs to proceed with close to random since the difference was so subtle. It would have been much easier if there was a way to measure for example user-friendliness and security, but there is not. One could measure aspects such as the maximum number of supported devices, but then again, some of the solutions provide custom device support which works just as well, which would mean those solutions get a infinitely high score on that aspect. It is in other words probably impossible to directly compare these alternatives.

The message to take from this section of discussion is - and this is probably the most important sentence in this report - **essentially all of the solutions listed in Section 5.1.2 on page 51 are excellent NMSs, and would be recommended both to Netcorp and any other person or company with similar requirements**. Picking out specifically Netcool/OMNIbus and OpManager as the two recommended solutions was a very hard decision. While most of the NMSs are quite similar in many ways, these two solutions have their own (minor) unique features that makes them stand out above the rest.

5.4.2 Limitations

There were some factors that limited both our efforts throughout the project and the final results. Our work was, for example, limited throughout the first and second step (according to the three-step approach) due to lack of data about certain NMSs. Not only was it hard to gain access to data about some NMSs, but it was sometimes even completely unavailable. Of course, in these cases we tried to contact the customer support or technical support for said NMS, which in some cases led to a satisfying response, and in some cases it led to a unsatisfying response or no response at all. In the two latter cases, the sales department for said NMS was contacted, but it was actually very common to get a unprofessional response denying us an answer since we are just students performing our thesis work, and instead they seek to contact Netcorp directly and sell their product to them, which, of course, did not end well.

The consequences of this lack of data could in the worst case result in the NMS being disapproved since we were unable to analyse it. In most cases, though, it resulted in a incomplete description of the NMS. This made it somewhat hard to compare all NMSs, since the NMSs had different data available.

A factor that limited our efforts in the third step of the three-step approach was the inability to gain access to trial-versions of NMSs. The practical testing does, of course, require us to have a copy of the software. This was not possible with for example IBM Tivoli Netcool/OMNIbus or HPE IMC. In the case of IBM we were able to meet up with Compose IT to have a discussion and they were to demonstrate the software for us. This demonstration, however, never happened. Nor did we get access to any trial version of Netcool/OMNIbus. Thus, we were unable to test this NMS further.

Another factor that limited our efforts in the third step was that we did not have access to Netcorp's real network for testing the NMSs. Thus, testing was limited to only a few representative devices in contrast to all possible devices that are currently in use on Netcorp's network. This means that our test results may be inaccurate, since our testing model is based on assuming *if the NMS supports device x, it should also support device y which is similar to x.* It also means that we cannot test if the NMS supports the required *number* of devices, since we did not have access to this number of devices in the lab environment.

One last limitation in our work was that we were unable to test support for the Accedian MetroNID during the last step. This, since we ourselves lacked the knowledge to configure the device correctly, and the network specialists at Netcorp could not configure it due to limited time. Hence, we were unable to test the NMSs for support for uncommon devices.

5.4.3 Honourable Mentions

There are several NMSs of great interest, but which for various reasons could not be considered further than the first step in the three-step approach. This section discusses these NMSs, why they where not considered further, and why they are still worth mentioning.

5.4.3.1 GroundWork Monitor

GroundWork Monitor [61] is a open platform NMS built completely on open source software, such as Nagios, Icinga, Cacti, Ganglia, and many more. By combining all these open source tools into one solution, GroundWork Monitor has a very wide area of use and can monitor basically every possible device. According to its developers, *"If [the device] is TCP/IP accessible, it is almost certainly monitorable by GroundWork. In many cases, such as networking gear, mobile devices, and Microsoft, we can even monitor it without TCP/IP"*[62].

GroundWork Monitor was dropped from consideration in the first step, due to its lack of a technical support department. While this seems like the only downside of this NMS, it is unfortunately a deal-breaker for Netcorp, since they depend upon an external technical support department.

5.4.3.2 Kratos NeuralStar

Kratos NeuralStar [63] is a NMS providing real-time intelligence, fault tolerance, centralised monitoring, and cyber-security readiness.

Kratos is definitely one of the companies who takes security seriously, which can easily be seen just by looking at their customer base, consisting of the US Defence Information System Agency, US Army, ViaSat Inc., and more, for whom security is essential.

In this case the deal-breaker was the lack of a first-line technical support department located in Sweden. However, in conversation with Kratos, it was said that they would not mind setting up an office and providing first-line support in Sweden if they saw value in it. For this, though, Netcorp would be required to present interesting enough future plans for expansion, for example becoming an Internet Service Provider (ISP).

5.4.3.3 Other Honourable Mentions

Other NMSs that did not make the cut due to lack of first-line technical support department located in Sweden are: NetBrain [26], Opsview [64], PathSolutions [65], Scrutinizer [66], and SolarWind NPM [25]. Also, RANCID [22] had to be dropped from consideration due to its global lack of support, not just in Sweden. While not making the cut, these honourable mentions are still very plausible solutions for Netcorp, as otherwise they meet all of the necessary requirements.

Chapter 6

Conclusions and Future Work

This chapter explains the conclusions obtained throughout analysis and evaluation described in this thesis and proposes a number of improvements, extensions, or complements that may be of interest in order to continue this work.

6.1 Conclusion

In this section we will state the conclusions and insights gained as result of this thesis project.

6.1.1 Goals

To briefly summarise the goals for this thesis project, as described in Section 1.4 on page 2, the primary goal was to find a solution suitable to replace Netcorp's current NMS. The solution should be future-proof for at least five years and should manage all the aspects of the FCAPS framework.

This goal, as far as we can tell, has been satisfied. Two NMSs has been selected as recommended as equally suitable replacements for the current system, Cisco LMS. They both address all the aspects of the FCAPS framework, and they both *should* be future-proof for at least five years. Of course, we cannot know if they will be suitable for Netcorp in five years, but based upon the information we have gathered about Netcorps requirements, they should both be suitable. Thus, as far as it is possible to tell today, this goal has been met.

The secondary goal was for us to gain experience and knowledge in the area, which we certainly have. We have not only gained knowledge about specific NMSs, we have also learned a lot of general knowledge about network monitoring in general, the protocols used for it, and the technologies behind it. We have also gained experience from experimenting with the solutions in a lab environment. According to the goals, this written thesis should also help Netcorp and others in the same area transition from their current system. This is another goal that we cannot tell as of today whether this goal has been met or not, although we hope it has and will meet this goal.

6.1.2 Insights and Suggestions for Further Work

For further work, a detailed analysis of the two presented solutions is required. This implies that the solutions should be implemented on Netcorp's infrastructure to test stability and ability to manage the current number of devices and the different device types on the network. A detailed cost analysis is required to better distinguish between these two solutions. Also, a deeper security evaluation is required to assure that they actually fulfil Netcorp's security needs.

Another aspect to analyse in further work would be to further analyse the remaining NMSs that we did not recommend, i.e, all the NMSs which were tested in step three. Only two of the five solutions were recommended by us, but as said in Section 5.4.1 on page 56, all the solutions that were tested in the last step are great solutions, hence a further analysis of these solutions would be worthwhile.

6.2 Future Work

This section describes what has been left undone by us, what the next obvious thing to be done is, and any hints we can give to the next person who will perform similar work.

6.2.1 What has Been Left Undone?

This section brings up aspects of our thesis project that we for various reasons were unable to analyse and evaluate. These aspects are still important, and are therefore interesting subjects for future work.

6.2.1.1 Testing Stability

As described in Section 5.4.2 on page 57, a limitation in our work was that we did not have access to Netcorp's real network, thus we could not test the stability of the NMSs in network environments with a large number of devices. It is therefore left for future work to test that each of the NMSs work in networks with 2,500 devices or more. Nor could we test how the NMSs were affected after being up for a long time, say, after several months. The system might become unstable after reaching these up-times, and might require a reboot or even a re-installation, which would require a lot of unnecessary work.

6.2.1.2 Cost Analysis and Comparison

The companies selling NMSs calculate the price using different methods. The most usual ways we encountered was to determine the cost depending on the number of devices to be managed by the NMS, depending on the number of network interfaces to be managed, or the number of hardware devices to be managed (such as storage drives, interfaces, and CPUs). Moreover, many sellers provide special discounts depending on factors such as the size of the company implementing the solution, the number of devices to be monitored by the NMS, and the geographical location of the company implementing the solution.

All these factors require a very time consuming process to perform a cost analysis of a NMS, and even more so, comparing these estimated to each other. Thus, we have not been able to compose a detailed cost analysis or comparison.

6.2.1.3 Evaluation of Security

As security is both difficult and time consuming to test properly, we have not been able to perform any in-depth testing of the security of each of these NMSs. Thus, this is an aspect that has been left undone and requires further testing to assure that the NMSs are using proper security measures.

Examples of security aspects we have not analysed and which require further evaluation are:

- Proper use of encryption, hashing, and salting of sensitive data, such as user passwords and other credential information.
- Assuring that connections are secure by using encryption, key exchange, handshakes, integrity checks, etc.
- Evaluating the security of the authentication process for users logging into the NMS. For example, is it possible to use two-factor authentication when logging on?
- Assuring there are no back doors into the NMS, security breaches, or other ways of exploiting the system.

6.2.1.4 Exploring Combinations of Three or More Tools

There might be scenarios where some networking tool does not provide all the aspects needed in a NMS, but in combination with one or more other tools, it would. As described in Section 3.1.2 on page 24, we only considered combinations of two networking tools, and by doing so did not find any suitable combinations. However, one could explore the possibilities of combining three or more tools into one solution. This is probably possible; although, it might not result in a stable and user-friendly solution, but rather result in what the Reddit user “nof” described Orion as - a “Frankenstein experiment”: *“something which does ’everything’, but all the components feel as if they are kludged together and it ends up doing a mediocre (at best) job of them all”*. Testing these combinations and evaluating the resulting solution would most certainly be an interesting future work.

6.2.2 Hints to the Next Person

For someone who wants to perform a similar analysis and evaluation of NMSs, there are some hints we can provide to facilitate the process:

- Construct a model dividing the analysis into different steps (or follow the model we constructed). This helped us structure our analysis, which made it easier to document each of the alternatives, which in its turn made it easier to evaluate these alternatives and conclude this work.
- If it is of great importance to have a first-line support department located in a specific country or region, make sure to investigate this as soon as possible. This criteria was definitely the one which lead to the most solutions being rejected in our case and will probably do so in yours as well. By eliminating these solutions early on in the process, a lot of otherwise unnecessary work can be avoided.
- When contacting the companies behind the NMS, try to get hold of the technical support department to gather information as they will likely give a more concrete answer. In contrast, the sales department is primarily trying to sell their product to you, thus they may avoid some questions or glorify the product.

6.3 Reflections

This last section in the report is a reflection on our methods, our work, and the result of the project. It also contains reflections about economical and environmental sustainability, as well as ethical considerations.

6.3.1 Method and Planning

The project has been well structured thanks to a well-defined layout early on in the project. This made the project easy to execute and to anticipate the time-span required for each segment. With the three-step approach we could split up the work into phases, and each phase could easily be divided between the two of us, which significantly raised our efficiency. Thus, our reflection on the planning and method of the project is that both were well performed, and there is not much to improve upon. The one thing we can think of that could have been done better is that the requirements set in step one could have been improved. Cisco Prime Infrastructure managed to get by and into step two, which it obviously should not have, hence, a set of better defined requirements was needed in step one. Other than this, we think our method was very well suited for this type of work.

6.3.2 Work Process

During our work in the first step, many of the NMSs were discarded due to us not being able to get suitable information about each of those NMSs. Even though we contacted the support or sales departments of each firm, in many cases we did not receive any replies to our inquiries. This inhibited our work a lot, but at the same time we were powerless and there was nothing *we* could improve. During the second step, we found that many of the NMSs are quite similar to one another, hence it was difficult to make a clear distinction between them and to decide which to evaluate further. Lastly, during the third step, we did not get a lab environment set up in reasonable time due to some unforeseen complications unrelated to our project, which resulted in Netcorp being unable to allocate much of their time for this.

6.3.3 Result

While most of the solutions tested in the third step are all viable solutions for Netcorp. The two solutions that we presented as the final NMSs stand out from the rest, but only slightly. This may not be the result either we or Netcorp expected, as the expectation was to find a solution which clearly stands out from the rest and is the best on the market. However, this does not seem to be possible. We are not completely satisfied with the result, but unfortunately it does not seem possible to get a better result, since most of the alternative solutions are so similar.

6.3.4 Economical and Environmental Sustainability

Since a NMS is usually completely software-based, one might not think there are any environmental aspects to consider. However, there is a rather big environmental aspect to consider, which also indirectly includes economical aspects.

A NMS basically has complete control over the managed network devices and can monitor the traffic flowing through each device, thus it should be possible to implement functionality in the network to increase energy efficiency. For example, the network can be monitored by the NMS in such way that each device can be independently set to idle (or completely turned off) when no traffic is being handled by that device. Furthermore, the NMS can track network activity for a period of time, and with the help of this gathered data, predict upcoming network activity and configure the network in the most efficient way to minimise energy consumption. Not only would this be more friendly to the environment, it would also decrease the cost of running the network.

A further exploration of this concept includes modern technology based on cloud computing, where it is possible to utilise hardware on-demand. In other words, by predicting network load based on statistics, the company can utilise precisely the required amount of hardware capacity for that specific moment, to maximise efficiency even more.

6.3.5 Ethical Considerations

There are some ethical considerations to reflect upon as well. When using a NMS, the network, including the traffic flowing through the network, is monitored. This could cause some serious privacy violations if not performed correctly. It is important that the company monitoring the network and the network traffic respects the customer's privacy. It is also important that the company protects the costumer's data from unauthorised parties. This can be done for example by encrypting the data.

Bibliography

[1] J. Case, M. Fedor, M. Schoffstall, and J. Davin, “Simple Network Management Protocol,” *Internet Request for Comments*, vol. RFC 1157, May 1990. [Online]. Available: https://www.ietf.org/rfc/rfc1157.txt

[2] Cisco, “SNMP Counters: Frequently Asked Questions,” Aug. 2007. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/26007-faq-snmpcounter.html

[3] J. Case, R. Mundy, D. Partain, and B. Stewart, “Introduction to Version 3 of the Internet-standard Network Management Framework,” *Internet Request for Comments*, vol. RFC 2570, Apr. 1999. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2570.txt

[4] J. Postel and J. Reynolds, “Telnet Protocol Specification,” *Internet Request for Comments*, vol. RFC 854, May 1983. [Online]. Available: https://tools.ietf.org/html/rfc854

[5] Tatu Ylonen and Chris Lonvick, “The Secure Shell (SSH) Transport Layer Protocol,” *Internet Request for Comments*, vol. RFC 4253, Jan. 2006. [Online]. Available: https://tools.ietf.org/html/rfc4253

[6] J. Galbraith and O. Saarenmaa, “SSH File Transfer Protocol,” *Internet Request for Comments*, vol. draft-ietf-secsh-filexfer-13, Jun. 2006. [Online]. Available: https://tools.ietf.org/html/draft-ietf-secsh-filexfer-13

[7] Mark K. Lottor, “Simple File Transfer Protocol,” *Internet Request for Comments*, vol. RFC 913, Sep. 1984. [Online]. Available: https://tools.ietf.org/html/rfc913

[8] E. Rescorla, “HTTP Over TLS,” *Internet Request for Comments*, vol. RFC 2818, May 2000. [Online]. Available: https://tools.ietf.org/html/rfc2818

[9] Netscape, “Netscape ISP Homepage.” [Online]. Available: http://isp.netscape.com/

[10] Cisco, "Cisco IOS NetFlow - Cisco," Mar. 2016. [Online]. Available: http://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html

[11] R. Hofstede, P. Čeleda, B. Trammell, I. Drago, R. Sadre, A. Sperotto, and A. Pras, "Flow Monitoring Explained: From Packet Capture to Data Analysis With NetFlow and IPFIX," *IEEE Communications Surveys Tutorials*, vol. 16, no. 4, pp. 2037–2064, Nov. 2014. doi: 10.1109/COMST.2014.2321898. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6814316

[12] Keith McCloghrie and Marshall T. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II," *Internet Request for Comments*, vol. RFC 1213, Mar. 1991. [Online]. Available: https://tools.ietf.org/html/rfc1213

[13] Cisco, "Cisco Prime LAN Management Solution 4.2 Data Sheet," Aug. 2014. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-lan-management-solution/data_sheet_c78-697479.html

[14] Cisco, "Installing and Migrating to Cisco Prime LAN Management Solution 4.2," 2014. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/install/guide/install.pdf

[15] Eric C. Rosen, Arun Viswanathan, and Ross Callon, "Multiprotocol Label Switching Architecture," *Internet Request for Comments*, vol. RFC 3031, Jan. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3031.txt

[16] Travis Keshav, "A Survey of Network Performance Monitoring Tools," Tech. Rep., 2006. [Online]. Available: http://www.cs.wustl.edu/~jain/cse567-06/ftp/net_perf_monitors1/index.html

[17] Alcatel-Lucent, "VitalSuite Performance Management System." [Online]. Available: https://www.alcatel-lucent.com/products/vitalsuite-performance-management-system

[18] CA Technologies, "CA Unified Infrastructure Management." [Online]. Available: http://www.ca.com/us/products/ca-unified-infrastructure-management.html

[19] IBM, "Tivoli Netcool/OMNIbus." [Online]. Available: http://www-03.ibm.com/software/products/sv/ibmtivolinetcoolomnibus

[20] Cynthia Harvey, "55 Open Source Replacements for Popular Networking Tools - Datamation," *Datamation*, Oct. 2010. [Online]. Available: http://www.datamation.com/article.php/3908601

[21] The OpenNMS Group, Inc., "OpenNMS." [Online]. Available: http://www.opennms.org/

[22] Shrubbery networks, inc., "RANCID." [Online]. Available: http://www.shrubbery.net/rancid/

[23] Zenoss Inc., "Zenoss." [Online]. Available: https://www.zenoss.com/

[24] Clayd0n, "Large Scale Network monitoring," Feb. 2014. [Online]. Available: https://www.reddit.com/r/networking/comments/1xt57j/large_scale_network_monitoring/

[25] SolarWinds Worldwide, LLC, "SolarWinds NPM." [Online]. Available: http://www.solarwinds.com/network-performance-monitor.aspx

[26] NetBrain Technologies, Inc., "NetBrain." [Online]. Available: http://www.netbraintech.com/

[27] Paessler AG, "PRTG Network Monitor." [Online]. Available: https://www.paessler.com/prtg

[28] The Cacti Group, Inc., "Cacti." [Online]. Available: http://www.cacti.net/

[29] Jimmy Conner, "CactiEZ." [Online]. Available: http://cactiez.cactiusers.org/

[30] Howard Jones, "Network Weathermap." [Online]. Available: http://network-weathermap.com/

[31] Observium Limited, "Observium." [Online]. Available: http://www.observium.org/

[32] Zabbix LLC, "Zabbix." [Online]. Available: http://www.zabbix.com/product.php

[33] Hewlett-Packard and HP Software Division, "HP OpenView." [Online]. Available: http://www8.hp.com/us/en/software/enterprise-software.html

[34] Wikipedia contributors, "Comparison of network monitoring systems," Apr. 2016. [Online]. Available: https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

[35] Anne Håkansson, "Portal of research methods and methodologies for research projects and degree projects," in *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013, p. 1. [Online]. Available: https://www.kth.se/social/files/55563b9df27654705999e3d6/Research%20Methods%20-%20Methodologies%281%29.pdf

[36] MagPress, "4 Tips to Make Sure Your Website is User Friendly," Mar. 2015. [Online]. Available: http://www.magpress.com/blog/4-tips-to-make-sure-your-website-is-user-friendly

[37] CA Inc., "CA Spectrum." [Online]. Available: http://www.ca.com/us/products/ca-spectrum.html

[38] CA Inc., "CA Spectrum Data Sheet," 2016. [Online]. Available: http://www.ca.com/content/dam/ca/us/files/data-sheet/ca-spectrum.PDF

[39] CA Inc., "CA eHealth." [Online]. Available: http://www.ca.com/us/products/ca-ehealth.html

[40] CA Inc., "CA Spectrum Mobile on App Store," Jul. 2015. [Online]. Available: https://itunes.apple.com/se/app/ca-spectrum-mobile/id932261863?mt=8

[41] CA Inc., "CA Spectrum Mobile on Google Play," Jul. 2015. [Online]. Available: https://play.google.com/store/apps/details?id=com.ca.SpectrumMobile

[42] Stephen Lawson. (2007, Jun.) CA's Spectrum tool now looks at human errors. InfoWorld. [Online]. Available: http://www.infoworld.com/article/2663380/networking/ca-s-spectrum-tool-now-looks-at-human-errors.html

[43] Cisco, "Cisco Prime Infrastructure." [Online]. Available: http://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html

[44] Cisco, "LMS - Cisco Prime Infrastructure Functional Comparison with Prime Infrastructure 2.0," Aug. 2014. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/prime-infrastructure/guide_c07-729089.html

[45] HP Software Division, "HP IMC." [Online]. Available: http://www8.hp.com/us/en/networking/network-management/

[46] HP Software Division, "HP IMC Data Sheet," Dec. 2015. [Online]. Available: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-0694ENW.pdf

[47] Hewlett-Packard, "HPE Network Automation." [Online]. Available: http://www8.hp.com/us/en/software-solutions/network-automation/

[48] Hewlett-Packard, "HPE NNMi Data Sheet," Jan. 2016. [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-7850ENW.pdf

[49] HP Software Division, "HPE Network Automation Data sheet," Jan. 2016. [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-5784ENW.pdf

[50] IBM, "Netcool Operations Insight." [Online]. Available: http://www-03.ibm.com/software/products/sv/netcool-operations-insight

[51] "Compose IT," 1987. [Online]. Available: http://compose.se/

[52] Cygate, "Effektivare systemdrift och driftledning." *Case*, vol. 2|08, Feb. 2008. [Online]. Available: http://www.mypaper.se/show/cygate/show.asp?pid=345207389865297&page=10

[53] Zoho Corporation and ManageEngine, "OpManager." [Online]. Available: https://www.manageengine.com/network-monitoring/

[54] ManageEngine, "Network Configuration Management, Change Management - Manage Configurations of Switches, Routers, Firewalls." [Online]. Available: https://www.manageengine.com/network-configuration-manager/

[55] op5 AB, "op5 Monitor Enterprise plus." [Online]. Available: www.op5.com/?wpfb_dl=598

[56] Lars Michelsen, "Welcome to NagVis Home! - NagVis.org." [Online]. Available: http://www.nagvis.org/

[57] Opmantek, "NMIS." [Online]. Available: https://opmantek.com/network-management-system-nmis/

[58] Opmantek, "NMIS Summary." [Online]. Available: https://opmantek.com/network-management-system-nmis/#Summary

[59] SevOne Inc., “SevOne.” [Online]. Available: https://www.sevone.com/

[60] SevOne, “Avoiding the Hidden Costs of Performance Monitoring Tools | SevOne.” [Online]. Available: https://www.sevone.com/white-paper/avoiding-hidden-costs-performance-monitoring-tools

[61] GroundWork Inc., “GroundWork Monitor.” [Online]. Available: http://www.gwos.com/

[62] GroundWork, “What We Monitor < GroundWork.” [Online]. Available: http://www.gwos.com/resources/what-we-monitor/

[63] Kratos Defense & Security Solutions, Inc., “Kratos NeuralStar.” [Online]. Available: http://www.kratosnetworks.com/products/network-management/neuralstar?=http://www.kratosnetworks.com/products/NeuralStar/dashboard_gallery/interface_view/

[64] Opsview Ltd., “Opsview.” [Online]. Available: https://www.opsview.com/

[65] PathSolutions, Inc., “PathSolutions.” [Online]. Available: http://www.pathsolutions.com/

[66] Plixer International, Inc., “Scrutinizer.” [Online]. Available: https://www.plixer.com/Scrutinizer-Netflow-Sflow/scrutinizer.html

[67] ossintegrators_dt, “Looking Into Different Network Monitoring Tools,” Aug. 2013. [Online]. Available: https://www.reddit.com/r/networking/comments/1jvjsq/looking_into_different_network_monitoring_tools/cbixpbl

[68] nkripper, “IBM Netcool/OMNIbus Experience,” Mar. 2014. [Online]. Available: https://www.reddit.com/r/networking/comments/1zzjgb/ibm_netcoolomnibus_experience/cfygkfa

Appendix A

Long lists

A.1 Wikipedia: List of Network Monitoring Systems

The following list of network monitoring systems was collected from Wikipedia[*] on March 14^{th} 2016:

- AccelOps
- AdRem NetCrunch
- AggreGate Network Manager
- Argus
- Argus - The all seeing
- Avaya Visualization Performance and Fault Manager (VPFM)
- CA Spectrum
- CA UIM (f.k.a. Nimsoft Monitor)
- Cacti
- Centina Systems NetOmnia
- Check_MK
- collectd
- EMC^2 Smarts
- ExtraHop
- Free Network Automatic Testing System (FreeNATS)
- Ganglia
- Glasswire
- GroundWork Inc.
- HP NNMi
- IBM Netcool/OMNIbus
- Icinga
- InterMapper
- IPHost Network Monitor

[*] https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

- isyVmon
- Kaseya Network Monitor
- Kaseya Traverse
- LiveAction
- LogicMonitor
- ManageEngine OpManager
- Monitorix
- Munin
- Nagios
- NetQoS Performance Center
- Network Instruments Observer Infrastructure
- NetXMS
- NeuralStar
- Observium
- op5 Monitor
- Open Knowledge Based Management (OpenKBM)
- OpenNMS
- Opmantek NMIS
- Opsview
- Objective Systems Integrators (OSI_2) NetExpert
- Power Admin (PA) Server Monitor
- PacketTrap
- Pandora Flexible Monitoring System (FMS)
- PathSolutions
- Performance Co-Pilot
- Redcell
- Riverbed (f.k.a. Optimized Network Engineering Tools (OPNET)'s AppResponse Xpert)
- ScienceLogic
- Scrutinizer
- Sensu
- ServersCheck
- SevOne
- Shinken
- Solarwinds
- Spiceworks
- TclMon
- uptime software
- Verax NMS
- VitalSuite
- Xymon/Hobbit
- Zabbix
- Zenoss

A.2 Complete List of Network Management Tools

- AccelOps
- AdRem NetCrunch
- Aerohive (HiveManager)
- AggreGate Network Manager
- Argus
- Argus - The all seeing
- Avaya VPFM
- CA Spectrum
- CA UIM (f.k.a. Nimsoft Monitor)
- Cacti
- CactiEZ
- Centina Systems NetOmnia
- Check_MK
- Cisco LMS
- Cisco Meraki
- Cisco Prime Infrastructure
- collectd
- Corvil
- EMC^2 Smarts
- Entuity
- Extreme Control Center (f.k.a. NetSight)
- FreeNATS
- Ganglia
- Glasswire
- GroundWork Monitor
- HP IMC
- HPE Network Automation
- HP NNMi
- IBM Tivoli Netcool/OMNIbus
- Icinga
- InfoVista VistaInsight
- InterMapper
- IPHost Network Monitor
- Ipswitch
- isyVmon
- Kaseya Network Monitor
- Kaseya Traverse
- Kratos NeuralStar
- LiveAction
- LogicMonitor
- LogicVein Net LineDancer
- ManageEngine OpManager
- Monitorix
- Munin
- Nagios
- NetBrain
- NetScout systems (and NetScout systems Fluke networks)
- NetXMS
- Observium
- op5 Monitor
- OpenNMS
- Opmantek NMIS
- Opsview
- OSI$_2$ NetExpert
- PA Server Monitor
- PacketTrap

- Pandora FMS
- PathSolutions
- Performance Co-Pilot
- PRTG
- RANCID
- Redcell
- Riverbed (f.k.a. OPNET's AppResponse Xpert)
- Rocket OpenKBM
- ScienceLogic
- Scrutinizer
- Sensu
- ServersCheck
- SevOne
- Shinken
- SolarWind NPM (Orion)
- Spiceworks
- TclMon
- uptime software
- Weathermap
- Verax NMS
- Viavi (f.k.a. Network Instruments Observer Infrastructure)
- VitalSuite
- Xirrus Management System
- Xymon/Hobbit
- Zabbix
- Zenoss

Appendix B

Detailed Results

B.1 OpManager's price list

Table B.1: The prices for the various licenses of OpManager - *J. Lidman, Account Manager, Inuit AB, May 17, 2016*

Renting licences 12 months:	**Price (SEK)**
Subscriber fee for 2,500 Devices Pack (Unlimited interfaces)	285,950
Subscriber fee for 5,000 Devices Pack (Unlimited interfaces)	455,950
Subscriber fee for 10,000 Devices Pack (Unlimited interfaces)	820,750
Purchase licenses 12 months + maintenance & support:	**Price (SEK)**
Single Installation License fee for 2,500 Devices Pack (Unlimited interfaces)	565,205
Maintenance and Support fee for 2,500 Devices Pack (Unlimited interfaces)	113,040
Total	678,245
Single Installation License fee for 5,000 Devices Pack (Unlimited interfaces)	899,955
Maintenance and Support fee for 5,000 Devices Pack (Unlimited interfaces)	179,995
Total	1,079,950
Single Installation License fee for 10,000 Devices Pack (Unlimited interfaces)	1,619,955
Maintenance and Support fee for 10,000 Devices Pack (Unlimited interfaces)	323,995
Total	1,943,950

B.2 Detailed data from step one

This appendix, split up into four figures, shows detailed data from an Excel document where step one (in the three-step approach) was documented.

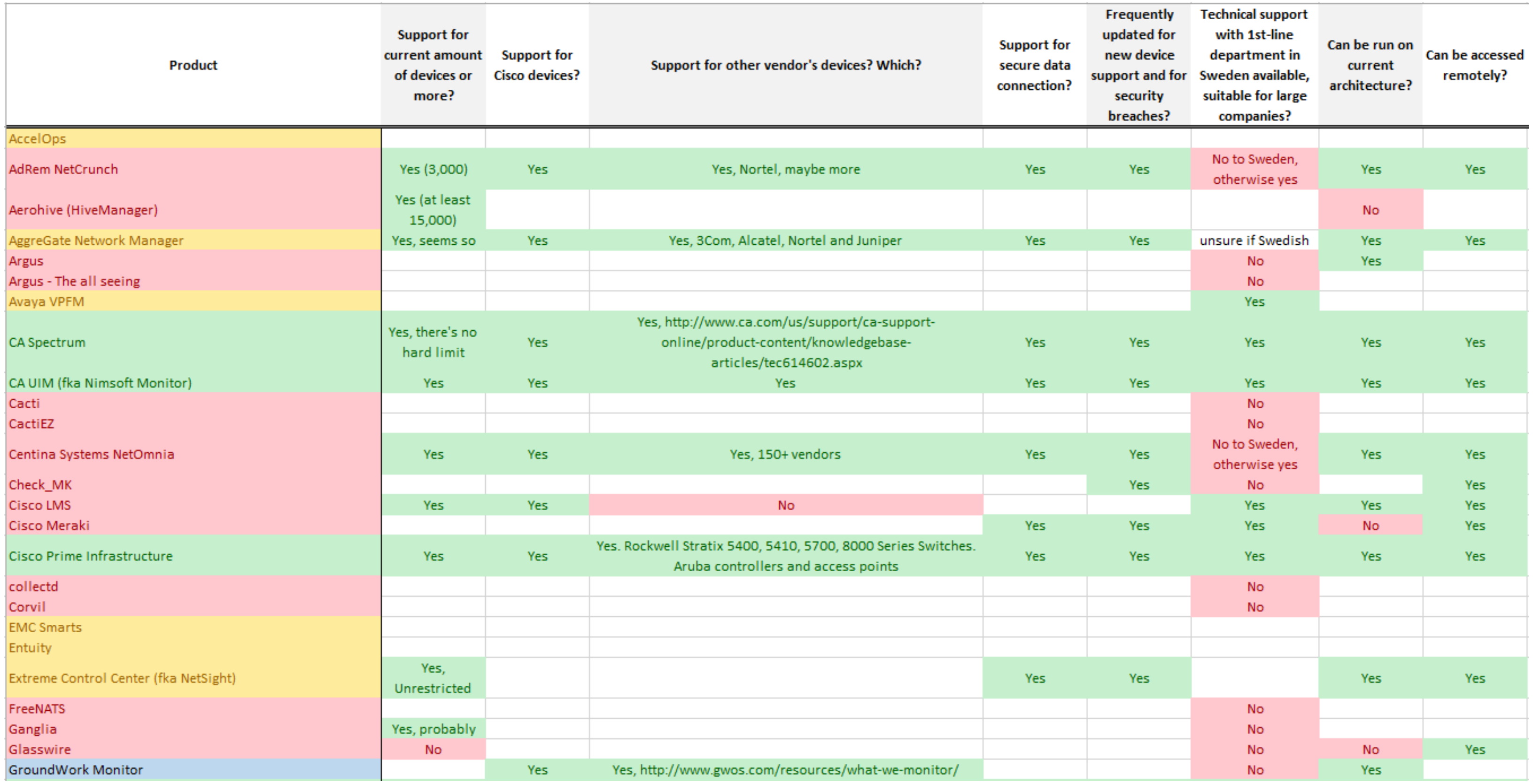
The left-most column in the document is colour-coded for easy reading. Below is a description for the meaning of each colour.

Red: This NMS was rejected because one or several of the requirements were not met, and is thus not inspected further in step two of the three-step approach.

Green: This NMS met all the requirements, and was thus approved for further inspection in step two.

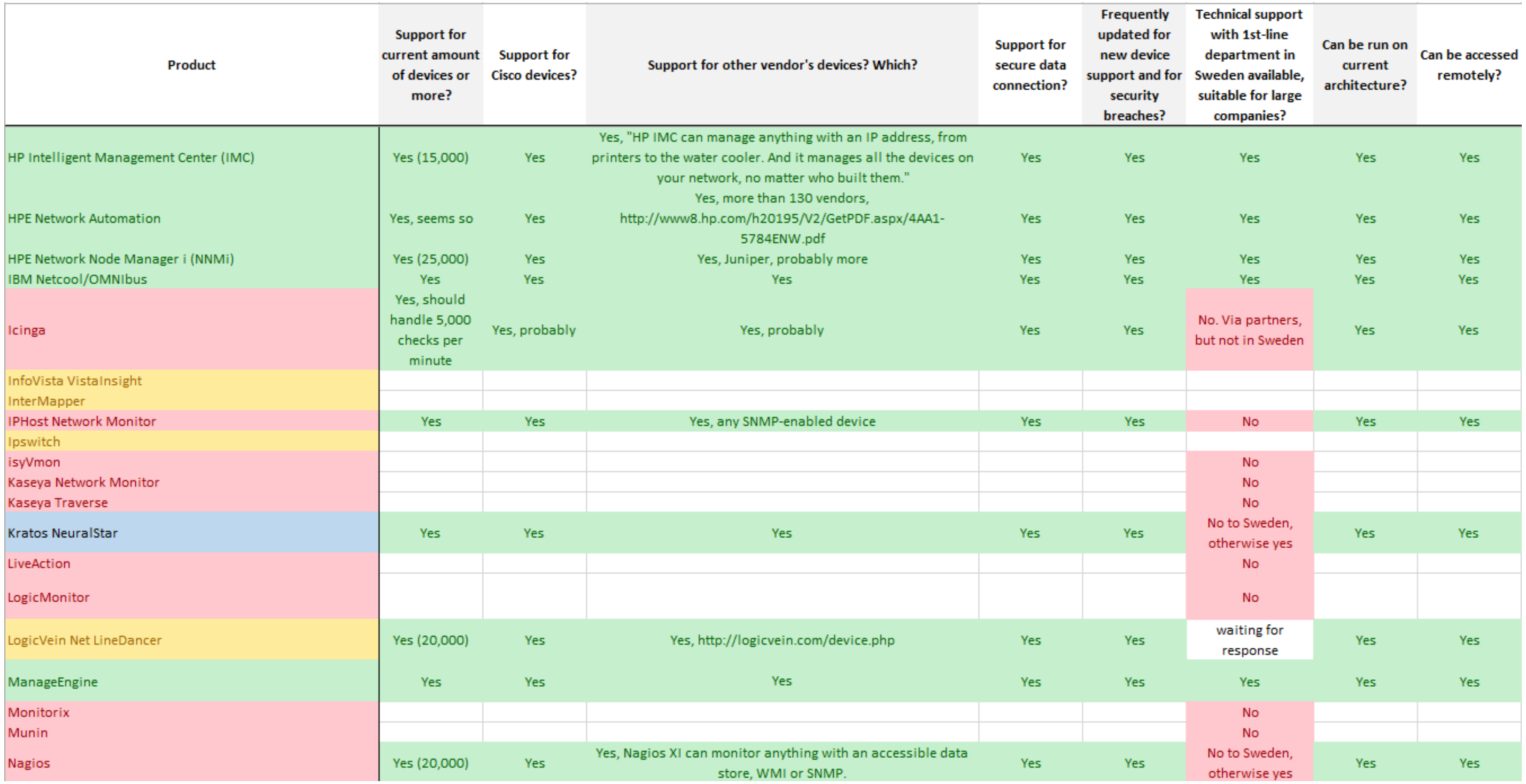
Yellow: Sufficient information about this NMS could not be found. Neither customer support, technical support, nor sales department could be reached to get hold of such information. It is thus not inspected further in step two.

Blue: This NMS was rejected because one or several of the requirements were not met, and is thus not inspected further in step two. *However*, despite being rejected, this NMS is very interesting and is brought up in Honourable mentions in Section 5.4.3 on page 58.



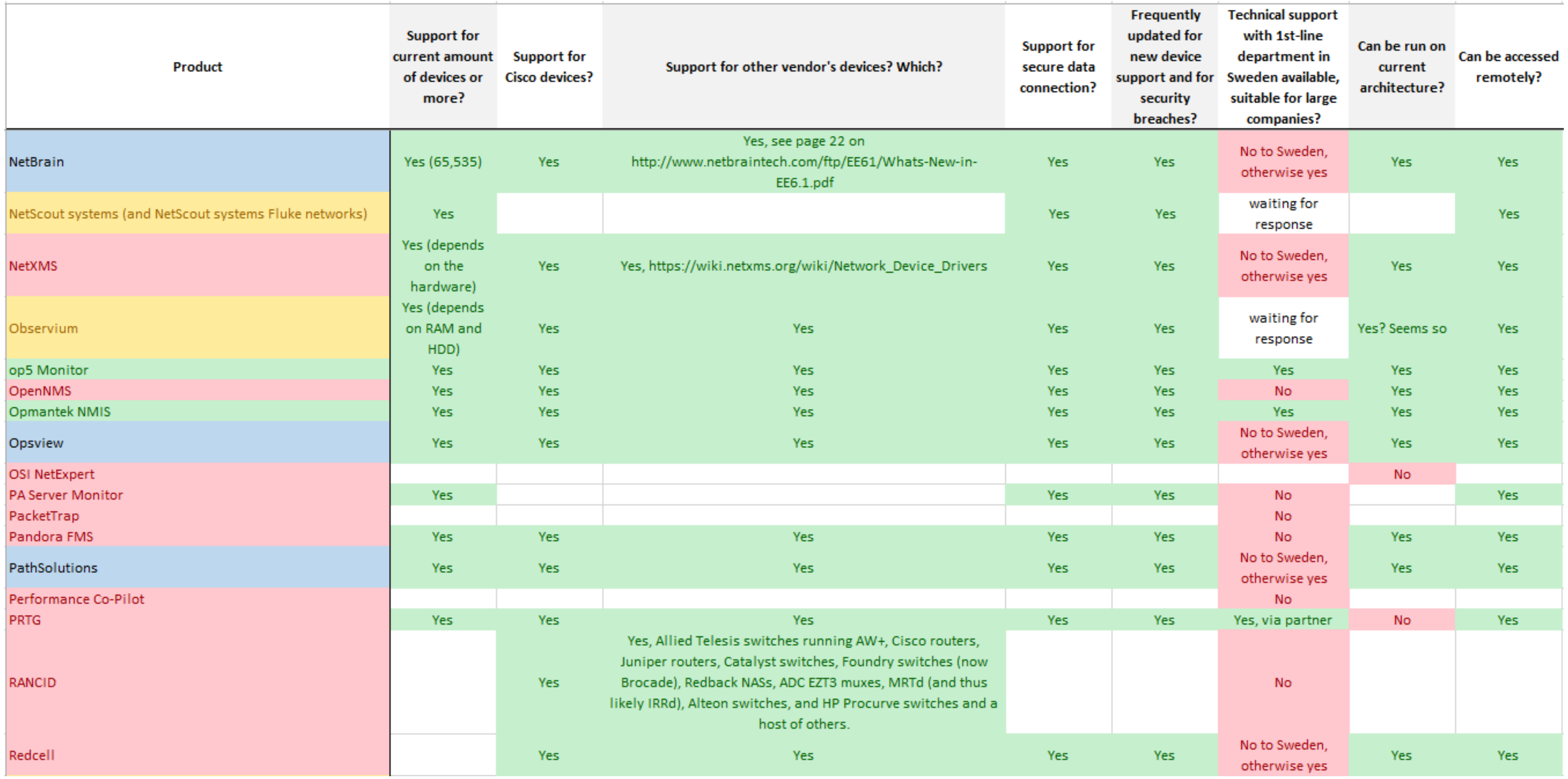
Product	Support for current amount of devices or more?	Support for Cisco devices?	Support for other vendor's devices? Which?	Support for secure data connection?	Frequently updated for new device support and for security breaches?	Technical support with 1st-line department in Sweden available, suitable for large companies?	Can be run on current architecture?	Can be accessed remotely?
AccelOps								
AdRem NetCrunch	Yes (3,000)	Yes	Yes, Nortel, maybe more	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
Aerohive (HiveManager)	Yes (at least 15,000)						No	
AggreGate Network Manager	Yes, seems so	Yes	Yes, 3Com, Alcatel, Nortel and Juniper	Yes	Yes	unsure if Swedish	Yes	Yes
Argus						No	Yes	
Argus - The all seeing						No		
Avaya VPFM						Yes		
CA Spectrum	Yes, there's no hard limit	Yes	Yes, http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec614602.aspx	Yes	Yes	Yes	Yes	Yes
CA UIM (fka Nimsoft Monitor)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cacti						No		
CactiEZ						No		
Centina Systems NetOmnia	Yes	Yes	Yes, 150+ vendors	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
Check_MK					Yes	No		Yes
Cisco LMS	Yes	Yes	No			Yes	Yes	Yes
Cisco Meraki				Yes	Yes	Yes	No	Yes
Cisco Prime Infrastructure	Yes	Yes	Yes. Rockwell Stratix 5400, 5410, 5700, 8000 Series Switches. Aruba controllers and access points	Yes	Yes	Yes	Yes	Yes
collectd						No		
Corvil						No		
EMC Smarts								
Entuity								
Extreme Control Center (fka NetSight)	Yes, Unrestricted			Yes	Yes		Yes	Yes
FreeNATS						No		
Ganglia	Yes, probably					No		
Glasswire	No					No	No	Yes
GroundWork Monitor		Yes	Yes, http://www.gwos.com/resources/what-we-monitor/			No	Yes	

Figure B.1: Figure 1 of 4 of an Excel document, showing detailed data from step one.



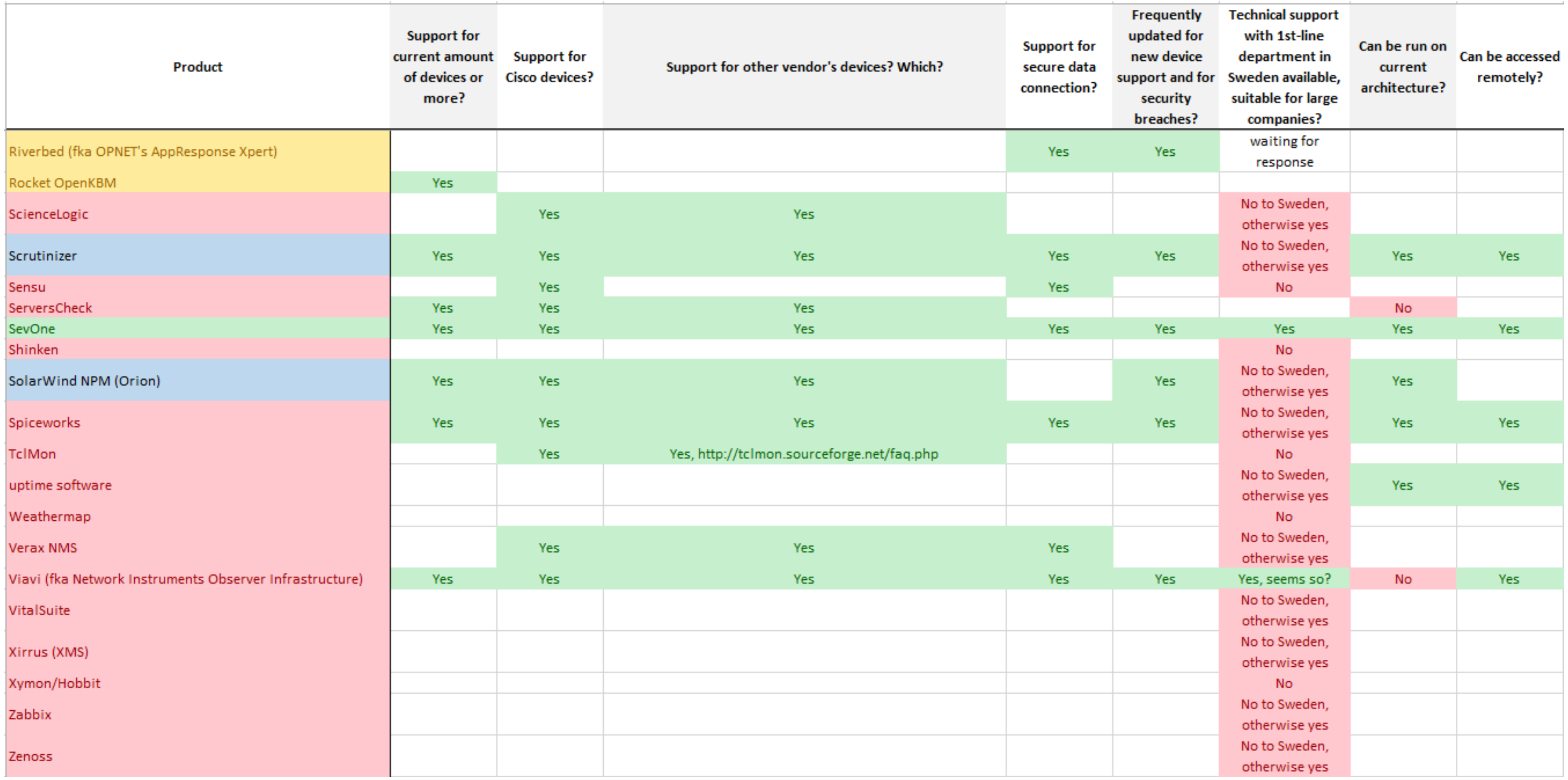
Product	Support for current amount of devices or more?	Support for Cisco devices?	Support for other vendor's devices? Which?	Support for secure data connection?	Frequently updated for new device support and for security breaches?	Technical support with 1st-line department in Sweden available, suitable for large companies?	Can be run on current architecture?	Can be accessed remotely?
HP Intelligent Management Center (IMC)	Yes (15,000)	Yes	Yes, "HP IMC can manage anything with an IP address, from printers to the water cooler. And it manages all the devices on your network, no matter who built them."	Yes	Yes	Yes	Yes	Yes
HPE Network Automation	Yes, seems so	Yes	Yes, more than 130 vendors, http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA1-5784ENW.pdf	Yes	Yes	Yes	Yes	Yes
HPE Network Node Manager i (NNMi)	Yes (25,000)	Yes	Yes, Juniper, probably more	Yes	Yes	Yes	Yes	Yes
IBM Netcool/OMNIbus	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Icinga	Yes, should handle 5,000 checks per minute	Yes, probably	Yes, probably	Yes	Yes	No. Via partners, but not in Sweden	Yes	Yes
InfoVista VistaInsight								
InterMapper								
IPHost Network Monitor	Yes	Yes	Yes, any SNMP-enabled device	Yes	Yes	No	Yes	Yes
Ipswitch								
isyVmon						No		
Kaseya Network Monitor						No		
Kaseya Traverse						No		
Kratos NeuralStar	Yes	Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
LiveAction						No		
LogicMonitor						No		
LogicVein Net LineDancer	Yes (20,000)	Yes	Yes, http://logicvein.com/device.php	Yes	Yes	waiting for response	Yes	Yes
ManageEngine	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Monitorix						No		
Munin						No		
Nagios	Yes (20,000)	Yes	Yes, Nagios XI can monitor anything with an accessible data store, WMI or SNMP.	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes

Figure B.2: Figure 2 of 4 of an Excel document, showing detailed data from step one.



Product	Support for current amount of devices or more?	Support for Cisco devices?	Support for other vendor's devices? Which?	Support for secure data connection?	Frequently updated for new device support and for security breaches?	Technical support with 1st-line department in Sweden available, suitable for large companies?	Can be run on current architecture?	Can be accessed remotely?
NetBrain	Yes (65,535)	Yes	Yes, see page 22 on http://www.netbraintech.com/ftp/EE61/Whats-New-in-EE6.1.pdf	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
NetScout systems (and NetScout systems Fluke networks)	Yes			Yes	Yes	waiting for response		Yes
NetXMS	Yes (depends on the hardware)	Yes	Yes, https://wiki.netxms.org/wiki/Network_Device_Drivers	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
Observium	Yes (depends on RAM and HDD)	Yes	Yes	Yes	Yes	waiting for response	Yes? Seems so	Yes
op5 Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
OpenNMS	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Opmantek NMIS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Opsview	Yes	Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
OSI NetExpert							No	
PA Server Monitor	Yes			Yes	Yes	No		Yes
PacketTrap						No		
Pandora FMS	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
PathSolutions	Yes	Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
Performance Co-Pilot						No		
PRTG	Yes	Yes	Yes	Yes	Yes	Yes, via partner	No	Yes
RANCID		Yes	Yes, Allied Telesis switches running AW+, Cisco routers, Juniper routers, Catalyst switches, Foundry switches (now Brocade), Redback NASs, ADC EZT3 muxes, MRTd (and thus likely IRRd), Alteon switches, and HP Procurve switches and a host of others.			No		
Redcell		Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes

Figure B.3: Figure 3 of 4 of an Excel document, showing detailed data from step one.



Product	Support for current amount of devices or more?	Support for Cisco devices?	Support for other vendor's devices? Which?	Support for secure data connection?	Frequently updated for new device support and for security breaches?	Technical support with 1st-line department in Sweden available, suitable for large companies?	Can be run on current architecture?	Can be accessed remotely?
Riverbed (fka OPNET's AppResponse Xpert)				Yes	Yes	waiting for response		
Rocket OpenKBM	Yes							
ScienceLogic		Yes	Yes			No to Sweden, otherwise yes		
Scrutinizer	Yes	Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
Sensu		Yes		Yes		No		
ServersCheck	Yes	Yes	Yes				No	
SevOne	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Shinken						No		
SolarWind NPM (Orion)	Yes	Yes	Yes		Yes	No to Sweden, otherwise yes	Yes	
Spiceworks	Yes	Yes	Yes	Yes	Yes	No to Sweden, otherwise yes	Yes	Yes
TclMon		Yes	Yes, http://tclmon.sourceforge.net/faq.php			No		
uptime software						No to Sweden, otherwise yes	Yes	Yes
Weathermap						No		
Verax NMS		Yes	Yes	Yes		No to Sweden, otherwise yes		
Viavi (fka Network Instruments Observer Infrastructure)	Yes	Yes	Yes	Yes	Yes	Yes, seems so?	No	Yes
VitalSuite						No to Sweden, otherwise yes		
Xirrus (XMS)						No to Sweden, otherwise yes		
Xymon/Hobbit						No		
Zabbix						No to Sweden, otherwise yes		
Zenoss						No to Sweden, otherwise yes		

Figure B.4: Figure 4 of 4 of an Excel document, showing detailed data from step one.

Appendix C

Reviews About IBM Tivoli Netcool/OMNIbus

The following reviews were taken from reddit:

"The con I'd say is this is a fairly complex suite of products due to its enterprise nature (needing to scale significantly and support many types of data and feeds), but with help installing, configuring and with training how to use the suite it's manageable (and powerful)." - ossintegrators_dt [67]

"I have 10+ years managing NOC servers and have used virtually every major Manager of Managers. My opinion: Netcool is the Cadillac of this realm. The only downside is that when IBM bought out Micromuse to get Netcool, they haven't really done much to improve the software." - nkripper [68]

TRITA-ICT-EX-2016:71

www.kth.se