Bachelor's thesis

Business and administration

Business Information Technology – Data communications

2012

Jesse Kuusisto

MAINTENANCE PROCESS OF NETWORKING DEVICES

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology – Data communications

2012 | 37

Esko Vainikka

Jesse Kuusisto

MAINTENANCE PROCESS OF NETWORKING DEVICES

The maintenance process is a critical part of any network. It is recommended to carry it out in eight steps: assess, advice, procure, provision, maintain, decommission, data destruction and disposal. The present bachelor's thesis focuses on the maintaining aspect of the maintenance process, but takes, nevertheless, into consideration the other parts as well.

The study was commissioned by Tieto Oyj, which needed an efficient way to take a proactive approach to be able to provide more network stability for its customers. The company uses a tool, HP Network Automation, which is able to assist in this process, but its usage is still in its early stages within the company. The plan is to create a basis for the life-cycle of the networking devices, which can be used in conjunction with HP's network automation to provide more stability, scalability, automation and to ease the technicians' work in maintaining this environment. The process will follow ITIL practices and use BMC Remedy's Organizational Management Tool as the enterprise resource planning system of choice to monitor the incident, change and problem -management.

The theoretical part of the thesis discusses literature and internet sources. In addition the data were gathered by consulting and interviewing Tieto specialists as well as vendors who provide the devices.

The empirical part consists of designing the whole process and discusses which steps to take and what to consider in order to create a process that is both practical and efficient. It also aims to calculate the time needed to add the devices to HP's network automation, set up their monitoring as well as the time needed to maintain them. This information makes it possible to apply the same process to other infras will as well.

KEYWORDS:

Network, Maintenance process, Networking devices, Tieto

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely – Tietoliikenne

2012 | 37

Esko Vainikka

Jesse Kuusisto

VERKKOLAITTEIDEN YLLÄPITOPROSESSI

Ylläpitoprosessi on kriittinen osa jokaista verkkoa. On suositeltavaa hoitaa se kahdeksassa vaiheessa: arvioi, neuvo, hanki, säännöstele, ylläpidä, pura, tuhoa ja hävitä tieto. Tämä opinnäytetyö keskittyy ylläpito-kohtaan silti muut vaiheet huomioon ottaen.

Tarve opinnäytetyölle tuli Tieto Oyj:ltä, joka tarvitsi tehokkaan lähestymistavan taatakseen enemmän verkon vakautta asiakkailleen. Tieto käyttää työkalua nimeltä HP Network Automation, joka avustaa prosessissa, mutta sen käyttö on yhä alkuaskeleillaan yhtiön sisällä. Suunnitelmana on luoda perustat verkkolaitteiden elinkaarelle, jota voidaan käyttää yhdessä HP:n network automationin kanssa vakauden, skaalautuvuuden ja automatisoinnin takaamiseksi, kuin myös avustamaan teknikkoja ylläpitämään tätä ympäristöä. Prosessi seuraa ITIL-käytäntöjä ja käyttää työkalua BMC Remedyn Organizational Management Tool toiminnanohjausjärjestelmänä monitoroimaan odottamatonta tapahtumaa, muutos ja ongelma – hallintaa.

Teoreettisen osan tutkimus koostuu kirjallisuudesta, internet-lähteistä ja Tiedon spesialistien konsultoinnista ja haastatteluista ja tavarantoimittajien tiedoista.

Empiirinen osio kattaa koko prosessin suunnittelun, mitä askeleita otetaan ja mitä huomioidaan, jotta prosessi on käytännöllinen ja tehokas. Se pyrkii myös laskemaan tarvitun ajan laitteiden viemiselle HP network automationiin, monitoroinnin asetuksille ja niiden ylläpidolle, jotta prosessin hyödyntäminen muissa infroissa on mahdollista.

ASIASANAT:

Network, Maintenance process, Networking devices, Tieto

CONTENT

FIGURES

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
CI	Configuration Item
DMZ	Demilitarized Zone
DWDM	Dense Wavelength Division Multiplexing
EoL	End-of-Life
EoS	End-of-Support
ERP	Enterprise Resource Planning
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTP	File Transfer Protocol
GUI	Graphical User Interface
HPNA	HP Network Automation
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IPSec	Internet Protocol Security
IPX	Internetwork Packet Exchange
ITIL	Information Technology Infrastructure Library
ITLM	Information Technology Lifecycle Management
MAC	Media Access Control
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NA	Network Automation
NAT	Network Address Translation
OMT	Organisational Management Tool
PCI DSS	Payment Card Industry Data Security Standard

RADIUS	Remote Authentication Dial In User Service
SDH	Synchronous Digital Hierarchy
SIP	Support Instruction Portal
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SOX	Sarbanes-Oxley Act
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
WDM	Wavelength-Division Multiplexing

DEFINITIONS

OMT	an ERP-system, used to monitor tickets and change managements.
FCAPS	ISO Telecommunications management network model and framework for network management.
ITIL	Set of practices for IT service management that focuses on aligning IT services with needs of business.
Bootstrap	Development of successively more complex and faster programming environment.
Bare metal	Devices that are booting up for the first time, often running some form of bootstrap OS.

1 INTRODUCTION

This thesis was done as an assignment for Tieto Finland Oyj who is the leading IT service company in Northern Europe providing IT and product engineering services. Other marketing names for Tieto are Tieto Corporation, Tieto Oyj, Tieto, Tieto-konserni, and TietoEnator. (Tieto Oyj 2012).

The thesis starts by going through all the theoretical aspects that were used in the making of this thesis and then follows it up by going through the implementation process that took place. The purpose of this thesis is to provide Tieto with an effective way of improving the maintenance of their hardware and improving the stability of their network by the usage of HPNA.

2 MAINTENANCE PROCESS IN GENERAL

Maintenance process is conducted for both hardware and software but the process itself has different phases for each of the two. In general, the aim of a maintenance process is to promote consistency which leads to increased reliability and performance, improved information and analytical processes for investment, maintenance and divestment, making it easier to identify performance problems, faulty parts and to help extend the lifetime of the asset. Integration with data mining and analytics tools further helps to manage the assets. (IBM 2012.)

The term maintenance, when attached to software, assumes a meaning profoundly different from the meaning it assumes in hardware, or any other maintenance process. Many engineering disciplines refer to maintenance as keeping something in working order, to keep its functionality in the same order as at its release time. This does not apply to software as it does not deteriorate with use and passing of time but there is still need to modify it. Software is infinitely malleable and therefore often perceived as the easiest part to change in a system. (Brooks 1987, 10-19.)

There are pre built network maintenance models, such as FCAPS –model, which consists of five main tasks:

Fault management. Errors such as dropped packets and erroneous frames in a LAN are typical even in a well-functioning network. These types of errors need to be logged and do not require correction unless they keep happening persistently. Some of these may be corrected automatically but others require an administrator's intervention. When errors occur, the root cause should be reported and other related faults suppressed. This will help to avoid overwhelming the administrator with reports of all related faults. SNMP traps are a way of automating this process. Administrator can configure a trap which will provide a notification when a set condition happens, such as a link going down. (Flextronics 2012.)

Configuration management. Tasks such as installation, identification and configuration of hardware and services. It also includes software and firmware management, change control, inventory management, monitoring and managing the deployment status of devices. The aims for configuration management include planning for scaling, simplifying configurations and backing up configuration images for network devices. (Cisco 2012.)

Accounting maintenance. Focus on how to distribute resources optimally among enterprise users. When there is lack of computing resources, it may be necessary to set a limit on their usage. Automatic actions should be taken on exceeding thresholds. RADIUS and TACACS are common protocols that are used for accounting.

Performance management. Gathering network statistics, evaluating system performance under both normal and degraded conditions and altering system mode of operation. (Flextronics 2012.)

Security management. Minimizing unauthorized or accidental access to network control functions. It is mainly enforced with authentication and encryption. (Flextronics 2012.)

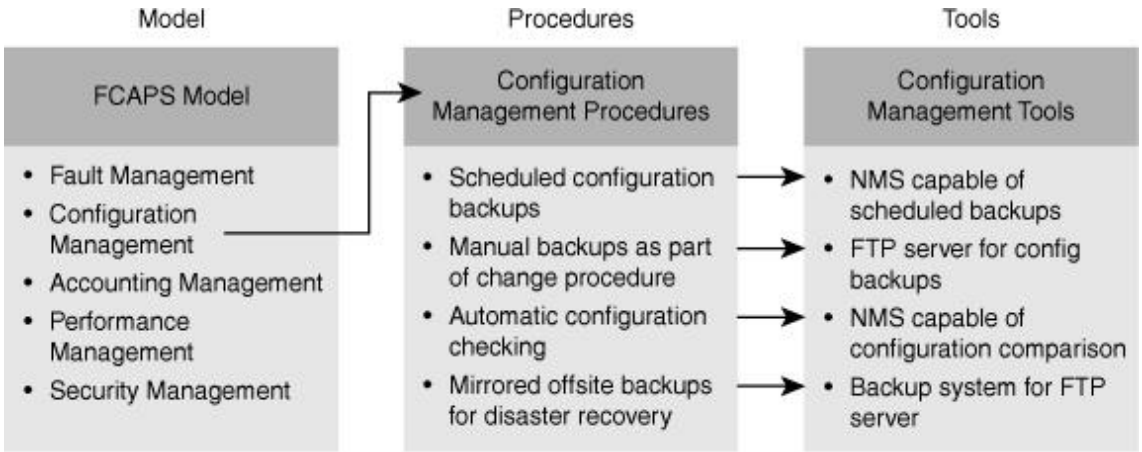

Figure 1.FCAPS Model (Cisco 2012).

Another option is to build a custom management model that meets the company's needs by taking elements from the different models and tailoring a specific suit for specific needs.

2.1 Maintenance process for hardware

By nature hardware maintenance is interrupt driven (hardware failures, outages etc.) but it is possible to prevent this by maintaining the equipment. The aim is to prevent problems before they can occur and therefore reduce downtime and decrease the amount of time it takes to fix a problem. This will lower the financial damage suffered and also increase customer satisfaction.

Ways to perfect hardware maintenance processes are:

• Scheduling maintenance breaks during off-hours

• Managing hardware life-cycle

• Optimizing monitoring

• Formalizing change-control procedures

• Establishing network documentation procedures and effective communication

• Planning for disaster recovery (Cisco 2012).

2.2 Maintenance process for software

The IEEE 1219-1998 software standards document defines software maintenance as "the modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment." Software maintenance is the concluding part of the software development process or life cycle. Software maintenance can have different meanings in the context of this standard, but the essential types of software maintenance are

- Emergency maintenance: unscheduled corrective maintenance performed to keep the system operational.

- Perfective maintenance: modification of a software product after delivery to improve performance or maintainability. This is done to improve performance and maintainability of software.
- Corrective maintenance: reactive modification of a software product performed after delivery to correct discovered faults. This appears as bug fixes.
- Adaptive maintenance: helps to keep the software usable in a changed or changing environment (IEEE standard 1219-1998).

Regarding software, the present thesis focuses on its life-cycle aspects. Software's code changes will be made by the manufacturer but some of the processes can be initiated by Tieto, if a need for a bug fix or a new feature is deemed necessary. This thesis will introduce a design for how often to revise for new software patches and how to plan for their end of support and end of life.

3 HP NETWORK AUTOMATION

As enterprise networks expand, the topologies also get more complex and must comply with regulations and security best practices. It is essential to manage the network in a secure and automated way to be effective in both performance and costs. HP Network Automation (NA) is an enterprise tool which tracks and regulates configuration and software changes across routers, switches, firewalls, load balancers and wireless access points. It provides the IT staff with a constant view of the network in real time and multiple monitoring and diagnostic tools to prevent problems. NA supports a huge load of devices from different vendors including Cisco, Nortel, F5 Networks and Extreme Networks. (HP 2009.)

NA monitors processes, assesses internal control adequacy, secures independent assurance and provides for independent audit. It helps to manage service levels, third-party services and performance and capacity, ensuring continuous service system security and allowing for easier cost identification and allocation. This thesis will use the word bare metal devices for devices that are booting up for the first time, often running some form of “bootstrap” OS. NA is only able to interact with the device in a very limited way when using a bare metal driver. In general, bare metal provisioning process is done in two parts:

Preparation – Bringing devices into the system and setting them to a point where they are capable of accepting configurations, firmware, OS etc. These devices can have a temporary location on the network, but they are not setup with the IP information that matches their intended location within the network. The idea of preparation is to get the device to a state where it can accept data NA intends to provision.

Prototyping – Prototyping is the process of defining and maintaining device templates. Templates provide the ability to define configurations, OS/file specifications and other device-specific information that can then be applied to

existing devices completely overwriting any pre-existing data. The template can be copied from a device which is already on the network.

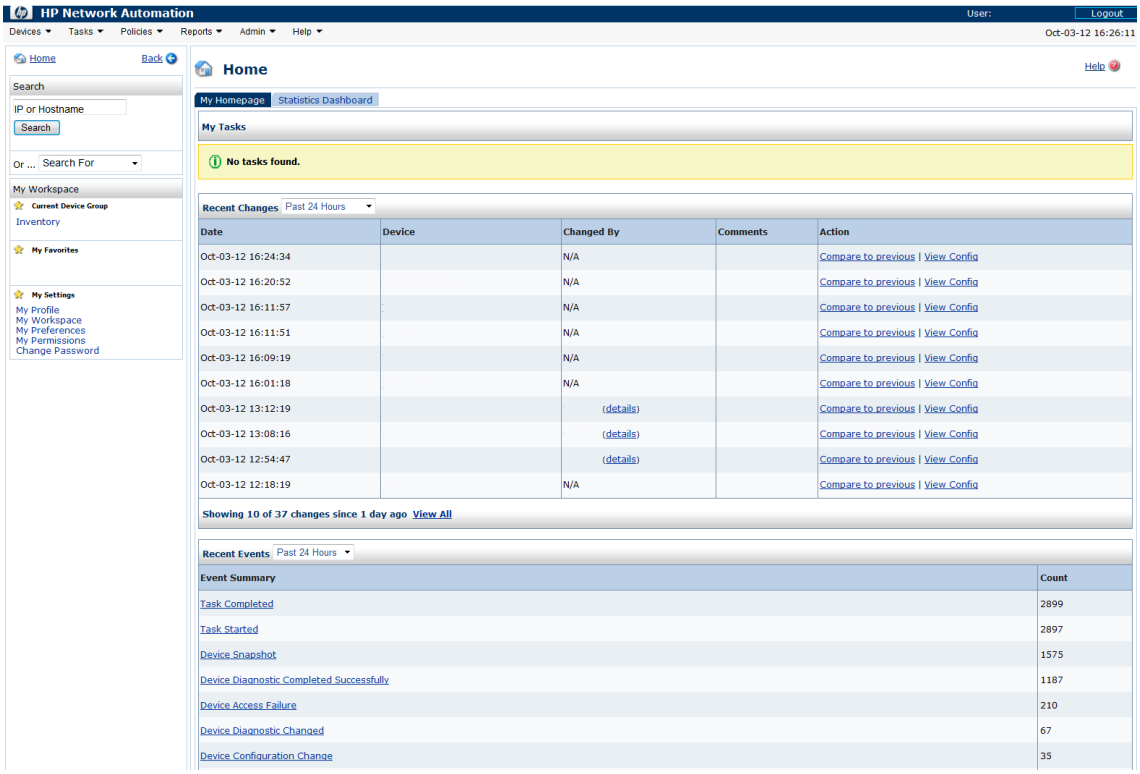

Figure 2. HP Network Automation main window.

3.1 Different core features

NA is able to auto-detect and assign correct device drivers to enable communication with the device. It takes a snapshot of the device to collect the system information and initial configuration and afterwards runs a set of core diagnostics, such as “NA Interfaces” and “NA Routing Table” to provide relevant information.

It is possible to set up a device hierarchy when adding or editing devices. As a result, when configuring a network diagram, it is possible to select which hierarchy layers to filter. E.g. to select to diagram the entire network (Inventory) and then filter on “Core” to get the Core devices – devices with a hierarchy layer set to Core. Diagramming enables gathering of topology data from network devices. The topology data, including Layer 3 IP addresses and subnets, and

Layer 2 details, spanning tree, MAC addresses and VLANs, provides a snapshot of the current state of the network. The following hierarchy layers are the default and additional ones can be added.

•Layer not yet set

•Core

•Distribution

•Access

•Edge.

Device groups

NA has the option to create device groups which allow users to organize devices into larger schemes based on their desires. Some general groups could be created based on geography/physical location or business unit/department and normal users are also able to create their own customized groups. Ideally the page of the device group includes one system group, the Inventory which contains all devices added to NA. The idea of adding hierarchy to groups helps to run tasks and reports against a set of them.

Tasks

Tasks are the primary method by which NA interacts with a network. They are specific actions which can be either scheduled or ran immediately. Task information can be checked from a specific page which provides results of performed tasks, such as snapshots to identify device and configuration changes. Some examples of tasks that could be run:

• Deploy configuration

• Run command script

• Deploy passwords

• Reboot device

•Synchronize start up and running configuration

•Update device software.

Reserving devices

With large networks, it is necessary to manage who is working with what, and at which times. The Device Reservation System enables reserving a device or a group of devices for a specific period of time and it notifies if there are conflicts. Devices affected by sub-tasks of a multi-task project are automatically reserved for the duration of the task.

Policies

It is possible to establish standards or best practices to ensure that the network meets the security, reliability and quality goals. By providing policy enforcement capability and integrated remediation, NA will automate the laborious task of validating that devices and configurations match the defined best practices, as well as the remediation steps required to bring the device back into compliance with the best practices mentioned above. Policy manager is also effective in meeting regulatory compliance requirements, such as PCI or SOX in a cost-effective and efficient manner by validating changes made to the devices and pointing out the noncompliant ones.

When running policy checks, each NA process rules and checks whether that rule applies to the device or not. The rules can be configured not to take into account certain devices based on different criteria such as model number, hostname and location. The rules can also be run as exceptions where their purpose is to exclude text they matche in the device configuration from consideration by the configuration rule it is part of. This is usually used when a greater number of devices do not comply with a rule, but the rule cannot be altered to fit all similar configurations.

3.2 Software

NA has the option to view which software is currently loaded on a device and to specify OS versions that are susceptible to security problems and then generate automatic alerts or responses when those versions are detected. Another feature assisting in software maintenance is the ability to schedule updates during custom hours. This also provides an audit trail for software upgrades to help keep up with ITIL's standards. NA also keeps up a software repository where current device images can be backuped and thus when in need of a recovery it can be handled quickly.

Connecting

NA supports single sign-on to network devices using the telnet or SSH protocol. The NA server acts as a telnet/SSH proxy. As the data transferred in telnet is in clear text format, SSH is a preferred method.

Support

Unless otherwise agreed with HP, under the HP Software Supported Versions Policy, HP will provide Support for the current and previous minor versions of the current major release and the latest minor version of the previous major release.

4 LIFE-CYCLE

A life-cycle means the whole lifetime of a device or software from when it has been created, to when it is supposed to "die" i.e. removed from production as well as the steps taken in-between of that (Figure 2). For software the life-cycle is not as essential as for hardware, since its lifetime goes hand in hand with hardware lifetime and it is already a finished product from life-cycle point of view. Software may still need updating in case a bug appears or if a need for an additional feature is found, but all of this is reactive instead of proactive and cannot be planned beforehand.

The hardware life-cycle starts at procurement, after which it will be configured for its job and then delivered to a planned location.

Figure 3. Life cycle processes (XTGLOBAL-USA 2012).

5 OSI-MODEL

The OSI-model is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a reference tool for understanding data communications between any two networked systems. It divides the communication into seven layers, starting from bottom: physical, data link, network, transport, session, presentation and application –layer. Each layer has its own functions to support the layer above it and to offer services to the layer below it. (Global Knowledge 2012.) In the content of the present thesis, the most relevant layers are the four lowest ones which focus on passing traffic through the network to an end system.

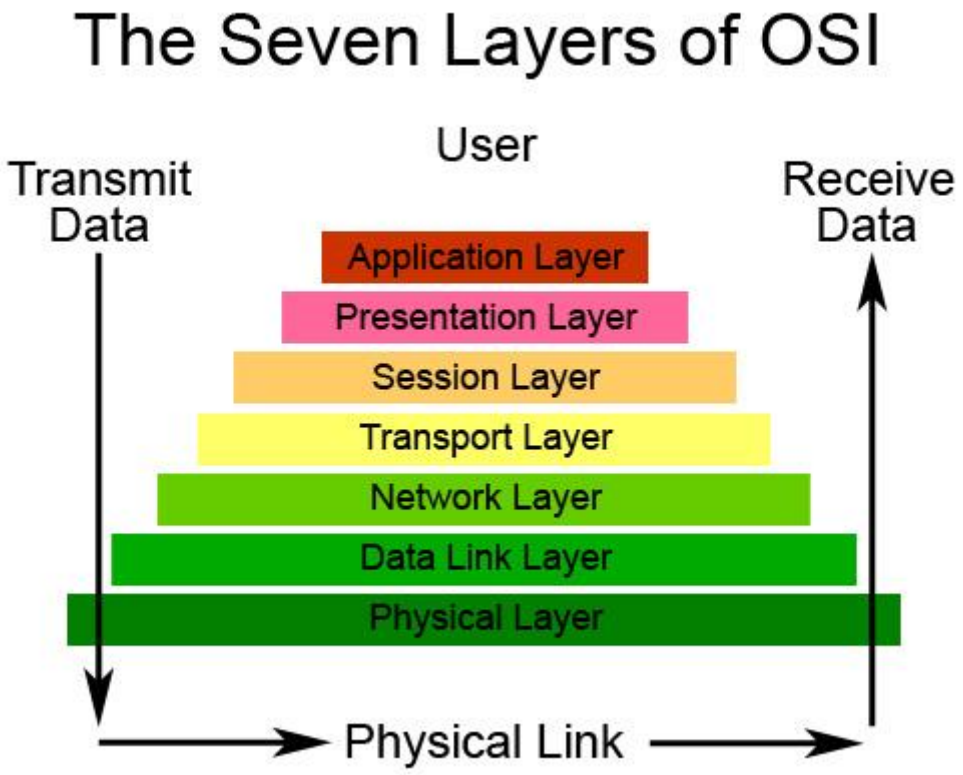

Figure 4. Different OSI-layers (WASHINGTON 2012).

Looking at the figure 4, it is clear to understand how the communication goes. As data passes through each layer, relevant information to that layer is attached

and this is called encapsulation. This is how each layer can communicate with its relevant layer at the destination. Also, since the layers are developed independently, this allows the development in each layer to progress without delays caused by the others (Sans 2012.)

5.1 Physical layer

Physical layer is the one at the bottom. This involves parts which can be seen such as cables, patch panels, jacks and optical fibers. The physical layer defines electrical and physical specifications for devices. Most notable protocols in this layer are the ones belonging to the IEEE 802 family: USB, Bluetooth, SONET, SDH, IEEE 1394 and hubs. The major functions are:

• Establishment and termination of a connection to a communications medium.

• Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.

• Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link. (ATIS 2012a.)

5.2 Data link layer

Data link layer is responsible for physical addressing, error correction and preparing the information for the media by packing raw bits from the physical layer into frames which can then be transferred from one host to another. Data link protocols handle features such as the size of the packet and that it is delivered to the correct recipient. It can also ensure that the sent data is the same as the received one. In case of an error, it will inform of it and proceed by retransmitting the data. (ATIS 2012b.)

Each device on the network has its own MAC address which is unique to the device. Common devices on this layer are switches that use MAC addresses to determine which port the packet is forwarded to.

5.3 Network layer

Network layer specifies how to get from one data-link region to another, which is called routing. The main protocol in this layer is IP, but in addition, there are other protocols such as IPX for LANs. Both of these can be used simultaneously on the same network, over the same physical-layer equipment, but they do not have to use the same data link layer protocol for framing. IP is usually framed using Ethernet II data link layer while IPX normally uses IEEE 802.2 with 802.3 Ethernet framing. It would not be possible to run an IP network using both simultaneously on the same segment, but it is quite common to configure all of the devices on the network to expect their IP frames in one format and IPX in another. (Dooley 2002, 7.)

5.4 Transport layer

Transport layer provides the end-to-end communication services for applications. It is responsible for delivering the data to the correct application. This is done by multiplexing data from different applications (forming data packets) and adding source and destination port numbers into the header of each packet.

The best known protocols used in this layer are transmission control protocol (TCP) and user datagram protocol (UDP). TCP provides reliable delivery by requesting retransmission of lost data and rearranging out-of-order data. It is utilized by www, e-mail, FTP and such where a reliable connection is needed. UDP, on the other hand, focuses on latency over reliability. It is preferred on applications such as VOIP and streaming where the loss of packets is not that serious and may only cause mild inconveniences. (Wikipedia 2012.)

6 IT INFRASTRUCTURE LIBRARY

IT Infrastructure Library or ITIL is a 20 year old and the most widely adopted framework for IT service management in the world. ITIL was created with two objectives in mind: first, to create comprehensive, consistent and coherent codes of best practice for quality IT service management promoting business effectiveness in the use of IT and second, to encourage the private sector to develop ITIL-related services and products. ITIL is vendor neutral and consists of ideas drawn from international practitioners, not academic theory about how things should be. ITIL is also non-proprietary i.e. anyone can apply its concepts freely. (ITIL 2012a.)

The most important benefit of ITIL is the alignment with business needs. It is an asset when IT can proactively recommend solutions regarding business's needs and simultaneously negotiate achievable service levels. Business and IT can work together more efficiently when they can agree on realistic service levels. The customer's expectations are also more easily met when they can be presented with consistent and predictable methods. ITIL also provides the ability to measure processes and therefore they can be better tuned for effectiveness. When predictable and consistent processes are used, they can be measured for example with an indicator such as Mean Time To Repair (MTTR) and that way the best course of action can be determined.

6.1 Process for incident and problem management

The goal for incident management is to "restore normal state IT service operations as quickly as possible to minimize the adverse impact on business operations" (ITILlibrary 2012). Managing all of this is done via the company's preferred ERP tool that logs all information regarding tickets, thus providing a way to prepare for future issues and to keep track of the SLA. While incident management aims to solve issues as soon as possible to meet the SLA, problem management deals with the root cause to provide permanent solutions.

6.2 Process for change management

Change management is a process that controls the execution of changes in a controlled manner to reduce risk and interruption. It ensures that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner. The purpose of the Change Management process is to ensure that standardized methods are used for the efficient and prompt handling of all changes and all changes are recorded in the Configuration Management System and thus the overall business risk is optimized (Cartlidge A. et al., 2007). Change management processes are often responsible for managing the change in hardware, communications equipment and software, system software, and all documentation and procedures associated with the running, support and maintenance of live systems (ITIL 2012b).

7 DIFFERENT HARDWARE

The networking devices discusses in the present thesis are switches, firewalls and load balancers. Routers used to be one of the most common networking devices, but as switches are capable of performing at layer 3, there are no dedicated routers used in the environment where the maintenance process is conducted at. All of the devices have subcategories such as outdoor or DMZ firewall which is necessary as this can dictate their use to a great extent. The wide difference it makes on the role of the device depending on how and when the device should be managed and which hardware is to be used. Certain devices such as DMZ firewalls also handle routing, which requires more performance from them, therefore requiring more efficient hardware.

Another major difference is the impact these devices have on the network. They all have an assigned impact value depending on their location and role on the network and this affects how they are dealt with should a problem arise. It also helps to visualize the scope of a problem and helps to locate all the affected systems, such as core switch affecting the whole network and a single blade switch having only a minor impact.

The impact is greatly reduced by the fact that most of the hardware is redundant which means that if one experiences an error, it does not affect the whole network as there is another one to perform the same job. Still, even a small spike on the DWDM can cause issues such as spanning tree to re-calculate and this in turn manifests as downtime on the network and may even require some devices to be rebooted to restore normal functionality to them.

The different impact levels used are:

1. Extensive / widespread

2. Significant / large

3. Moderate / limited

4. Minor / localized.

The impact levels depend on what is affected, whether it is network, service, customer system, servers or something else and the amount of users that are affected. From the most common to the rarest impact level used are three, two, one then four which gives a good idea about the scope of things.

7.1 Switch

A switch is a networking device that connects network segments or network devices. Normally it is a multi-port network bridge which processes and routes data on layer two, but switches that also work on layer three are becoming more and more common. When a switch receives a message it only sends it to the recipients it was meant for, unlike a hub which transmits the message to everyone else on its network. If traffic copying to multiple network sensors is required, switches are able to do that with port mirroring.

Layer two switches have four ways for forwarding traffic: Store and forward, cut through, fragment free and adaptive switching and at layer three, a switch differs very little from a router. It is able to support same routing protocols as network routers and both of them inspect incoming packets and make dynamic routing decisions based on the source and destination addresses. Switches normally cost less and do not possess the WAN ports and WAN features normally present in traditional routers. At layer four, switches are capable of NAT and load distribution. It may include a stateful firewall, a VPN concentrator or be an IPSec security gateway.

In this study the switches are grouped into different categories depending on their role and location on the network.

- Core switch
- Access switch
- Blade switch

• Intra/aggregation switch

• DMZ switch

• Internet switch.

All of this affects the impact switches have on the network and that in turn affects the maintenance plan required for them. In a best practice scenario, all of the switches are redundant, which reduces the impact greatly but nevertheless, the failure of a LAN switch is rather significant.

7.2 Firewall

Firewalls can be software or hardware based, and either stateless – making simple decisions, requiring less memory and working faster – or stateful, in which the firewall maintains content about active sessions and uses that information to hasten things up. Firewalls normally work on layers three and four but they can also work on application layer, though it is more uncommon. At layer three, a firewall can determine if a packet is from a trusted source but doesn't concern with its contents or what other packets are associated with it. At transport layer the firewall has a little more information about the packet and is able to grant or deny access depending on more sophisticated criteria and at the application level, the firewall has plenty of information and can be extremely selective in granting access. (Vicomsoft 2012). Firewalls also appear at different jobs, from packet filters to application level gateways to routing.

7.3 Router

Routers are not relevant in the context of this thesis due to the fact that Tieto mainly usies layer three switches and firewalls for routing purposes. There are, however, a couple of routers in the field, but they are not dedicated for the environment the thesis focuses on.

Routers can include switching modules and thus the line between a router and a switch is really thin. As a layer three switch is able to route, it could arguably be called a router as well.

7.4 Load balancer

A Load balancer is based on the concept that the load is sent to the most appropriate server. The distinction between a physical server and application services running on it, allows a load balancer to individually interact with the applications rather than the underlying hardware. This allows load balancing based on the service instead of host, making it more effective.

A normal load balancing transaction is as follows (Figure 5):

1. The client attempts to connect with the service on the load balancer.

2. The load balancer accepts the connection and after deciding which host should receive the connection, changes the destination IP (and possibly port) to match the service of the selected host (note that the source IP of the client is not touched).

3. The host accepts the connection and responds back to the original source, the client, via its default route, the load balancer.

4. The load balancer intercepts the return packet from the host and now changes the source IP (and possible port) to match the virtual server IP and port, and forwards the packet back to the client.

5. The client receives the return packet, believing that it came from the virtual server and continues the process. (F5 2012.)

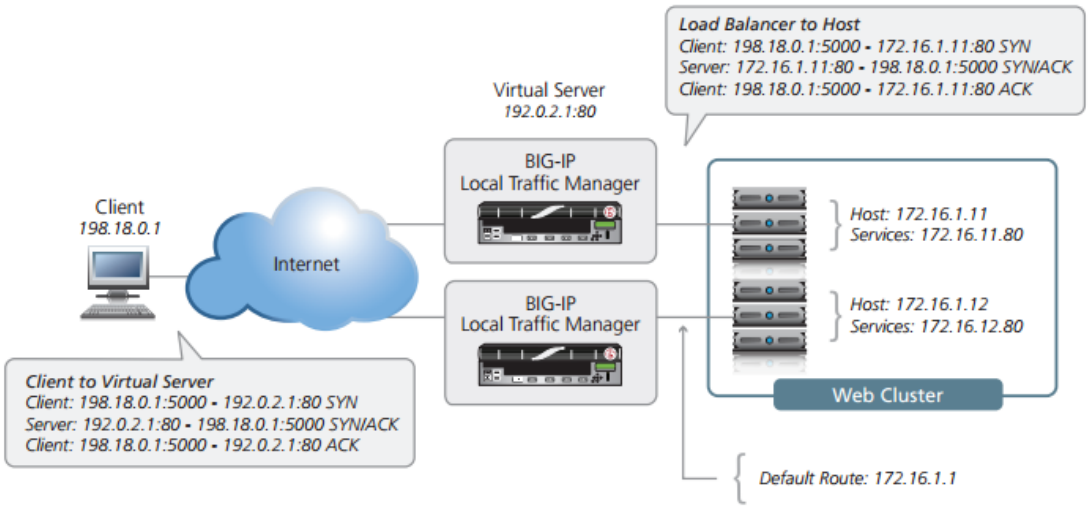

Figure 5. Load balancing.

7.5 DWDM

Dense wavelength division multiplexing is an extension of WDM; basically it is a form of frequency division multiplexing. It multiplexes multiple optical signals on a single optical fiber by using different wavelengths (colors). Multiplexing means sending multiple signals or streams of information through a circuit simultaneously, to form a single complex signal and then recovering the signals at the end point.

DWDM consists of different main components which are:

• **Terminal multiplexer.** Contains one wavelength converting transponder for each wavelength signal it will carry. It receives the signal, converts it to electrical domain and retransmits it.

• **Intermediate line repeater.** Placed every 80-100 km to amplify signal.

• **Intermediate optical terminal.** Remote amplification site for signal that may have traversed up to 140 km or more.

• **DWDM terminal demultiplexer.** Breaks multi-wavelength signal back to individual signals and outputs them on separate fibers.

8 DOCUMENTATION DURING THE PROCESS

A document is something that contains information which serves as a proof or evidence. It can range from pictures to writing or even a coin which is bearing a revealing mark or symbol.

In networking, documentation is used to cut short the time it takes to plan and troubleshoot networks. Some still do not consider documentation as an important part of projects and would rather avoid spending money on it. However, this might back-fire when something goes wrong and the lack of documentation delays fixing the issue. Even an hour added to networks downtime can be extremely costly for a business.

Building a document is usually divided into seven phases:

- Preliminary study
- Defining
- Planning
- Execution
- Testing
- Deployment
- Maintenance.

Most of the phases are not done in an order since it is common to work on many of them at the same time, so their completion does not depend on the others. It is generally easier to do documentation while planning as the details are still freshly in the memory.

Work and configuration instructions

NA was a rather new tool for Tieto, which had only very few people using it and in really small quantities. Nevertheless, there was plenty of information available regarding its use, especially a user manual and lab work to practice its use. Gathering and learning this information was a part of my job in order to be able to complete the maintenance process. NA comes with a GUI so it was not too

hard to use, but it does still provide wide access to a network so its credentials have to be limited regarding different needs; mine being only rights to view the networking components and a couple of other options such as mapping a topology for certain datacenters.

In order to add the devices, we had to do it via specific technicians as I was unable to use my credentials for it, but I still supplied the required knowledge to complete the process and also compiled all the information into a short manual for how to add a device and set up the monitoring.

9 IMPLEMENTATION PROCESS

The thesis began by being presented with a task of improving the maintenance process of a client of Tieto, and I was told that the tool to assist this process was going to be HP Network Automation. I started the development by searching for and studying all the possible information about the network, which was to be maintained. That included different Visio diagrams, excel files containing device's information and plenty of other documentation about the network's infrastructure. I also had two reviews which were made by Cisco that consisted of a wide research into two of Tieto's network cores and reviewed everything from configuration to the support required by the device. This also acted as a basis as to why I was presented with this task of improving the overall pre-emptive maintenance, as there was lack of it and I was also asked to make it as applicable to other networks as possible.

After the preliminary studying of the material, I decided the next logical step would be to gather the necessary information into one place, in this case that was an excel file. This included names and addresses for the devices as well as the hardware they consisted of. As I lacked some knowledge about the area, the parameters were not finalized right away and actually changed around a lot. I ended up adding the devices' MTBF and impact values due to their relevancy for setting up the health check cycle. The list contained other parameters as well, but they were later removed because I found them irrelevant and wanted to stay in the defined subject without venturing too far away.

When the necessary basis for gathering the information was complete, the next part was filling up the whole table. Some of it was easy to acquire, such as implementation dates for the devices, as they had been updated not long time ago and were all found in a single excel file, but others were harder to come by due to the inaccuracy of the information that a couple of different sources had. The inaccurate information generally presented itself in SIP's infrastructure section, and this was due to lack of maintenance and also in OMT's CI tables, where the problem was similar. I took a step towards that problem and fixed the

ones that presented themselves by making an incident ticket about the wrong information and sending it to a correct source. I also had to interview the respective specialists for each of the device categories to confirm the accuracy of the information. The last source for information was the vendors who provided me with the MTBF values based on the hardware type of the device, which had to be the exact models used. I also received information about the end of support/life dates which confused me at the beginning, as I was not very experienced with the different hardware models.

9.1 Applying the information

With all the relevant information gathered up, I had to apply it for creating a maintenance schedule for different devices. The feasibility of applying an update, its impact, MTBF and type of the device defined how often it would be a good and practical time to check for a new update. Where switches hardly ever require new updates, firewalls and load balancers are a different case and have their schedule set for more frequent checking, in this case twice as often. Simultaneously while planning the process, I took some steps to upload the devices into NA. In order to do that, firewalls had to be opened between NA and the devices which were to be added. It required telnet, SSH and SNMP connections open from NA to the device and TFTP, FTP, SCP and syslog open from the device to NA. Also the user had to have an HTTPS connection opened from his/her VPN's IP-address to NA to be able to access it, unless he/she preferred to use one of Tieto's jump-servers. Also the hostname of the device, address and SNMP community had to be known, plus whether it belonged to AAA or not.

Since one of the things NA monitored was software's life-cycle, I decided to go one step further and create some standardization to a change plan that would hasten the process of conducting a software update -change. At this point I did not have much personal experience apart from having observed a couple of them being processed, so it brought some additional work to the thesis. Fortunately, I was able to contact one of the problem managers of Tieto, who was proficient in the change process and she provided valuable help in this. Later after having made a change plan for another project myself, I came back to this and made some further changes, which proved to be a lot easier with some practical experience on the issue. The changes were minor but the whole change management process was so delicate that even a minor issue could get it delayed or rejected. I also noticed that standardizing the software update would not be feasible as it is significantly more extensive process than I had earlier anticipated.

9.2 Looking back at the application of information

If I were to carry out this process again, with the knowledge I have now gained, I would do a couple of things differently. This is because the process got delayed due to different issues, such as problems in ordering the credentials and an error in a firewall management software, that prevented making changes to it. In addition the holiday season was problematic and delayed the later parts of the project rather significantly because of the inability to contact the required specialists.

The first thing I would have done differently would be to order the credentials right away, for every necessary person. After that, I would order the required firewall openings in order to be able to add the devices. The reason I would do this is that I had first researched all the content that required those steps, and when that was ready, I ordered the credentials and openings and now had to wait for them while the next step was already complete. Of course I had planned other activities to take place during the time, but the delay was longer than expected. I would say this problem resulted from the fact that I did not have enough prior experience in these kinds of projects and therefore could not estimate the effort different specialists needed to do in order to get these done, which resulted in an inability to estimate the time needed.

The biggest risks I would say emerged from the delays caused by multiple vacations during the summer which delayed adding the devices to HPNA. Alone this would not have been so critical, but combined with the fact that the most critical specialists for this project had to dedicate most of their time working in an urgent project for the same customer made it worse. Another issue that I faced was a critical person having an error with a tool that creates credential requests for NA. As this tool was malfunctioning, a technician was unable to get his credentials for a long time, again making us unable to enable the devices. We were also facing problems with DMZ-firewall management software going

haywire, preventing us from adding new rules to it, but as my vacation coincided with this the issue caused only a minor delay.

9.3 The final results

Once the process was to be completed, it was to provide Tieto with increased pre-emptive monitoring, as well as a backup network for the device images, which was previously lacking. Another important part was having the hardware and software lifetime and MTBF known, and thus the future provisions and costs regarding them were easier to prepare for. All this added together, will significantly enhance the stability of these devices and minimize the risks caused by general life-cycle management (or the lack of it). It should cut downtime shorter in the long run and allow the maintenance to be more proactive than reactive.

REFERENCES

ATIS 2012a. Referenced 15.6.2012 http://www.atis.org/glossary/default.aspx.

ATIS 2012b. Referenced 15.6.2012 http://www.atis.org/glossary/definition.aspx?id=6928.

Brooks, F. P. Jr. 1987. “No Silver Bullet”, IEEE Computer, 20(4):10-19.

Cartlidge, A. et al. 2007.

Cisco 2012. Referenced 12.6.2012 http://ciscodocuments.blogspot.fi/2011/05/chapter-01-planning-maintenance-for.html.

Dooley, Kevin, 2002. Designing Large-Scale LANs. O’Reilly & Associates.

F5 2012. Load Balancing 101: Nuts and Bolts. Referenced 10.8.2012 http://www.f5.com/pdf/white-papers/load-balancing101-wp.pdf.

Flextronics 2012a. Referenced 6.7.2012 http://marco.uminho.pt/~dias/MIECOM/GR/Projs/P2/fcaps-wp.pdf.

Global Knowledge 2012. The OSI Model. Referenced 17.6.2012 http://www.globalknowledge.com/training/whitepaperdetail.asp?pageid=502&wpid=171&country=United+States.

HP 2009. Network Automation 7.5 Essentials Student Guide. Manual.

IBM 2012. Referenced 1.7.2012 http://www.ibm.com/solutions/cisco/us/en/solution/A256086H65566Z83.html.

IEEE standard 1219-1998. Maintenance. Referenced 15.6.2012 http://homes.ieu.edu.tr/~kkurtel/Documents/IEEE%20Std%201219-1998%20Software%20Maintenance.pdf.

ITIL 2012a. The Basics. Referenced 15.7.2012 http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf.

ITIL 2012b. Official site. Referenced 3.6.2012 http://www.itil-officialsite.com/

Itillibrary 2012. ITIL Incident Management Referenced 17.9.2012 http://www.itlibrary.org/index.php?page=Incident_Management.

Quocirca 2012. 8 step ITLM.

Sans 2012. SANS Institute InfoSec Reading Room. Referenced 10.7.2012 http://www.sans.org/reading_room/whitepapers/protocols/understanding-security-osi-model_377.

Tieto 2012. About us. Referenced 7.6.2012 http://www.tieto.com/about-us.

Vicomsoft 2012. Firewalls. Referenced 18.8.2012 http://www.vicomsoft.com/learning-center/firewalls.

Washington 2012. Teaching and Learning Tools. Referenced 19.11.2012 http://www.washington.edu/lst/help/computing_fundamentals/networking/osi.

Transport layer 2012, wikipedia. Referenced 10.10.2012 http://en.wikipedia.org/wiki/Transport_layer

XTGLOBAL 2012. IBM's optimized datacenter process. Referenced 19.11.2012 http://xtglobal-usa.com/site/wp-content/uploads/2011/02/AssetLifecycle11.jpg