

# MAD-Network Monitoring

## Diplomarbeit 2014/15

Porcic Alin, Ranalter Daniel, Singh Manpreet

Betreuer: Dr. Michael Weiss

Höhere Technische Bundes Lehr- und Versuchsanstalt Anichstraße  
Abteilung Höhere Elektronik und Technische Informatik  
5bHEL

30. Januar 2015

# Inhaltsverzeichnis

<b>1</b>	<b>Abstract</b>	<b>3</b>
<b>2</b>	<b>Einleitung</b>	<b>4</b>
2.1	Aufgabenstellung . . . . .	4
2.2	Aufteilung . . . . .	4
<b>3</b>	<b>Theorie zu den einzelnen Gebieten der Arbeit</b>	<b>5</b>
3.1	Informatik von Stojanovic Marko . . . . .	5
3.1.1	Programmiersprachen . . . . .	5
3.1.2	Multithreading . . . . .	5
3.2	Protokolle und Netzwerkgrundlagen von Ranalter Daniel . . . . .	6
3.2.1	Grundlagen . . . . .	6
3.2.2	Protokolle . . . . .	7
3.2.3	Netzwerksicherheit . . . . .	8
3.3	E-Mail von Singh Manpreet . . . . .	8
3.3.1	Allgemein E-Mail und Notification . . . . .	8
3.3.2	E-Mail . . . . .	8
3.4	Oberfläche . . . . .	9
3.4.1	Allgemein User Interface (UI) von Manpreet Singh . . . . .	9
3.4.2	Grahpical User Interface (GUI) von Manpreet Singh . . . . .	9
3.4.3	Command Line Interface (CLI) von Alin Porcic . . . . .	10
3.5	Datenbank von Stojanovic Marko . . . . .	10
3.5.1	Allgemeines . . . . .	11
3.5.2	Datenbanksysteme . . . . .	11
3.5.3	Relationales Datenbankmanagementsystem (RDBMS) . . . . .	11
3.5.4	Zugriffe . . . . .	12
3.5.5	Sprachen . . . . .	12
3.5.6	SQLite . . . . .	12
3.6	Kryptologie von Porcic Alin . . . . .	13
3.6.1	Allgemeines . . . . .	13
3.6.2	Kryprographie . . . . .	14
3.6.3	Kryptoanalyse . . . . .	14
3.6.4	Verschlüsselungsverfahren . . . . .	15
<b>4</b>	<b>Möglichkeiten der Realisierung Allgemein von Ranalter Daniel</b>	<b>17</b>

<b>5</b>	<b>Programmrealisierung</b>	<b>18</b>
5.1	JobSystem von Porcic Alin und Ranalter Daniel . . . . .	18
5.2	Notification von Singh Manpreet . . . . .	18
5.3	Database von Stojanovic Marko . . . . .	18
5.3.1	MAD-DB . . . . .	18
5.3.2	Programmcode . . . . .	18
5.4	Logging von Ranalter Daniel . . . . .	18
<b>6</b>	<b>User Manual von Procic Alin</b>	<b>19</b>
<b>7</b>	<b>Quellenverzeichnis</b>	<b>20</b>

# Kapitel 1

## Abstract

lorem ipsum

# Kapitel 2

## Einleitung

lorem ipsum

### 2.1 Aufgabenstellung

lorem ipsum

### 2.2 Aufteilung

lorem ipsum

# Kapitel 3

## Theorie zu den einzelnen Gebieten der Arbeit

lorem ipsum

### 3.1 Informatik von Stojanovic Marko

lorem ipsum

#### 3.1.1 Programmiersprachen

lorem ipsum

**Was ist eine Programmiersprache?**

lorem ipsum

**C#**

lorem ipsum

**Wie funktioniert C#** lorem ipsum

**Vor- und Nachteile** lorem ipsum

#### 3.1.2 Multithreading

lorem ipsum

**Was ist ein Thread**

lorem ipsum

**Konzept von Multithreading**

lorem ipsum

**Wie funktioniert Multithreading** lorem ipsum

**Hardware** lorem ipsum

**Software** lorem ipsum

**Arten von Multithreading** lorem ipsum

**Vor- und Nachteile**

## **3.2 Protokolle und Netzwerkgrundlagen von Rainer Daniel**

Diese Abhandlung wird die Netzwerkgrundlagen welche auf das „Ethernet“-Protokoll aufsetzen besprochen. Es gibt noch diverse andere, wie zum Beispiel „Token Ring“, auf welche hier im folgenden jedoch nicht näher eingegangen wird, da, abgesehen davon, dass Ethernet auch bei der praktischen Durchführung verwendet wurde, Ethernet das am häufigsten genutzte Layer 1 Protokoll darstellt.

### **3.2.1 Grundlagen**

In der Netzwerktechnik gibt es mehrere verschiedene grundlegende Konzepte auf welche hier eingegangen werden soll.

#### **Der Host**

Mit dem Term „Host“, wird, in dem Zusammenhang der Netzwerktechnik, ein Gerät beschrieben, welches über das Netzwerk mit anderen Hosts verbunden ist und theoretisch in der Lage ist an der Kommunikation teilzunehmen. Damit ein Host zur Kommunikation in der Lage ist, benötigt er mehrere Dinge.

Zu diesen gehört Hardware technisch gesehen, mindestens eine Netzwerkkarte mit einer Art von Möglichkeit sich in das Netz einzuklinken. Diese Möglichkeit kann aus einem Ethernet Anschluss oder einer Antenne, welche in der Lage ist, das 2,4 GHz Band und/oder das 5GHz Band zu empfangen und in diesem Band zu senden.

Auf der Softwareseite benötigt ein Host im Grunde drei Dinge welche ihn dazu ermöglichen eine Konversation mit einem anderen Host zu führen.

**MAC-Adressen** lorem ipsum

**IP-Adressen** lorem ipsum

**Ports** lorem ipsum

**Schichtenmodel**

lorem ipsum

**OSI** lorem ipsum

**TCP/IP** lorem ipsum

**Beispiel für Kommunikationsablauf**

lorem ipsum

**Client-Server Verhältnis**

lorem ipsum

### **3.2.2 Protokolle**

lorem ipsum

**Ethernet**

lorem ipsum

**Address Resolution Protocol - ARP**

lorem ipsum

**Sicherheitsaspekte** lorem ipsum

**Internet Protocol - IP**

lorem ipsum

**IPv4** lorem ipsum

**IPv6**

**User Datagram Protocol - UDP**

lorem ipsum

**Transmission Control Protocol - TCP**

lorem ipsum

**Dynamic Host Configuration Protocol - DHCP**

lorem ipsum

**Domain Name System - DNS**

lorem ipsum



**Internet Control Message Protocol - ICMP**

lorem ipsum

**ICMP Echo Request/Response - Ping** lorem ipsum

**File Transport Protocol - FTP**

lorem ipsum

**Simple Network Managing Prorocol - SNMP**

lorem ipsum

**Management Information Base** lorem ipsum

**SNMPv2/SNMPv2c** lorem ipsum

**SNMPv3** lorem ispum

**Hypertext Transfer Protcol - HTTP**

lorem ipsum

**3.2.3 Netzwerksicherheit**

lorem ipsum

**3.3 E-Mail von Singh Manpreet**

lorem ipsum

**3.3.1 Allgemein E-Mail und Notification**

lorem ipsum

**Senden**

lorem ipsum

**Graphische Erklärung** lorem ipsum

**Empfangen**

lorem ipsum

**IMAP** lorem ipsum

**POP** lorem ipsum

### **3.3.2 E-Mail**

lorem ipsum

#### **Ursprung/Entstehung**

lorem ipsum

#### **Bedeutung heute**

lorem ipsum

#### **Zukünftig** lorem ipsum

#### **Probleme**

lorem ipsum

#### **Kleine Probleme** lorem ipsum

#### **Große Probleme - Gefahren** lorem ipsum

#### **Sicherheit**

lorem ipsum

#### **Versuche** lorem ipsum

#### **Was kann ich tun?** lorem ipsum

## **3.4 Oberfläche**

lorem ipsum

### **3.4.1 Allgemein User Interface (UI) von Manpreet Singh**

lorem ipsum

#### **Geschichte**

lorem ipsum

#### **UIs**

lorem ipsum

#### **Zukünftig**

lorem ipsum

### 3.4.2 Graphical User Interface (GUI) von Manpreet Singh

lorem ipsum

#### **Bedeutung**

lorem ipsum

#### **Wichtigkeit**

lorem ipsum

**Marktführende** lorem ipsum

**Wichtige Operating System GUIs** lorem ipsum

#### **Vor- und Nachteile**

lorem ipsum

#### **Möglichkeiten der Realisierung**

lorem ipsum

#### **Genauer**

lorem ipsum

**Realisierung** lorem ipsum

**Graphikkarte oder Prozessor** lorem ipsum

### 3.4.3 Command Line Interface (CLI) von Alin Porcic

lorem ipsum

#### **Allgemeines**

CLI steht für 'Command Line Interface' (text-basierende Schnittstelle) und darunter versteht man Schnittstellen, die die Eingabe eines Nutzers in Form von Text interpretiert und diese dann ausführt.

#### **Geschichte**

Speziell bei unix-ähnlichen Betriebssystemen, aber auch bei vielen anderen Systemen, sind text-basierende Schnittstellen in unterschiedlichster Form implementiert.

#### **Vor- und Nachteile**

lorem ipsum

## **3.5 Datenbank von Stojanovic Marko**

lorem ipsum

### **3.5.1 Allgemeines**

lorem ipsum

#### **Geschichte**

lorem ipsum

#### **Definitionen**

lorem ipsum

#### **Effizienz**

lorem ipsum

#### **Funktionen**

lorem ipsum

#### **Anwendungen**

lorem ipsum

### **3.5.2 Datenbanksysteme**

lorem ipsum

#### **Datenbankmanagementsysteme**

lorem ipsum

#### **Datenbank**

lorem ipsum

### **3.5.3 Relationales Datenbankmanagementsystem (RDBMS)**

lorem ipsum

#### **Prinzip eines RDBMS**

lorem ipsum

#### **Tabellen**

lorem ipsum

## **Alternative Datenbankmanagementsysteme**

lorem ipsum

**Information Management System** lorem ipsum

**Netzwerkdatenbankmodell** lorem ipsum

**Hierarchisches Datenbankmodell** lorem ipsum

### **3.5.4 Zugriffe**

lorem ipsum

#### **Zugriffsmöglichkeiten**

lorem ipsum

#### **Sicherheit**

lorem ipsum

#### **Gleichzeitige Zugriffe**

lorem ipsum

### **3.5.5 Sprachen**

lorem ipsum

#### **Verwaltungsgetrennte Sprachen**

lorem ipsum

**Abfragen und Manipulieren der Daten** lorem ipsum

**Datenbankstruktur** lorem ipsum

**Berechtigungen** lorem ipsum

#### **SQL**

lorem ipsum

### **3.5.6 SQLite**

lorem ipsum

**Geschichte**

lorem ipsum

**Eigenschaften**

lorem ipsum

**Datentypen**

lorem ipsum

**Syntax**

lorem ipsum

**Befehle**

lorem ipsum

**Vor- und Nachteile**

lorem ipsum

**Vorteile** lorem ipsum

**Nachteile** lorem ipsum

## 3.6 Kryptologie von Porcic Alin

### 3.6.1 Allgemeines

Die Kryptologie, eine sehr alte Kunst, die sich mit der Verbergung von Information befasst, hat in der heutigen modernen Zeit einen sehr wichtigen Stellenwert eingenommen und ist nicht mehr wegzudenken. Unzählige Informationen werden weltweit kreuz und quer ausgetauscht und dabei kommt es öfter vor, dass die zu übertragenden Informationen einen bestimmten Wert haben können. Der Wert dieser Informationen geht dann verloren, wenn ein Unbefugter den Sinn bzw. die Aussage dieser Informationen verstehen kann. Damit das nicht passiert, werden kryptographische Systeme entwickelt, um die Lesbarkeit von Informationen zu verhindern bzw. zu erschweren.

Kein kryptographisches System ist perfekt - die Rechenleistung der Computer steigt stetig weiter an und daher verlieren Systemen über die Zeit an Sicherheit. Daher werden immer neue kryptographische Systeme gebraucht, die den Anforderungen des heutigen modernen Zeitalters gerecht werden.

Es kommt öfter vor, dass die Kryptologie mit der Steganographie gleichgesetzt wird. Jedoch ist die Steganographie die Kunst Informationenim Trägermedium selber zu verstecken. Anders wie in der Kryptologie, wendet die Steganographie keine mathematische Verfahren an, um die Informationen zu verstecken, sondern verstecken die Informationen

im Träger selbst (z.B. Grashalbe im Bild).

Die Kryptologie reicht weit in die Vergangenheit der Menschheit zurück - schon seit 2500 Jahren sind Methoden bekannt, die die Lesbarkeit von Informationen erschwert. In Sparta zum Beispiel hat die Regierung ein Pergament Band um einen Zylinder spiralförmig aufgespannt und die zu ermittelnde Nachricht über die verschiedenen Ringe der Pergaments geschrieben. Die Entschlüsselung gelang nur dann, wenn man einen Zylinder mit dem gleichem Durchmesser besaß.

Caesar, als Beispiel, verwendete einen sogenannten Verschiebechiffre. Er verschob die Buchstaben des Alphabets um drei Zeichen. Nur die Personen, die Lesen konnten und wussten wie oft die Buchstaben verschoben werden mussten, konnten den Sinn hinter dem verschlüsseltem Text interpretieren.

Auch im Zweiten Weltkrieg war die Verschlüsselung das A und O. Der Funkt war zu dieser Zeit ein sehr wichtiges Übertragungsmedium und jeder konnte alles mithören. Daher benötigte man starke Systeme, um die Vertraulichkeit der Kommunikation zu bewerkstelligen. Die Alliierten konnten den Enigma-Code der Deutschen knacken und gewannen den Krieg.

Heute verlassen sich Milliarden Menschen auf kryptographische Verfahren, ohne es zu wissen. Das einfache Surfen im Internet, das Absenden einer E-Mail, das Herunterladen von Dateien oder die Abspeicherung von Passwörtern erfolgen alle unter komplizierten kryptographischen Verfahren.

### **3.6.2 Kryptographie**

lorem ipsum

#### **Geschichte der Kryptographie**

lorem ipsum

**Klassische Kryptographie** lorem ipsum

**Moderne Kryptographie** lorem ipsum

#### **Ziele der Kryptographie**

lorem ipsum

#### **Methoden**

lorem ipsum

### **3.6.3 Kryptoanalyse**

lorem ipsum

## **Geschichte der Kryptoanalyse**

lorem ipsum

## **Ziele der Kryptoanalyse**

lorem ipsum

## **Methoden**

lorem ipsum

### **3.6.4 Verschlüsselungsverfahren**

lorem ipsum

#### **Symmetrische Verschlüsselungsverfahren**

lorem ipsum

**Merkmale** lorem ipsum

**Nennenswerte symmetrische Verschlüsselungssysteme** lorem ipsum

**DES** lorem ipsum

**3DES** lorem ipsum

**IDEA** lorem ipsum

**CAST** lorem ipsum

**RC4** lorem ipsum

**RC5, RC5a, RC6** lorem ipsum

**A5** lorem ipsum

**Blowfish** lorem ipsum

**Twofish** lorem ipsum

**AES** lorem ipsum

#### **Asymmetrische Verschlüsselungsverfahren**

lorem ipsum



**Merkmale** lorem ipsum

**Digitale Signatur** lorem ipsum

**Zertifikate** lorem ipsum

**Nennenswerte asymmetrische Verschlüsselungssysteme** lorem ipsum

**Diffie-Hellman** lorem ipsum

**RSA** lorem ipsum

**ElGamal** lorem ipsum

**Hybride Verschlüsselungsverfahren**

lorem ipsum

**Merkmale** lorem ipsum

**Nennenswerte hybride Verschlüsselungssysteme** lorem ipsum

**IPsec** lorem ipsum

**TLS/SSL** lorem ipsum

**PGP** lorem ipsum

**Hash-Verfahren**

lorem ipsum

**Merkmale** lorem ipsum

**Nennenswerte Hashsysteme** lorem ipsum

**MD2, MD4, MD5** lorem ipsum

**SHA** lorem ipsum

**RIPEMD** lorem ipsum

# Kapitel 4

## Möglichkeiten der Realisierung Allgemein von Ranalter Daniel

lorem ipsum

# Kapitel 5

## Programmrealisierung

lorem ipsum

### 5.1 JobSystem von Porcic Alin und Ranalter Daniel

lorem ipsum

### 5.2 Notification von Singh Manpreet

lorem ipsum

### 5.3 Database von Stojanovic Marko

#### 5.3.1 MAD-DB

lorem ipsum

#### Erklärung

lorem ipsum

#### Grafische Übersicht

lorem ipsum

#### 5.3.2 Programmcode

lorem ipsum

### 5.4 Logging von Ranalter Daniel

lorem ipsum

# Kapitel 6

## User Manual von Procic Alin

lorem ipsum

# Kapitel 7

## Quellenverzeichnis

lorem ipsum