RUHR-UNIVERSITÄT BOCHUM

RUB

Betrieb großer Infrastrukturen ein Praxisbericht

Andreas Jobs – RUB-NOC

heise Netze Tour 2014 – Netzwerk im Griff

Überblick

- Die Ruhr-Universität Bochum
- Verwaltung
- Monitoring

Überblick

Die Ruhr-Universität Bochum

- ca. 42.500 Studierende
- ca. 5.600 Mitarbeiter/Mitarbeiterinnen

- 4,5 km^2 Campusfläche
- 350.000 m^2 Hauptnutzfläche der Gebäude

Überblick

Luftaufnahme RUB 2014 Tuxyso / Wikimedia Commons / CC-BY-SA-3.0

Überblick

Network Operation Center der RUB

- Abteilung vom Dezernat 5.I
  – Gebäudemanagement und -betrieb
- 7 Personen
- Hauptaufgaben: Netzwerk- und E-Mail-Infrastruktur

Überblick

Netzwerk

- ca. 86.200 Switchports (davon ca. 73.300 Netzwerkanschlüsse)
- 1.760 Netzwerkkomponenten (davon 479 Accesspoints)
- 520 Standorte in 88 Gebäuden

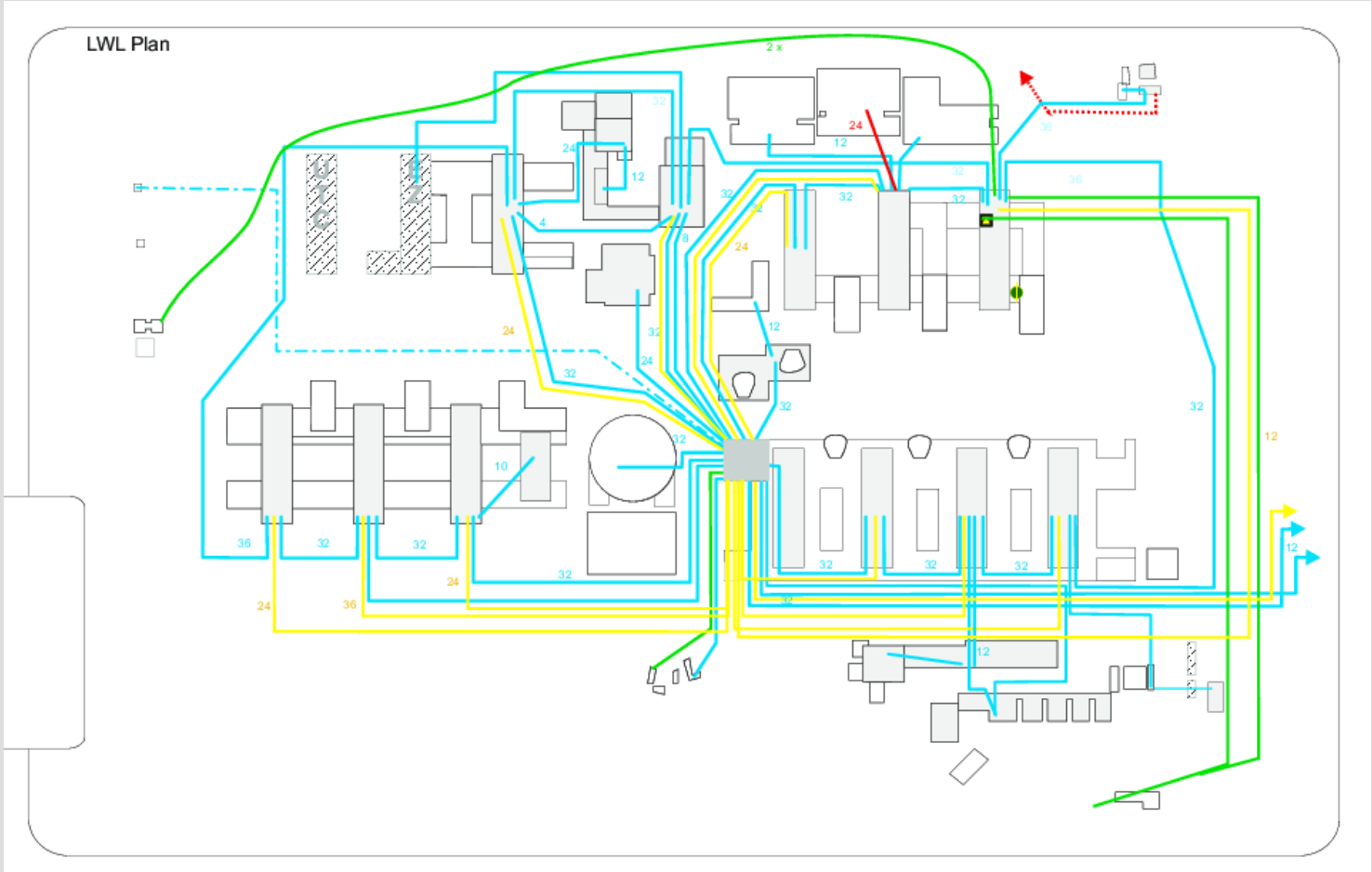
E-Mail

- ca. 103.250 E-Mail-Konten
- ca. 144TB Speicherplatz

Überblick

- Versorgungskanal unterhalb der RUB für Strom-, Gas- und Wasserversorgung
- Alle größeren Gebäude sternförmig vernetzt
- Glasfaserverbindungen auch zu den Nachbargebäuden

Überblick



Schematische Darstellung der Backbone-Verbindungen

Überblick

- 1-2 Gebäudeverteiler pro (Hoch-)Gebäude
- 2-4 Etagenverteiler pro Etage
- Kupferleitungen zu den Datenenddosen

Überblick

Anbindung diverser Außenliegenschaften:

- Glasfaserleitungen eines lokalen ISP
- Ethernet- bzw. DSL-Mietleitungen

Anbindungsgeschwindigkeiten variieren zwischen 16MBit/s (DSL) und 10GBit/s (Darkfiber)

Überblick

Internetanbindung

- 10GBit/s via DFN
- 2x1GBit/s via TMR
- eigene AS-Nummer
- LIR

zusätzlicher „Ruhr-Backbone"

- Darkfiber-Verbindungen zwischen BOC, DOR, DUE
- je 1x10GBit/s produktiv
- je 2x1GBit/s reserve

Entwicklung – Netz

Start der flächendeckenden Vernetzung im Jahr 2000

- Backbone: 155MBit/s bzw. 622MBit/s ATM Verbindungen
- geplant mit 2 Netzwerkanschlüssen pro Mensch
- Etagenverteiler: 3-5 24port 100Mbit Switches (Cisco 2924) angeschlossen über 1-2 100MBit/s Verbindungen

Entwicklung – Netz

Stand heute:

- Backbone: 10GBit/s Ethernet Verbindungen
- geplant mit 4-6 Netzwerkanschlüssen pro Mensch
- Etagenverteiler: 3-5 48port Gbit Switches angeschlossen über 10GBit/s Verbindungen

Entwicklung – E-Mail

E-Mail-System im Jahr 2000:

- ca. 20.000 E-Mail-Konten auf einer SUN
- 100MB Quota

Heute:

- > 100.000 E-Mail-Konten verteilt auf 7 Mailbox-Server
- 1GByte Quota (selbständig erweiterbar auf 10GByte)

Verwaltung

Verantwortlichkeiten / Organisationsstruktur:

- NOC hat Netzhoheit
- Verantwortlichkeiten für Netzanschlüsse delegierbar an Fakultät/Institut/Lehrstuhl
- öffentliche Netzwerkanschlüsse nur mit Authentifizierung nutzbar

Verwaltung

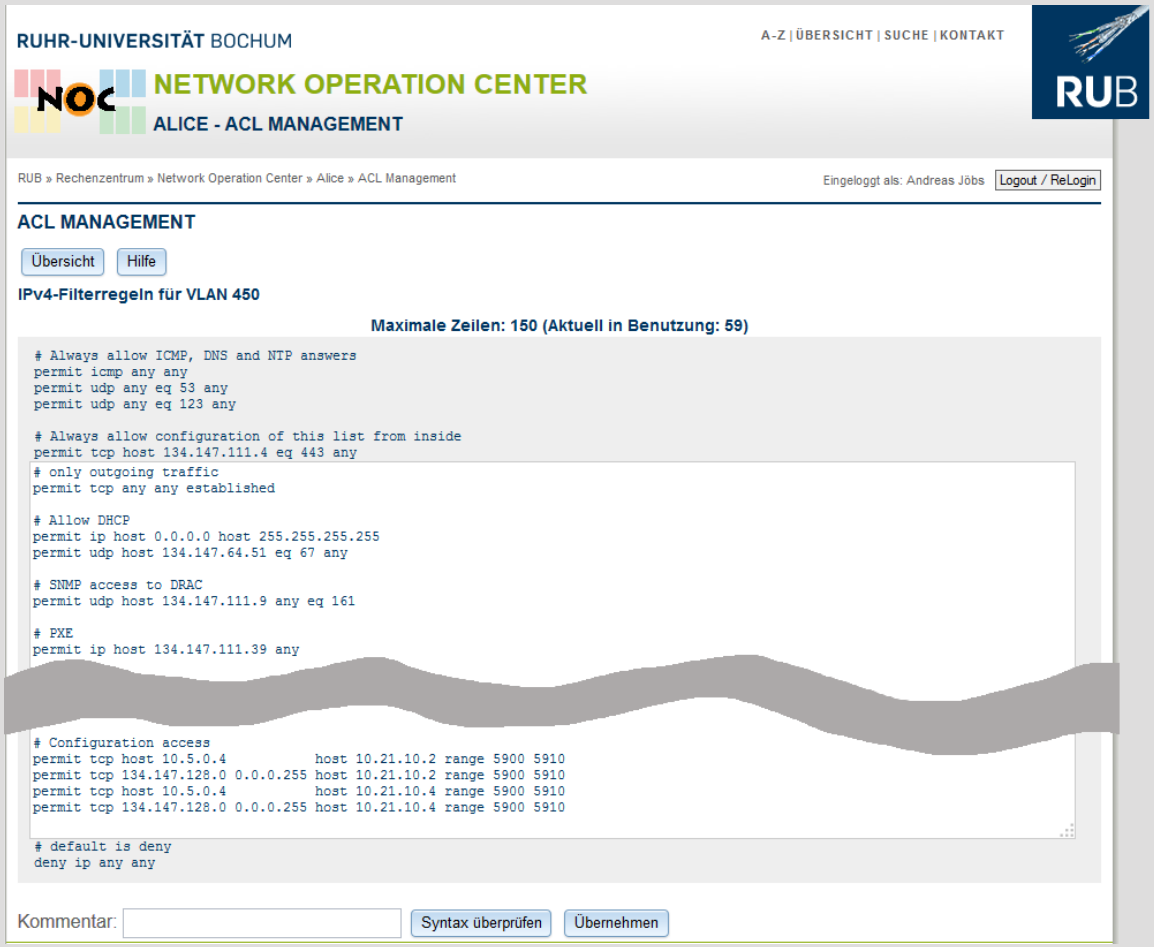
Zum Tagesgeschäft gehören:

- Neues Subnetz an Institut vergeben
- Änderungen an Vlan-Filterlisten
- Raumzuordnungen ändern sich

Wichtig:
$\Rightarrow$ Zuordnung Institut $\Leftrightarrow$ Subnetz / Vlan
$\Rightarrow$ Zuordnung Netzwerkanschlussdose $\Leftrightarrow$ Switchport.

Verwaltung

Netzverantwortliche können Vlan-Filterlisten selbst bearbeiten:



Verwaltung

Raumzuordnungen

- Kein Zugriff auf das Raumbuch der RUB
- Raumzuordnungen über geschaltete Netze
- Nutzer „sieht” alle Räume in denen „sein” Netz geschaltet ist

Anschlusszuordnungen

- Patchfeldport als Label auf Netzanschlussdose
- Switchport Beschreibung enthält Patchfeldport und Zielraum

Verwaltung

Netzanschlussdose

`13 VT1-A 14`	Gebäude NAS, Erdgeschoß, Raum 15
`03/252/5`	Gebäude NAF, Etage 03, Raum 252
`V.300-I 9-16`	Schrank 40, Serverraum IC 05

Switchport Beschreibung

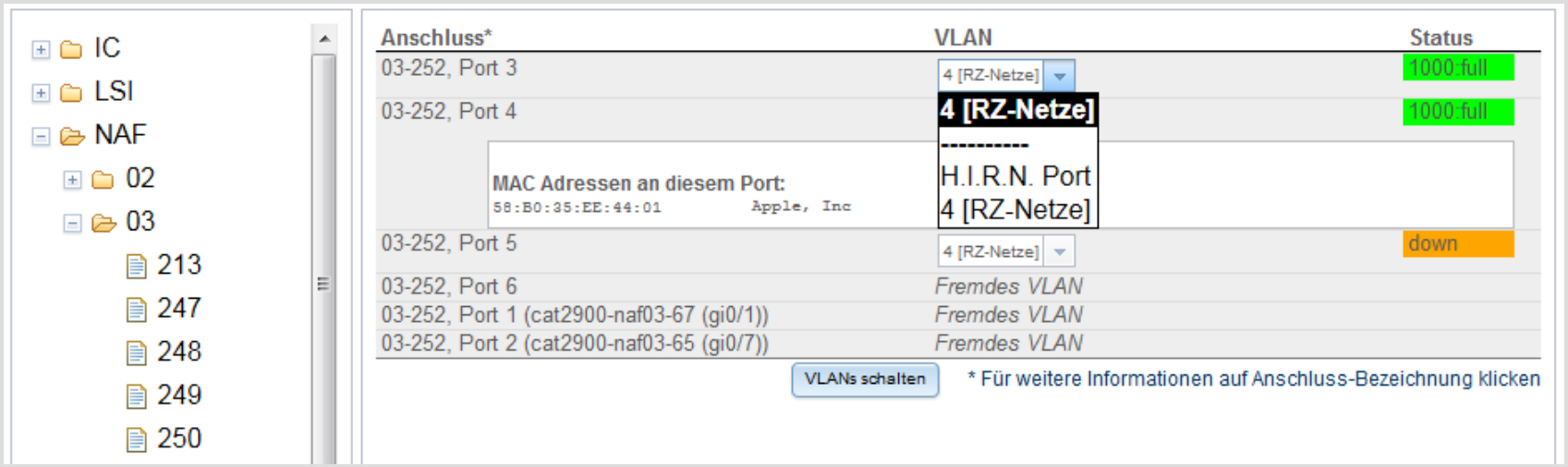
```
A;VT.1;A;14;13 VT1-A 14;14;NAS/0/15
A;Temprack4;D;14;03-252;5;NAF/03/252
A;V.300;I;10;V.300-I 9, 10, ... 16;2;IC/05/Schrank 40
```

Switch Standort

```
RUB;CAMPUS;NAS;0;EDV
```

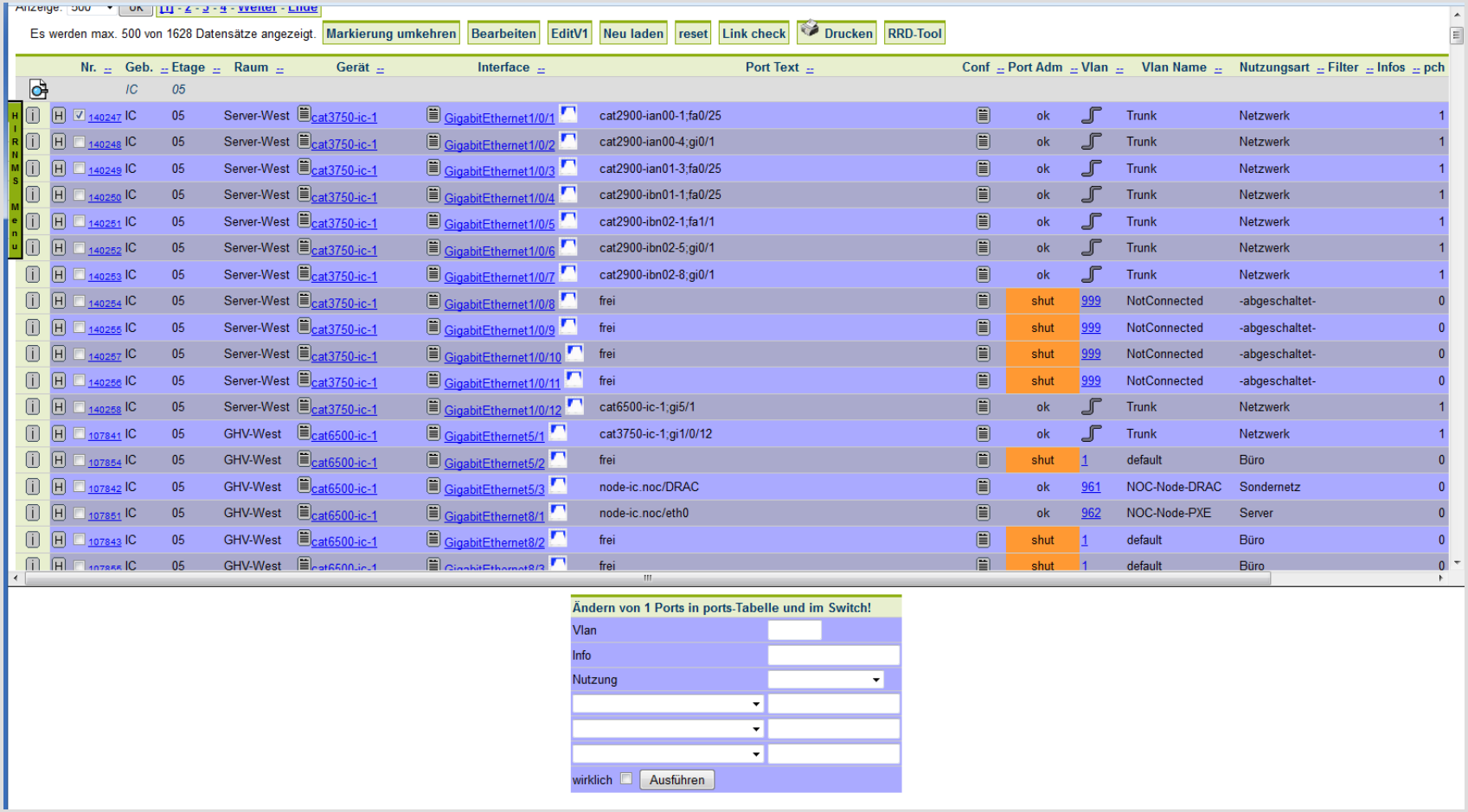
Verwaltung

Netzverantwortliche können Netzwerkanschlussdosen selbst beschalten:



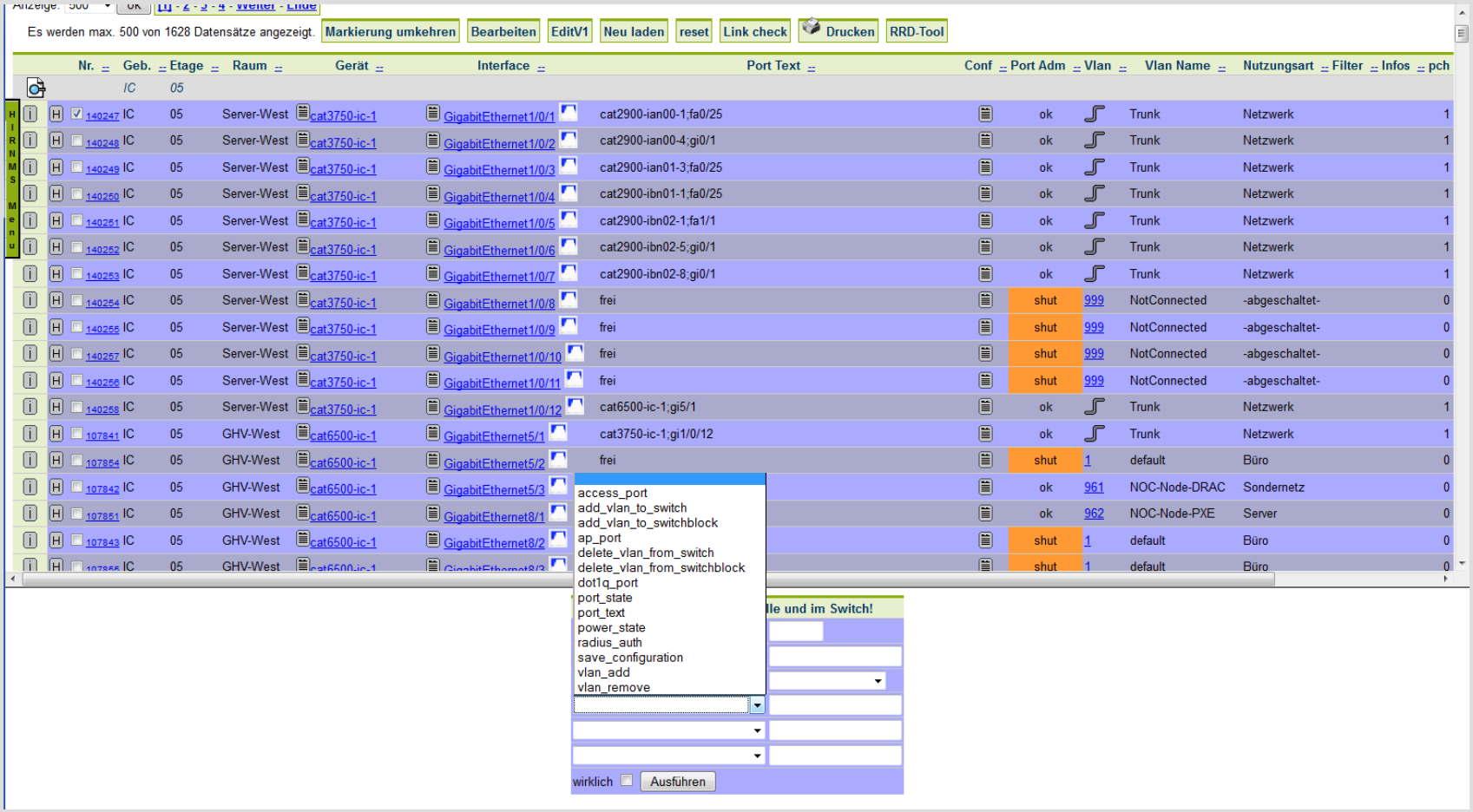
Verwaltung

Switchport Verwaltung aus Sicht des NOC:



Verwaltung

Switchport Verwaltung aus Sicht des NOC:



Verwaltung

Das Herz der Netzverwaltungstools:

Die HIRN-Module

- Verbinden Datenbank mit Switch-Hardware
- Setzen logische Operation in CLI-Kommandos um
- Durch objektorientierte Implementierung einfach erweiterbar für andere Hardware und/oder andere Modelle

Verwaltung

Die HIRN-Module (HIRN.pm)

- Device.pm
  - Cisco.pm
    - enterprises_9_5_44.pm
    - …
  - Dell.pm
    - enterprises_674_10895_3031.pm
    - …
  - HP.pm
  - Nexans.pm

Verwaltung

`HIRN::Device` kapselt ein L2-/L3-Gerät

Attribute

- Name, Hersteller, OID, Location
- Interfaces, Information / Configuration
- Neighbors, Uplink-Port, MAC-/ARP-Information

Aktionen

- (CLI-)Kommando ausführen
- Vlan konfigurieren
- Access- / Tagged-Port konfigurieren
- Switchblock Kommandos

Verwaltung

Auf `HIRN::Device` setzen (fast) alle Verwaltungstools auf.

Scriptkopf

```
#!/opt/perl/bin/perl

use strict;
use warnings;
use HIRN;
...
```

Monitoring

- Was?
- Womit?

Monitoring – Tools

Opensource Tools

- Icinga
- Cricket
- Munin
- NeDi

Monitoring – Tools

Icinga – Netzwerk

- Environment (Temperatur / Lüfter)
- SNMP-Location

Icinga – Server

- Port geöffnet?
- Service verfügbar?
- Service funktioniert?
- …

Hostabhänigkeiten aber keine Dienstabhänigkeiten konfiguriert.

Monitoring – Tools

Icinga Konfiguration für Switche weitestgehend automatisiert:

- Nächtlicher Job ermittelt für jedes Gerät das Elterngerät
- morgendlicher Job erzeugt eine Icinga Konfiguration mit korrekten `parent` Konfigurationen

Monitoring – Tools

Cricket / Munin

Datenerfassung mit RRDtool

- nach Möglichkeit ein Datum pro RRD-Datei
- kalkulierbarer Platzbedarf
- eigene Tools um Daten zu visualisieren

Monitoring – Tools

NeDi

NetworkDiscovery

- findet Geräte via ARP, CDP, LLDP, …
- automatische Erfassung aller Interfaces
- erzeugt RRDgraphen für jedes Gerät / Interface

Monitoring – Tools

Interface Graphen

Problem: zu langsam

- Ein NeDi Lauf braucht 6-8 Stunden
- ca. 1.200 Geräte müssen per SNMP abgefragt werden
- 4 SNMP Variablen / Gerät, 10 SNMP Variablen / Interface
- mehr als 120.000 RRD-Dateien müssen beschrieben werden

- . . . und das Ganze in weniger als 5 Minuten

Monitoring – Tools

Lösung: `perfi.pl` – NeDi's interface grapher on steroids

- `Net::SNMP::XS` nonblocking mit 10 Sekunden Timeout
- Schreibt RRD-Dateien in eine RAM-Disk
- Wrapperscript sichert Daten in einem TAR-Archiv (26GByte)
- Bootvorgang packt dieses TAR automatisch aus

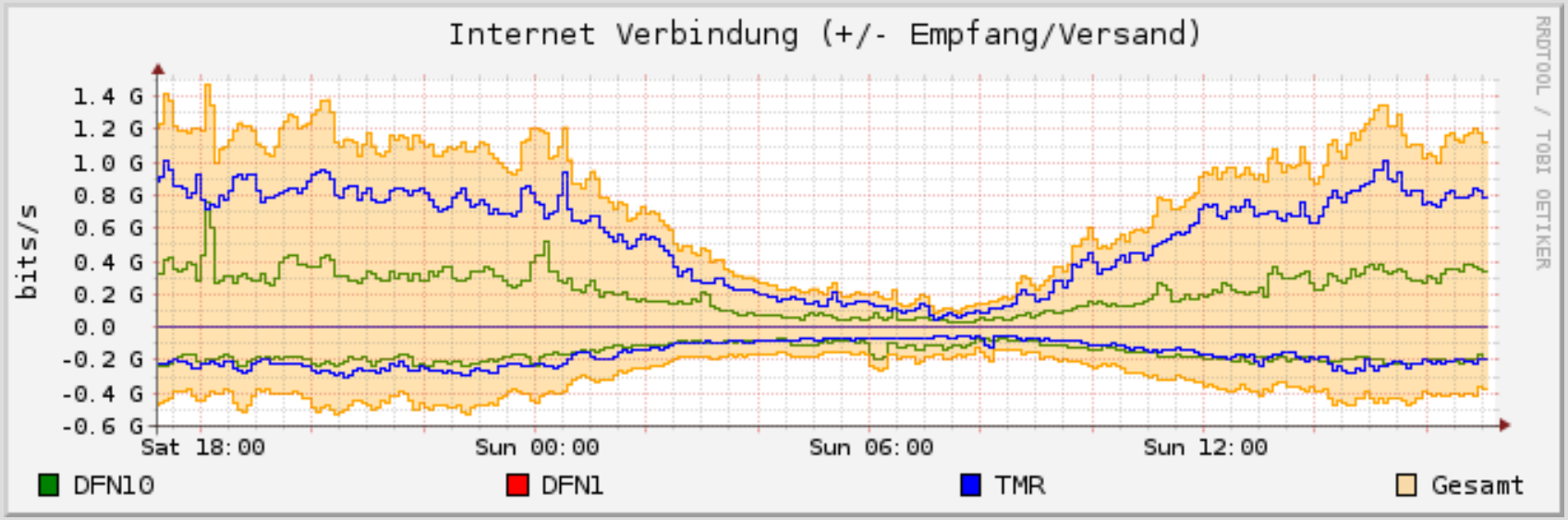
- weniger als 1 Minute für einen Durchlauf
- danach 3-5 Minuten für die Archivierung

Monitoring – Tools

Auswertung / Nutzung

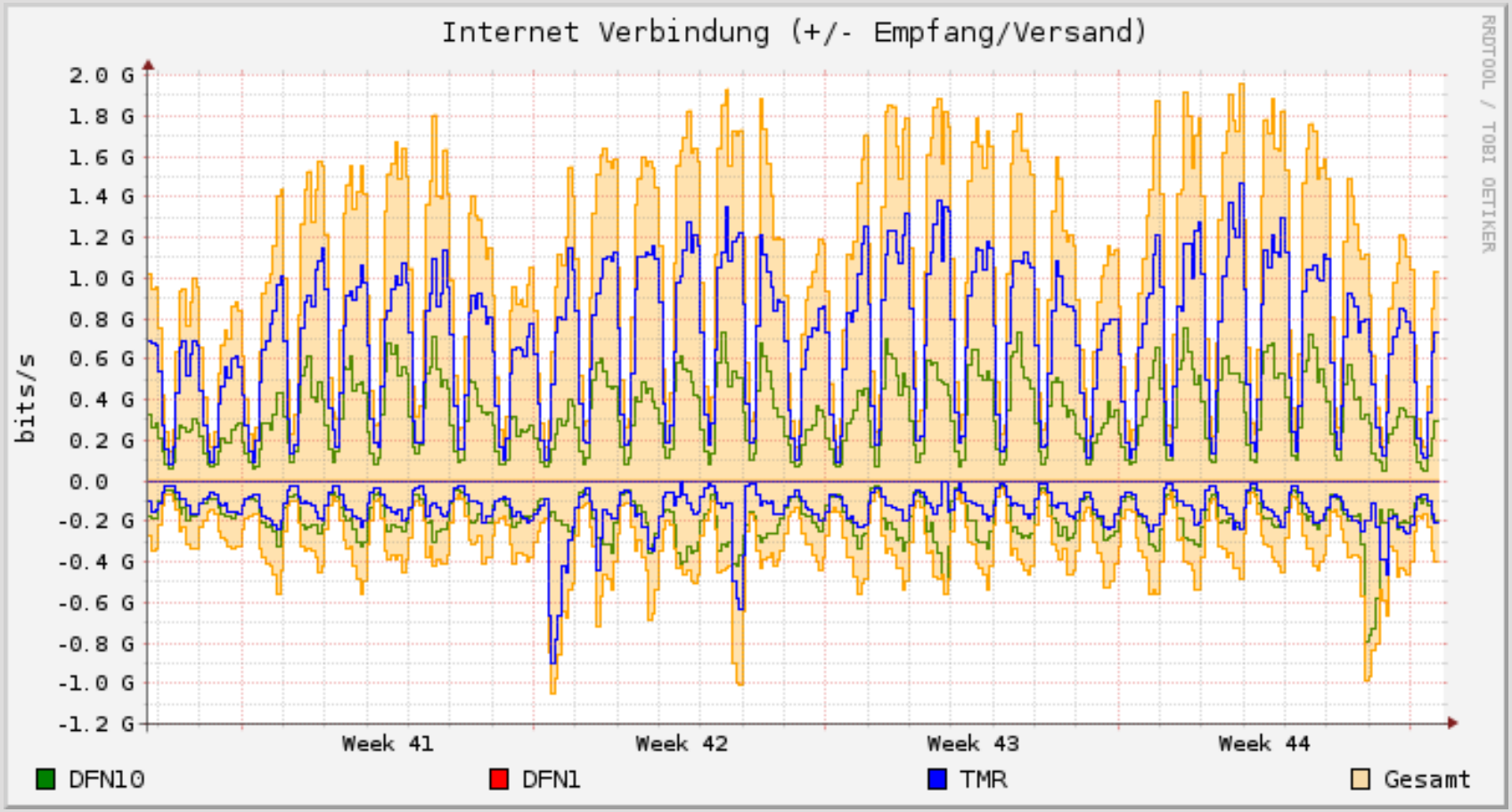
- `y_rrdgraph` erstellt Graphen aus RRDs verschiedener Anwendungen
- `proxygraph` erstellt vordefinierte Graphen (für Kunden, Webseiten, etc.)

Monitoring – Tools



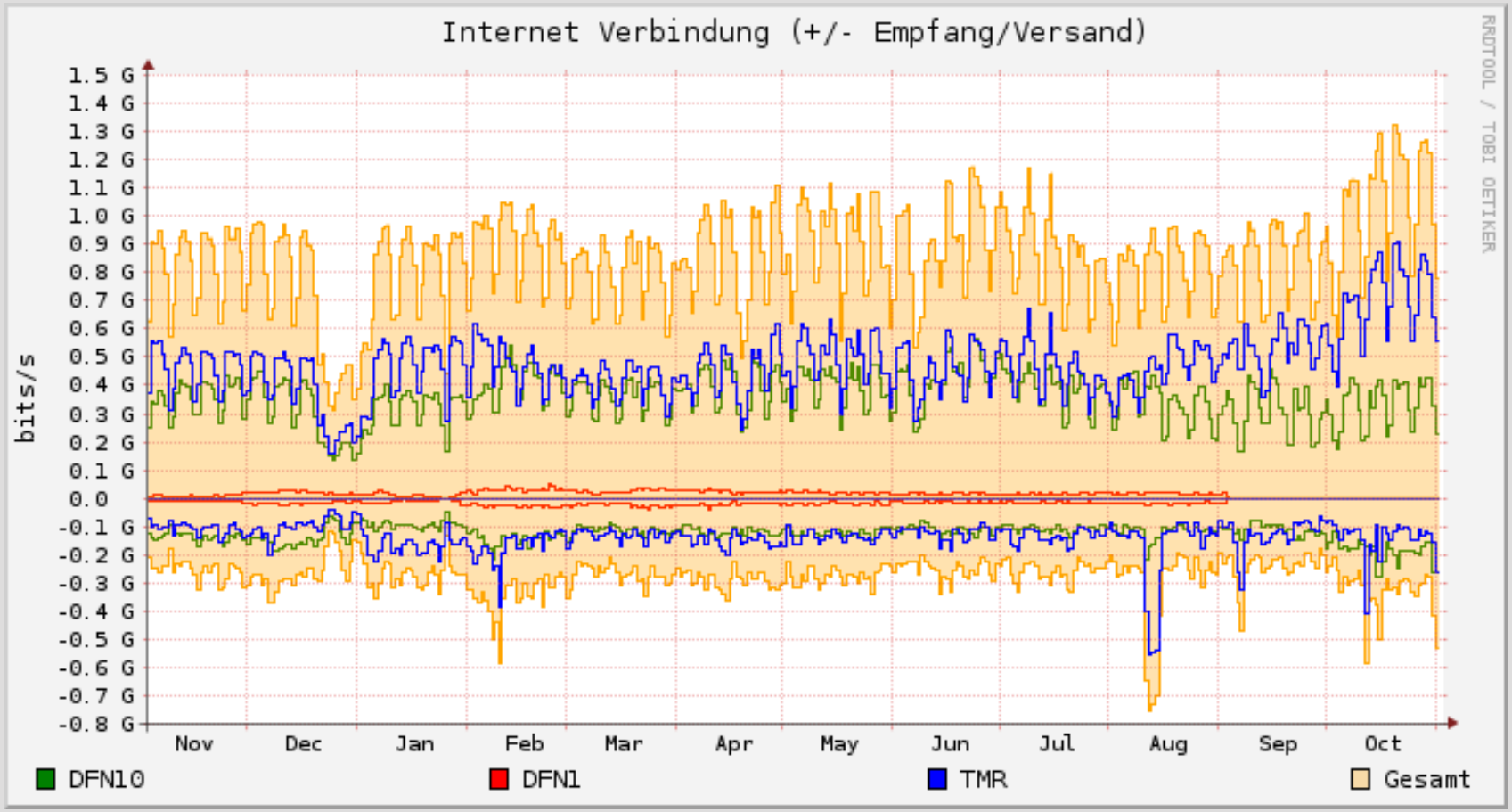
Grafik von der Übersichtsseite „Wie ist die Universität ans Internet angebunden”.

Monitoring – Tools



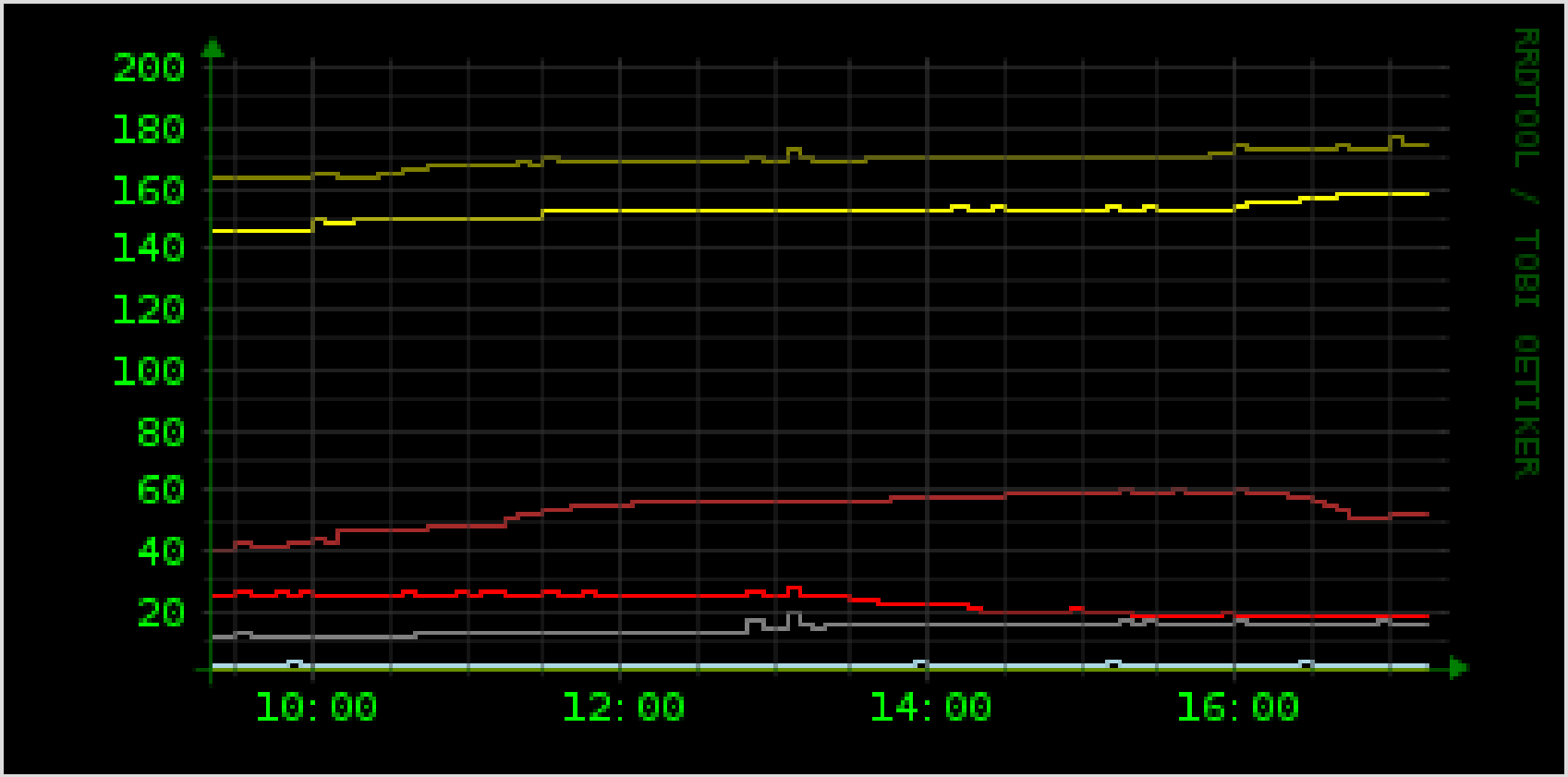
Internet Datenverkehr – Monatsübersicht

Monitoring – Tools



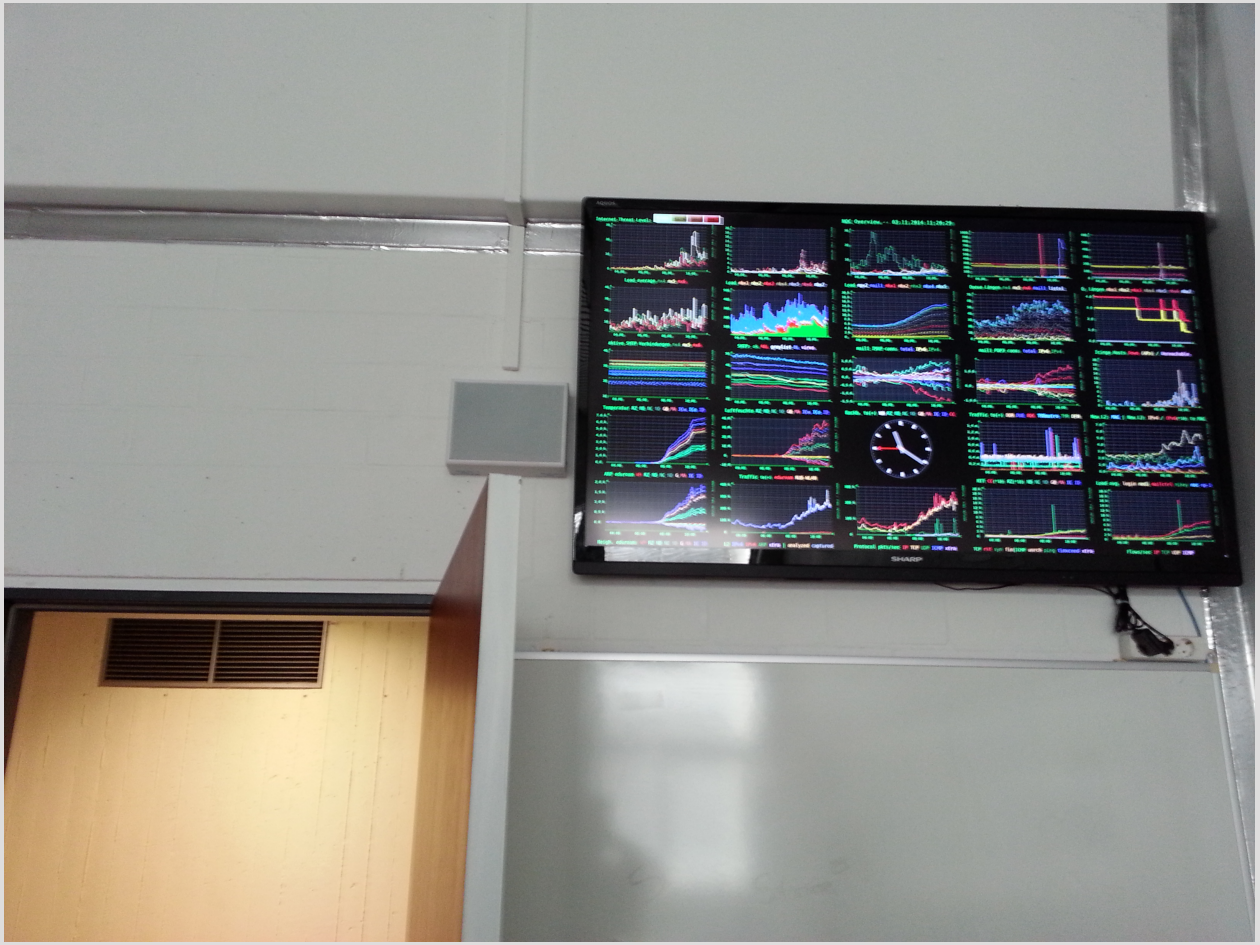
Internet Datenverkehr – Jahresübersicht

Monitoring – Tools

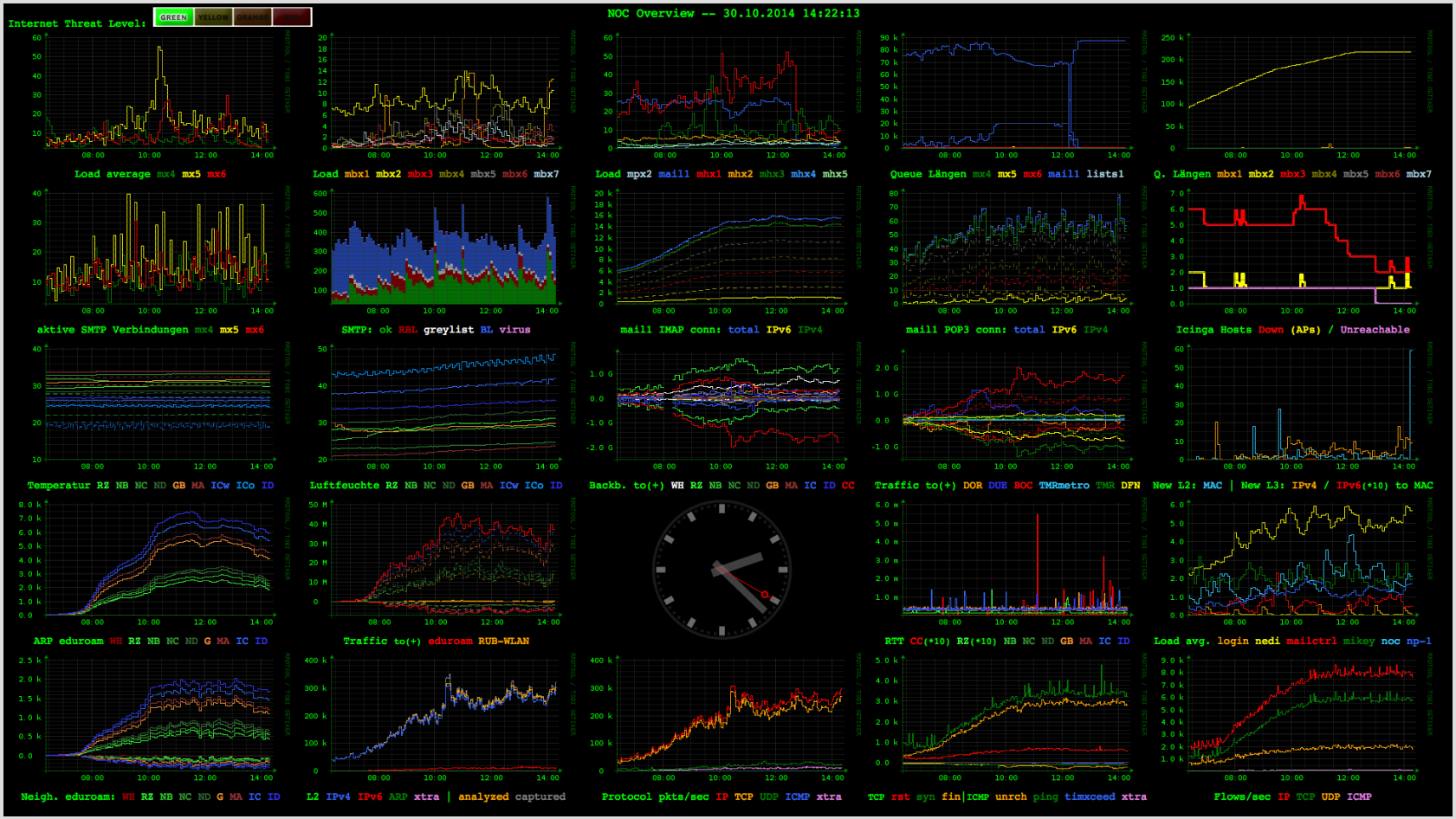


Alle Queues aller Mailboxserver in einem Graphen

Monitoring – Tools

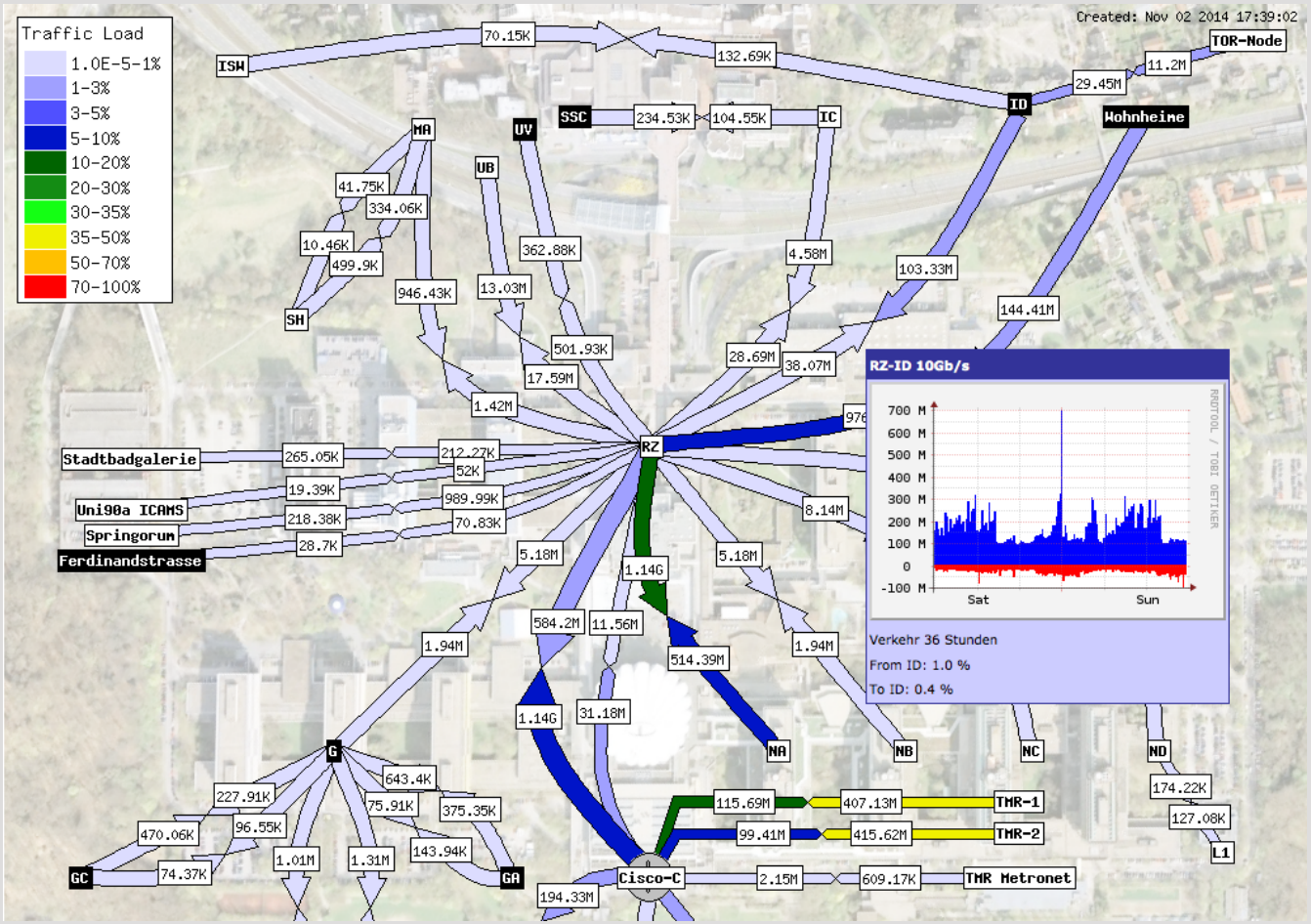


Monitoring – Tools



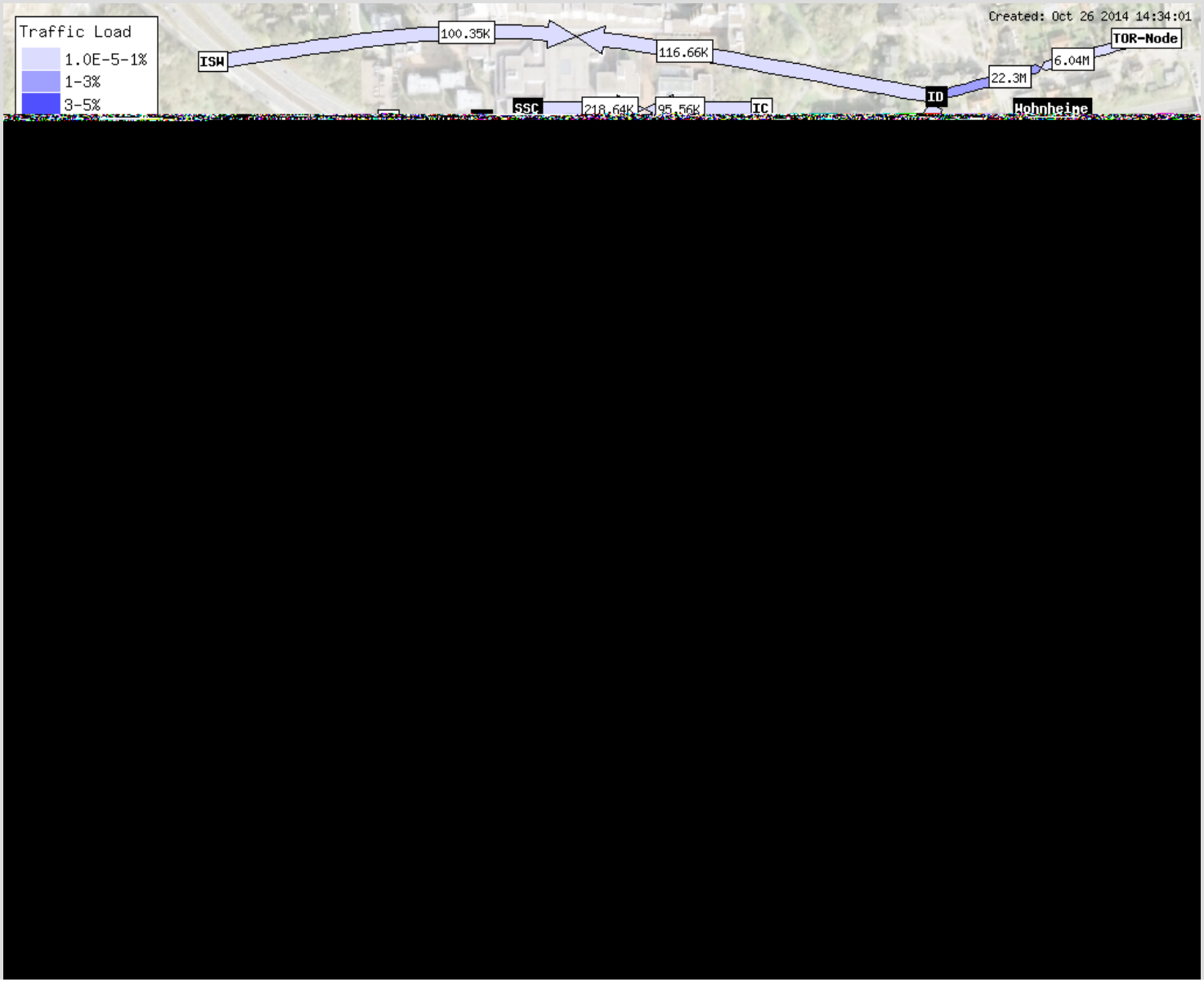
Alle Queues aller Mailboxserver in einem Graphen bei einem eingefangenen Spammer.

Monitoring – Tools



Das (aktuelle) Netzwetter.

Überblick


Traffic Load
1.0E-5-1%
1-3%
3-5%
Created: Oct 26 2014 14:34:01
ISW
100.35K
116.66K
TOR-Node
6.04M
22.3M
ID
Hohnheine
SSC
218.64K
95.56K
IC

Fragen?

Fragen?

- Vielen Dank für die Aufmerksamkeit

Links

- Icinga
  `https://www.icinga.org/`
- Munin
  `http://munin-monitoring.org/`
- NeDi
  `http://www.nedi.ch/`
- RRDtool
  `http://oss.oetiker.ch/rrdtool/`
- RUB Netzwetter
  `http://nedi.noc.rub.de/netweather/` bzw.
  `http://nedi.noc.rub.de/netweather/videos/`