

Betrieb großer Infrastrukturen ein Praxisbericht

Andreas Jobs – RUB-NOC

heise Netze Tour 2014 – Netzwerk im Griff



- Die Ruhr-Universität Bochum
- Verwaltung
- Monitoring

Die Ruhr-Universität Bochum

- ca. 42.500 Studierende
- ca. 5.600 Mitarbeiter/Mitarbeiterinnen
- 4,5 km² Campusfläche
- 350.000 m² Hauptnutzfläche der Gebäude



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

Network Operation Center der RUB

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

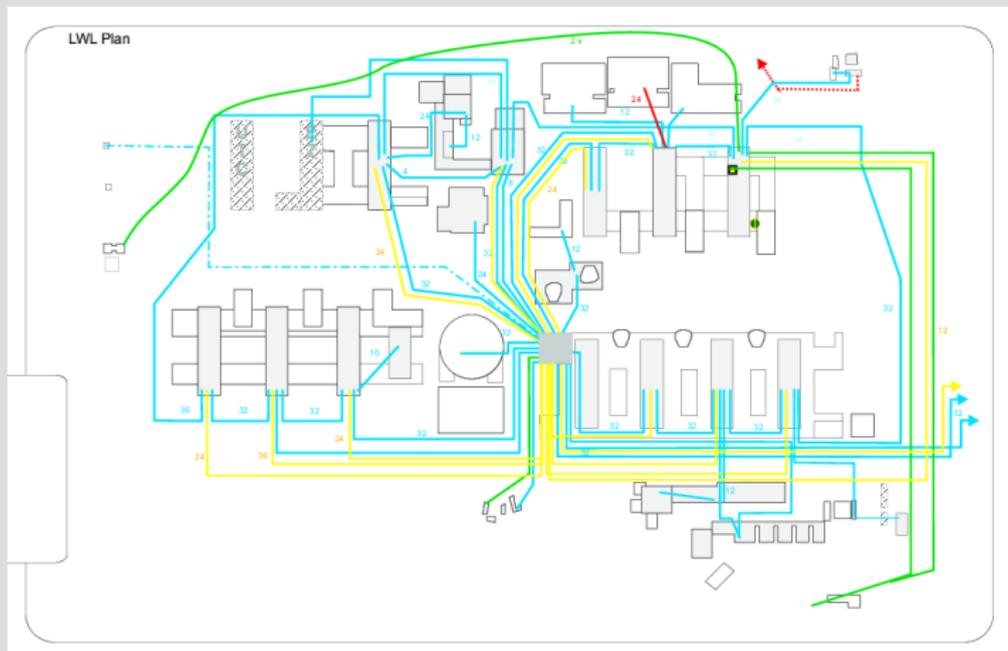
Netzwerk

- 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

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



Schematische Darstellung der Backbone-Verbindungen

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

Anbindung diverser Außenliegenschaften:

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

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

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

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

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

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)

Verantwortlichkeiten / Organisationsstruktur:

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

Zum Tagesgeschäft gehören:

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

Wichtig:

⇒ Zuordnung Institut \Leftrightarrow Subnetz / Vlan

⇒ Zuordnung Netzwerkanschlusdose \Leftrightarrow Switchport.

Netzverantwortliche können Vlan-Filterlisten selbst bearbeiten:

RUB - UNIVERSITÄT BOCHUM

A-Z | ÜBERSICHT | SUCHE | KONTAKT

NOC NETWORK OPERATION CENTER
ALICE - ACL MANAGEMENT

RUB

RUB » Rechenzentrum » Network Operation Center » Alice » ACL Management Engelggt als: Andreas Jobs [Logout / ReLogin](#)

ACL MANAGEMENT

[Übersicht](#) [Hilfe](#)

IPv4-Filterregeln für VLAN 450

Maximale Zeilen: 150 (Aktuell in Benutzung: 59)

```
# Always allow ICMP, DNS and NTP answers
permit icmp any any
permit udp any eq 53 any
permit udp any eq 123 any

# Always allow configuration of this list from inside
permit tcp host 134.147.111.4 eq 443 any
# only outgoing traffic
permit tcp any any established

# Allow DHCP
permit ip host 0.0.0.0 host 255.255.255.255
permit udp host 134.147.64.51 eq 67 any

# SNMP access to ERAC
permit udp host 134.147.111.9 any eq 161

# PXE
permit ip host 134.147.111.39 any

# Configuration access
permit tcp host 10.5.0.4 host 10.21.10.2 range 5900 5910
permit tcp host 134.147.128.0 0.0.0.255 host 10.21.10.2 range 5900 5910
permit tcp host 10.5.0.4 host 10.21.10.4 range 5900 5910
permit tcp host 134.147.128.0 0.0.0.255 host 10.21.10.4 range 5900 5910

# default is deny
deny ip any any
```

Kommentar: [Syntax überprüfen](#) [Überschreiben](#)

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

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

Netzverantwortliche können Netzwerkanschlussdosen selbst beschalten:

The screenshot shows a network management interface with a sidebar on the left and a main configuration area on the right. The sidebar contains a tree view of folders: IC, LSI, NAF, 02, 03, 213, 247, 248, 249, and 250. The main area displays a table of network connections with columns for 'Anschluss*', 'VLAN', and 'Status'. The table lists several ports, including '03-252, Port 3', '03-252, Port 4', and '03-252, Port 5'. Port 4 is highlighted with a tooltip showing '4 [RZ-Netze]'. Below the table, there is a button labeled 'VLANs schalten' and a note: '* Für weitere Informationen auf Anschluss-Bezeichnung klicken'. A tooltip for 'MAC Adressen an diesem Port:' shows '58:50:25:EE:44:01 Apple, Inc'.

Anschluss*	VLAN	Status
03-252, Port 3	4 [RZ-Netze]	1000 full
03-252, Port 4	4 [RZ-Netze]	1000 full
MAC Adressen an diesem Port: 58:50:25:EE:44:01 Apple, Inc		
03-252, Port 5	4 [RZ-Netze]	down
03-252, Port 6	Fremdes VLAN	
03-252, Port 1 (cat2900-naf03-67 (gi0/1))	Fremdes VLAN	
03-252, Port 2 (cat2900-naf03-65 (gi0/7))	Fremdes VLAN	

VLANs schalten * Für weitere Informationen auf Anschluss-Bezeichnung klicken

Switchport Verwaltung aus Sicht des NOC:

The screenshot displays a network management interface with a table of switch ports and a configuration dialog. The table lists various ports across different servers and buildings, with columns for status, configuration, and usage. A dialog box is open, allowing for the modification of port settings.

No.	Geb.	Etage	Raum	Gerät	Interface	Port Text	Conf.	Port Adm.	Vlan	Vlan Name	Nutzungsart	Filter	Infos	pch
145201	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/1	cat2900-iam00-1.fso/25	ok	ok	999	Trunk	Netzwerk			1
145208	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/2	cat2900-iam00-4.g0/1	ok	ok	999	Trunk	Netzwerk			1
145209	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/3	cat2900-iam01-3.fso/25	ok	ok	999	Trunk	Netzwerk			1
145200	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/4	cat2900-ibn01-1.fso/25	ok	ok	999	Trunk	Netzwerk			1
145201	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/5	cat2900-ibn02-1.fso/1	ok	ok	999	Trunk	Netzwerk			1
145202	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/6	cat2900-ibn02-5.g0/1	ok	ok	999	Trunk	Netzwerk			1
145203	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/7	cat2900-ibn02-8.g0/1	ok	ok	999	Trunk	Netzwerk			1
145204	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/8	frei	shut	999	999	NotConnected	-abgeschaltet-			0
145205	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/9	frei	shut	999	999	NotConnected	-abgeschaltet-			0
145206	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/10	frei	shut	999	999	NotConnected	-abgeschaltet-			0
145207	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/11	frei	shut	999	999	NotConnected	-abgeschaltet-			0
145208	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/12	frei	shut	999	999	NotConnected	-abgeschaltet-			0
145209	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/13	cat6500-ic-1.g5/1	ok	ok	951	Trunk	Netzwerk			1
145210	KC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/14	cat3750-ic-1.g1/0/12	ok	ok	952	Trunk	Netzwerk			1
145211	KC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/2	frei	shut	1	1	default	Buro			0
145212	KC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/3	node-ic.noc/DRAC	ok	ok	951	NOC-Node-DRAC	Sondermetz			0
145213	KC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/1	node-ic.noc/with0	ok	ok	952	NOC-Node-PXE	Server			0
145214	KC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/2	frei	shut	1	1	default	Buro			0
145215	KC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/3	frei	shut	1	1	default	Buro			0

Ändern von 1 Ports in ports-Tabelle und im Switch!

Vlan:

Info:

Nutzung:

wirklich Ausführen

Switchport Verwaltung aus Sicht des NOC:

Es werden max. 500 von 1620 Datensätze angezeigt. [Markierung umkehren](#) [Bearbeiten](#) [Edit/V1](#) [Neu laden](#) [reset](#) [Link check](#) [Drucken](#) [RRD-Tool](#)

Nr.	Geb.	Etage	Raum	Gerät	Interface	Port Text	Conf	Port Adm	Vlan	Vlan Name	Nutzungsart	Filter	Infos	pch
150240	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/1	cat2900-ian00-1.fab/25	ok	Trunk	Netzwerk	1				
150241	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/2	cat2900-ian00-4.gi0/1	ok	Trunk	Netzwerk	1				
150242	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/3	cat2900-ian01-3.fab/25	ok	Trunk	Netzwerk	1				
150243	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/4	cat2900-ian01-1.fab/25	ok	Trunk	Netzwerk	1				
150244	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/5	cat2900-ian02-1.fab/1	ok	Trunk	Netzwerk	1				
150245	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/6	cat2900-ian02-5.gi0/1	ok	Trunk	Netzwerk	1				
150246	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/7	cat2900-ian02-8.gi0/1	ok	Trunk	Netzwerk	1				
150247	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/8	frei	shut	999	NotConnected	-abgeschaltet-	0			
150248	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/9	frei	shut	999	NotConnected	-abgeschaltet-	0			
150249	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/10	frei	shut	999	NotConnected	-abgeschaltet-	0			
150250	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/11	frei	shut	999	NotConnected	-abgeschaltet-	0			
150251	IC	05	Server-West	cat3750-ic-1	GigabitEthernet1/0/12	cat6500-ic-1.gi5/1	ok	Trunk	Netzwerk	1				
167841	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/1	cat3750-ic-1.gi10/12	ok	Trunk	Netzwerk	1				
167842	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/2	frei	shut	1	default	Büro	0			
167843	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/3	access_port	ok	951	NOC-Node-DRAC	Sondermetz	0			
167844	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/4	add_vlan_to_switch	ok	352	NOC-Node-PXE	Server	0			
167845	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/5	ap_port	shut	1	default	Büro	0			
167846	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/6	delete_vlan_from_switch	shut	1	default	Büro	0			
167847	IC	05	GHV-West	cat6500-ic-1	GigabitEthernet5/7	delete_vlan_from_switchblock	shut	1	default	Büro	0			

Werkzeuge und im Switch!

- port_state
- port_text
- power_state
- radius_auth
- save_configuration
- vlan_add
- vlan_remove

wirklich [Ausführen](#)

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

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

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

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

Scriptkopf

```
#!/opt/perl/bin/perl  
  
use strict;  
use warnings;  
use HIRN;  
...
```

- Was?
- Womit?

Opensource Tools

- Icinga
- Cricket
- Munin
- NeDi

Icinga – Netzwerk

- Environment (Temperatur / Lüfter)
- SNMP-Location

Icinga – Server

- Port geöffnet?
- Service verfügbar?
- Service funktioniert?
- ...

Hostabhängigkeiten aber keine Dienstabhängigkeiten konfiguriert.

Icinga Konfiguration für Switche weitestgehend automatisiert:

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

Cricket / Munin

Datenerfassung mit RRDtool

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

NeDi

NetworkDiscovery

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

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

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

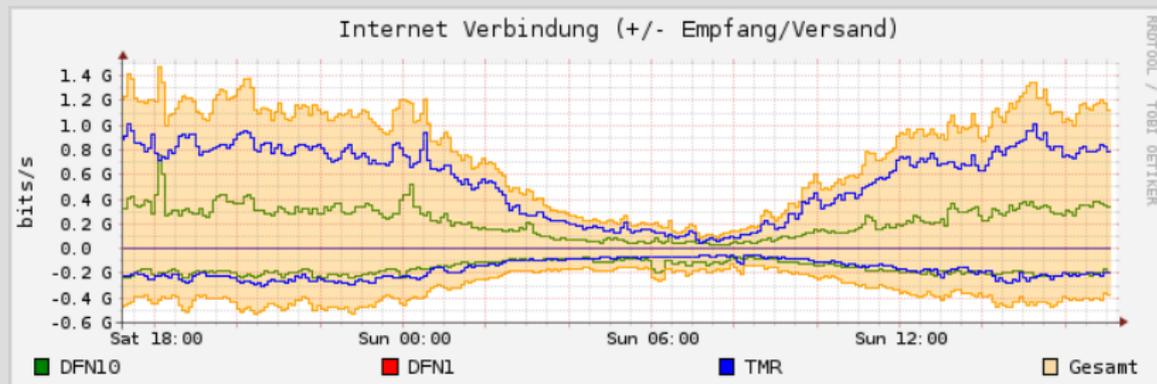
- `Net::SNMP::XS` nonblocking mit 10 Sekunden Timeout
- Schreibt RRD-Dateien in eine RAM-Disk
- Wrapperscript sichert Daten in einem TAR-Archiv (26GByte)
- Bootvorgang packt dieses TAR automatisch aus

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

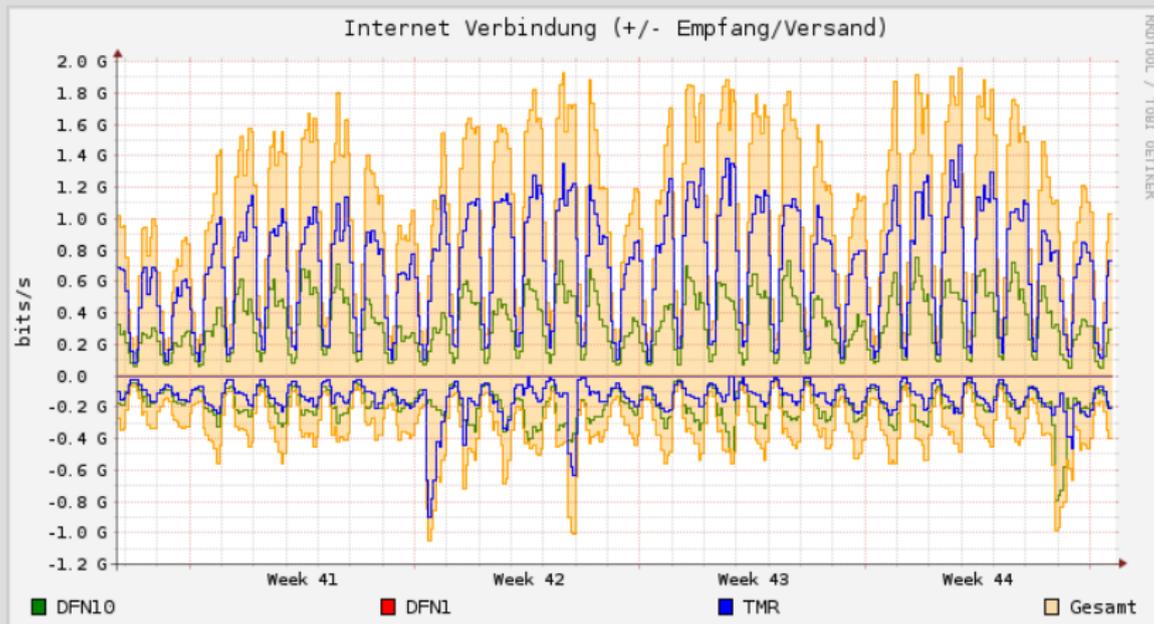
Auswertung / Nutzung

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

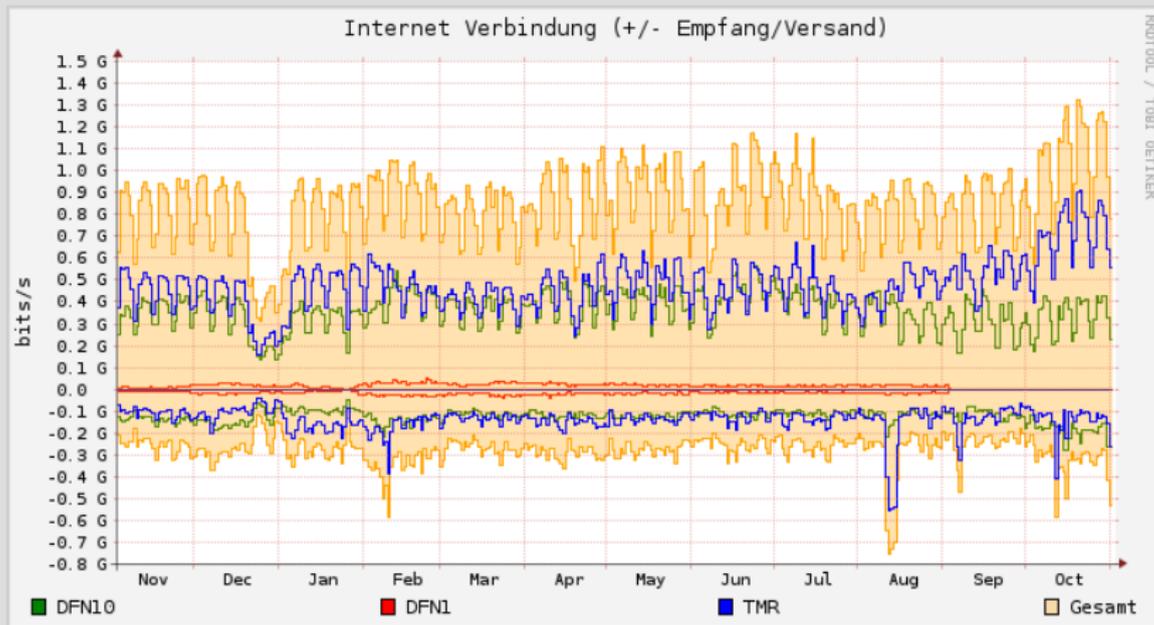
Monitoring – Tools



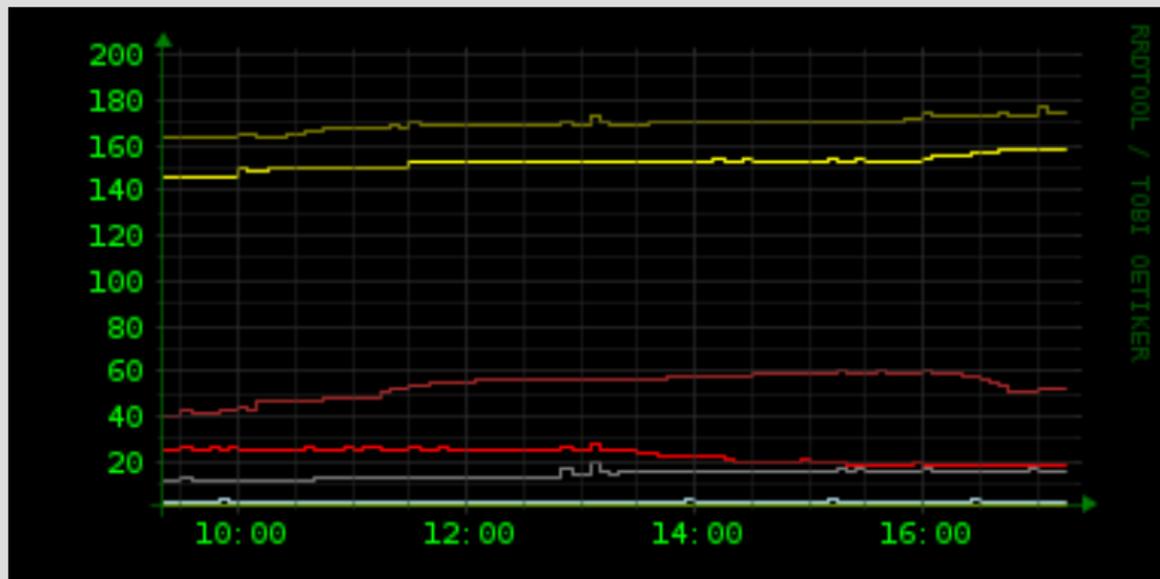
Grafik von der Übersichtsseite „Wie ist die Universität ans Internet angebunden“.



Internet Datenverkehr – Monatsübersicht



Internet Datenverkehr – Jahresübersicht

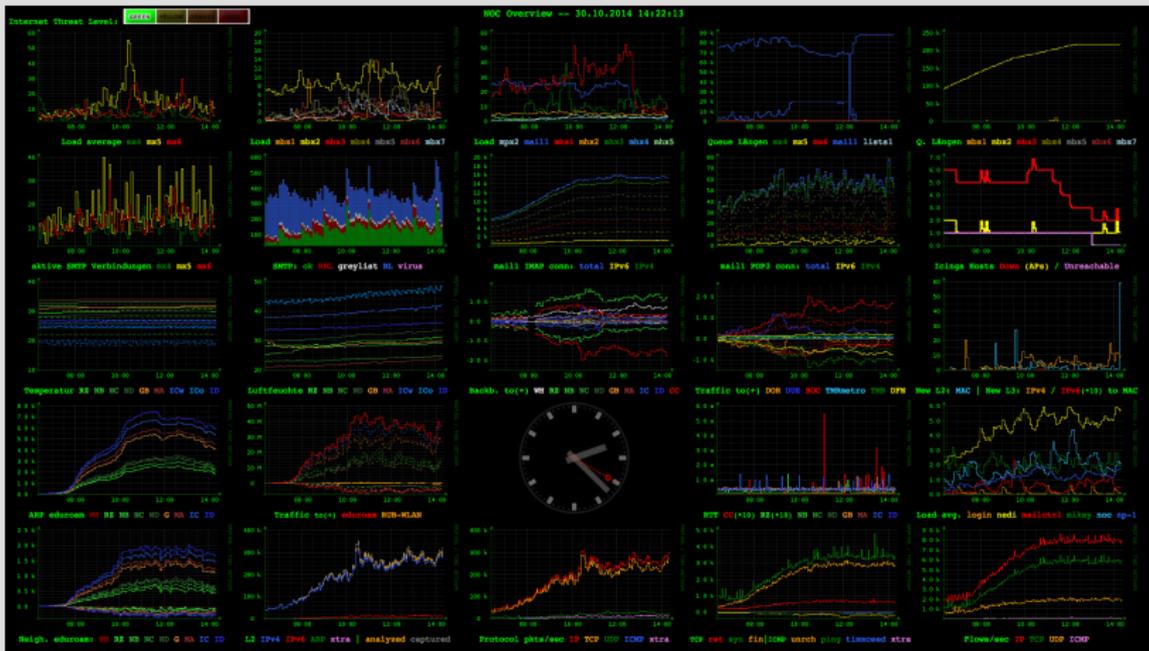


Alle Queues aller Mailboxserver in einem Graphen

Monitoring – Tools

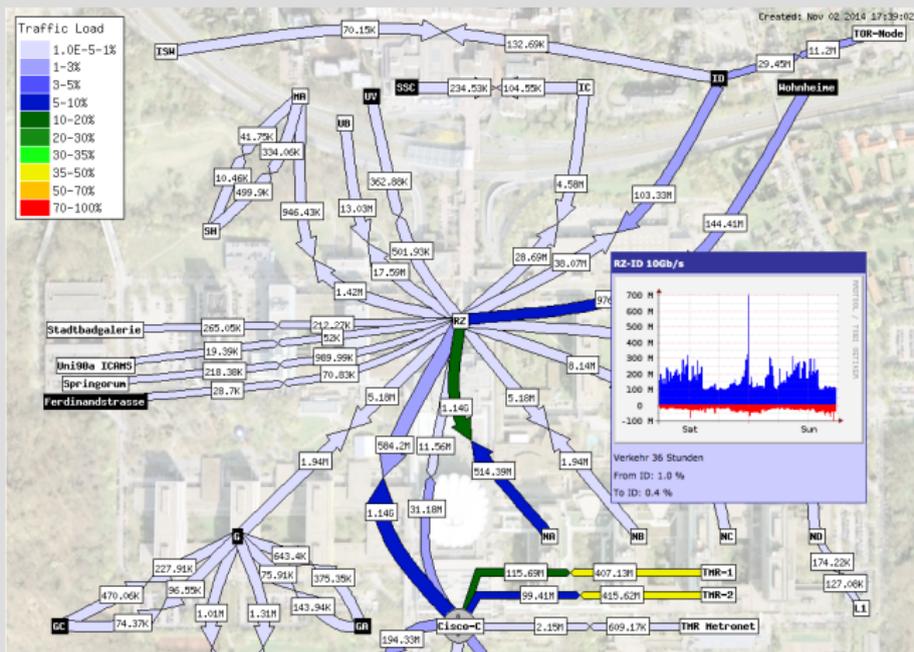


Monitoring – Tools

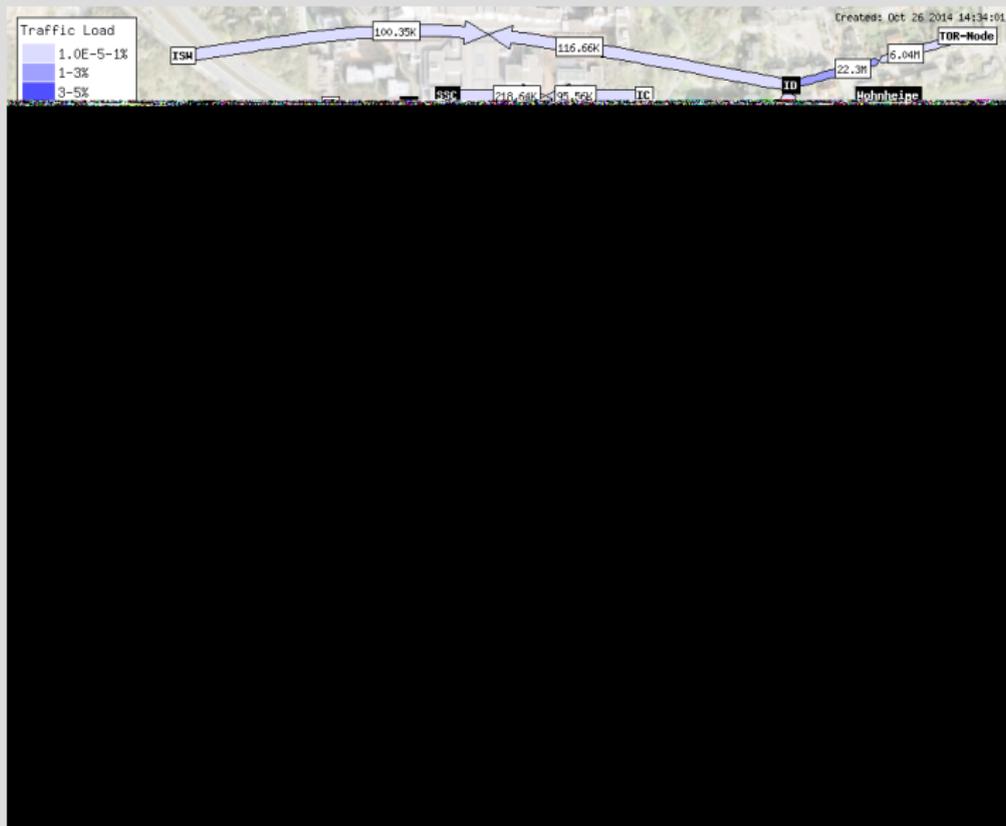


Alle Queues aller Mailboxserver in einem Graphen bei einem eingefangenen Spammer.

Monitoring – Tools



Das (aktuelle) Netzwerter.



Fragen?

- Vielen Dank für die Aufmerksamkeit

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