

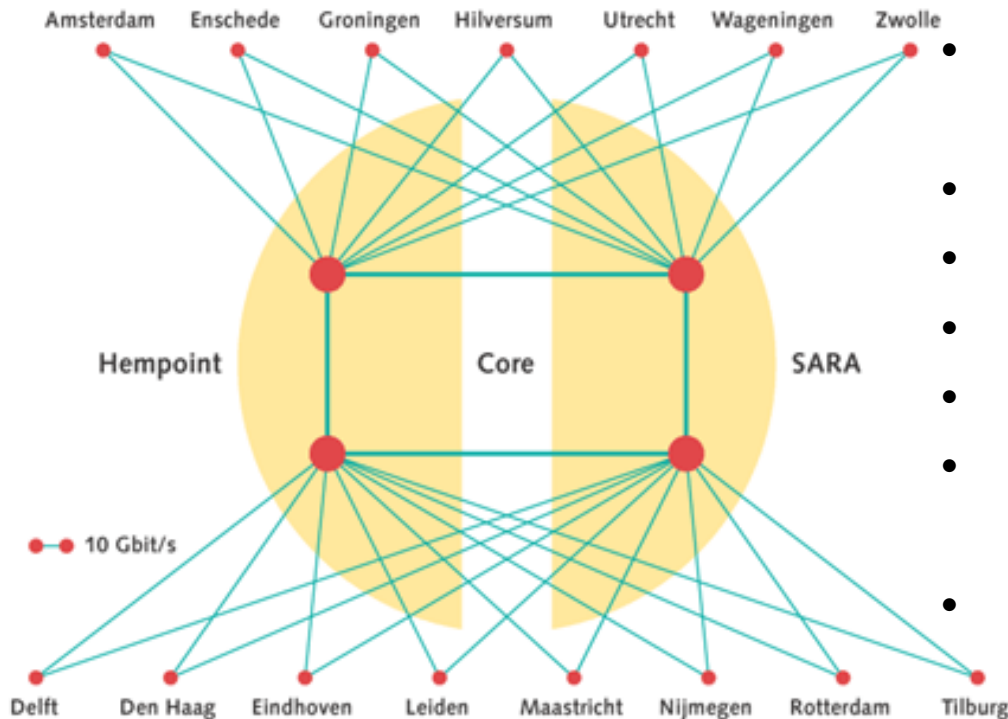


NERD:  
Network Emergency Responder &  
Detector

Wim.Biemolt@surfnet.nl

2<sup>nd</sup> FloCon, Pittsburgh, September, 2005.

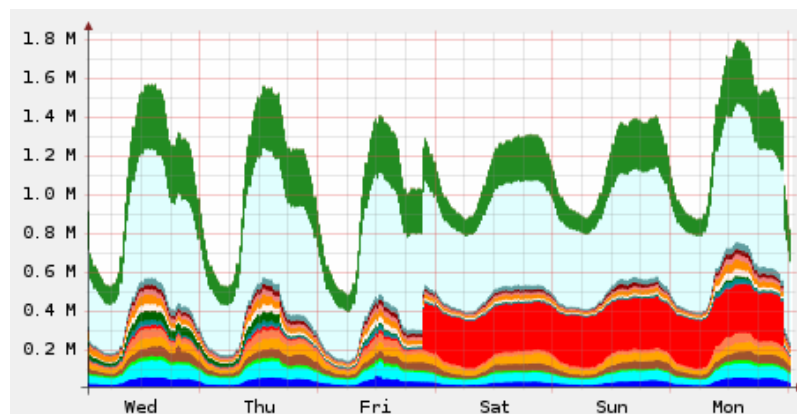
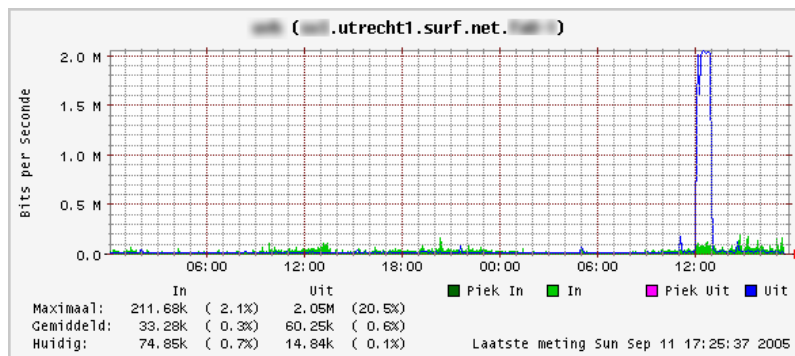
# SURFnet5 network



- Operational
  - Since September 2001
- Cisco 12416 routers
- Backbone: 10Gbps
- Connections: 1Gbps
- Dual stack (6PE)
- Incident detection
  - SURFnet & TNO: 2002
- Decommissioning
  - End of December 2005

# Incident response tools

- SURFstat
  - mrtg/rrdtool
- Research
  - syslog
  - Netflow
    - promising at the required speeds (>10 Gbps)
    - sampled (ip flow-sampling-mode packet-interval 100)
  - Full data analysis requires high-end equipment
- Prototype
  - cflowd (caida)
    - no longer supported
  - gnuplot, mysql, php
  - Not open-source



# Prototype



**N**etwork **E**mergency **R**esponder & **D**etector



Show all alarms from  days ago, up to  days ago.

The alarms between 2005-09-11 and 2005-09-12

The query took approximately 0.019 seconds.

- NETFLOW
- [Alarms](#)
- [ddos-rs v2](#)
- [spammeris](#)
- [Configuration](#)
- [Overall summary](#)
- [Analyse](#)
- [List](#)
- SYSLOG
- [Alarms](#)
- [TOP 10](#)
- [Rules](#)
- [Messages](#)
- [PoP-map](#)
- [Search](#)

Destination IP address	Hostname	Flows per 5 minutes	Average packets per flow	Average bytes per flow	Average destination port	Starttime	Stoptime	Continuing
<a href="#">140.193.122.1</a>	hulst-hulst.computer.com	6542	1	157	47467	2005-09-11 14:15:07	2005-09-11 14:39:06	1
<a href="#">131.111.29.102</a>	hawaii.ac.jp	29700	1	74	39930	2005-09-11 14:33:05	2005-09-11 14:39:06	1
<a href="#">216.19.108.10</a>	-	5555	1	142	47329	2005-09-11 14:39:06	2005-09-11 14:39:06	1
<a href="#">194.193.122.1</a>	co.uk	15955	1	157	47286	2005-09-11 11:03:03	2005-09-11 11:27:03	0
<a href="#">216.19.108.10</a>	-	4012	1	149	47560	2005-09-11 09:45:06	2005-09-11 09:45:06	0

# Alarm

131. [REDACTED]

[REDACTED].ac.jp

Perform :

[Whois](#)

[Traceroute](#)

[Nmap](#)

PS. Nmap is a portscanner, not everybody appreciates being portscanned. Use at your own risk.

Click on the following filenames to see detailed information:

[flows.20050911.14:42:52+0200](#)

[flows.20050911.14:37:49+0200](#)

[flows.20050911.14:32:46+0200](#)

Switch to this IP address:

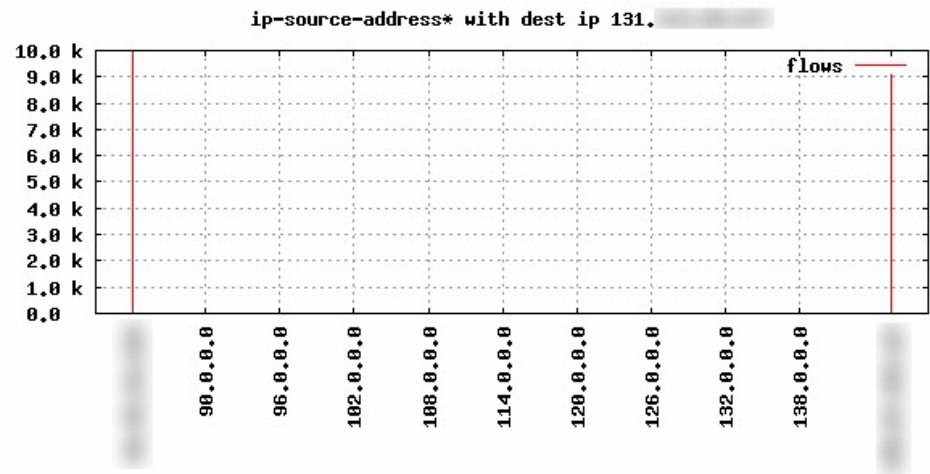
Go

# Analyse

Flow file:  protocol:  not   
src IP addr:  not  dst IP addr:  not   
src port:  dst port:   
exp IP addr:  not  src ifindex:  dst ifindex:

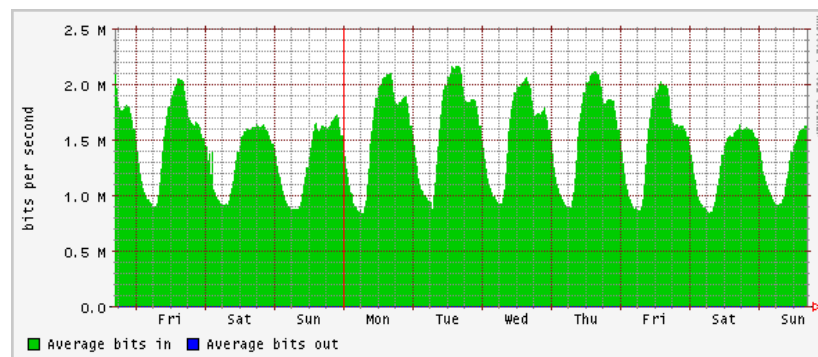
Report 1: type:  fields:  sort:   
Report 2: type:  fields:  sort:   
Report 3: type:  fields:  sort:   
Report 4: type:  fields:  sort:

Report type: ip-source-address  
Records: 5  
Min val:   
Max val:   
[Raw data](#)  
[Try to group raw data](#)

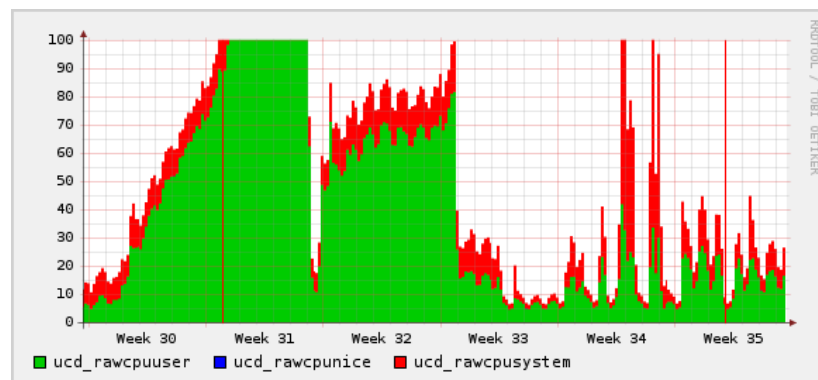


# Hardware

- Dell PowerEdge 1650
  - 04-2002, RedHat 7
  - 1x 1.4GHz, 1GB, 3x 36GB
- Dell PowerEdge 2650
  - 12-2003, FreeBSD 4.11
  - 2x 3GHz, 4GB, 5x 146GB
- Dell PowerEdge 2850
  - 10-2004, FreeBSD 5.4
  - 2x 3.4GHz, 6GB, 6x 146GB
- Dell PowerEdge 2850
  - 06-2005, FreeBSD 6.0
  - 2x 3.6GHz, 4GB, 6x 300GB
- SunFire V240
  - 12-2004, Solaris 10
  - 2x 1.5GHz, 4GB, 4x 146GB



<http://www.switch.ch/tf-tant/floma/sw/samplicator/>



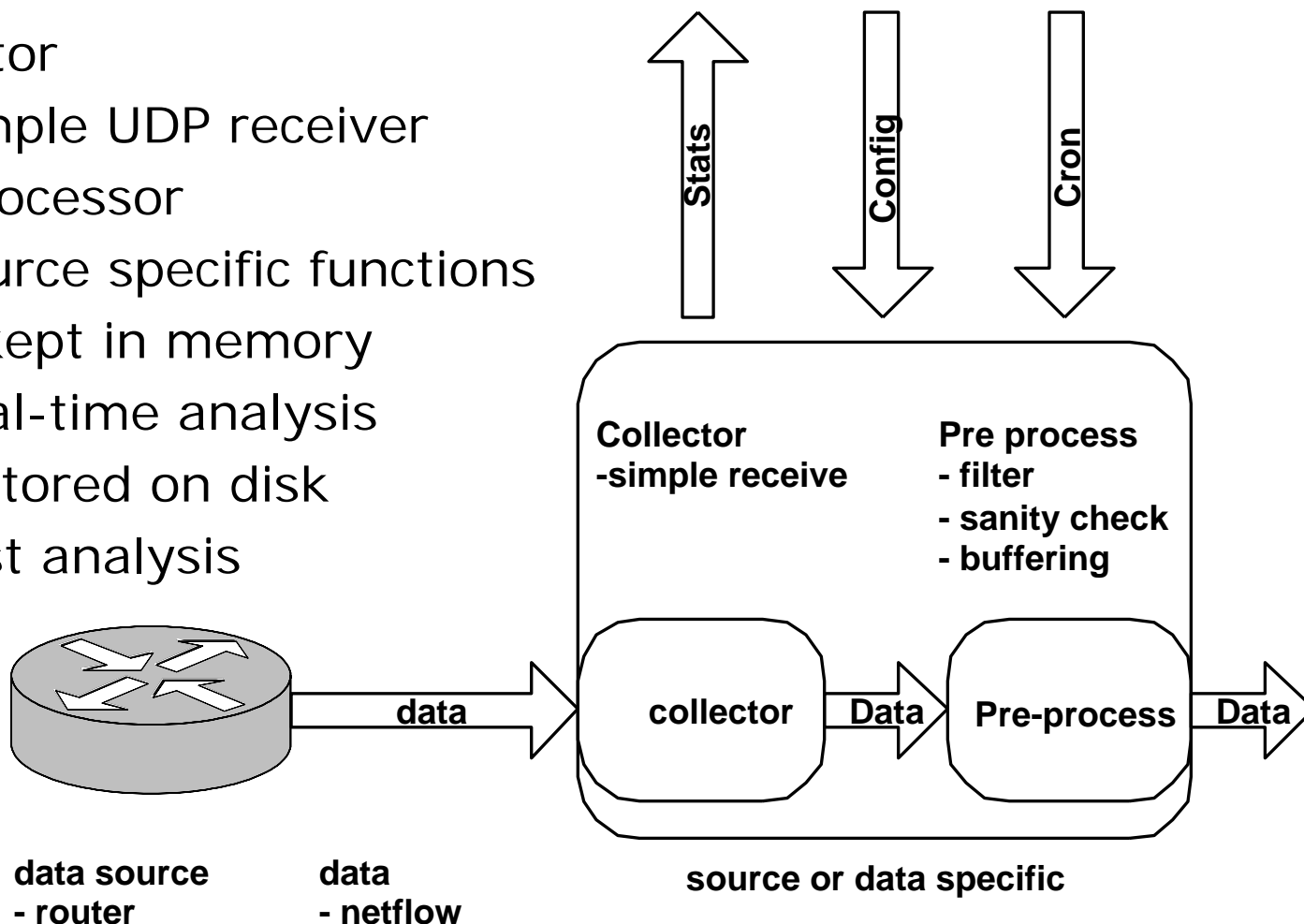
# Some specs of the new NERD

- nerdd, analysis
  - boost libraries, MySQL database, php, plplot
- Netflow versions
  - V5 (tested)
  - V9 (IPFIX)
- Platforms tested
  - FreeBSD
  - Linux
- Apache Open Source Licence v2.0



# Software Architecture

- Collector
  - Simple UDP receiver
- Pre-processor
  - Source specific functions
- Data kept in memory
  - Real-time analysis
- Data stored on disk
  - Post analysis



# Real-time and post analysis

- Real time analysis
  - Rules can be used for 'real-time' analysis
    - A rule is a combination of filters, clusters and a threshold for some metric (e.g. number of flows)
  - Example of a rule
    - Filter "port=445", cluster "dst IP", threshold=1000 flows/min
  - Results in an alarm if a host receives more than 1000 flows/min on TCP port 445
  - Output formatting: alarm in database
  - Every x minutes the rules (1...n) are executed
- Post analysis
  - Executed at user request
  - Rules without threshold
  - Output formatting: flow-tools like text file, graphical output

# Functionality – Filters & Clusters

- Sample of Netflow data

src	prt	dst	prt
10.0.0.1	2000	10.0.0.2	23
10.0.0.3	1000	10.0.0.2	22
10.0.0.6	2000	10.0.0.2	22
10.0.0.1	1000	10.0.0.3	23
10.0.0.1	1000	10.0.0.3	23

- Example: filter “src port=2000”

src	prt	dst	prt
10.0.0.1	2000	10.0.0.2	23
10.0.0.6	2000	10.0.0.2	22

- Example: filter, cluster “dst port” & count flows

prt	# of flows
22	1
23	1

# Real-time analysis - configuration

The screenshot shows the NERD configuration interface. At the top, the logo for NERD (Network Emergency Responder & Detector) is visible. Below the logo, there are navigation tabs: Alarms, Analysis, and Settings (which is currently selected). There are also icons for search, help, and information.

## Rules for real-time analysis

On the left side, there are configuration options for the source and timing:

- Source: nerdd memory
- timeIntervalSec: 300
- sleepTimeSec: 200

Two rules are defined:

- Rule1:** Filtered by destination IP address (ipv4\_dst\_addr) and destination port (dst\_port). The filter expressions are: ipv4\_dst\_addr != [redacted], dst\_port != 53, and dst\_port != 80.
- Rule2:** Filtered by source IP address (ipv4\_src\_addr) and source port (src\_port). The filter expressions are: ipv4\_src\_addr != [redacted], src\_port != 53, and src\_port != 80.

Each rule is associated with a cluster:

- Cluster1:** Associated with Rule1. It has a count of flows and a threshold of 6000.
- Cluster2:** Associated with Rule2. It has a count of flows and a threshold of 6000.

At the bottom, there are buttons for "Reset" and "Save Changes".

# Alarms

NERD  
Network Emergency Responder & Detector

Alarms
Analysis
Settings
✖
?
i

... 1 2 3 4 5 6 7 8 9 10 ...

Starttime	Stoptime ↓	Rulename	Alarm message (key, keyval, counterval)	Limit	Cont.	Analyse
03-Sep-2005 11:52:15	06-Sep-2005 13:13:17	rule5	<b>ipv6_dst_addr ff02:</b> ...	1	Yes	Analyse
06-Sep-2005 08:14:05	06-Sep-2005 13:13:17	rule5	<b>ipv6_dst_addr 2001:</b> ... <b>has 10 flows.</b>	1	Yes	Analyse
06-Sep-2005 11:35:43	06-Sep-2005 13:04:53	rule5	<b>ipv6_dst_addr ff02:</b> ...	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 13:04:53	rule5	<b>ipv6_dst_addr fe80:</b> ... <b>as 2 flows.</b>	1	No	Analyse
06-Sep-2005 12:51:28	06-Sep-2005 13:04:53	rule5	<b>ipv6_dst_addr 2001:</b> ... <b>has 6 flows.</b>	1	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	<b>ipv4_dst_addr 130:</b> ... <b>08 flows.</b>	800	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	<b>ipv4_dst_addr 145:</b> ...	800	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	<b>ipv4_dst_addr 145:</b> ... <b>939 flows.</b>	800	No	Analyse
06-Sep-2005 12:43:02	06-Sep-2005 12:48:02	rule5	<b>ipv6_dst_addr 2001:</b> ... <b>has 4 flows.</b>	1	No	Analyse
06-Sep-2005 12:43:02	06-Sep-2005 12:48:02	rule5	<b>ipv6_dst_addr fe80:</b> ... <b>as 4 flows.</b>	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 12:31:13	rule5	<b>ipv6_dst_addr 2001:</b> ... <b>has 11 flows.</b>	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 12:31:13	rule5	<b>ipv6_dst_addr fe80:</b> ... <b>as 5 flows.</b>	1	No	Analyse
06-Sep-2005 11:48:23	06-Sep-2005 12:14:22	rule4	<b>ipv4_dst_addr 130:</b> ... <b>03 flows.</b>	800	No	Analyse
06-Sep-2005 11:52:33	06-Sep-2005 12:14:22	rule5	<b>ipv6_dst_addr 2001:</b> ... <b>has 4 flows.</b>	1	No	Analyse
06-Sep-2005 12:00:58	06-Sep-2005 12:14:22	rule5	<b>ipv6_dst_addr fe80:</b> ... <b>as 7 flows.</b>	1	No	Analyse

Search  in keyval Search

Delete alarms older than 7 days Delete

# Analysis – IPv4

The screenshot displays a network analysis tool interface. At the top, a graph titled "cluster3" shows the distribution of flows over time. The y-axis is labeled "flows" and ranges from 0.0 to 1.0. The x-axis is labeled "dst\_port" and ranges from 36000 to 60000. The graph shows several vertical red lines representing individual flows, with a higher density between 48000 and 51000. The period is specified as "2005-09-06 12:38:52 - 2005-09-06 12:48:03".

Below the graph is a "Debug Info" button. The main interface is divided into several sections:

- NERD-flow archive:** A dropdown menu set to "sampled (100)".
- Flow Statistics:**

First flow:	04-Sep-2005 23:27:23
Last flow:	11-Sep-2005 15:54:41
# flows:	55117147
Avg flow/s:	95
- Filter:** A section with an "Add Expression" button and two filter rules:
  - ipv4\_dst\_addr = [value]
  - timestamp\_arrival > 06-Sep-2005 12:38
  - timestamp\_arrival < 06-Sep-2005 12:48
- Cluster List:** A list of clusters with their respective fields and control buttons:
  - Cluster0: Del, Add field, ipv4\_src\_addr
  - Cluster1: Del, Add field, ipv4\_dst\_addr
  - Cluster2: Del, Add field, src\_port
  - Cluster3: Del, Add field, dst\_port
- Buttons:** "Reset" and "Analyse" buttons at the bottom left, and "add new cluster" at the bottom right.

# Analysis – IPv6

NERD  
Network Emergency Responder & Detector

Alarms **Analysis** Settings

Back

```
# --- ---- Report Information --- ----
# build-version: 1
# Cluster name: cluster0
#
# Description:
# Threshold: 0
# timeFirst:2005-09-06 08:14:05
# timeLast:2005-09-06 13:13:18
# recn: ipv6_src_addr,flows

2001:610:510:0:0:0:0:0 = 5
2001:610:508:0:0:0:0:0 = 2
```

Back

NERD  
Network Emergency Responder & Detector

Alarms **Analysis** Settings

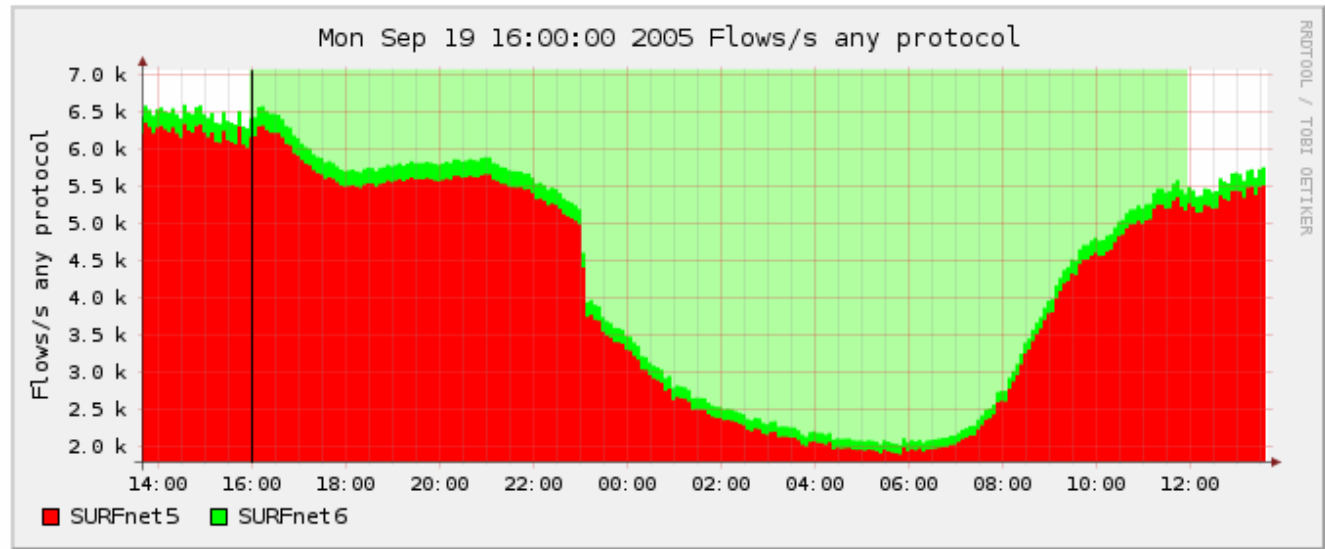
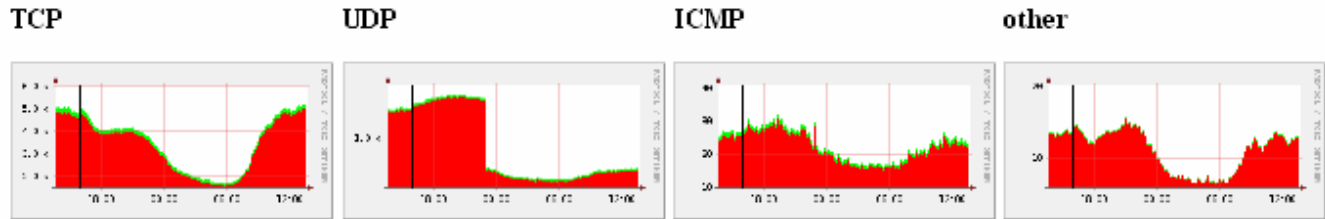
Back

```
# --- ---- Report Information --- ----
# build-version: 1
# Cluster name: cluster0
#
# Description:
# Threshold: 0
# timeFirst:2005-09-06 08:14:05
# timeLast:2005-09-06 13:13:18
# recn: ipv6_src_addr,flows

2001:610:510:0:0:0:0:0 = 398
2001:610:508:110:0:0:0:0 = 123
2001:610:0:800b:0:0:0:0 = 68
fe80::20a:41ff:fe60:3ee1 = 43
2001:610:1:400a:0:0:0:0 = 36
2001:610:508:192:0:0:0:0 = 36
2001:610:508:110:0:0:0:0 = 27
2001:610:0:800a:0:0:0:0 = 11
2001:610:1:80be:0:0:0:0 = 7
```

Back

# SURFnet6



Statistics timeslot Sep 19 2005 - 16:00 - Sep 20 2005 - 12:00

Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Traffic:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> SURFnet5	3.8 K/s	19.5 K/s	14.5 K/s	4.6 K/s	29.9 /s	337.4 /s	120.0 Mb/s	89.6 Mb/s	28.8 Mb/s	27.5 Kb/s	1.6 Mb/s
<input checked="" type="checkbox"/> SURFnet6	170.4 /s	663.9 /s	573.6 /s	84.8 /s	2.4 /s	3.1 /s	3.4 Mb/s	3.2 Mb/s	249.4 Kb/s	1.5 Kb/s	22.9 Kb/s

Display:  Sum  Rate



# Current Research and Development

- Geant2 JRA2
  - NERD is one of the monitoring toolsets
- LOBSTER project
  - Integration
- Student
  - Analysis and visualisation of worm behaviour
- Ph.D. from Vrije Universiteit (VU)
  - Interaction of Netflow and Full Packet inspection
- From application to framework
  - Other data sources, combining different data
  - Other data output

# Questions

- More information and download of NERD
  - [www.nerdd.org](http://www.nerdd.org)

