Zurich Research Laboratory

# IBM Aurora Flow-Based Network Profiling System

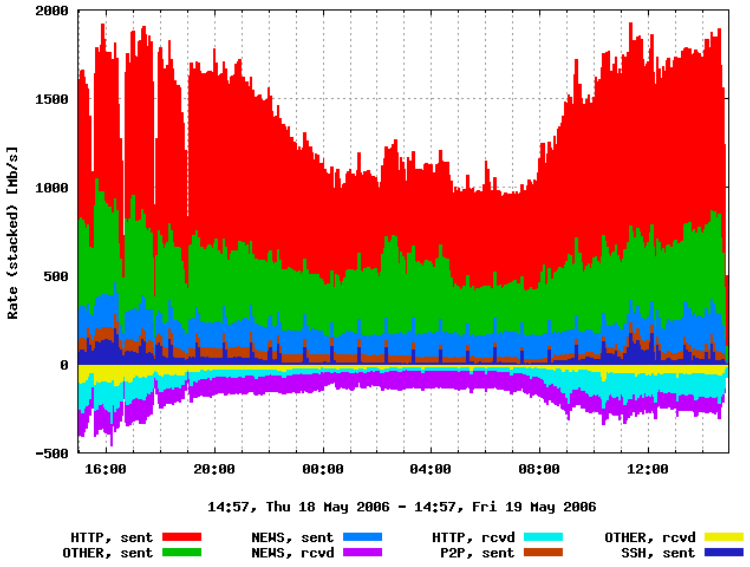
## Technical Aspects

http://www.zurich.ibm.com/aurora/
Email: <aurora@zurich.ibm.com>

# AURORA

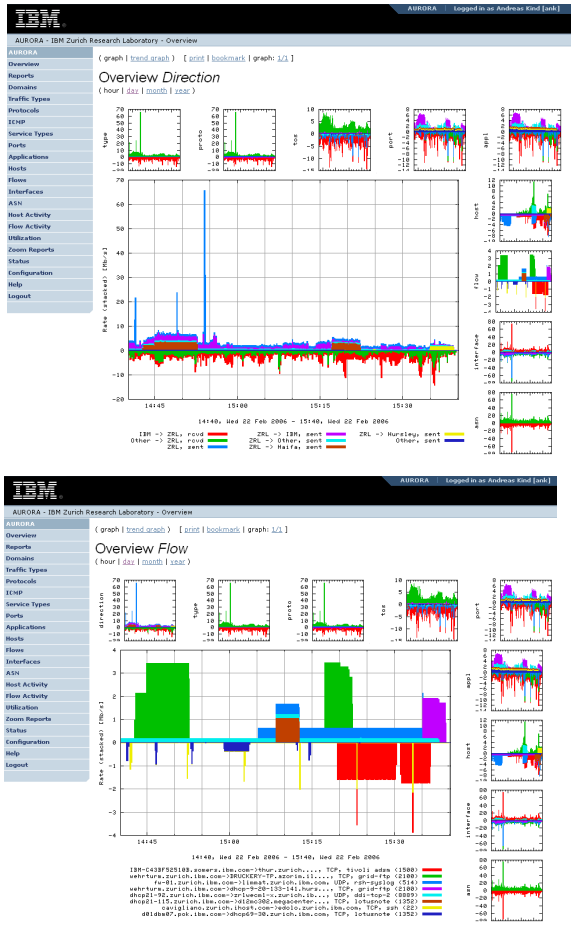
- R&D in IBM Zurich Research Laboratory
- Designed for high traffic sites
- Used in small businesses to very large sites
- Trying to find new innovative ways to represent network statistics
- A Research Project
  but commercially available (also as a ‘free’ trail, send an email for info)

# The name AURORA

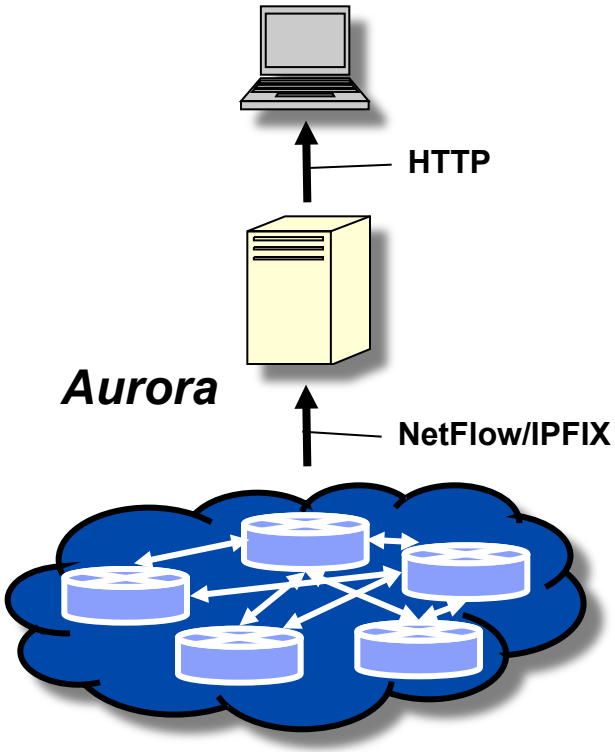


# Overview

- Understanding network traffic flows in IT infrastructures
- Benefits
  - Bandwidth usage by application, domains, hosts, ports, protocols, traffic types
  - Reduction of network outage times and identification of network congestion causes
  - Detection of long-term trends in network utilization
  - Understanding server dependencies to support IT infrastructure transition (eg, to UMI)
- Applied techniques
  - High performance aggregation database for large NetFlow volumes
  - Intelligent traffic pattern recognition



# NetFlow, IPFIX, sFlow




- NetFlow is de-facto standard by Cisco
- In future superseded by IETF IPFIX
- sFlow mostly similar to NetFlow
- SNMP is not appropriate for flow-based network profiling, but can be used to monitor other variables in an environment
- Flow definition

  A flow is a set of packets passing an observation point in the network during a certain time interval.

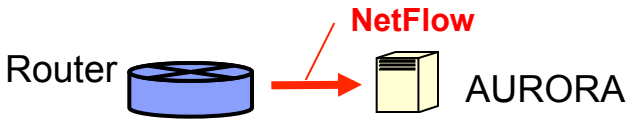
  All packets belonging to a particular flow have a set of common properties derived from the data contained in the packet and from the packet treatment at the observation point

NetFlow: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

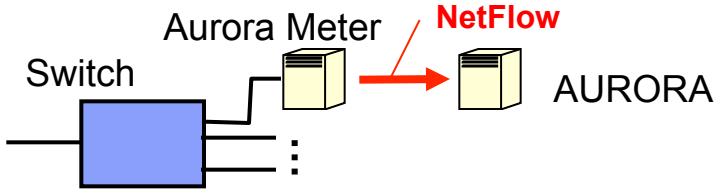
IPFIX: http://www.ietf.org/html.charters/ipfix-charter.html

# Operation Modes

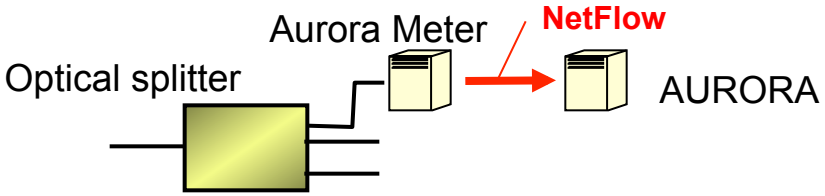
## Real-time mode; router NetFlow enabled



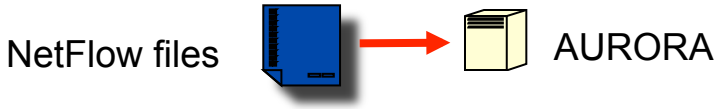

## Real-time mode; NetFlow probe via port mirroring




## Real-time mode; NetFlow probe via optical splitter




## Off-line mode; NetFlow probe



# Hespera

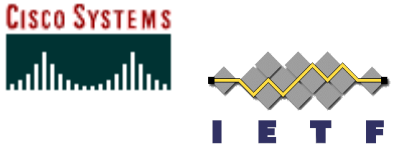
*In case your routers/ switches don't support (hardware) NetFlow.*

- *Pcap-based*
- *Collects packets*
- *Creates:*
  - *NetFlow v5/9*
  - *IPFIX*

# The NetFlow Scalability Challenge

| | *Flow Rate* | *NetFlow Volume* | *Data Volume* |
|---|---|---|---|
| ***Small Network*** | <100 flows/s | <260 MB/d | <260 MB/d |
| ***300 People Site*** | 300 flows/s | 780 MB/d | 200 GB/d |
| ***Single Core Router*** | 5’000 flows/s | 20 GB/d | 7 TB/d |
| ***Large ISP*** | >2 M flows/s | >4 TB/d | >2 PB/d |

# Feature Overview

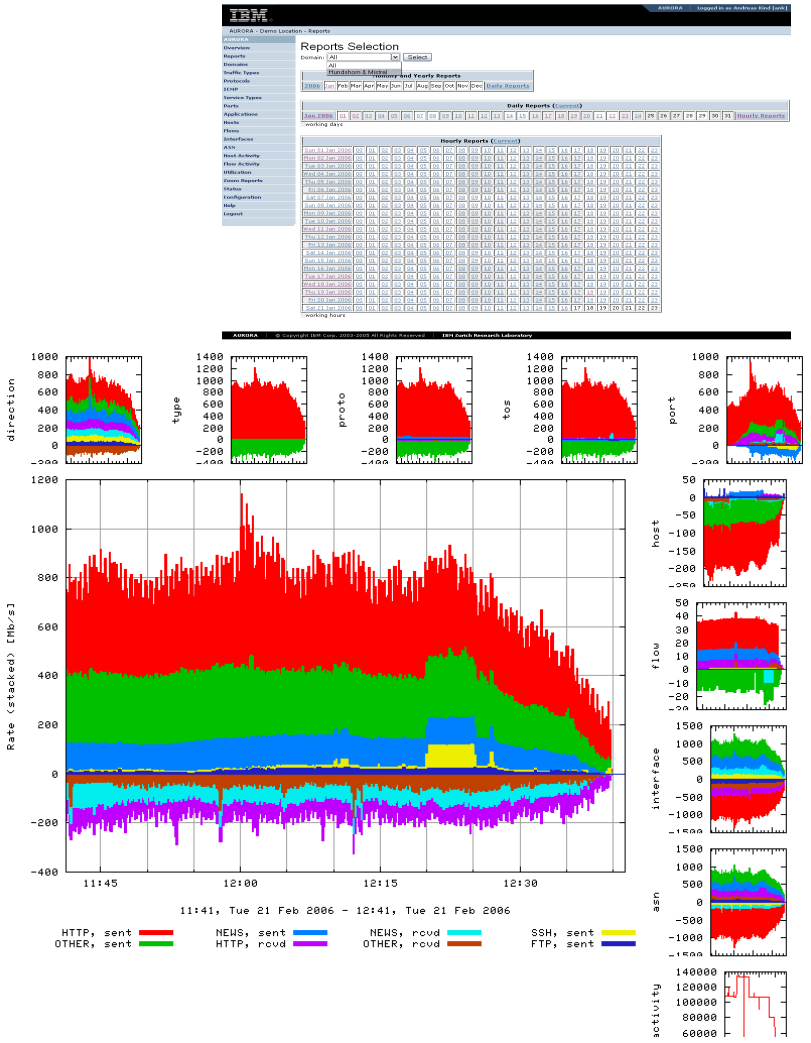



- NetFlow v1, v5, v6, v7, v8, v9, IETF IPFIX and sFlow collection, analysis, reporting
- Pre-generation of detailed reports in HTML, PDF, XML and TXT
  - Hourly, daily, monthly, yearly reporting periods
  - Utilization, domain, protocol, port, application, host, flow, ToS, ASN, and ICMP reports
  - Reports regarding average packet and flow statistics (eg, duration, volume)
- Ad-hoc zoom reports
- Support for very high flow rates
  - Example: ~40K flows/s on dual 2GHz server with 2GB memory, 150MB 5min flow files
  - Depends mostly on how much details one wants to see.
  - Distributed deployment with NetFlow or incremental database forwarding on
- Domain and site separation
- NetFlow forwarding
- IPv6 support at data and control plane
- GUI and language customization (Unicode-enabled)

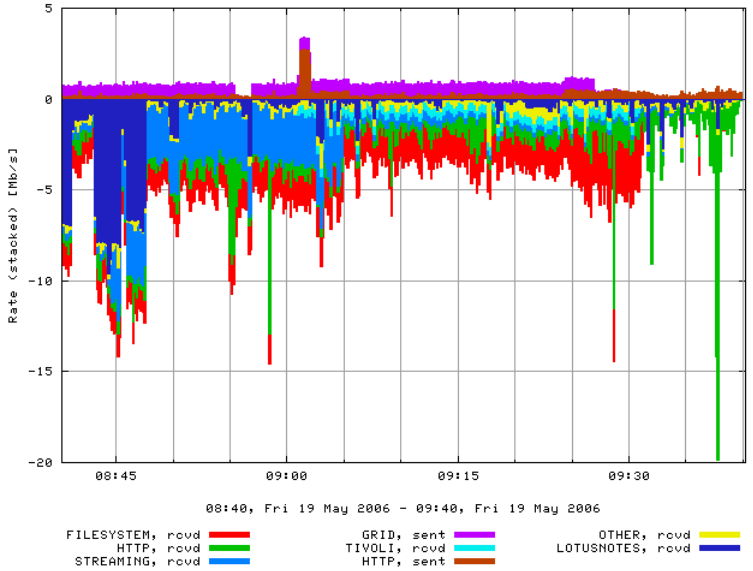
- Available for Linux; tested on Unix (AIX, Solaris, Open/FreeBSD, Mac OS X)

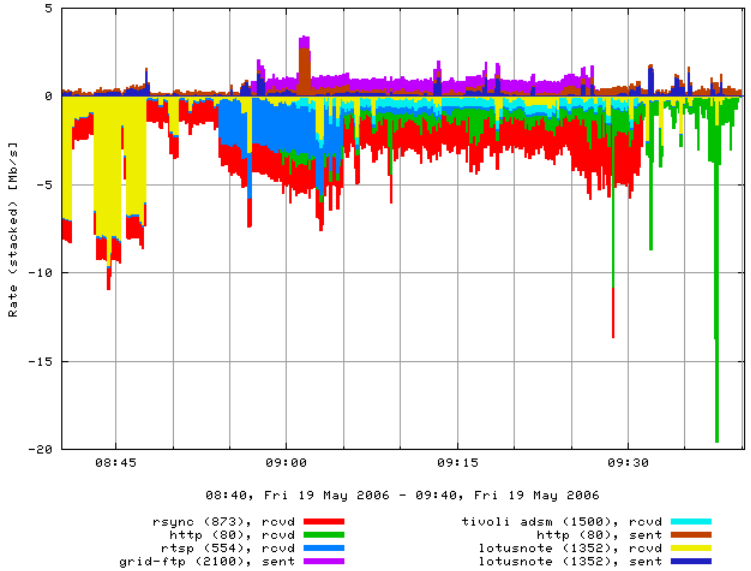
# Traffic Views and Standard Reports

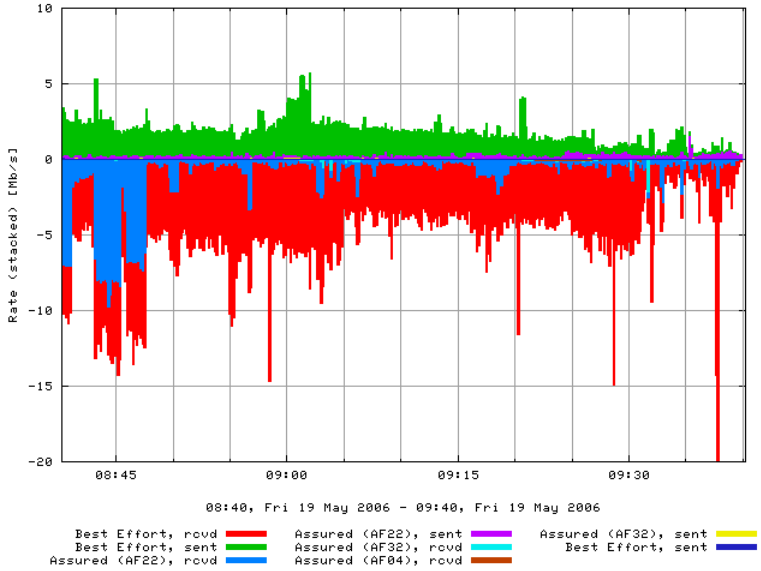
- Traffic views
  - Current hour/day/month/year
- Standard reports
  - Generated reports for fixed periods
  - HTML, PDF, XML, textual
- Filter reports
  - Filtered standard reports
- Zoom reports
  - Generated in real-time with user-defined filter
- Aspects in views and reports
  - Domains, protocols, hosts, ports, applications, service/traffic types, sessions, utilization

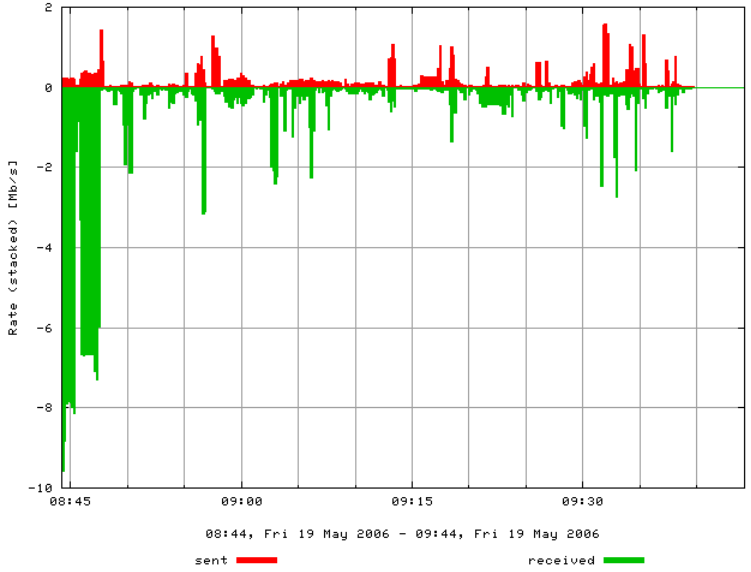


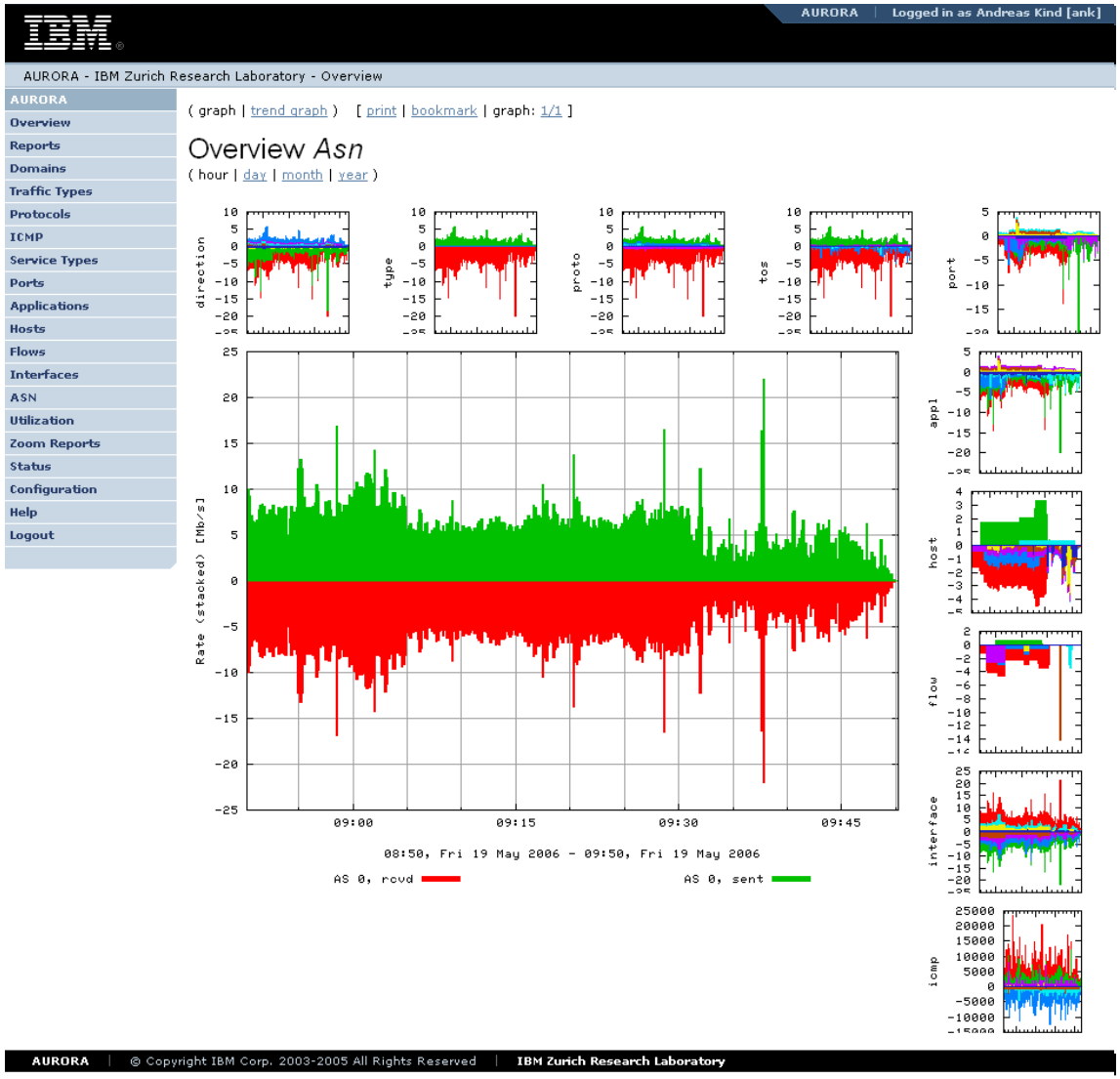
# Daily Direction and Flow Views

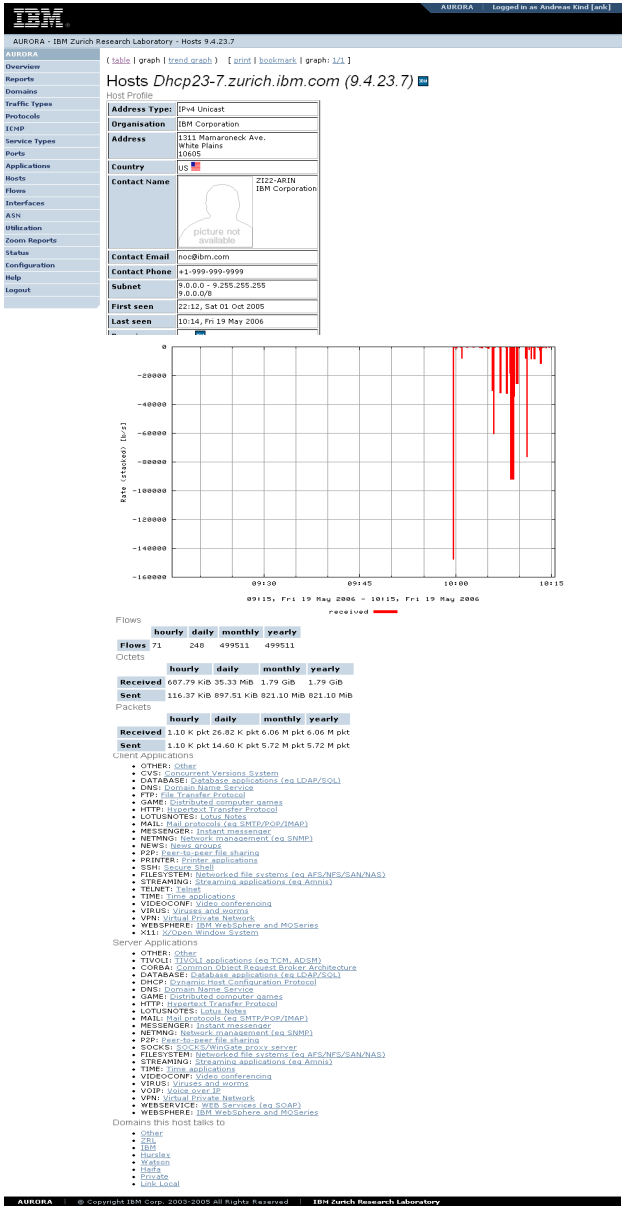



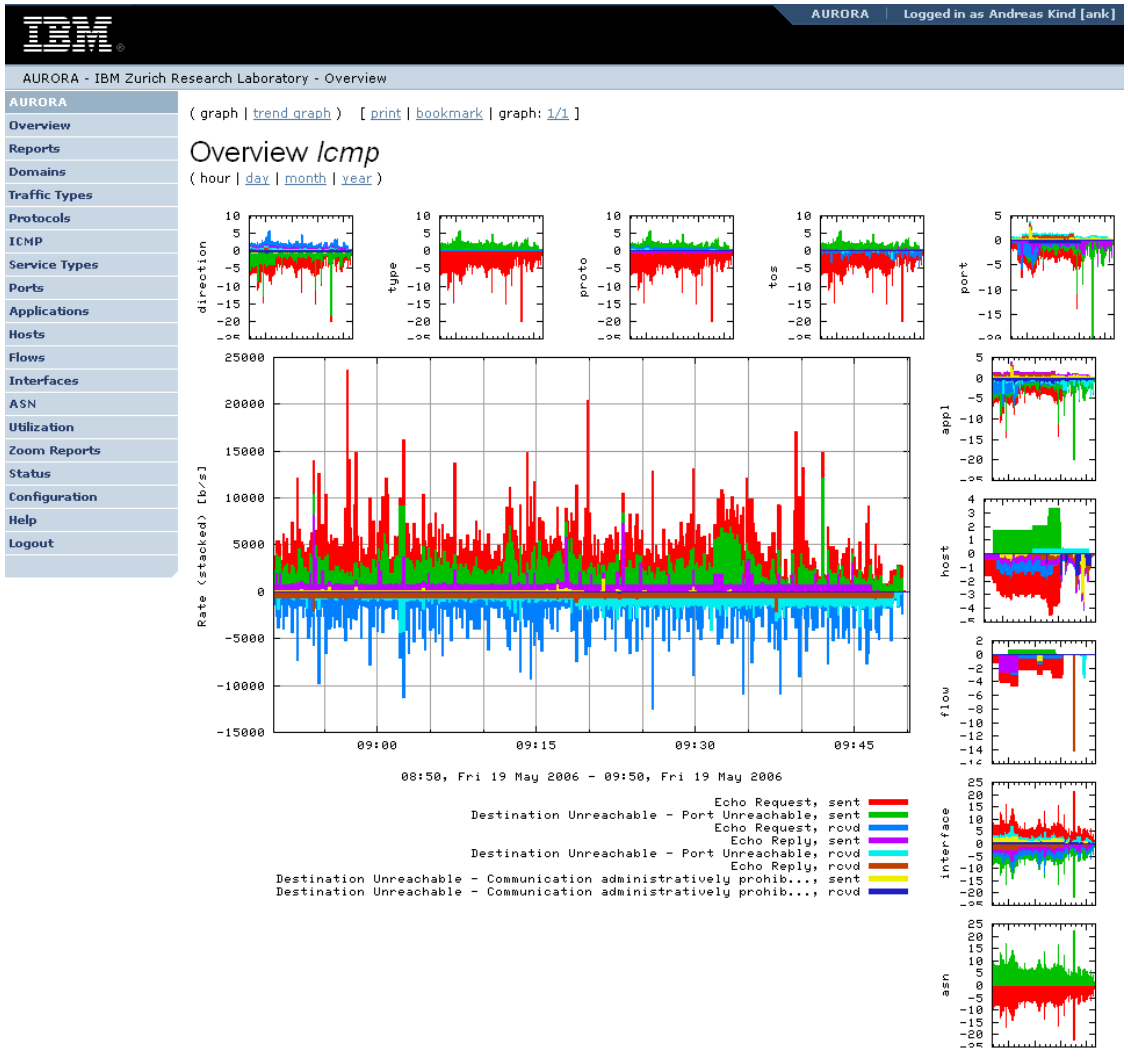



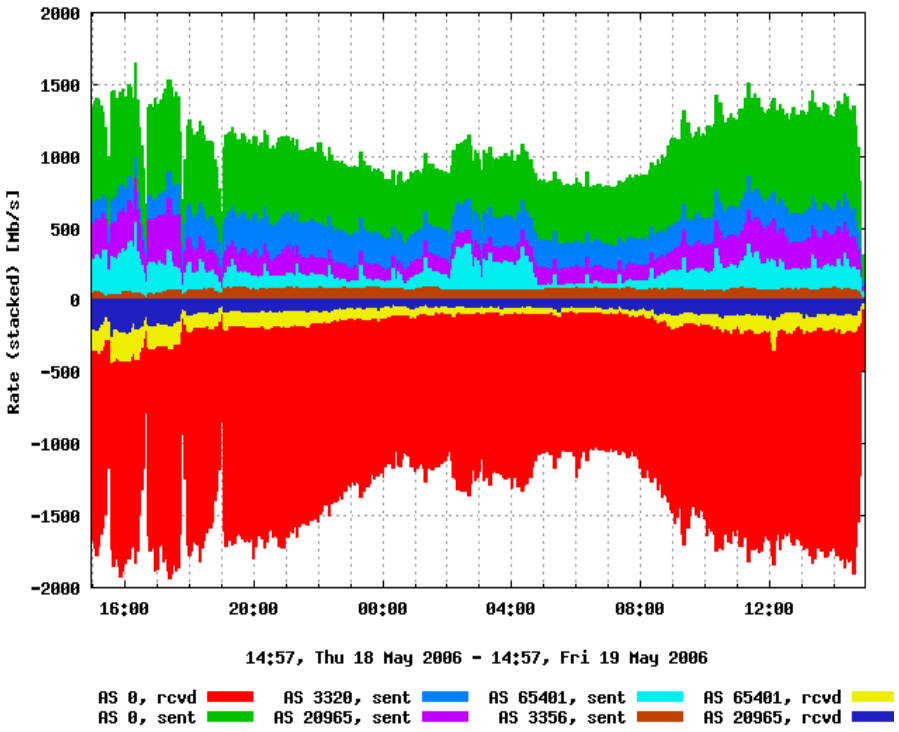



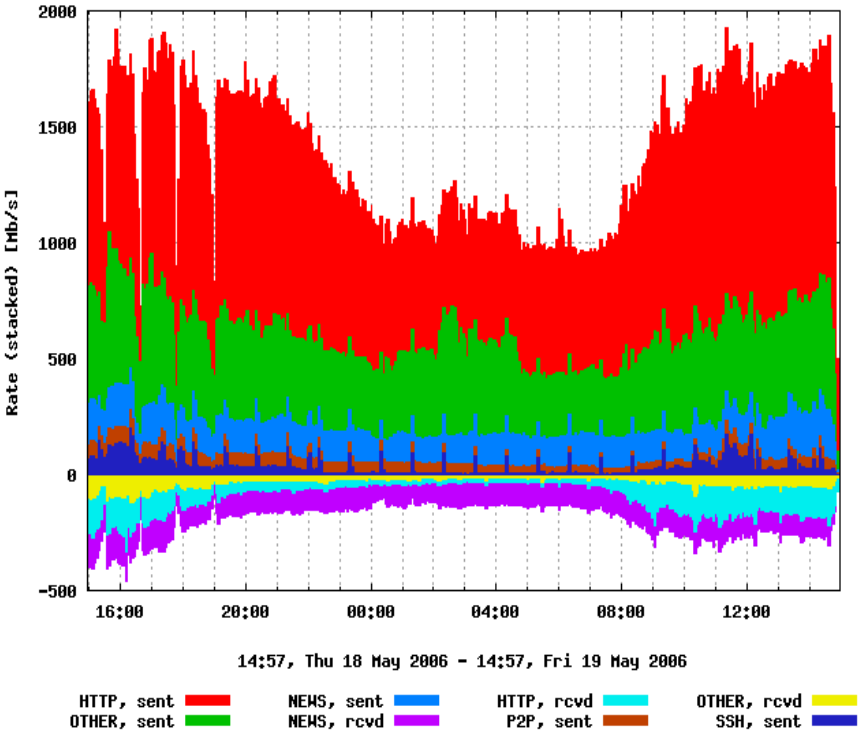


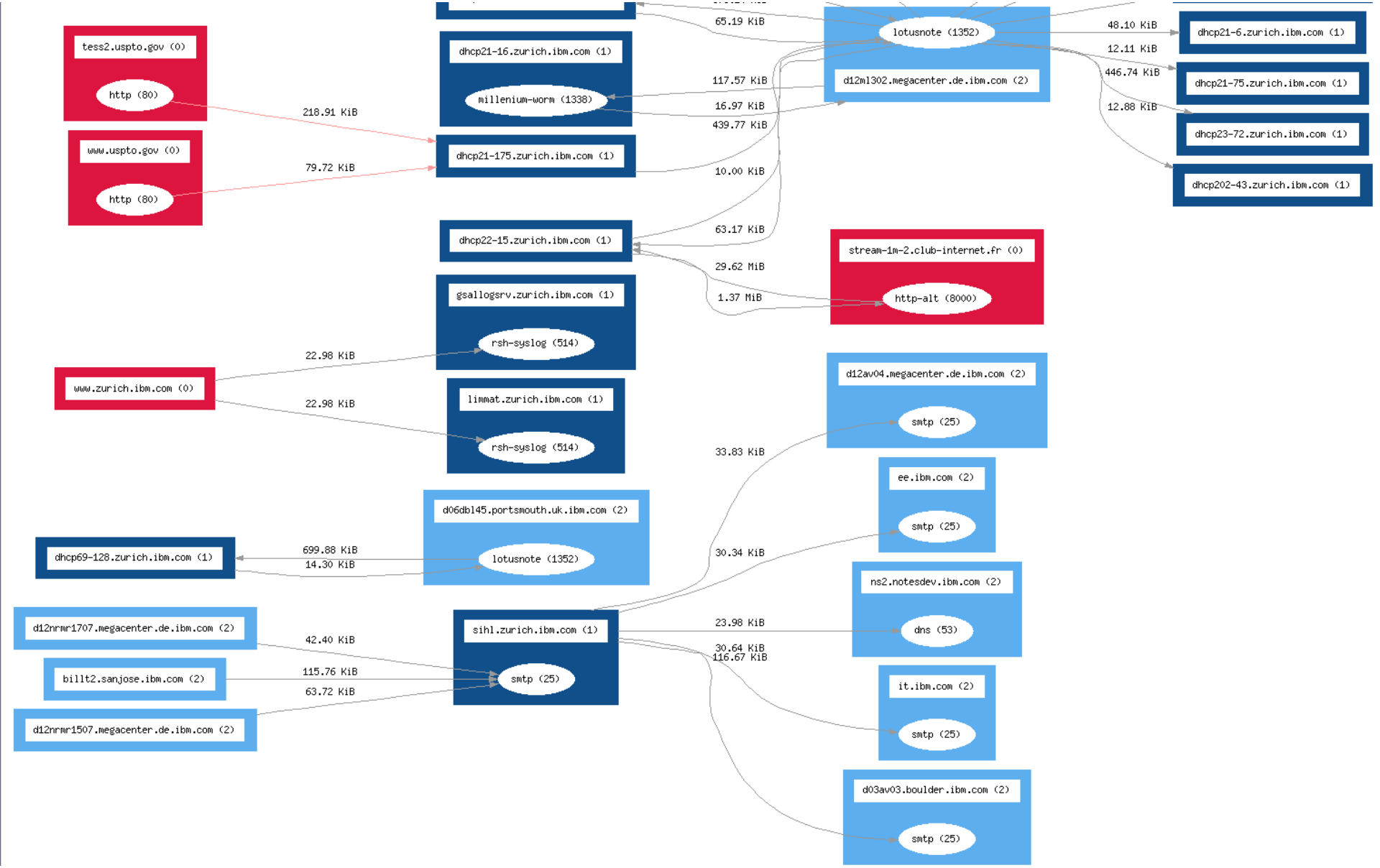


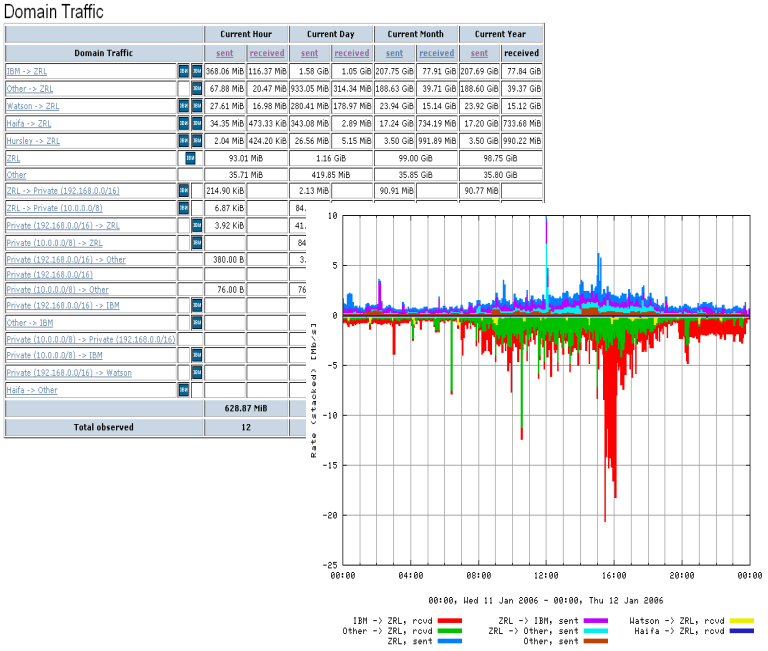
# Traffic Example at an ISP





# Domains




```
DOMAIN="IBM"
LOCAL=0
SUBNET="9.0.0.0/8"
FLAG=/aurora/flags/ibm.gif

DOMAIN="ZRL"
LOCAL=1
SUBNET="9.4.0.0/16 2001:620:20::/48"
FLAG=/aurora/flags/zrl.gif

DOMAIN="My First Servers"
FILTER="ipv4 either 10.10.19.184 or ipv4 either 10.10.19.204"
DOMAIN_MODE=FilterReport
REPORTS="direction type proto tos flow interface icmp"
FLAG=/aurora/flags/ibm.gif

DOMAIN="My First Router (IF 1)"
FILTER="ipv4 router 1@10.10.170.139"
REPORTS="direction proto port appl host"
```

# Filter specifics

```
<expr> = not <expr> |
         <expr> (and|or) <expr> |
         version (ipv4|ipv6) |
         (ipv6|ipv4) <dir_ip> [not] <prefix>[/<prefixlength>] |
         type [not] (unicast|multicast) |
         proto [<op>] <number> |
         (icmp|icmptype|icmpcode) <number> |
         port <dir> [<op>] <number> |
         app <name> |
         domain <dir> [<op>] <number> |
         asn [<op>] <number> |
         (packets|octets) [<op>] <number> |
         true | false |
         set (proto|port|app|domain|asn) <number> |
         trigger <name>

<dir> =  src | dst | both | either
<dir_ip> = <dir> | router | router_src | router_dst | nexthop
<op> = eq | == | ne | != | ge | >= | gt | > | more | le | <= | lt | < | less
```

```
# Filter on address range
ipv4 either 10.10.0.0/16

# Filter on http(s) traffic
port either 80 or port either 443

# Define http traffic domain
((ipv4 src 9.4.0.0/16 and set domain src 7) or true) and \
((ipv4 dst 9.4.0.0/16 and set domain dst 7) or true) or true

# Set application based on a source IP and port
ipv4 src 192.0.2.0/25 and port src 80 set app FOO

# Trigger an event on corrupted flows and drop these flows
not ((octets gt 200000000 or packets gt 20000000) and trigger HUGE_FLOW)
```

# Traffic Filter

- Used for …
  - Record modification rules (eg, set application, IP to domain mapping)
  - Standard filter reports
  - Event notification
  - Zoom reports
- Examples
  - Set application

    ```
    FILTER="ipv4 src 192.0.2.0/23 and port src 80 set app 5"
    ```

  - Aggregate to a single IP address

    ```
    FILTER="ipv4 src 192.0.2.0/23 and port src 80 set ipv4 src
    192.0.2.1"
    ```

  - Define LotusNotes cluster

    ```
    FILTER="app LOTUSNOTES and (ipv4 src 192.0.2.0/23 set dom
    src 1) or (ipv4 dst 192.0.2.0/23 set dom dst 1)"
    ```

# Filter Domains

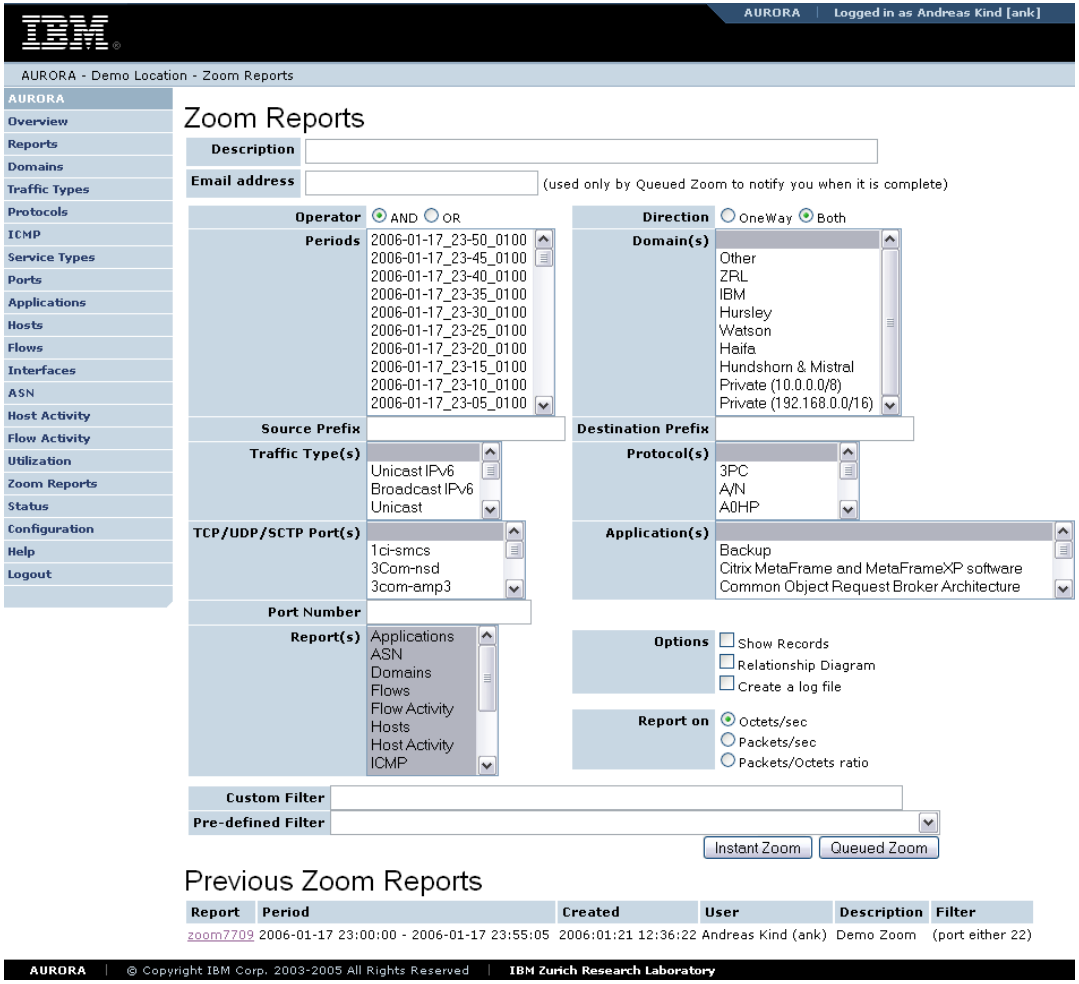
- Users can be bound to a filter domain

```
DOMAIN="My First Servers"
FILTER="ipv4 either 10.10.19.184 or ipv4 either 10.10.19.204"
DOMAIN_MODE=FilterReport
REPORTS="direction type proto tos flow interface icmp"
FLAG=/aurora/flags/ibm.gif

DOMAIN="My First Router (IF 1)"
FILTER="ipv4 router 1@10.10.170.139"
REPORTS="direction proto port appl host flow icmp"
```

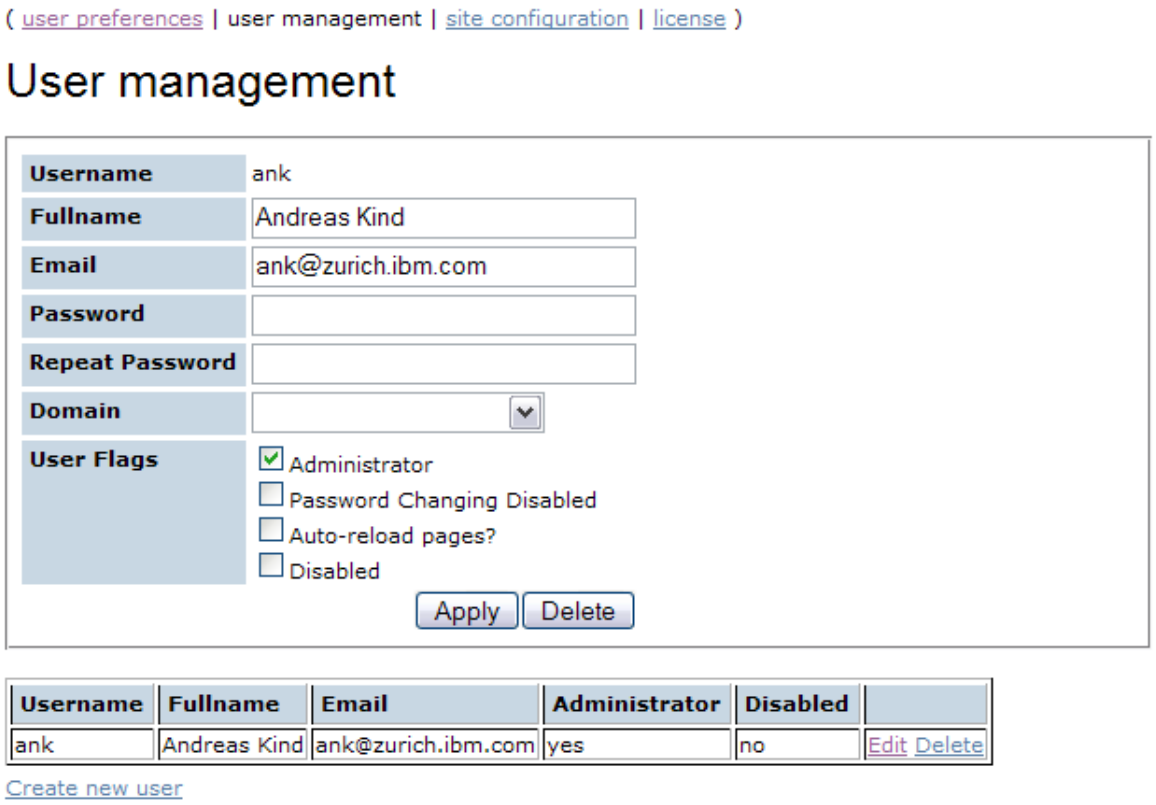
# Events

```
# Event target definition
eventtarget SYSLOG syslog info
eventtarget TEC tec udp://foo.zurich.ibm.com

# Event definition
event HUGE_FLOW        description    "Very large flow"
event HUGE_FLOW        threshold      0
event HUGE_FLOW        period         0
event HUGE_FLOW        output         SYSLOG message "Huge
  Increase: T=%tag%@%offset% R=%source% F=%first% L=%last% S=%src%
  D=%dst% P=%protocol% O=%octets% p=%packets% T=%threshold%"

# Event filter
POST_FILTER="! ((octets gt 200000000 or packets gt 200000000) and
  trigger HUGE_FLOW)"
```

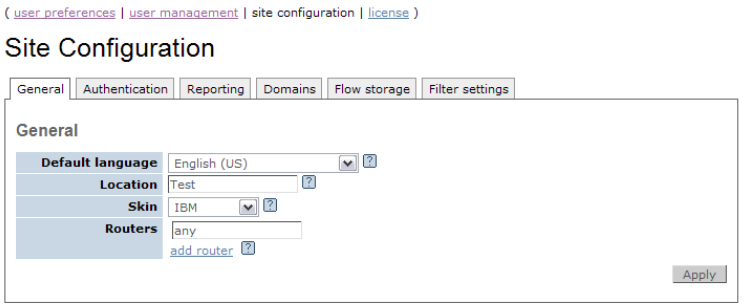
# Zoom Reports

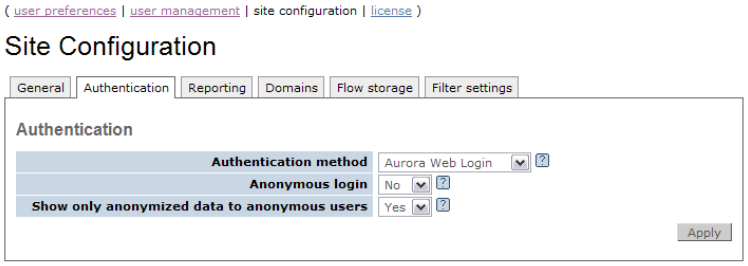


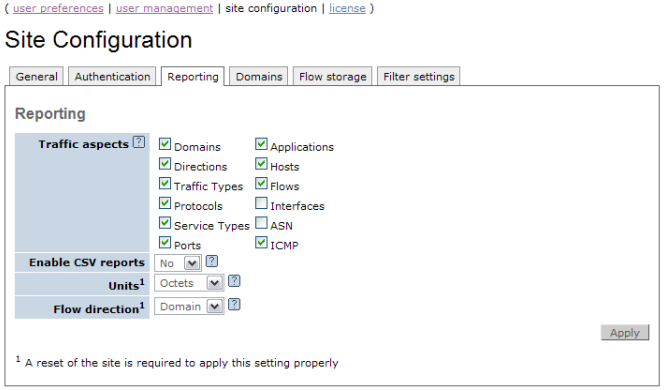
# User Management

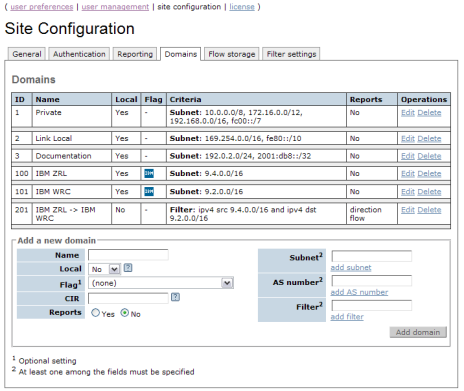


# Configuration



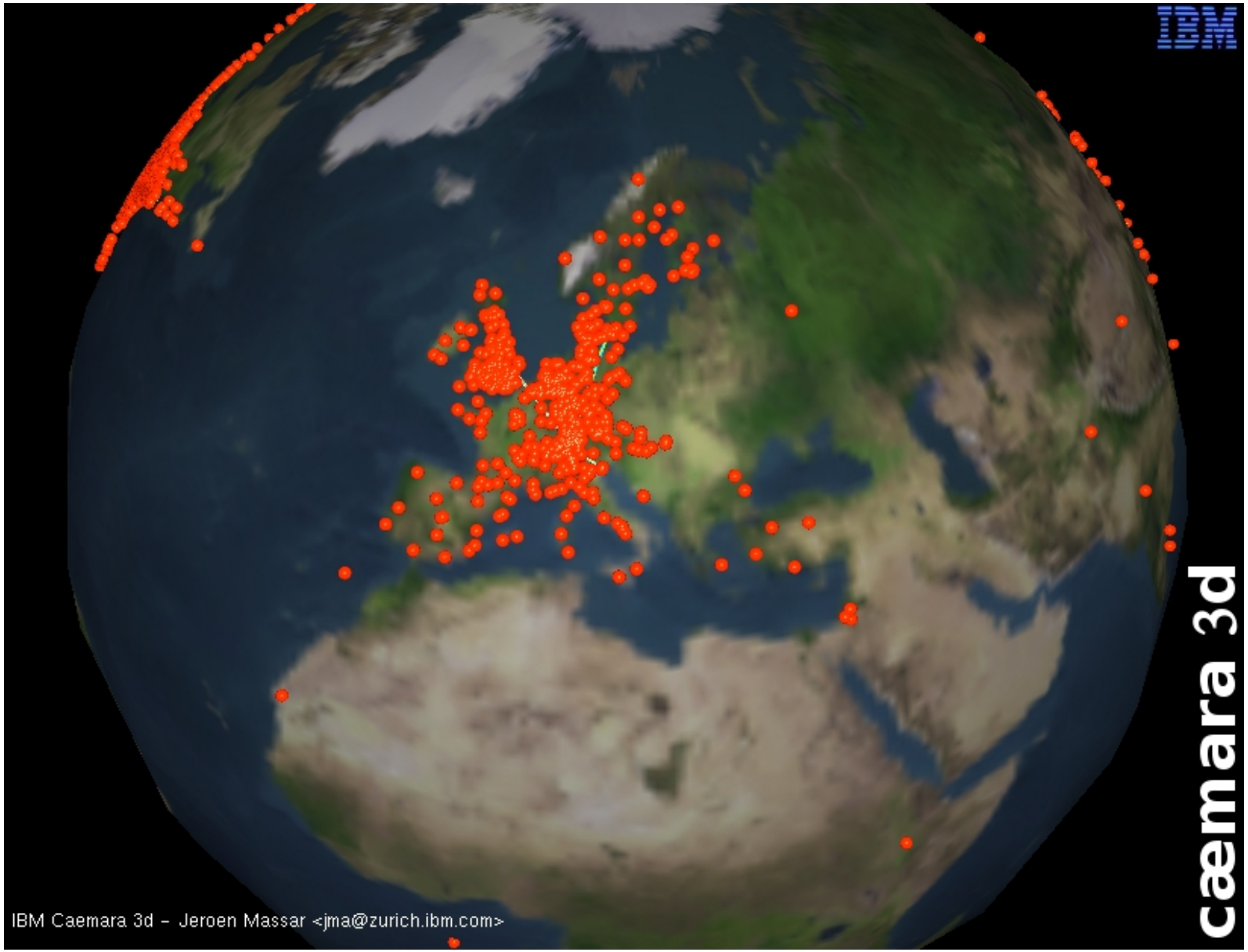



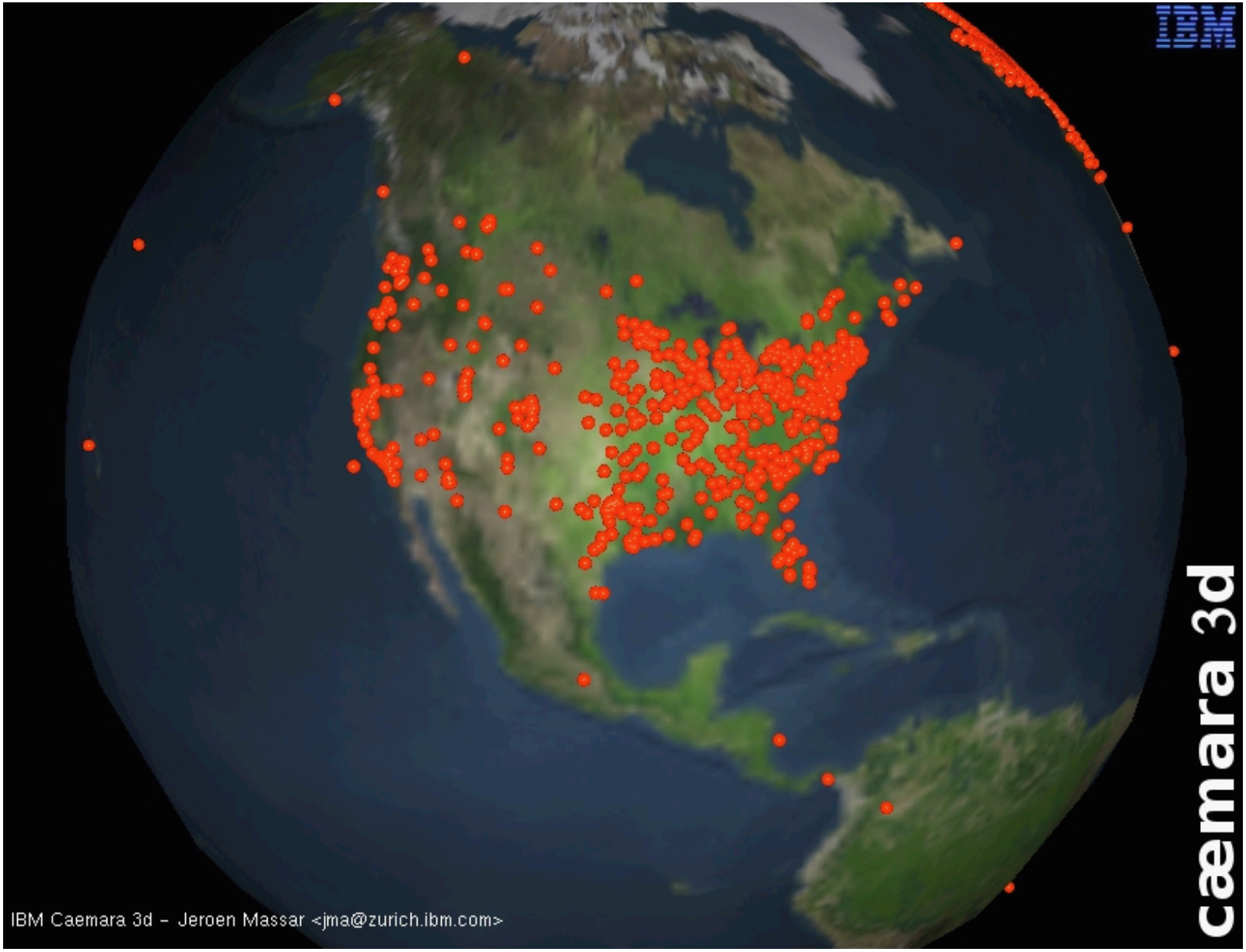



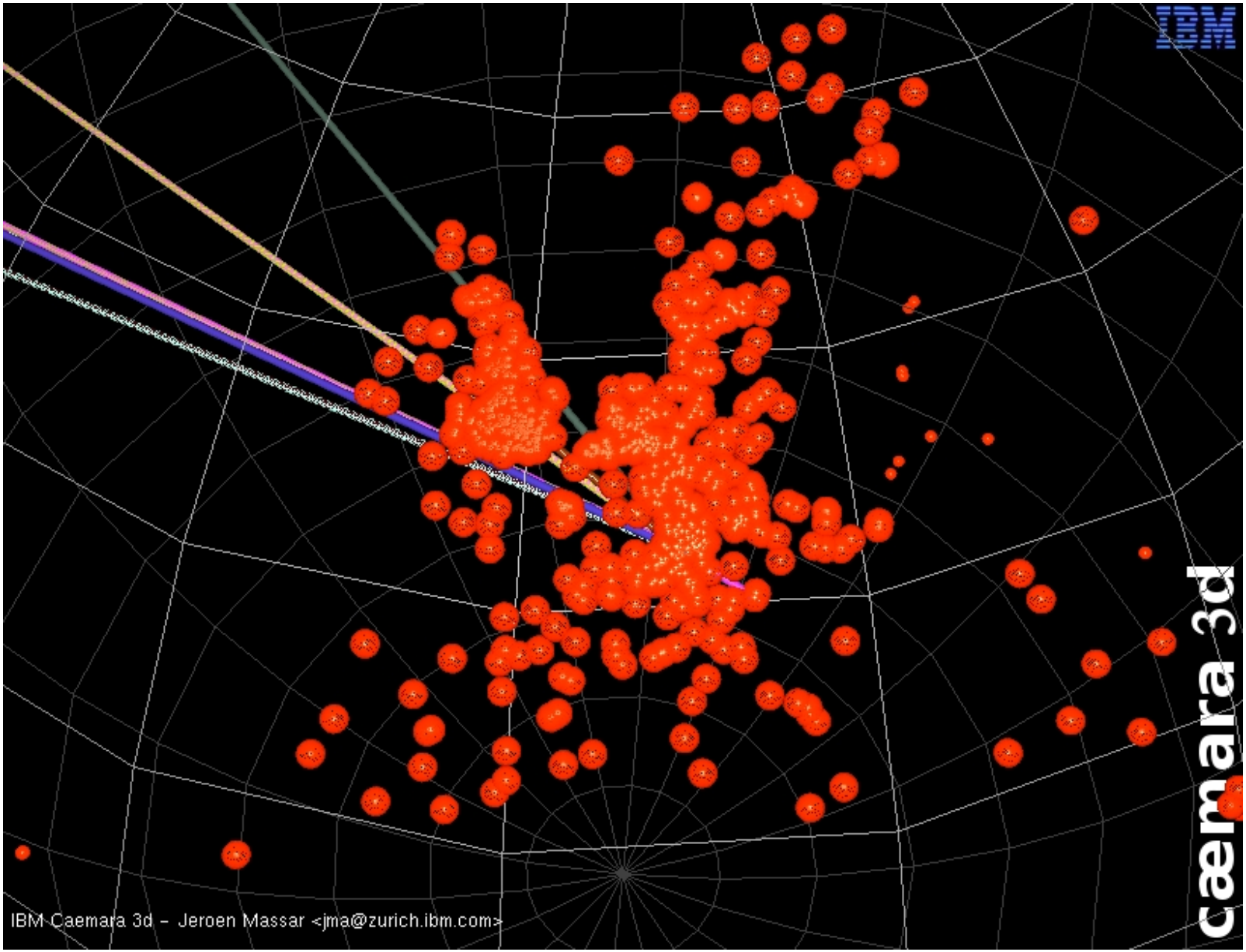



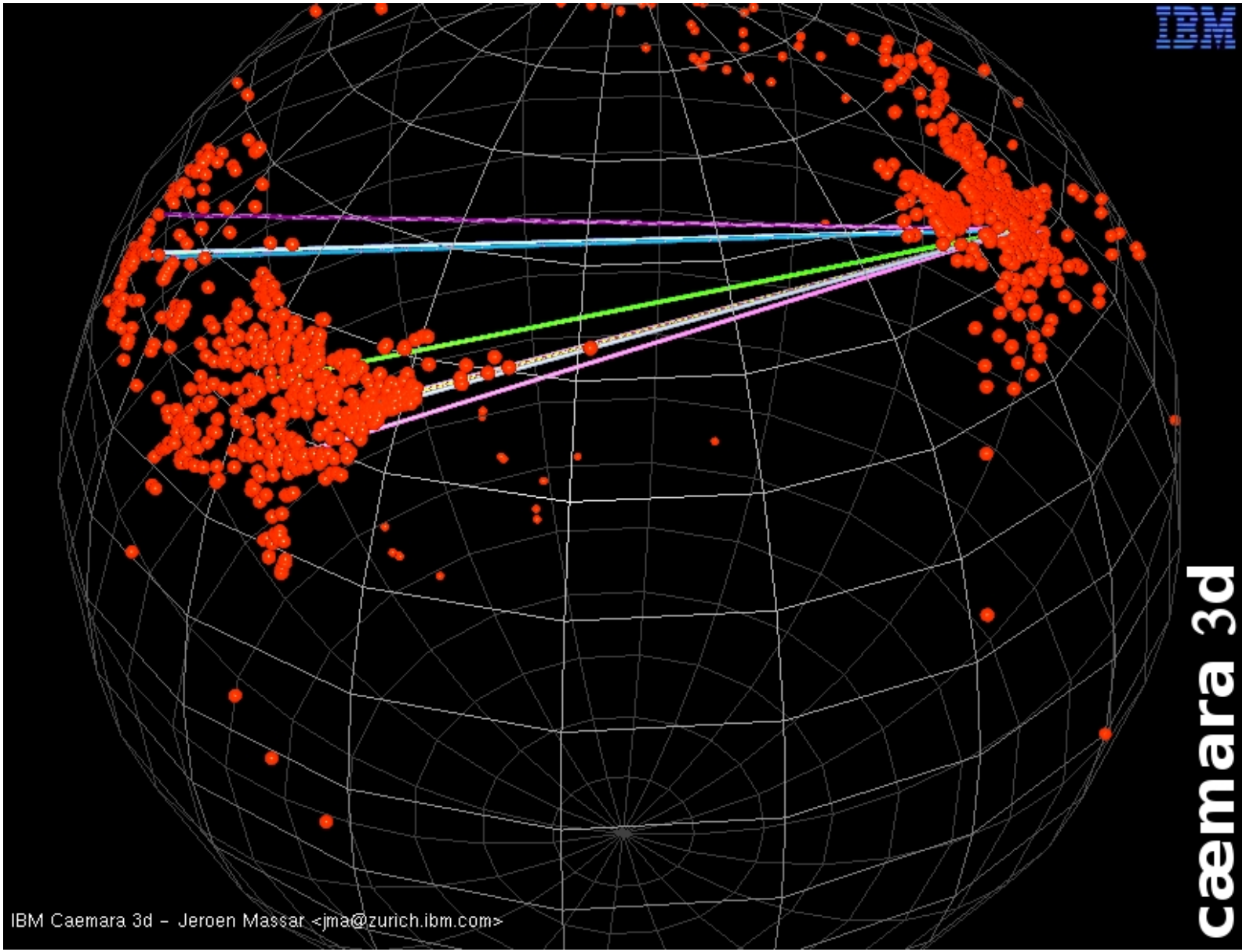
# Backend normal text files

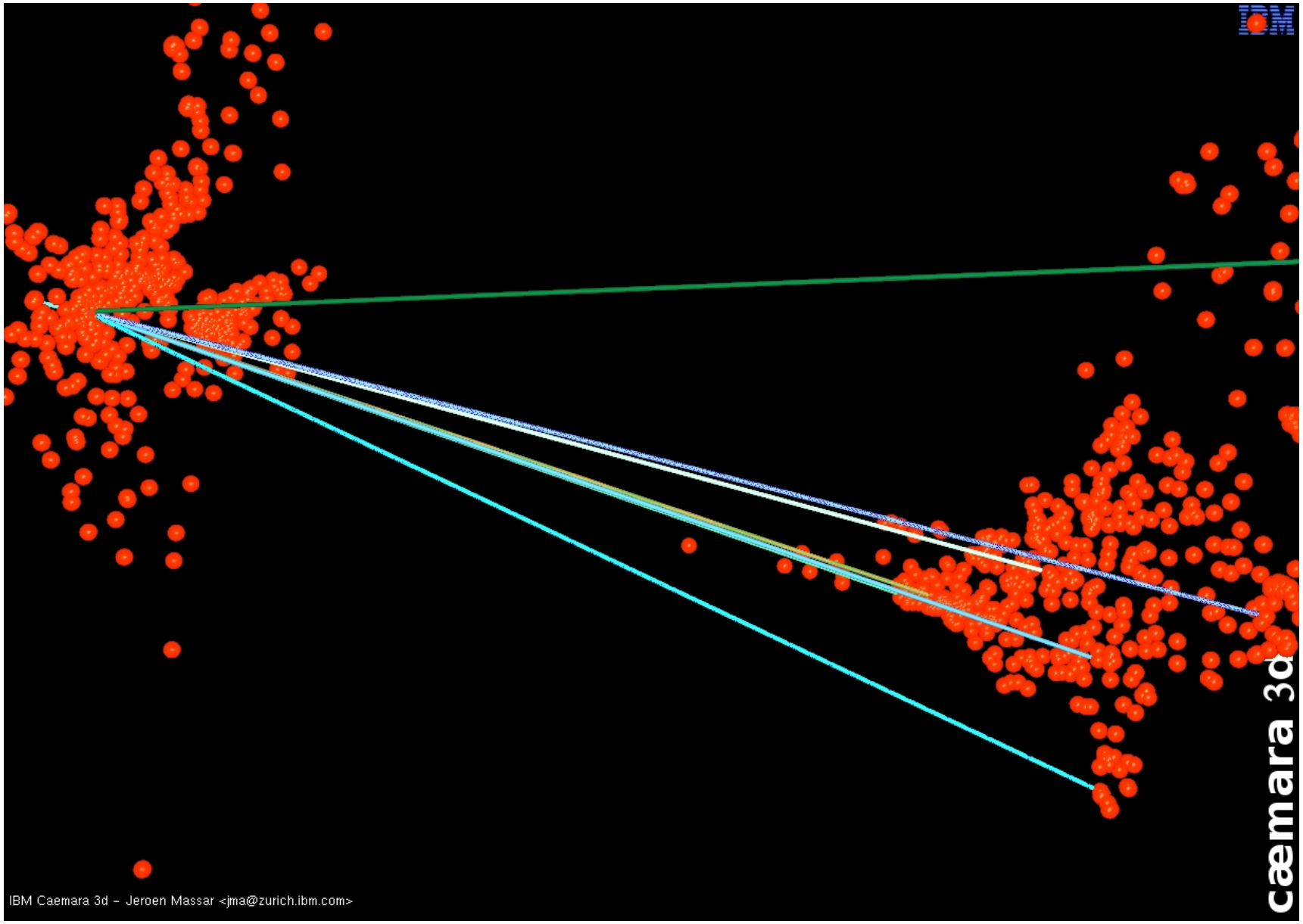
```
LOCATION="WAN Monitoring"
ROUTERS=any

LANGUAGE=english_us
SKIN=ibm

AUTH_METHOD=aurora

COLLECT=octets
REPORTS="domain direction type proto tos port appl host flow interface"

# Local Swiss Department A
DOMAIN="Department A"
ID=1
SUBNET="10.10.1.0/24"
LOCAL=1
FLAG=/aurora/flags/ch.gif

# Local Swiss Department B
DOMAIN="Department B"
ID=2
SUBNET="10.10.2.0/24"
LOCAL=1
FLAG=/aurora/flags/ch.gif

# Remote US Department C
DOMAIN="Department C"
ID=3
SUBNET="11.11.1.0/24"
LOCAL=0
FLAG=/aurora/flags/us.gif

# Remote German Department D
DOMAIN="Department D"
ID=4
SUBNET="11.11.2.0/24"
LOCAL=0
FLAG=/aurora/flags/de.gif

FLOWFILE_ZIP_PERIOD=86400
ZIP=bzip2
```









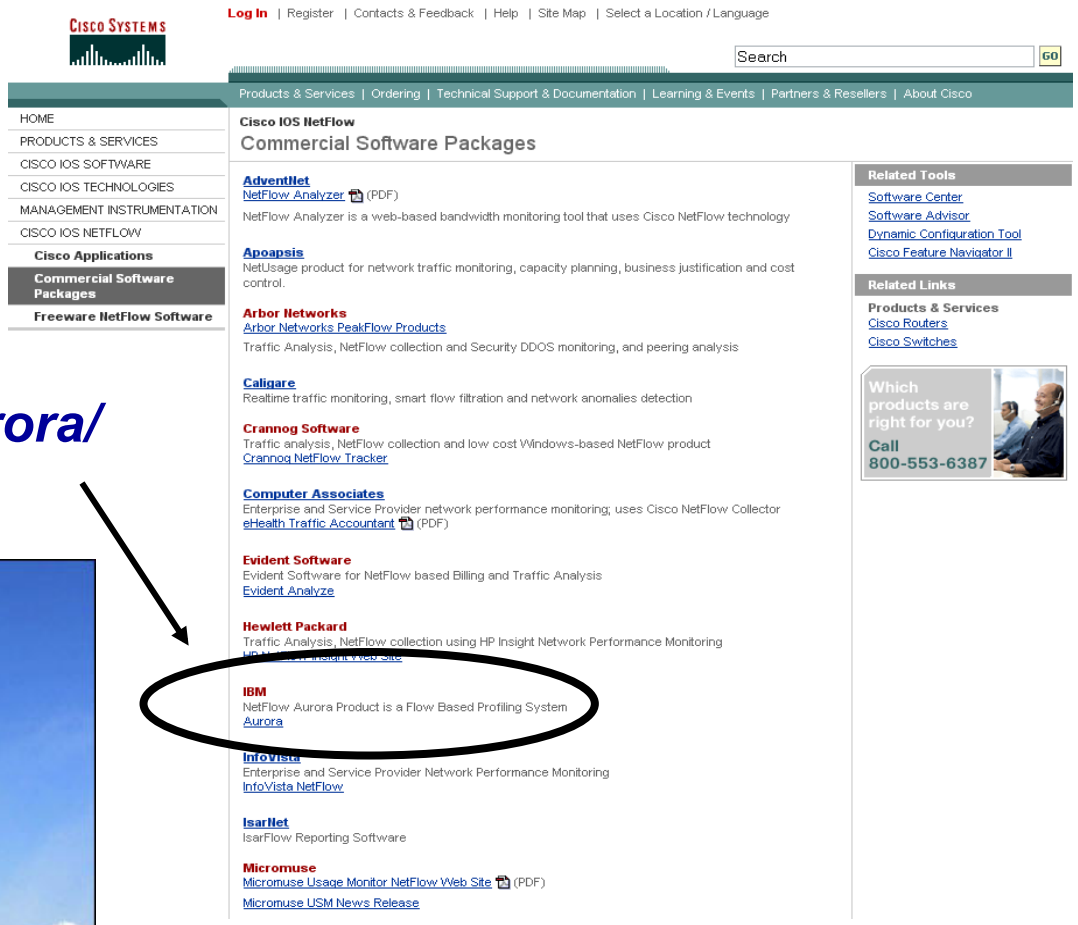


# Soon...

- BGP awareness
  - Where is my traffic going and where is it coming from
  - Helps in determining who to peer with
- Anomaly Detection
  - What traffic is not normal in my network
- New “Web2.0” interface

# Thanks!

**www.zurich.ibm.com/aurora/**




For more Information please, contact aurora@zurich.ibm.com