



Zurich Research Laboratory

# ***IBM Aurora Flow-Based Network Profiling System***

## ***Technical Aspects***

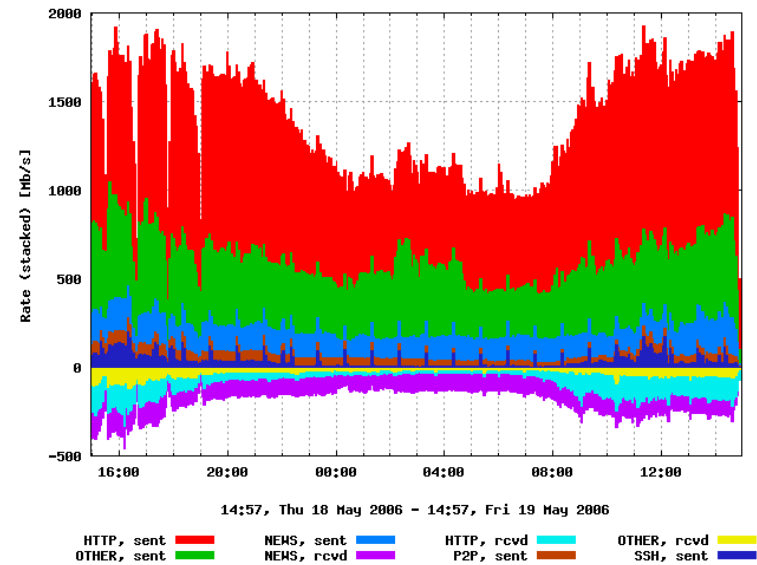
<http://www.zurich.ibm.com/aurora/>  
Email: <[aurora@zurich.ibm.com](mailto:aurora@zurich.ibm.com)>

# 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*

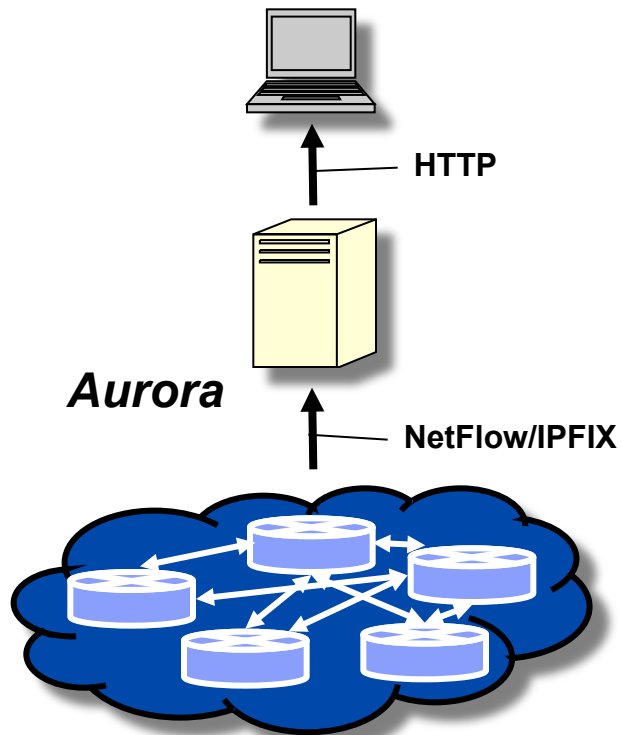


# Overview

- 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- In future superseded by IETF IPFIX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

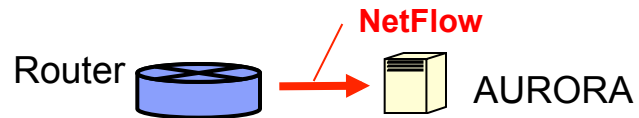
NetFlow: [http://www.cisco.com/en/US/products/ps6601/products\\_ios\\_protocol\\_group\\_home.html](http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html)

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

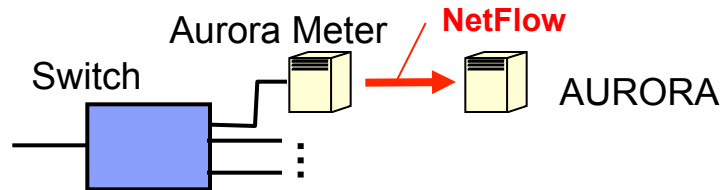


# Operation Modes

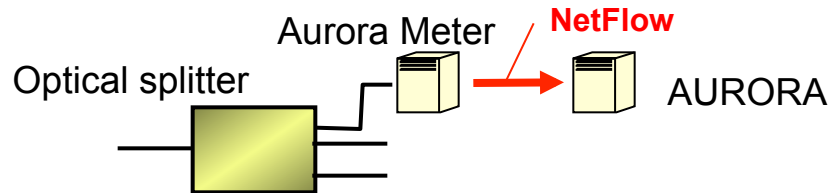
## Real-time mode; router NetFlow enabled



## 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*

```

ank@zannone:~
HesperaRemote controlling tcp://foo:hello@localhost using: flow top bytes
-----
Generic : [h]elp, [a]bout, [i]nterval, [c]ommand, [q]uit
Flow Top : [b]ytes, [p]ackets
Status : [I]nfo, [U]sage, [F]lows, [P]ackets, [T]hread, [D]rivers, [L]og
-----
201 Flow Top (bytes) hash version src-ip src-port dst-ip dst-port proto-num/prot
o-txt packets bytes
fb16c767 4 9.4.12.43 22 9.4.71.21 41098 6/tcp 1437 927486
d9335b07 4 9.4.68.163 22 9.4.70.54 1816 6/tcp 237 92094
22c6bfac 4 9.4.12.42 22 9.4.65.161 33408 6/tcp 285 50730
f8d2497f 4 9.4.12.45 22 9.4.71.21 41096 6/tcp 272 49404
e467a235 4 9.4.70.54 1816 9.4.68.163 22 6/tcp 197 15780
d414d616 4 9.4.64.245 0 224.0.0.13 0 103/pim 200 12532
625a32da 4 9.4.64.246 1985 224.0.0.2 1985 17/udp 201 12462
d2a9515a 4 9.4.64.246 0 224.0.0.13 0 103/pim 76 4796
2c850dec 4 9.4.12.44 22 9.4.71.21 59517 6/tcp 36 2664
9d7943ff 6 fe80::2d0:ff:fe8a:400 0 fe80::2d0:ff:fe8a:400 0 103/pim 14 1904
99391ccf 6 fe80::2d0:ff:fe83:a000 0 fe80::2d0:ff:fe83:a000 0 103/pim 12 1632
bd3ee506 4 9.4.64.245 1985 224.0.0.2 1985 17/udp 18 1114
7f3bdd76 4 9.4.70.19 137 9.4.71.255 137 17/udp 7 644
202 Complete...

```

# *The NetFlow Scalability Challenge*

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



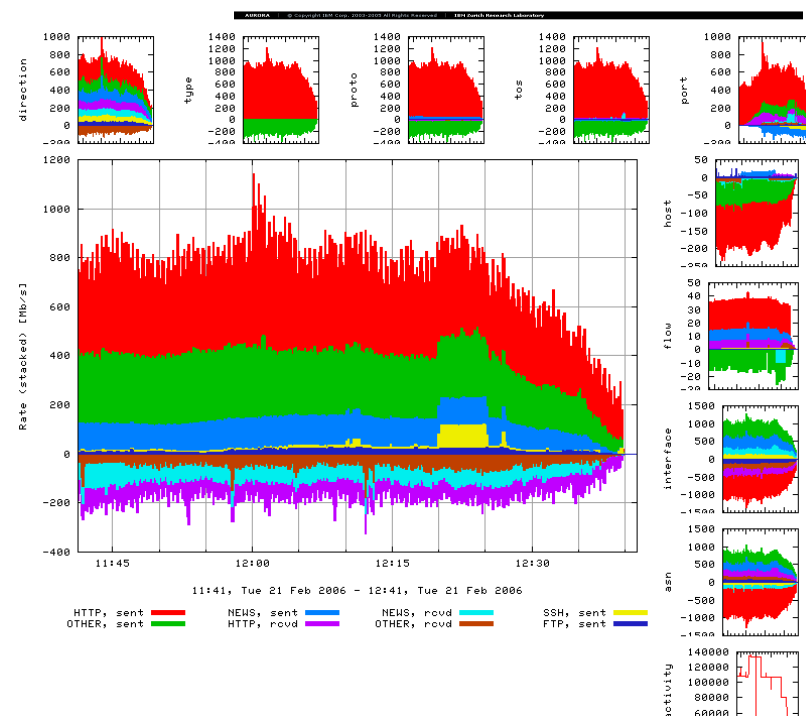
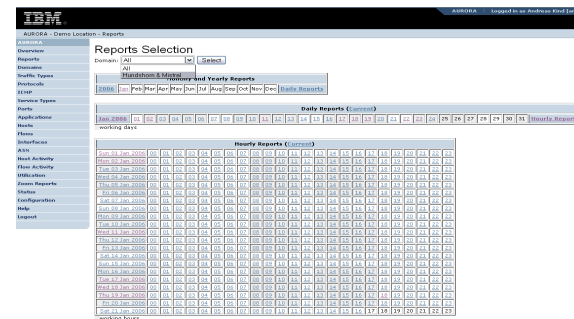
# Feature Overview



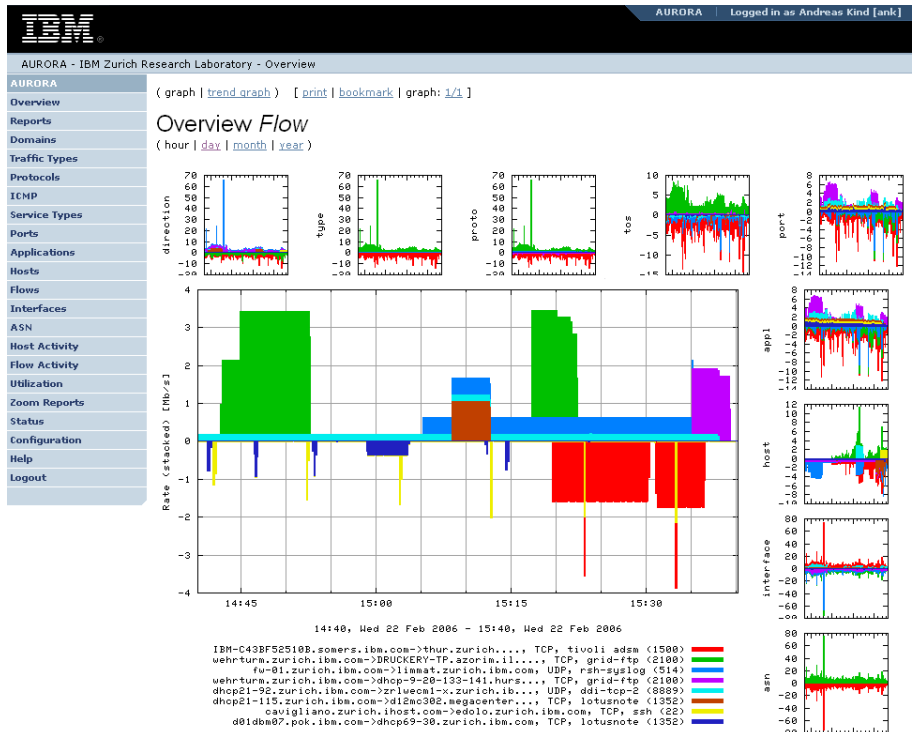
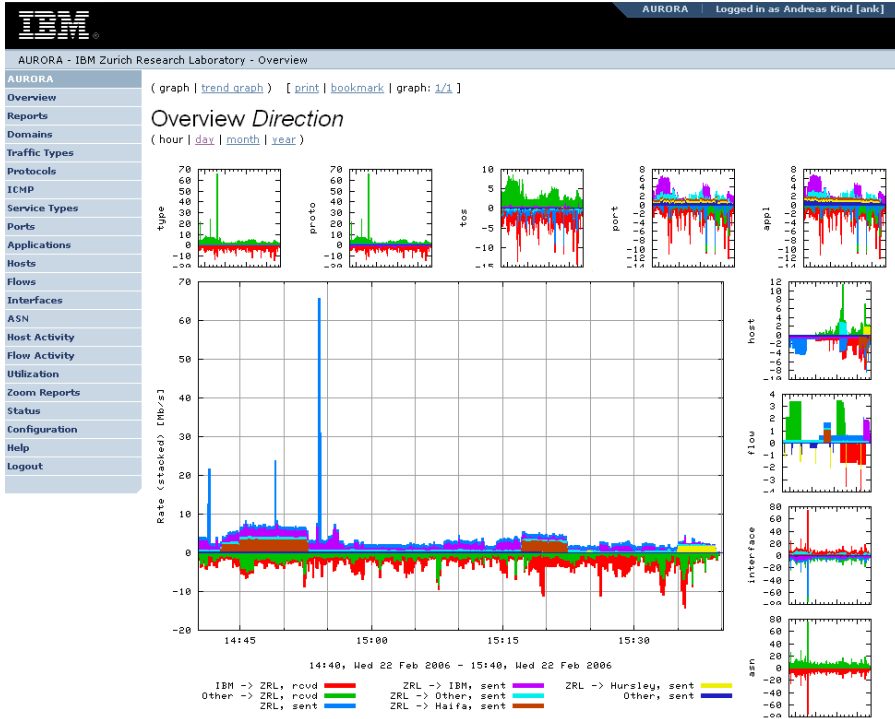
- NetFlow v1, v5, v6, v7, v8, v9, IETF IPFIX and sFlow collection, analysis, reporting
- Pre-generation of detailed reports in HTML, PDF, XML and TXT
  - Hourly, daily, monthly, yearly reporting periods
  - Utilization, domain, protocol, port, application, host, flow, ToS, ASN, and ICMP reports
  - Reports 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)

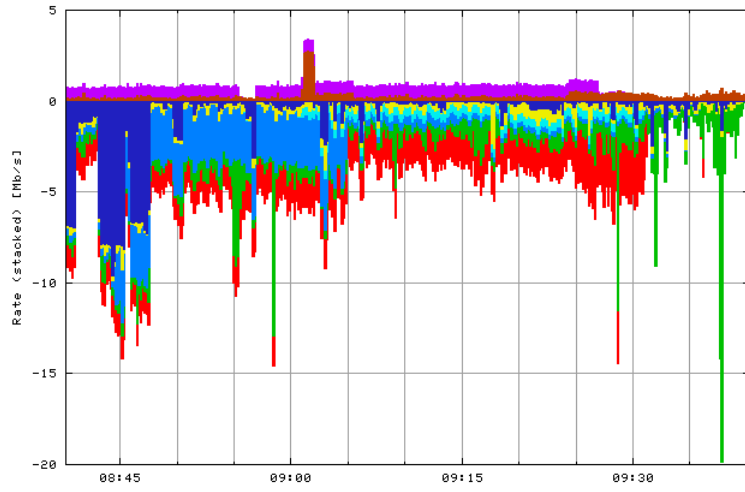
# Traffic Views and Standard Reports

- 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



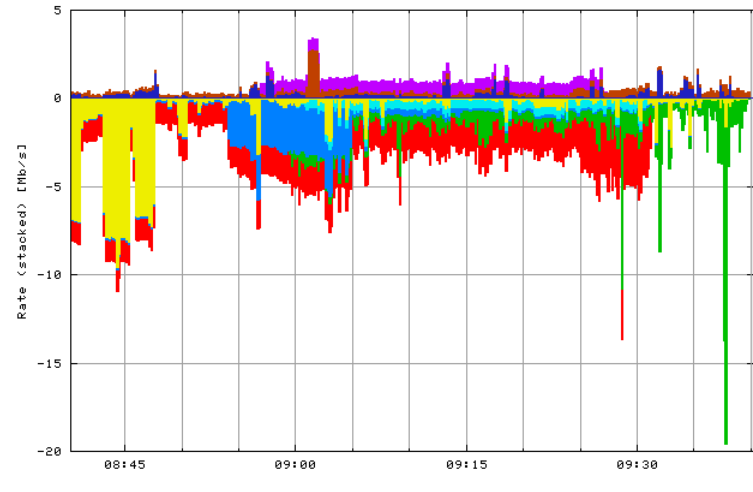
# Daily Direction and Flow Views





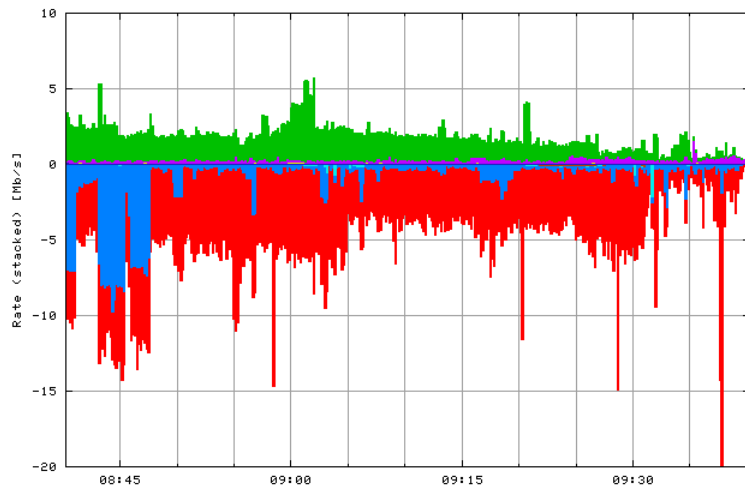
08:40, Fri 19 May 2006 - 09:40, Fri 19 May 2006

FILESYSTEM, rcvd	GRID, sent	OTHER, rcvd
HTTP, rcvd	TIVOLI, rcvd	LOTUSNOTES, rcvd
STREAMING, rcvd	HTTP, sent	



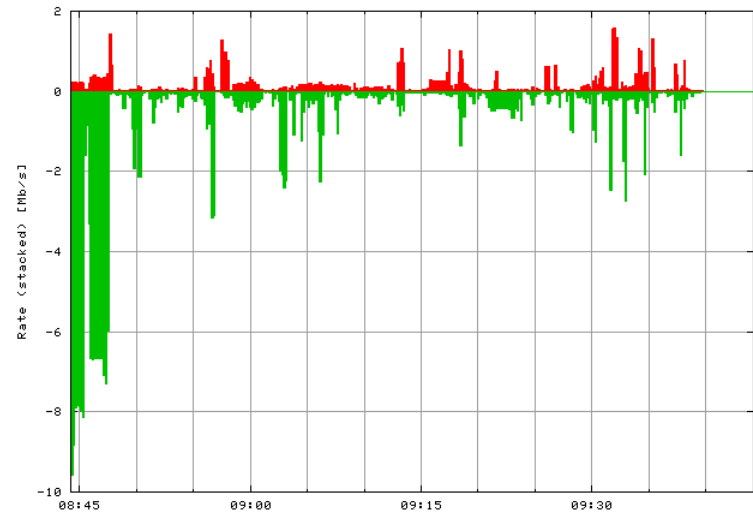
08:40, Fri 19 May 2006 - 09:40, Fri 19 May 2006

rsync (873), rcvd	tivoli adm (1500), rcvd
http (80), rcvd	http (80), sent
rtsp (554), rcvd	lotusnote (1352), rcvd
grid-ftp (2100), sent	lotusnote (1352), sent



08:40, Fri 19 May 2006 - 09:40, Fri 19 May 2006

Best Effort, rcvd	Assured (AF22), sent	Assured (AF32), sent
Best Effort, sent	Assured (AF32), rcvd	Best Effort, sent
Assured (AF22), rcvd	Assured (AF04), rcvd	



08:44, Fri 19 May 2006 - 09:44, Fri 19 May 2006

sent	received
------	----------



AURORA - Logged in as Andreas Kind [ank]

---

**Hosts** | graph | trend graph | print | bookmark | graph 1/1

Hosts **Dhcp23-7.zurich.ibm.com (9.4.23.7)**

Host Profile

Address Type:	IPv4 Unicast
Organization:	IBM Corporation
Address:	5311 Watermark Ave. White Plains 10606
Country:	US
Contact Name:	Z122-ARIN IBM Corporation
Contact Email:	hcc@ibm.com
Contact Phone:	+1-999-999-9999
Subnet:	9.0.0.0 - 9.255.255.255 9.0.0.0/8
First seen:	22.12, Sat 01 Oct 2005
Last seen:	10.14, Fri 19 May 2006

---

**Flows**

hourly daily monthly yearly

Flows 71 240 499511 499511

Octets

hourly	daily	monthly	yearly
Received	607.79 MB	26.33 MB	1.79 GB
Sent	116.37 MB	897.51 MB	821.10 MB

Packets

hourly	daily	monthly	yearly
Received	1.10 k	26.82 k	6.06 M
Sent	1.10 k	14.60 k	5.72 M

Client Applications

- OTHER: other
- CVS: Concurrent Versions System
- DATABASE: Database applications (ex LDAP/SOAP)
- DNS: Domain Name Service
- FTP: File Transfer Protocol
- GAME: Distributed computer games
- HTTP: Hypertext Transfer Protocol
- LOTUSNOTES: Lotus Notes
- MAL: Mail protocols (ex SMTP/POP/IMAP)
- MESSANGER: Instant messenger
- NETWING: Network management (ex SNMP)
- NEWS: News groups
- POP: Post-office protocol
- POWERFR: Power applications
- SSH: Secure Shell
- FILESYSTEM: Networked file systems (ex AFP/NFS/SAN/NAS)
- STREAMING: Streaming applications (ex Amn)
- TELNET: Telnet
- TIME: Time applications
- VIDEOCONF: Video conferencing
- VOIP: Voice and streams
- VPN: Virtual Private Network
- WEBSERVICE: IBM WebSphere and MSOffice
- WWW: World Wide Web

Server Applications

- OTHER: other
- TRIVOLI: TRIVOLI applications (ex TCM, ADAM)
- CORBA: Common Object Request Broker architecture
- DATABASE: Database applications (ex LDAP/SOAP)
- DNS: Domain Name Service
- DNS: Dynamic Host Configuration Protocol
- DNS: Domain Name Service
- GAME: Distributed computer games
- HTTP: Hypertext Transfer Protocol
- LOTUSNOTES: Lotus Notes
- MAL: Mail protocols (ex SMTP/POP/IMAP)
- MESSANGER: Instant messenger
- NETWING: Network management (ex SNMP)
- POP: Post-office protocol
- POWERFR: Power applications
- SSH: Secure Shell
- FILESYSTEM: Networked file systems (ex AFP/NFS/SAN/NAS)
- STREAMING: Streaming applications (ex Amn)
- TIME: Time applications
- VIDEOCONF: Video conferencing
- VOIP: Voice and streams
- VOIP: Voice over IP
- VPN: Virtual Private Network
- WEBSERVICE: IBM WebSphere and MSOffice
- WWW: World Wide Web

Domains this host talks to

- other
- ibm
- zurich
- zurich.ibm.com
- zurich.ibm.com
- zurich.ibm.com
- zurich.ibm.com
- zurich.ibm.com

Rate (stacked) [B/s]

09:15, Fri 19 May 2006 - 10:15, Fri 19 May 2006

received

AURORA - Logged in as Andreas Kind [ank]

---

AURORA - IBM Zurich Research Laboratory - Overview

**AURORA**

Overview

Reports

Domains

Traffic Types

Protocols

ICMP

Service Types

Ports

Applications

Hosts

Flows

Interfaces

ASN

Utilization

Zoom Reports

Status

Configuration

Help

Logout

(graph | [trend graph](#)) [ [print](#) | [bookmark](#) | graph: 1/1 ]

## Overview icmp

(hour | [day](#) | [month](#) | [year](#))

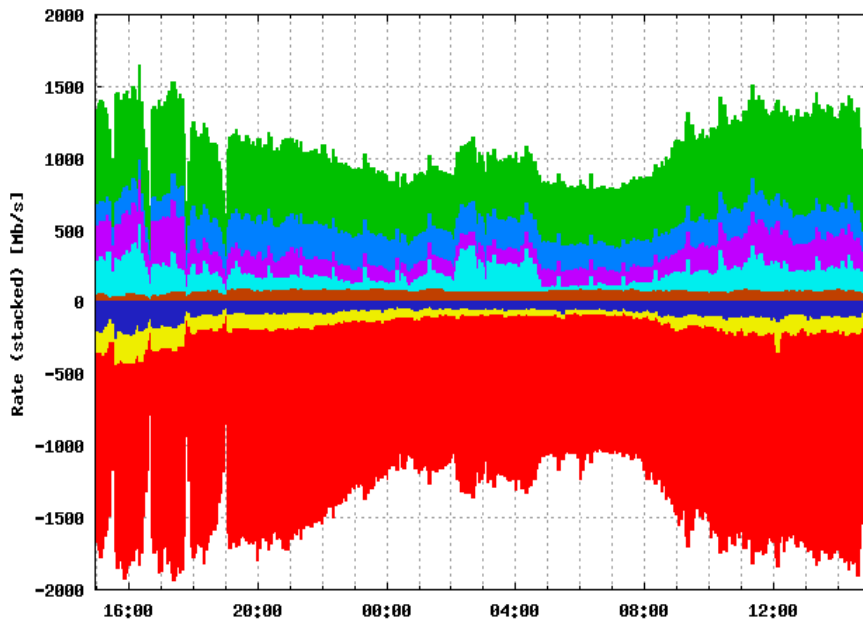
08:50, Fri 19 May 2006 - 09:50, Fri 19 May 2006

- Echo Request, sent
- Destination Unreachable - Port Unreachable, sent
- Echo Request, roud
- Echo Reply, sent
- Destination Unreachable - Port Unreachable, roud
- Echo Reply, roud
- Destination Unreachable - Communication administratively prohib..., sent
- Destination Unreachable - Communication administratively prohib..., roud

- Echo Request, sent
- Destination Unreachable - Port Unreachable, sent
- Echo Request, roud
- Echo Reply, sent
- Destination Unreachable - Port Unreachable, roud
- Echo Reply, roud
- Destination Unreachable - Communication administratively prohib..., sent
- Destination Unreachable - Communication administratively prohib..., roud

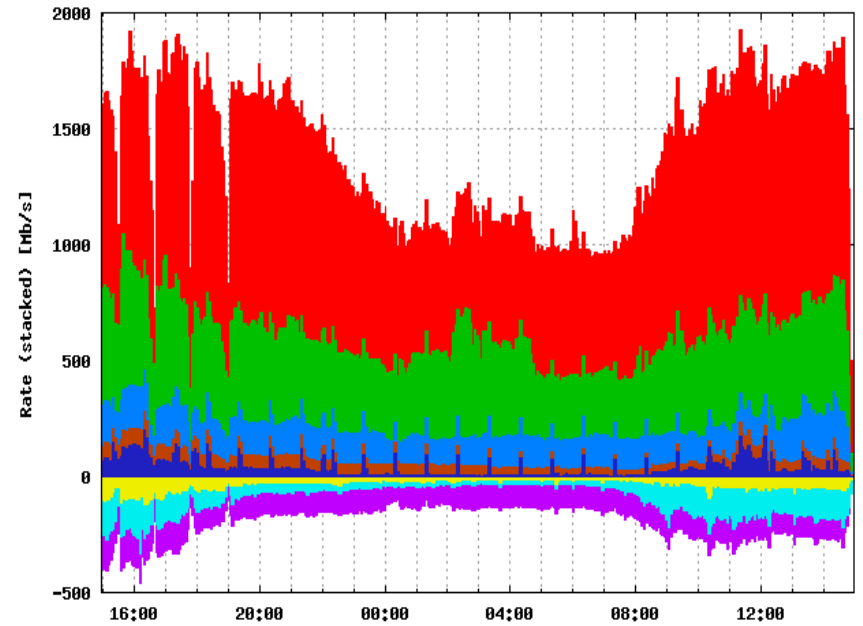


# Traffic Example at an ISP



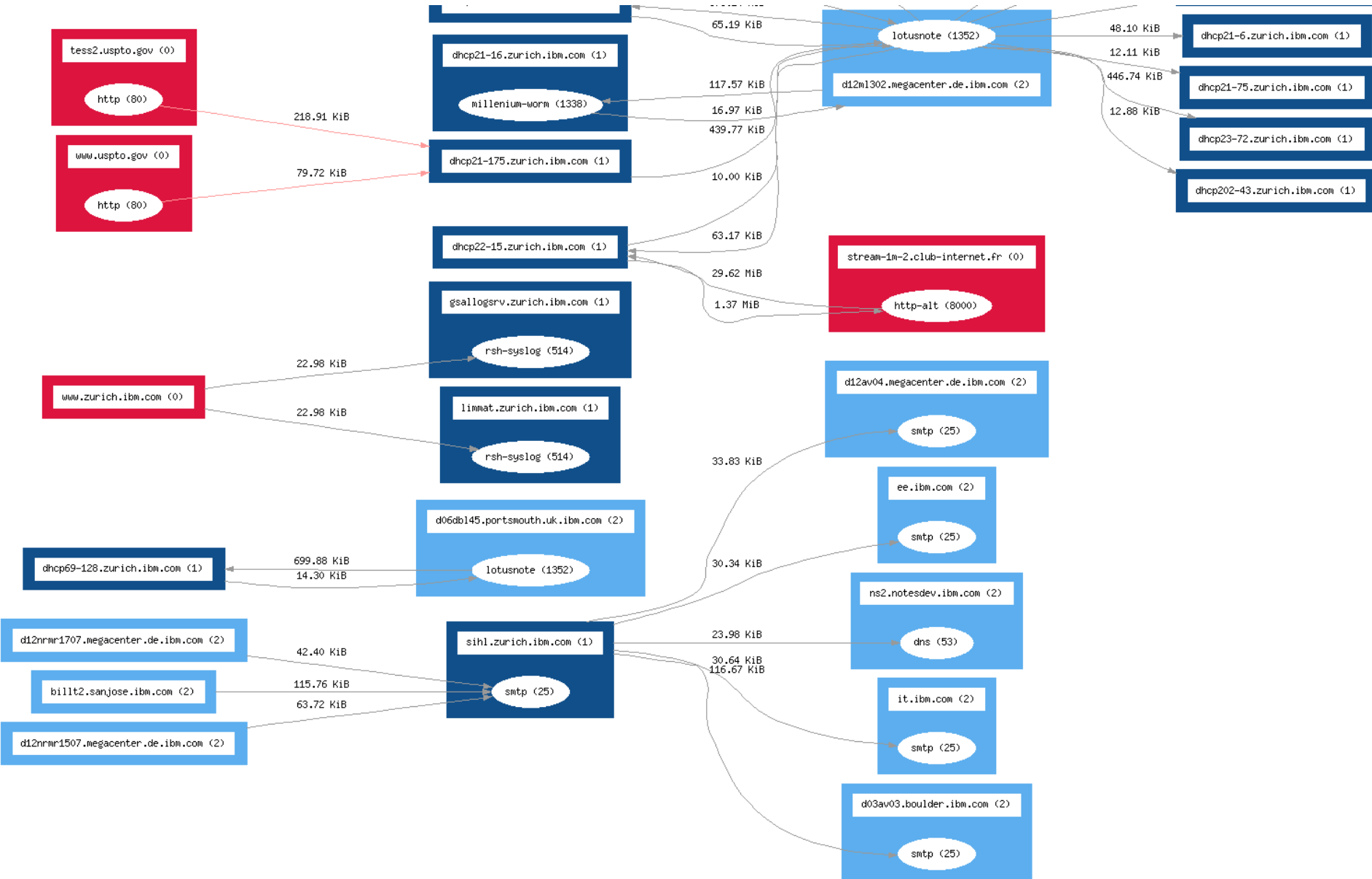
14:57, Thu 18 May 2006 - 14:57, Fri 19 May 2006

AS 0, rcvd	AS 3320, sent	AS 65401, sent	AS 65401, rcvd	
AS 0, sent	AS 20965, sent	AS 3356, sent	AS 20965, rcvd	



14:57, Thu 18 May 2006 - 14:57, Fri 19 May 2006

HTTP, sent	NEWS, sent	HTTP, rcvd	OTHER, rcvd
OTHER, sent	NEWS, rcvd	P2P, sent	SSH, sent



# Domains

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

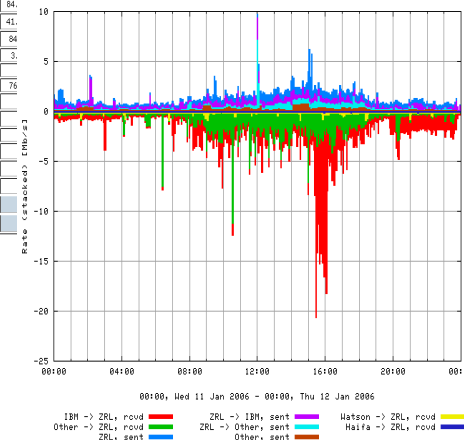
```
DOMAIN="ZRL"
LOCAL=1
SUBNET="9.4.0.0/16 2001:620:20::/48"
FLAG=/aurora/flags/zrl.gif
```

```
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"
```

Domain Traffic

Domain Traffic	Current Hour		Current Day		Current Month		Current Year	
	sent	received	sent	received	sent	received	sent	received
IBM -> ZRL	568.04 MB	114.37 MB	1.59 GB	1.05 GB	207.75 GB	77.41 GB	207.49 GB	77.84 GB
Other -> ZRL	67.88 MB	20.47 MB	933.05 MB	314.34 MB	188.63 GB	39.71 GB	188.60 GB	39.37 GB
Watson -> ZRL	27.61 MB	16.99 MB	200.41 MB	178.97 MB	23.94 GB	15.14 GB	23.92 GB	15.12 GB
Häfa -> ZRL	34.25 MB	473.33 KIB	343.08 MB	2.89 MB	17.24 GB	734.19 MB	17.20 GB	733.88 MB
Hursley -> ZRL	2.04 MB	424.20 KIB	25.56 MB	5.15 MB	3.50 GB	991.89 MB	3.50 GB	990.22 MB
ZRL	93.01 MB		1.16 GB		99.00 GB		98.75 GB	
Other	35.71 MB		419.85 MB		35.85 GB		35.80 GB	
ZRL -> Private (192.168.0.0/24)	214.90 KIB		2.13 MB		90.91 MB		90.77 MB	
ZRL -> Private (10.0.0.0/8)	6.87 KIB		84					
Private (192.168.0.0/16) -> ZRL	3.92 KIB		41					
Private (10.0.0.0/8) -> ZRL			84					
Private (192.168.0.0/16) -> Other	380.00 B		3					
Private (192.168.0.0/16)								
Private (10.0.0.0/8) -> Other	76.00 B		76					
Private (192.168.0.0/16) -> IBM								
Other -> IBM								
Private (10.0.0.0/8) -> Private (192.168.0.0/16)								
Private (10.0.0.0/8) -> IBM								
Private (192.168.0.0/16) -> Watson								
Häfa -> Other								
<b>Total observed</b>	<b>628.07 MB</b>		<b>12</b>					



# 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|icmp|type|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

AURORA | Logged in as Andreas Kind [ank]

---

AURORA - Demo Location - Zoom Reports

**AURORA**

- Overview
- Reports
- Domains
- Traffic Types
- Protocols
- ICMP
- Service Types
- Ports
- Applications
- Hosts
- Flows
- Interfaces
- ASN
- Host Activity
- Flow Activity
- Utilization
- Zoom Reports
- Status
- Configuration
- Help
- Logout

## Zoom Reports

**Description**

**Email address**  (used only by Queued Zoom to notify you when it is complete)

**Operator**  AND  OR

**Periods** 2006-01-17\_23-50\_0100  
2006-01-17\_23-45\_0100  
2006-01-17\_23-40\_0100  
2006-01-17\_23-35\_0100  
2006-01-17\_23-30\_0100  
2006-01-17\_23-25\_0100  
2006-01-17\_23-20\_0100  
2006-01-17\_23-15\_0100  
2006-01-17\_23-10\_0100  
2006-01-17\_23-05\_0100

**Source Prefix**

**Traffic Type(s)** Unicast IPv6  
Broadcast IPv6  
Unicast

**TCP/UDP/SCTP Port(s)** 1ci-smcs  
3Com-nsd  
3com-amp3

**Port Number**

**Report(s)** Applications  
ASN  
Domains  
Flows  
Flow Activity  
Hosts  
Host Activity  
ICMP

**Direction**  OneWay  Both

**Domain(s)** Other  
ZRL  
IBM  
Hursley  
Watson  
Haifa  
Hundshom & Mistral  
Private (10.0.0.0/8)  
Private (192.168.0.0/16)

**Destination Prefix**

**Protocol(s)** 3PC  
A/N  
A0HP

**Application(s)** Backup  
Citrix MetaFrame and MetaFrameXP software  
Common Object Request Broker Architecture

**Options**  Show Records  
 Relationship Diagram  
 Create a log file

**Report on**  Octets/sec  
 Packets/sec  
 Packets/Octets ratio

**Custom Filter**

**Pre-defined Filter**

Instant Zoom Queued Zoom

### Previous Zoom Reports

Report	Period	Created	User	Description	Filter
<a href="#">zoom7709</a>	2006-01-17 23:00:00 - 2006-01-17 23:55:05	2006-01-21 12:36:22	Andreas Kind (ank)	Demo Zoom	(port either 22)

AURORA
© Copyright IBM Corp. 2003-2005 All Rights Reserved | IBM Zurich Research Laboratory

# User Management

( [user preferences](#) | [user management](#) | [site configuration](#) | [license](#) )

## User management

<b>Username</b>	ank
<b>Fullname</b>	<input type="text" value="Andreas Kind"/>
<b>Email</b>	<input type="text" value="ank@zurich.ibm.com"/>
<b>Password</b>	<input type="password"/>
<b>Repeat Password</b>	<input type="password"/>
<b>Domain</b>	<input type="text"/> ▼
<b>User Flags</b>	<input checked="" type="checkbox"/> Administrator <input type="checkbox"/> Password Changing Disabled <input type="checkbox"/> Auto-reload pages? <input type="checkbox"/> Disabled
<input type="button" value="Apply"/> <input type="button" value="Delete"/>	

Username	Fullname	Email	Administrator	Disabled	
ank	Andreas Kind	ank@zurich.ibm.com	yes	no	<a href="#">Edit</a> <a href="#">Delete</a>

[Create new user](#)

# Configuration

( [user preferences](#) | [user management](#) | [site configuration](#) | [license](#) )

## Site Configuration

General Authentication Reporting Domains Flow storage Filter settings

**General**

**Default language** English (US)

**Location** Test

**Skin** IBM

**Routers** any

( [user preferences](#) | [user management](#) | [site configuration](#) | [license](#) )

## Site Configuration

General Authentication Reporting Domains Flow storage Filter settings

**Authentication**

**Authentication method** Aurora Web Login

**Anonymous login** No

**Show only anonymized data to anonymous users** Yes

( [user preferences](#) | [user management](#) | [site configuration](#) | [license](#) )

## Site Configuration

General Authentication Reporting Domains Flow storage Filter settings

**Reporting**

**Traffic aspects**

Domains  Applications

Directions  Hosts

Traffic Types  Flows

Protocols  Interfaces

Service Types  ASN

Ports  ICMP

**Enable CSV reports** No

**Units**<sup>1</sup> Octets

**Flow direction**<sup>1</sup> Domain

<sup>1</sup> A reset of the site is required to apply this setting properly

( [user preferences](#) | [user management](#) | [site configuration](#) | [license](#) )

## Site Configuration

General Authentication Reporting Domains Flow storage Filter settings

**Domains**

ID	Name	Local	Flag	Criteria	Reports	Operations
1	Private	Yes	-	Subject: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fe80::/7	No	<a href="#">Edit</a> <a href="#">Delete</a>
2	Link Local	Yes	-	Subject: 169.254.0.0/16, fe80::/10	No	<a href="#">Edit</a> <a href="#">Delete</a>
3	Documentation	Yes	-	Subject: 192.0.2.0/24, 2001:db8::/32	No	<a href="#">Edit</a> <a href="#">Delete</a>
100	IBM ZRL	Yes	<input checked="" type="checkbox"/>	Subject: 9.4.0.0/16	No	<a href="#">Edit</a> <a href="#">Delete</a>
101	IBM WRC	Yes	<input checked="" type="checkbox"/>	Subject: 9.2.0.0/16	No	<a href="#">Edit</a> <a href="#">Delete</a>
201	IBM ZRL -> IBM WRC	No	-	Filter: ipv4 src 9.4.0.0/16 and ipv4 dst 9.2.0.0/16	direction flow	<a href="#">Edit</a> <a href="#">Delete</a>

**Add a new domain**

**Name:**

**Local:** No

**Flag:** (none)

**Criteria:**

**Reports:**  Yes  No

**Subject:**

**AS number:**

**Filter:**

<sup>1</sup> Optional setting  
<sup>2</sup> At least one among the fields must be specified

# 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"

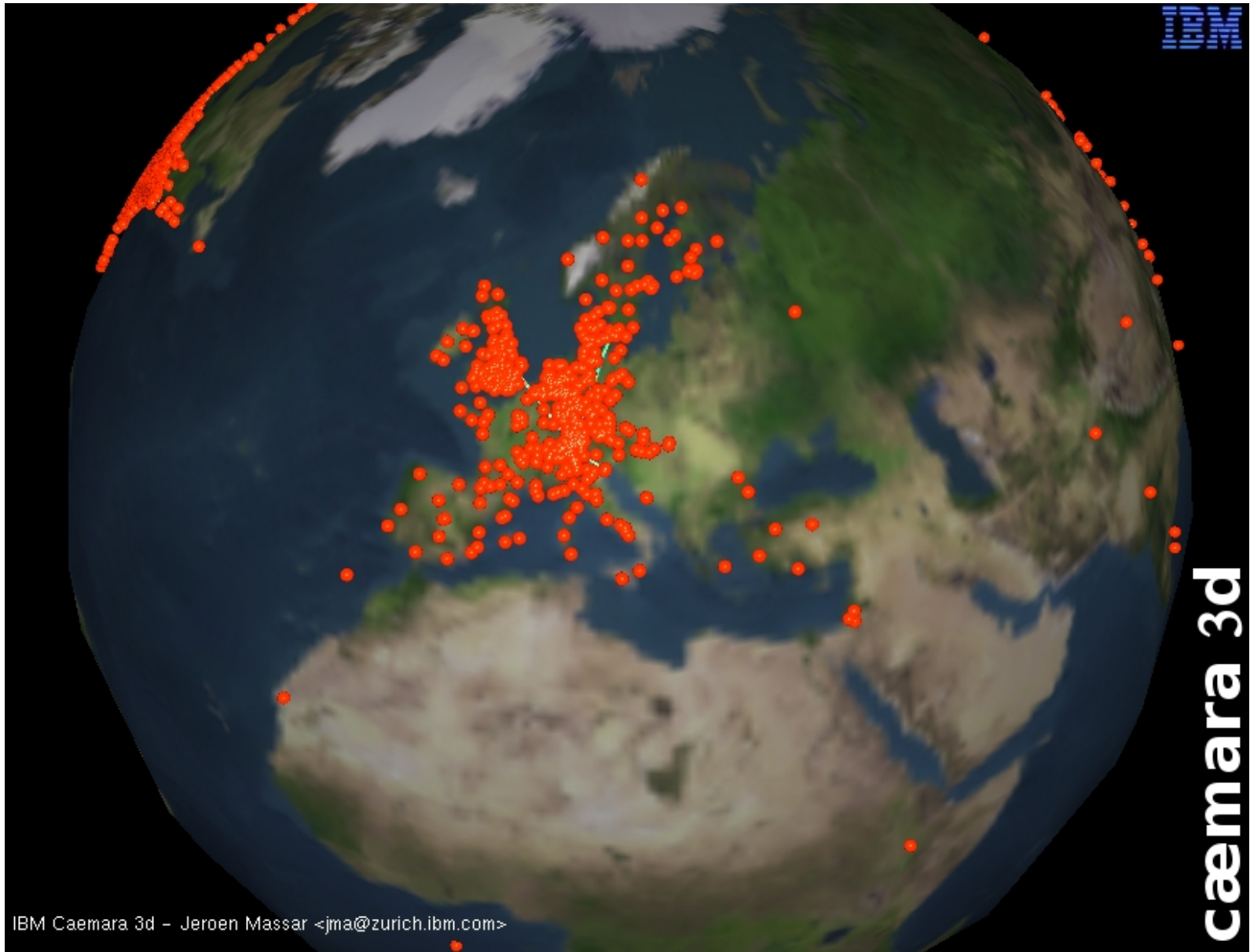
# Local Swiss Department A
DOMAIN="Department A"
ID=1
SUBNET="10.10.1.0/24"
LOCAL=1
FLAG=/aurora/flags/ch.gif

# 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

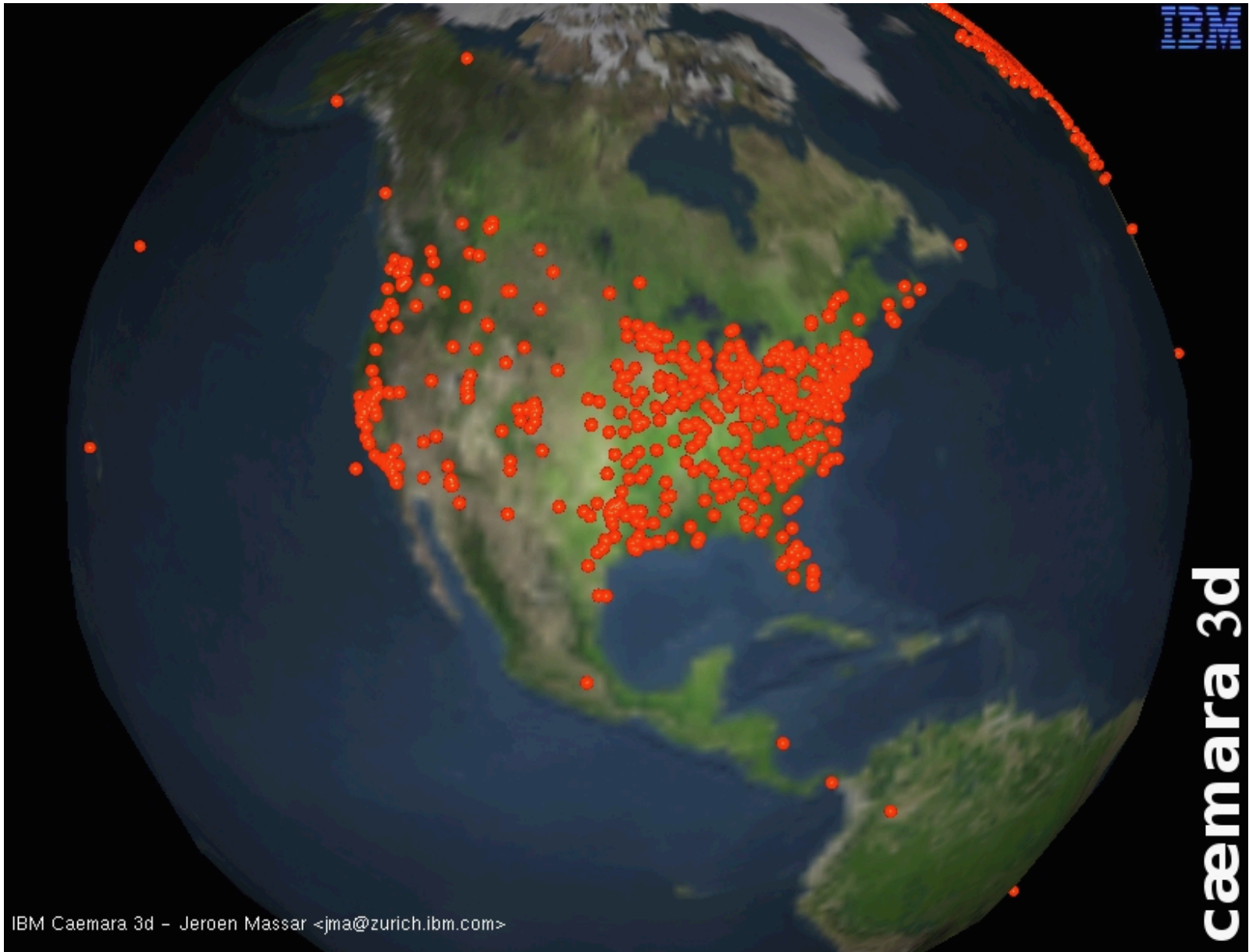
# Remote German Department D
DOMAIN="Department D"
ID=4
SUBNET="11.11.2.0/24"
LOCAL=0
FLAG=/aurora/flags/de.gif

FLOWFILE_ZIP_PERIOD=86400
ZIP=bzip2
```

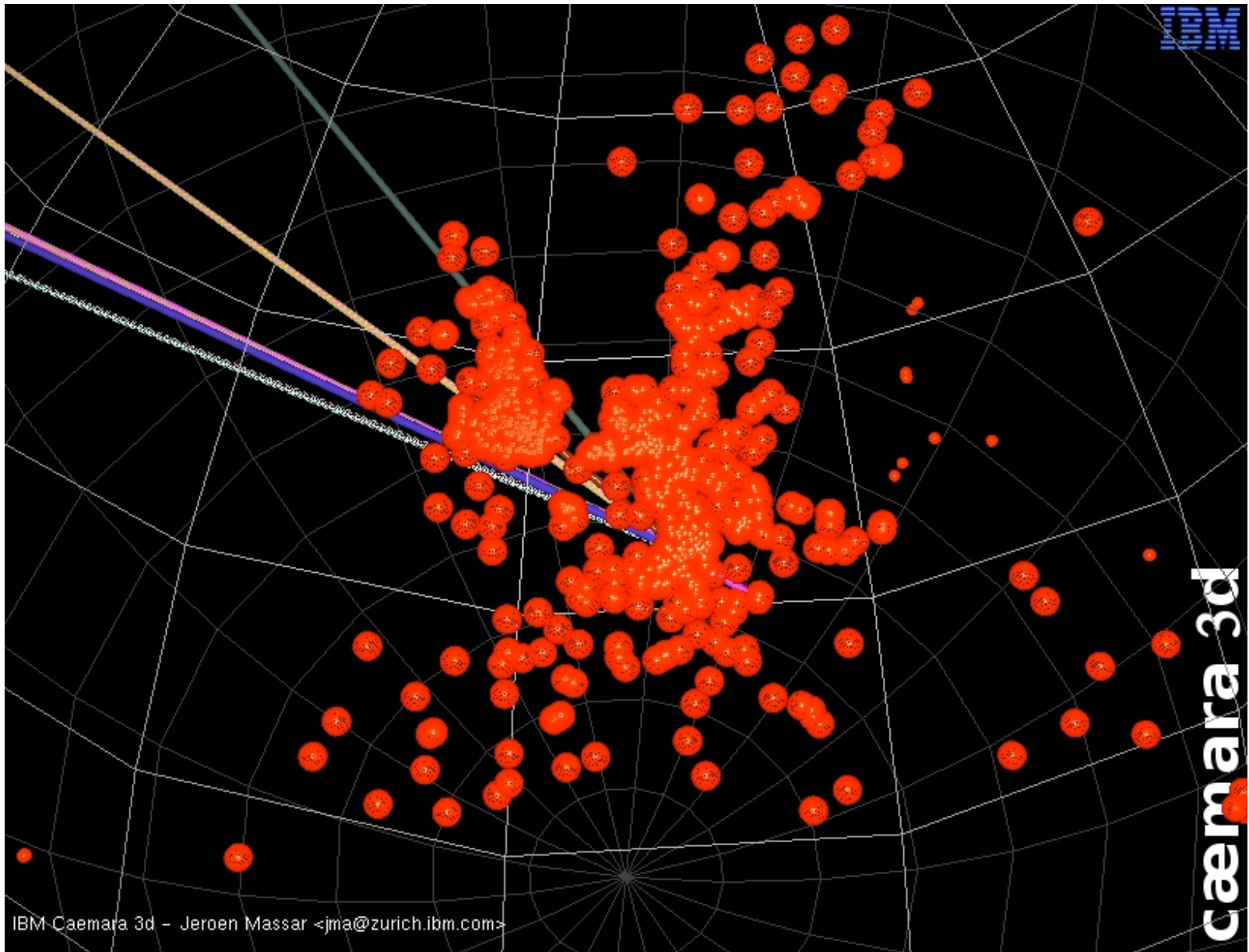


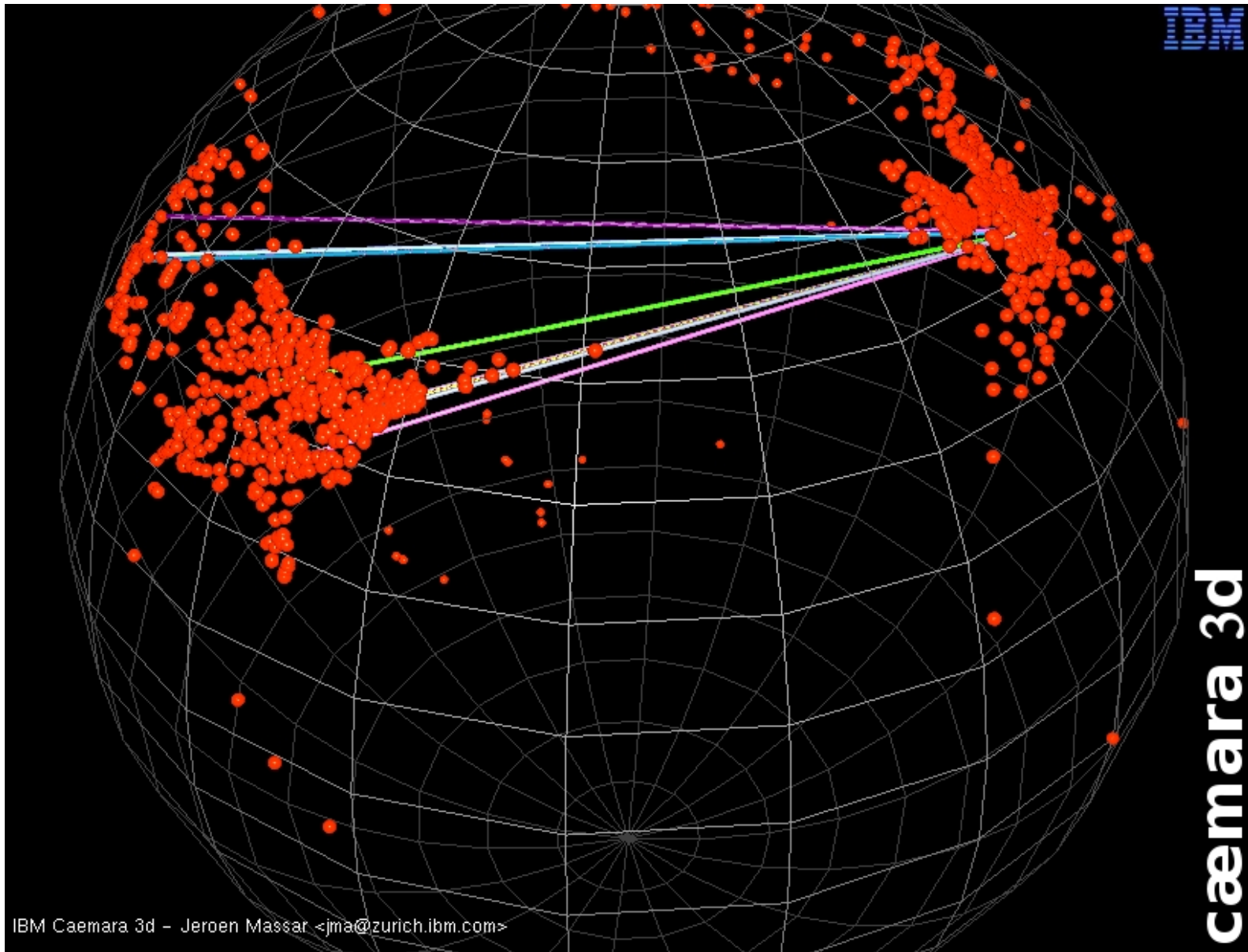
IBM Caemara 3d - Jeroen Massar <jma@zurich.ibm.com>

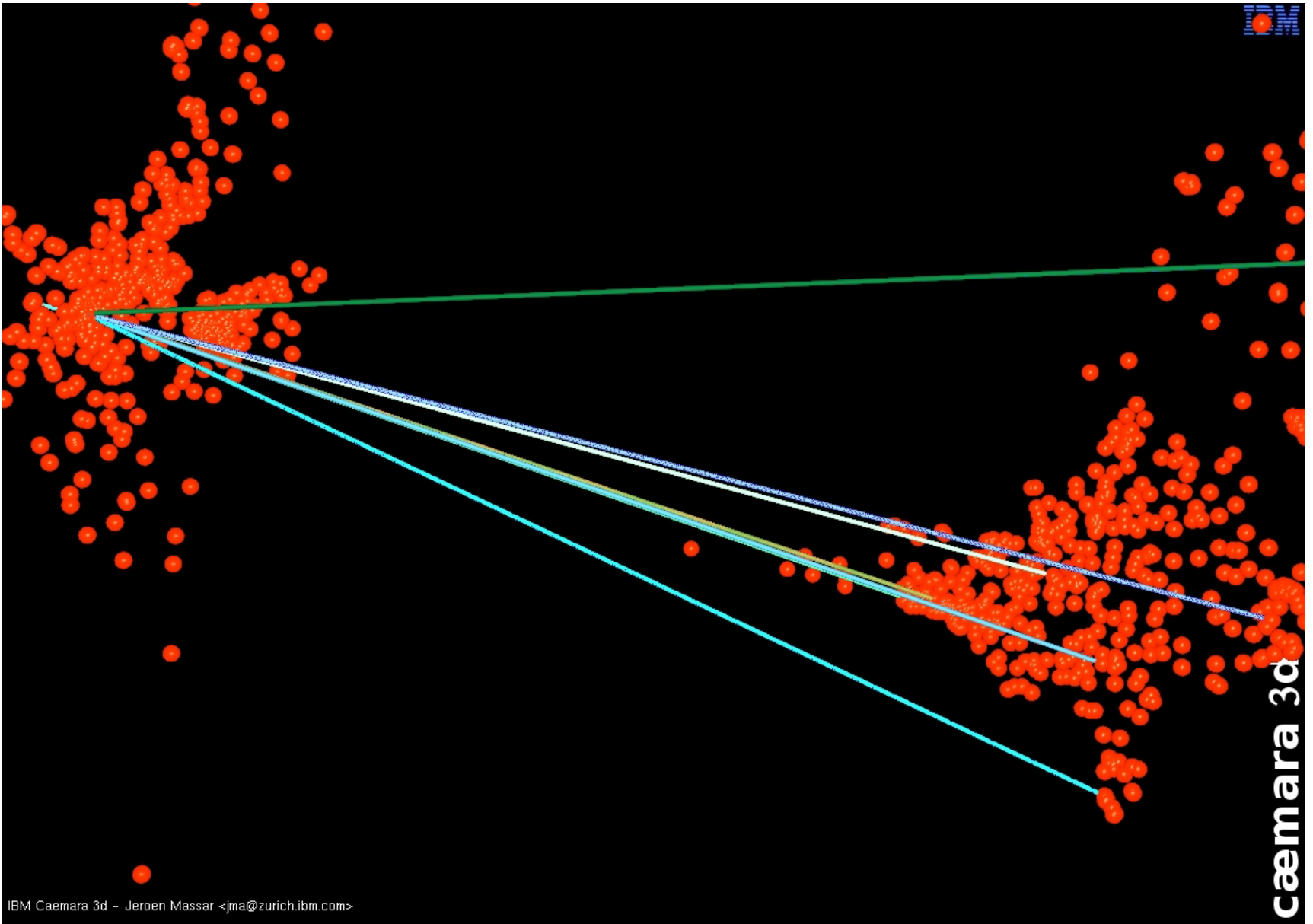




IBM Caemara 3d - Jeroen Massar <jma@zurich.ibm.com>







IBM Caemara 3d - Jeroen Massar <jma@zurich.ibm.com>



# 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/](http://www.zurich.ibm.com/aurora/)



**CISCO SYSTEMS**

Log In | Register | Contacts & Feedback | Help | Site Map | Select a Location / Language

Search

Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco

HOME  
 PRODUCTS & SERVICES  
 CISCO IOS SOFTWARE  
 CISCO IOS TECHNOLOGIES  
 MANAGEMENT INSTRUMENTATION  
 CISCO IOS NETFLOW  
**Cisco Applications**  
**Commercial Software Packages**  
 Freeware NetFlow Software

**Cisco IOS NetFlow Commercial Software Packages**

**AdventNet**  
[NetFlow Analyzer](#) (PDF)  
 NetFlow Analyzer is a web-based bandwidth monitoring tool that uses Cisco NetFlow technology

**Anopsis**  
 NetUsage product for network traffic monitoring, capacity planning, business justification and cost control.

**Arbor Networks**  
[Arbor Networks PeakFlow Products](#)  
 Traffic Analysis, NetFlow collection and Security DDOS monitoring, and peering analysis

**Caligare**  
 Realtime traffic monitoring, smart flow filtration and network anomalies detection

**Crannog Software**  
 Traffic analysis, NetFlow collection and low cost Windows-based NetFlow product  
[Crannog NetFlow Tracker](#)

**Computer Associates**  
 Enterprise and Service Provider network performance monitoring, uses Cisco NetFlow Collector  
[eHealth Traffic Accountant](#) (PDF)

**Evident Software**  
 Evident Software for NetFlow based Billing and Traffic Analysis  
[Evident Analyze](#)

**Hewlett Packard**  
 Traffic Analysis, NetFlow collection using HP Insight Network Performance Monitoring  
[HP Insight Web Site](#)

**IBM**  
 NetFlow Aurora Product is a Flow Based Profiling System  
[Aurora](#)

**InfoVista**  
 Enterprise and Service Provider Network Performance Monitoring  
[InfoVista NetFlow](#)

**IsarItet**  
 IsarFlow Reporting Software

**Micromuse**  
[Micromuse Usage Monitor NetFlow Web Site](#) (PDF)  
[Micromuse USM News Release](#)

**Related Tools**  
[Software Center](#)  
[Software Advisor](#)  
[Dynamic Configuration Tool](#)  
[Cisco Feature Navigator II](#)

**Related Links**  
**Products & Services**  
[Cisco Routers](#)  
[Cisco Switches](#)

**Which products are right for you?**  
 Call 800-553-6387

For more Information please, contact [aurora@zurich.ibm.com](mailto:aurora@zurich.ibm.com)