Building a solution for active monitoring of the Swedish Internet.

RIPE 51, Amsterdam
Rickard Dahlstrand
rd@tilde.se

Background

- The Demeter concept was build for distributed measurement of availability, performance, services and infrastructure.
- 4 large installations running at Södersjukhuset, Sveriges Radio, Nic-se and Sitic (PTS). All these had specific need for distributed measurement.
- They are running measurements for TCP bandwidth, UDP jitter, ICMP RTT, service availability (DNS) and more..

Timeline

2003- A distributed dns-monitoring system at Nic-se.

2004- 2 installations of a distributed bandwidth-measurement system at Södersjukhuset and Sveriges Radio.

2004- Generic Internet service testing platform launched for distributed monitoring of websites, mail-servers etc. (0 customer)

2005- Sitic phase 0 was launched, using the setup from the Internet-service.

2005- Sitic phase 1 in planning-stage.

The Sitic-project

What is Sitic's interest in this project?

- Everyone shall have access to a broad range of communications services.
- The services shall be easy to use, affordable and of good quality.
- The consumer shall have access to clear information about rights and obligations.
- The consumer shall be well informed in order to easily be able to choose among various services and various service suppliers.
- Sweden shall have a robust infrastructure for communications services and an active exchange of information in IT security issues.

Context

- Well, we are all living in Sweden. So the scope is quite local. =)
- Telia (Skanova) is the big player for broadband access due to it's previously tax-funded copper-infrastructure (DSL).
- Government has funded communal fiber-infrastructure. DSL is however still used in many cases for the "last mile".
- "Fiber to the home" is only available in large cities.

Internet Monitor - Phase 0

- Proof of concept!
- 9 measurement points at different Swedish internet-operators
- Low/no-cost internet connections are used (eq. to friends and family)
- Each point is pinging each other measurement point once every minute and reports back to a central server
- Sitic rented the system, Tilde runs it.
- Launched Mars 2005
- EOL Nov 2005

Goals for phase 0

- Does this type of measurement system work as a concept?
- Can we draw any conclusions from these tests?
- How is peering and transit affecting availability?
- Are there availability problems between operators?

The system

DISCLAMER! These measurements does not represent any real operator availability!

SITIC - Sveriges IT-incidentcentrum - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://www.sitic.se/ Go

Aktuellt - virus/maskar/trojaner

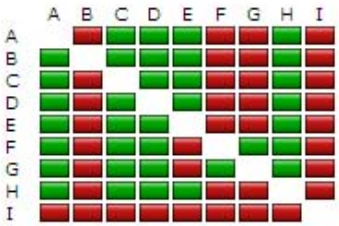
Arkiv

2005-08-18 Flera maskar utnyttjar sårbarhet i Windows tjänst Plug and Play

2005-08-15 Zotob.A utnyttjar sårbarhet i Microsoft Windows

...eller generell virusinformation

Hur mår internet just nu?



Senast uppdaterad: 051011 18:01

Matrisen visar en sammanställning över 9 svenska internetoperatörer och hur typiska användare hos dessa kan nå tjänster hos de övriga operatörerna.

- All trafik flyter bra
- Mindre trafikstörningar
- Svåra trafikstörningar
- Måldata saknas

Klicka här för mer information

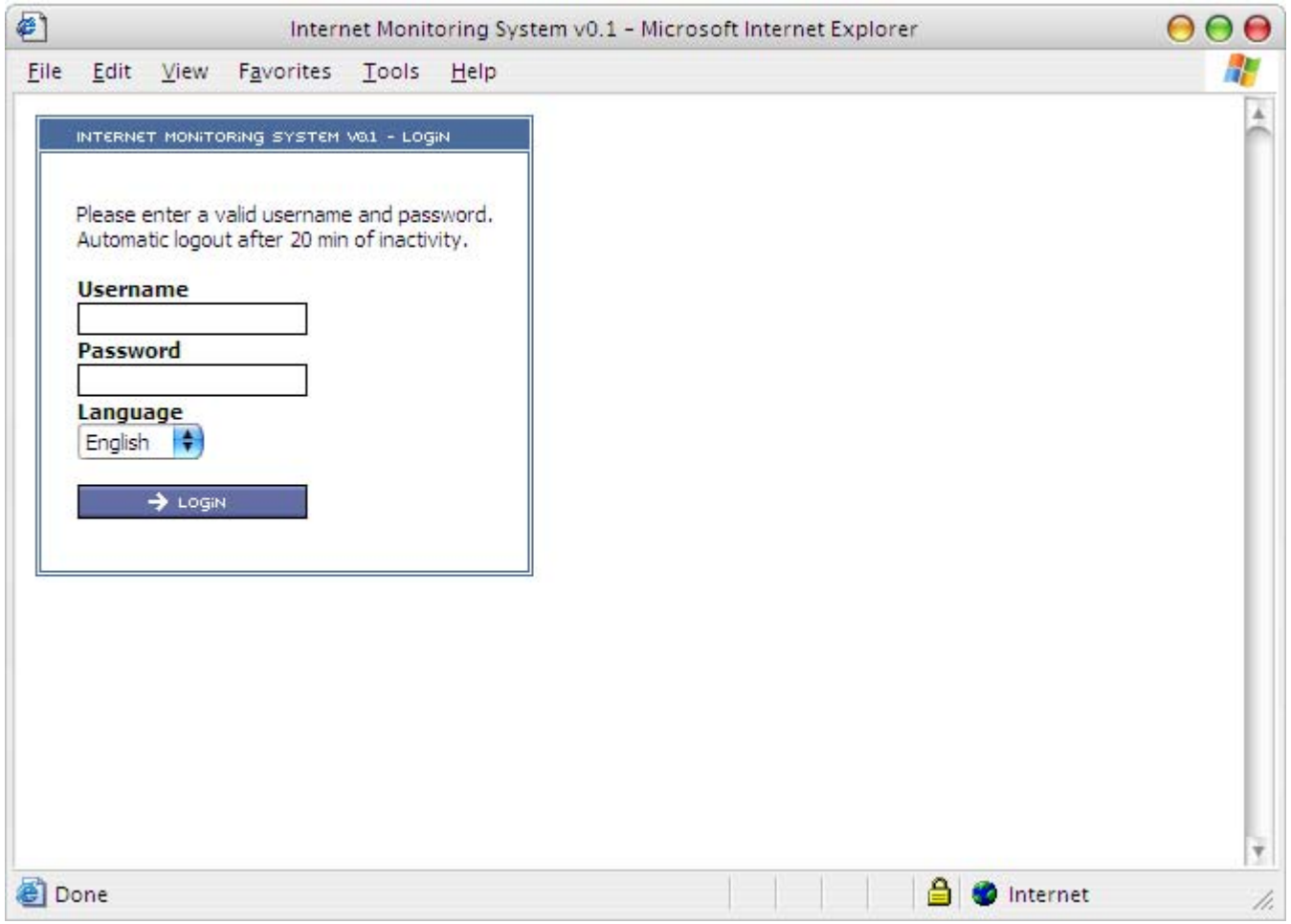
Kaspersky antivirusbibliotek är sårbart för en "heap"-baserad buffertöverflödesattack som vid effektivt utnyttjande kan leda till total kontroll över det sårbara systemet.

2005-09-27

SR05-116 **RealPlayer och Helix Player - formatsträngsbug**

RealNetworks RealPlayer och Helix player för UNIX/Linux är sårbara för en formatsträngsbug. Detta kan leda till att kod exekveras som den användare som kör den sårbara applikationen.

Internet


Internet Monitoring System v0.1 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
INTERNET MONITORING SYSTEM V0.1 - LOGIN
Please enter a valid username and password.
Automatic logout after 20 min of inactivity.
Username
Password
Language
English
LOGIN
Done
Internet

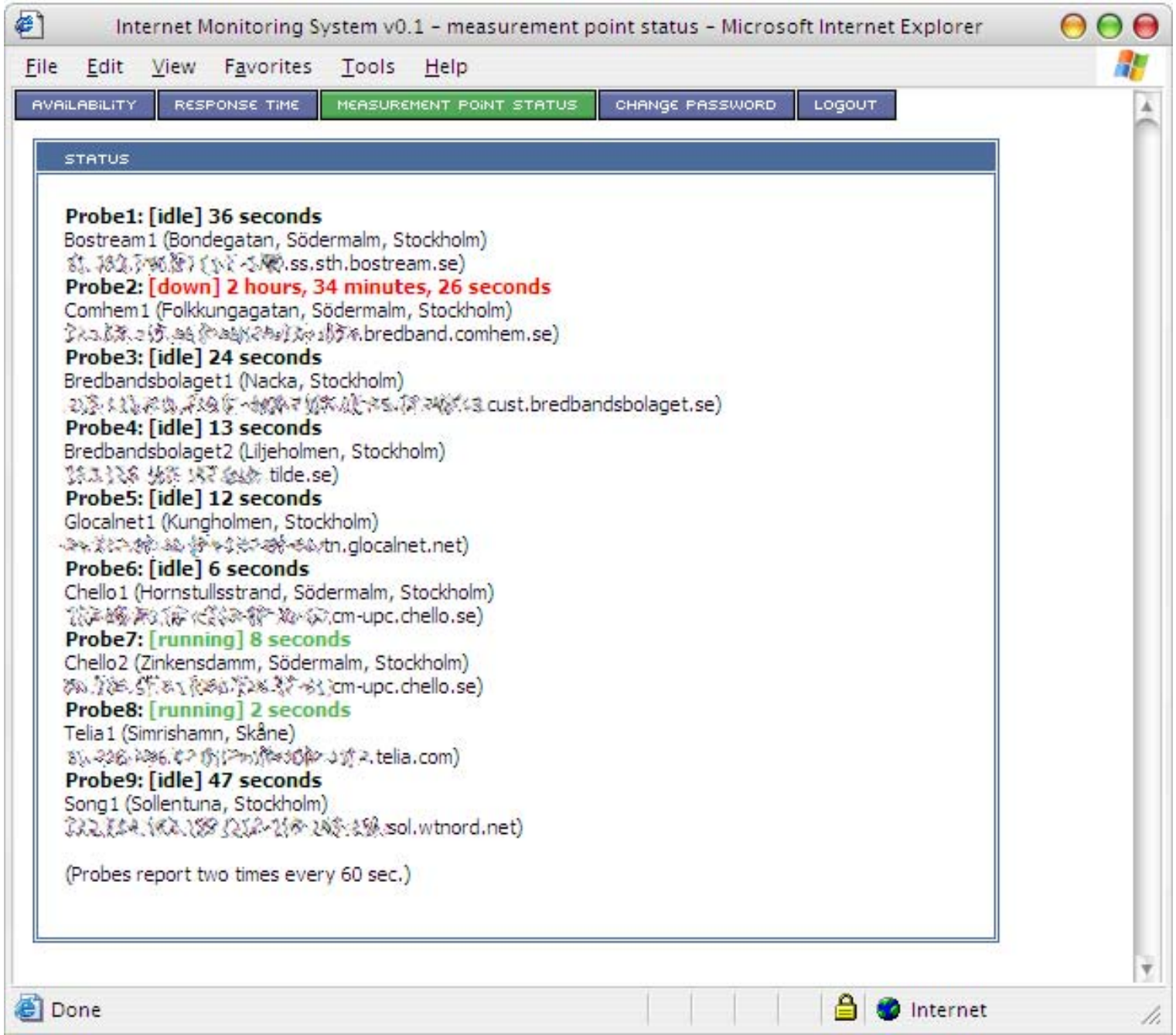
Measurement collection

Each minute a script is run at the measurement point.

1. The scripts start by sleeping a pre-defined number of seconds according to which probe is running on. (To allow for measurements to be done without affecting each other.)
2. The script connect to the server using https and gets a list of IP's to measure to. (Most ip's are dynamic)
3. 5 ICMP-messages are sent to each IP and RTT max,min,avg and stddev are collected.
4. All measurement-data is sent back to the server using https and added to the database.

```
#!/bin/sh
#     ____                          _
#    |  _ \  ___ _ __ ___   ___| |_ ___ _ __
#    | | | |/ _ \ '_ ` _ \ / _ \ __/ _ \ '__|
#    | |_| |  __/ | | | | |  __/ ||  __/ |
#    |____/ \___|_| |_| |_|\___|\__\___|_|
# Demeter Test System (c)Tilde 2004
# $Id: demeterechoperf.sh,v 1.1 2005/02/01 06:26:06 rd Exp $

PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/bin
version="02"
myname=`/bin/hostname` 2> /dev/null

ping="/sbin/ping"
awk="/usr/bin/awk"
wget="/usr/local/bin/wget"

case "$myname" in
probe1)      del=0;;
probe2)      del=6;;
probe3)      del=12;;
probe4)      del=18;;
probe5)      del=24;;
probe6)      del=30;;
probe7)      del=36;;
probe8)      del=42;;
probe9)      del=48;;
*)           del=0;;
esac

sleep ${del}
```

```
# Load servers from server-file
servers=`${wget} https://XXX.XXX.XXX.XXX/getservers?probe=${myname} --no-check
     certificate --tries=3 –timeout=3 -q -O-`

# Add the versionnumber, date and time first to the data.
demres=`date "+%Y%m%d;%H%M%S"`
demres="${version};${demres}"

# loop through all the servers in the list of servers
for serv in ${servers}; do

    pingsrv=`echo "${serv}" | awk -F \; '{print $2}'`
    serv=`echo "${serv}" | awk -F \; '{print $1}'`

    # Run ping and connect to serv using ICMP with a 5 queries
    # i=pause w=timeout -n -q =quite c=number of pings
    x=`${ping} -i.1 -w2 -n -q -c 5 ${pingsrv} 2> /dev/null | grep round-trip| awk
     '{print $4}' | awk -F / '{print $1";"$2";"$3";"$4}'`

    # If successful add the server-ip and response time to the data.
    if [ "${x}" != "" ] ; then
        demres="${demres};${serv};${x}"
    else
        demres="${demres};${serv};U;U;U;U"
    fi

done

resp=`${wget} "https://XXX.XXX.XXX.XXX/reportdta?probe=${myname}&result=${demres}"
     --no-check-certificate --tries=1 --timeout=30 -q -O-`

exit 0
```


Internet Monitoring System v0.1 – measurement point status – Microsoft Internet Explorer
File Edit View Favorites Tools Help
AVAILABILITY
RESPONSE TIME
MEASUREMENT POINT STATUS
CHANGE PASSWORD
LOGOUT
STATUS
Probe1: [idle] 36 seconds
Bostream1 (Bondegatan, Södermalm, Stockholm)
.ss.sth.bostream.se)
Probe2: [down] 2 hours, 34 minutes, 26 seconds
Comhem1 (Folkkungagatan, Södermalm, Stockholm)
.bredband.comhem.se)
Probe3: [idle] 24 seconds
Bredbandsbolaget1 (Nacka, Stockholm)
cust.bredbandsbolaget.se)
Probe4: [idle] 13 seconds
Bredbandsbolaget2 (Liljeholmen, Stockholm)
tilde.se)
Probe5: [idle] 12 seconds
Glocalnet1 (Kungholmen, Stockholm)
tn.glocalnet.net)
Probe6: [idle] 6 seconds
Chello1 (Hornstullsstrand, Södermalm, Stockholm)
cm-upc.chello.se)
Probe7: [running] 8 seconds
Chello2 (Zinkensdamm, Södermalm, Stockholm)
cm-upc.chello.se)
Probe8: [running] 2 seconds
Telia1 (Simrishamn, Skåne)
.telia.com)
Probe9: [idle] 47 seconds
Song1 (Sollentuna, Stockholm)
sol.wtnord.net)
(Probes report two times every 60 sec.)
Done
Internet

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer

File Edit View Favorites Tools Help

AVAILABILITY | RESPONSE TIME | MEASUREMENT POINT STATUS | CHANGE PASSWORD | LOGOUT

MONTHLY STATISTICS | BOSTREAM 1 | COMHEM 1 | BREDBANDSBOLAGET 1 | BREDBANDSBOLAGET 2 | GLOCALNET 1 | CHELLO 1 | CHELLO 2 | TELIA 1 | SONG 1

HISTORY - AVAILABILITY FOR THE LAST MONTH (CLICK ON HEADLINE TO CHANGE SORTING)

From	To	Availability
Song1	Telia1	89.83%
Song1	Bostream1	91.44%
Song1	Chello1	92.21%
Bredbandsbolaget1	Telia1	93.45%
Bredbandsbolaget2	Telia1	93.45%
Glocalnet1	Telia1	93.46%
Chello2	Telia1	93.46%
Chello1	Telia1	93.47%
Comhem1	Telia1	93.49%
Chello2	Bostream1	95.07%
Bredbandsbolaget2	Bostream1	95.07%
Glocalnet1	Bostream1	95.07%
Comhem1	Bostream1	95.08%
Bredbandsbolaget1	Bostream1	95.09%
Chello1	Bostream1	95.16%
Glocalnet1	Chello1	95.77%
Song1	Comhem1	95.78%
Bredbandsbolaget1	Chello1	95.88%
Bredbandsbolaget2	Chello1	95.9%
Comhem1	Chello1	95.9%
Song1	Chello2	95.97%
Telia1	Chello1	95.97%
Bostream1	Chello1	96%
Chello2	Chello1	96.05%
Song1	Bredbandsbolaget1	96.16%
Bostream1	Telia1	96.19%
Comhem1	Song1	96.19%
Bostream1	Song1	96.25%
Song1	Bredbandsbolaget2	96.26%
Song1	Glocalnet1	96.28%
Glocalnet1	Song1	96.28%
Chello1	Song1	96.35%
Telia1	Song1	96.36%
Bredbandsbolaget1	Song1	96.38%
Bredbandsbolaget2	Song1	96.4%
Chello2	Song1	96.41%

Done

Internet

Client connectivity problems

- Crashing (ADLS/Cable)-modems
- “last mile” infrastructure problems (ADLS/cable mainly)
- Unscheduled maintenance (There are no scheduled!)
- Power outages
- Portal login-problems
- DHCP-problems
- Problems in the operators distribution-infrastructure
- Operator buy-out (Infrastructure moved to new core-infrastructure)
- Vacuum-cleaners that need the power outlet. =)

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer

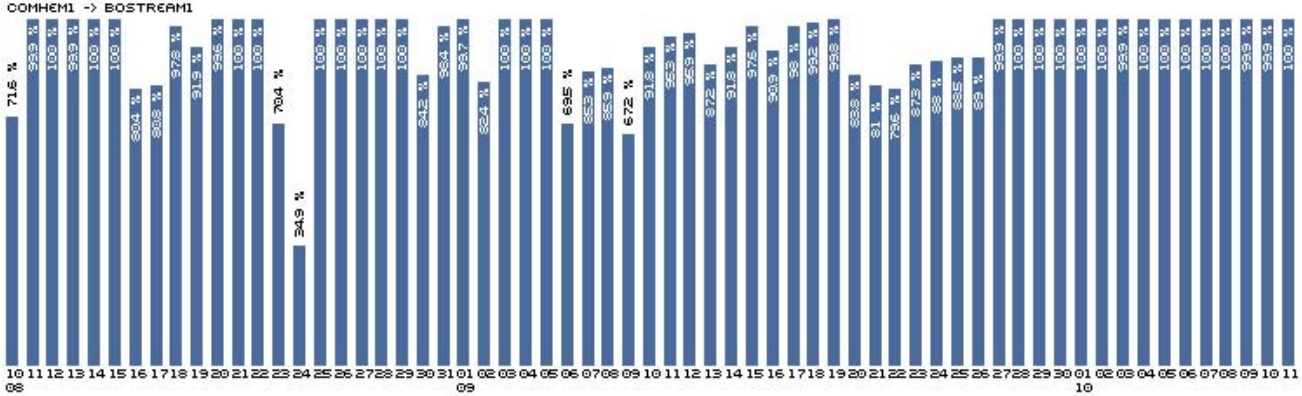
File Edit View Favorites Tools Help

AVAILABILITY | RESPONSE TIME | MEASUREMENT POINT STATUS | CHANGE PASSWORD | LOGOUT

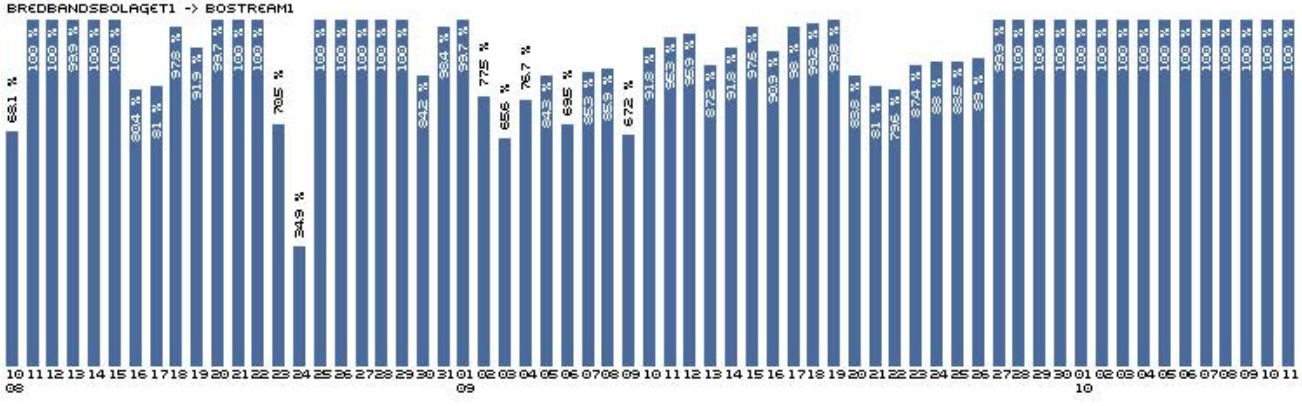
MONTHLY STATISTICS | BOSTREAM 1 | COMHEM 1 | BREDBANDSBOLAGET 1 | BREDBANDSBOLAGET 2 | GLOCALNET 1 | CHELLO 1 | CHELLO 2 | TELIA 1 | SONG 1

HISTORY - AVAILABILITY FOR THE LAST 62 DAYS PER DAY FOR MEASUREMENTS FROM BOSTREAM 1

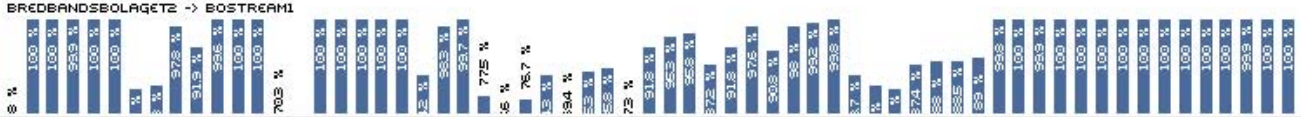
COMHEM1 -> BOSTREAM1



BREDBANDSBOLAGET1 -> BOSTREAM1



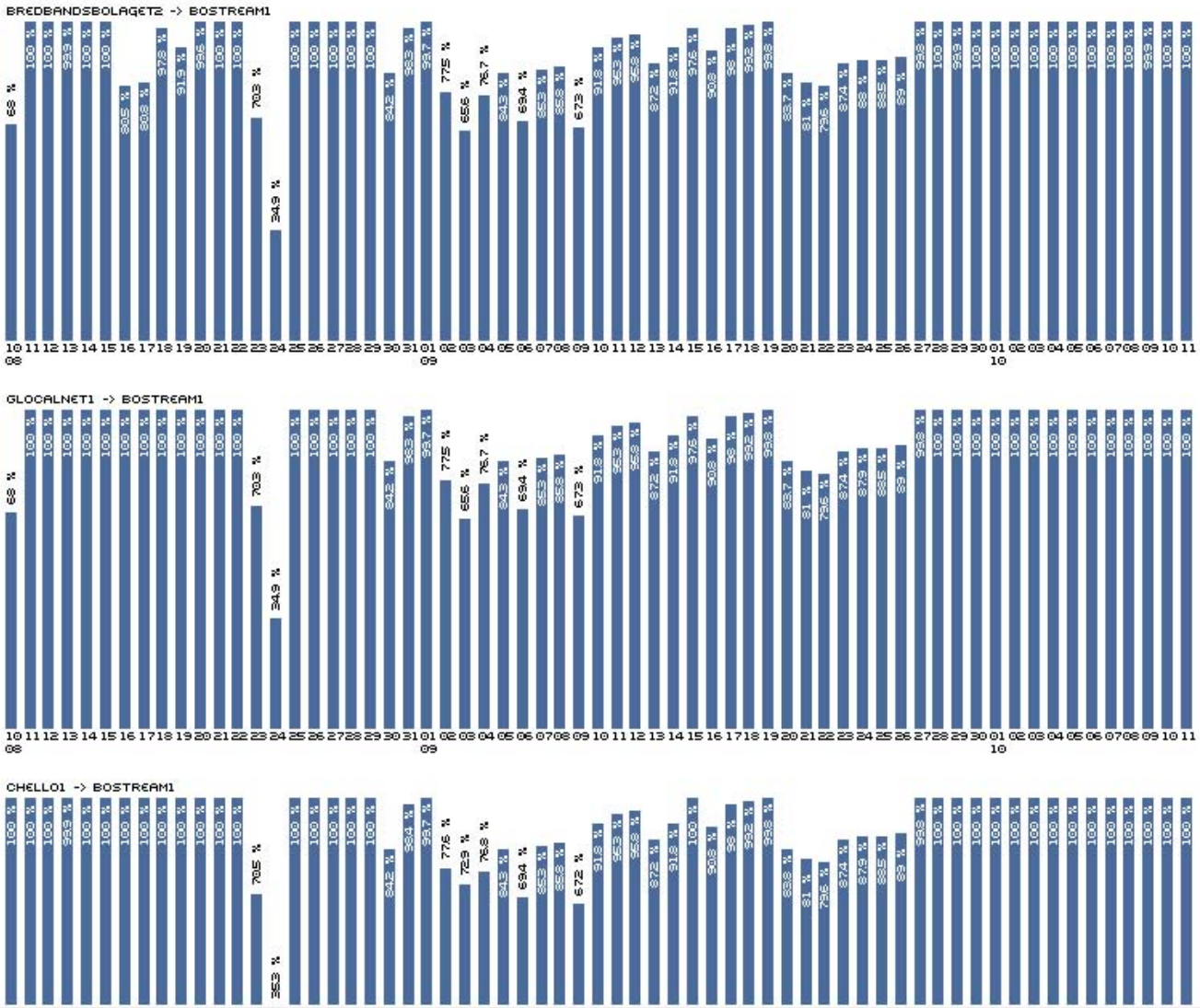
BREDBANDSBOLAGET2 -> BOSTREAM1



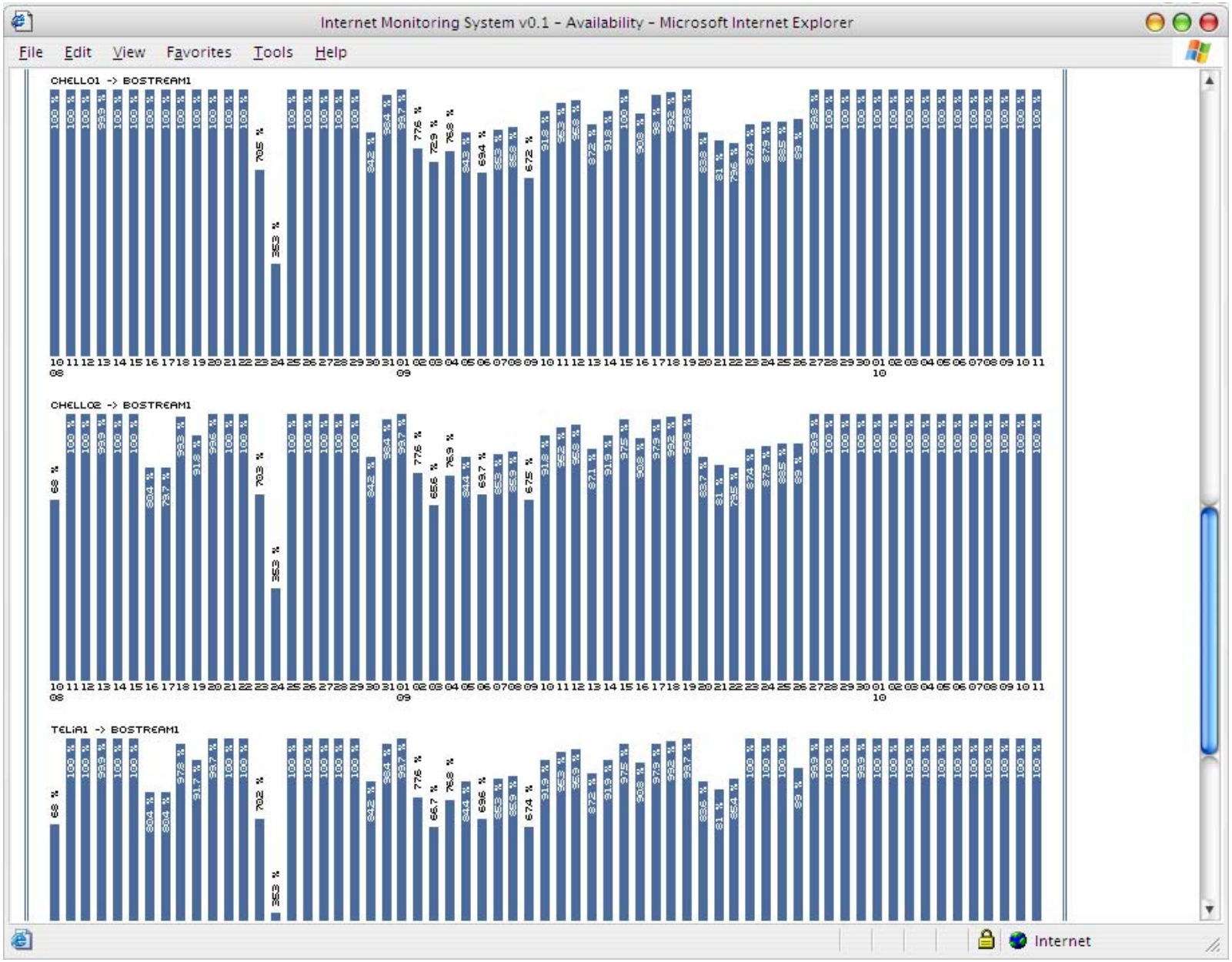
Internet

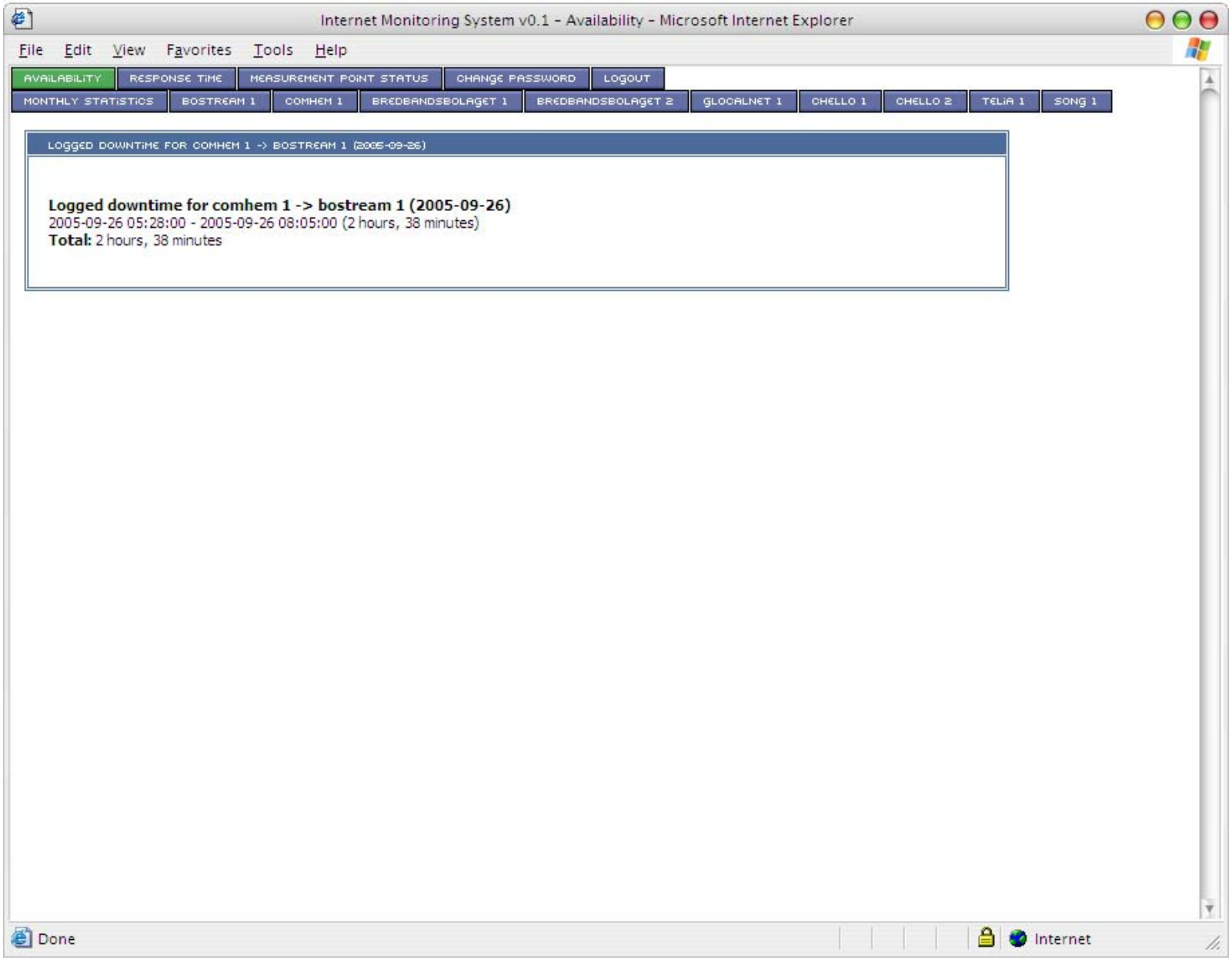
Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer

File Edit View Favorites Tools Help



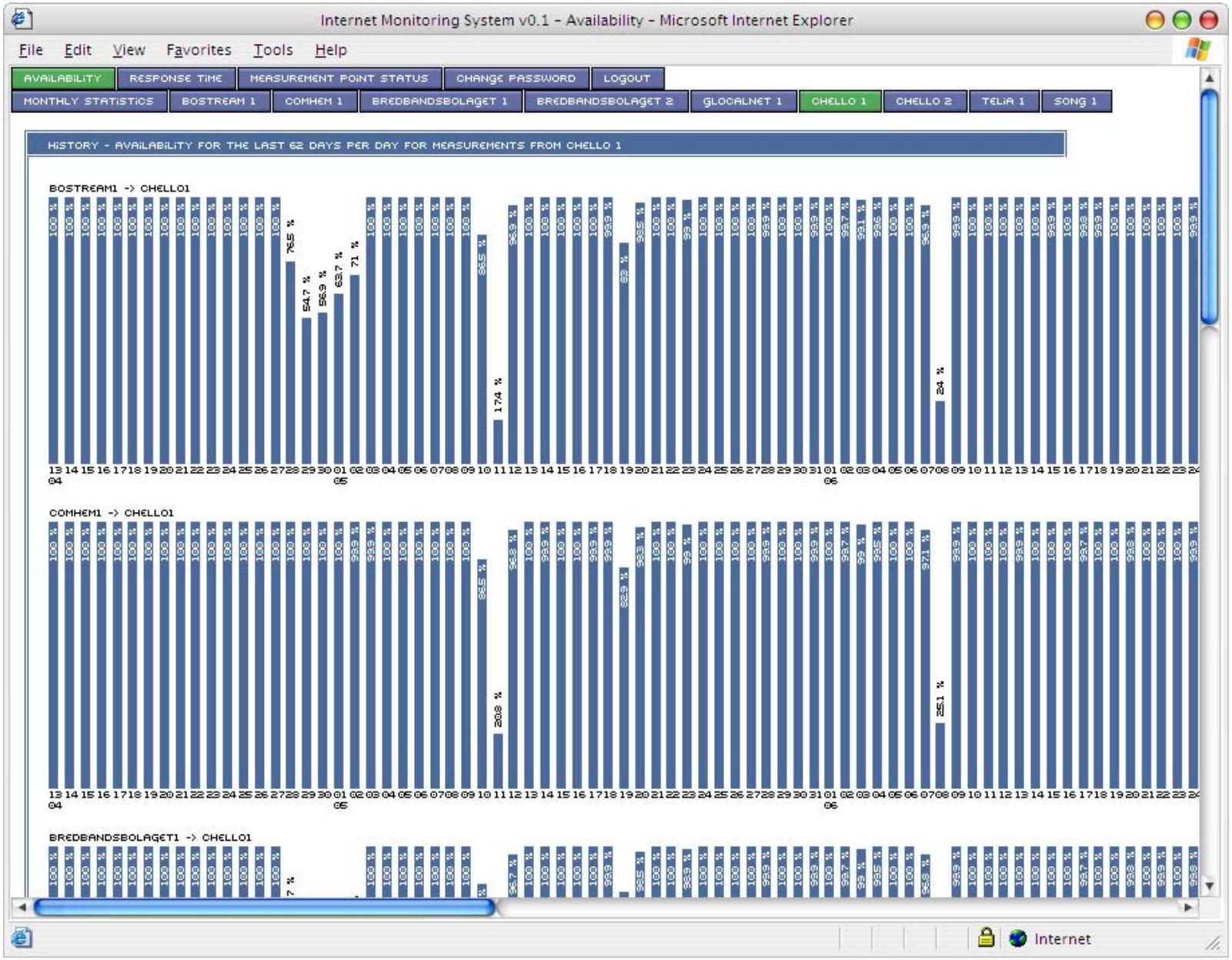
Internet

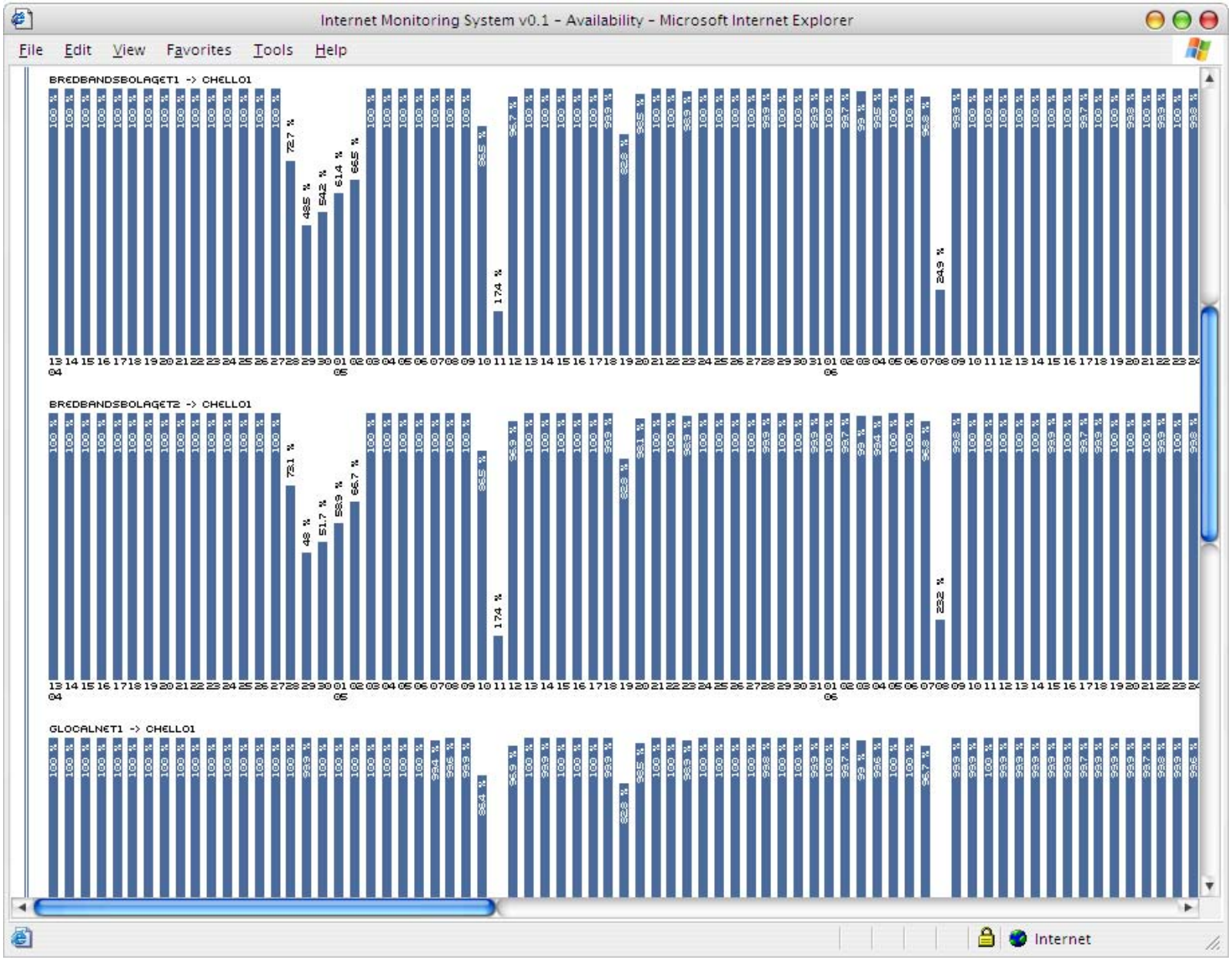

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
CHELLO1 -> BOSTREAM1
CHELLO2 -> BOSTREAM1
TELIA1 -> BOSTREAM1
Internet

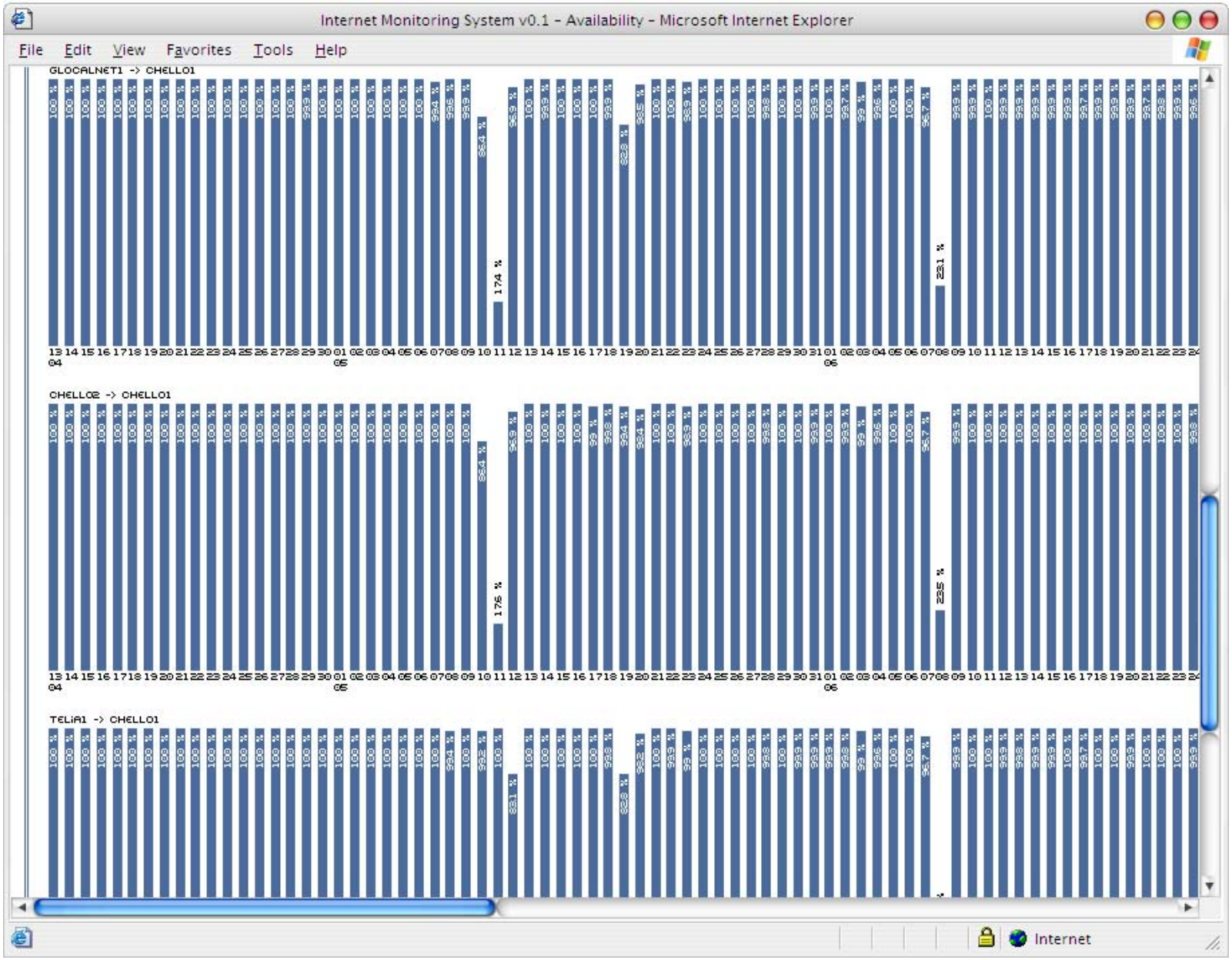

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
AVAILABILITY
RESPONSE TIME
MEASUREMENT POINT STATUS
CHANGE PASSWORD
LOGOUT
MONTHLY STATISTICS
BOSTREAM 1
COMHEM 1
BREDBANDSBOLAGET 1
BREDBANDSBOLAGET 2
GLOCALNET 1
CHELLO 1
CHELLO 2
TELIA 1
SONG 1
LOGGED DOWNTIME FOR COMHEM 1 -> BOSTREAM 1 (2005-09-26)
Logged downtime for comhem 1 -> bostream 1 (2005-09-26)
2005-09-26 05:28:00 - 2005-09-26 08:05:00 (2 hours, 38 minutes)
Total: 2 hours, 38 minutes
Done
Internet

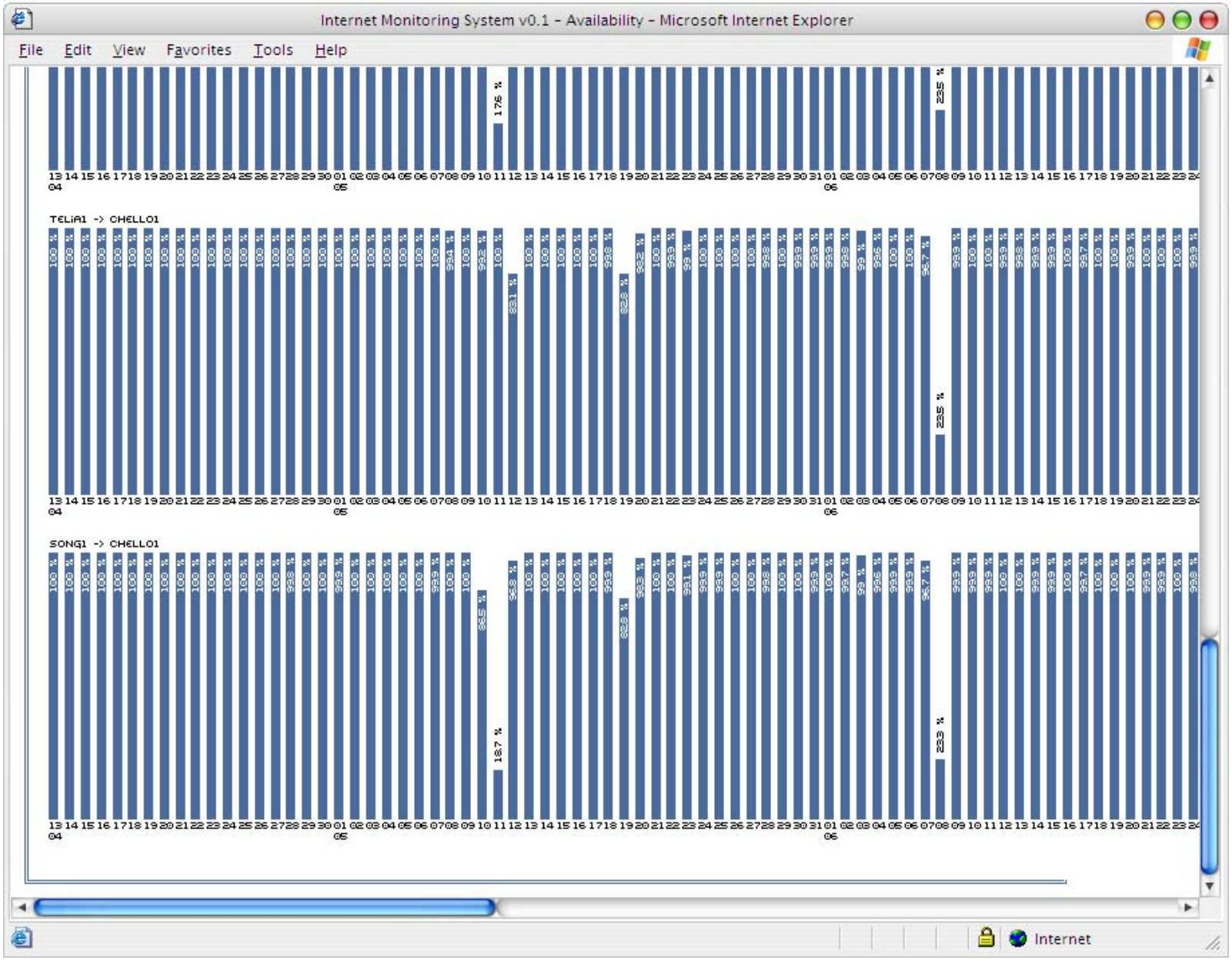
Routing problems between operators

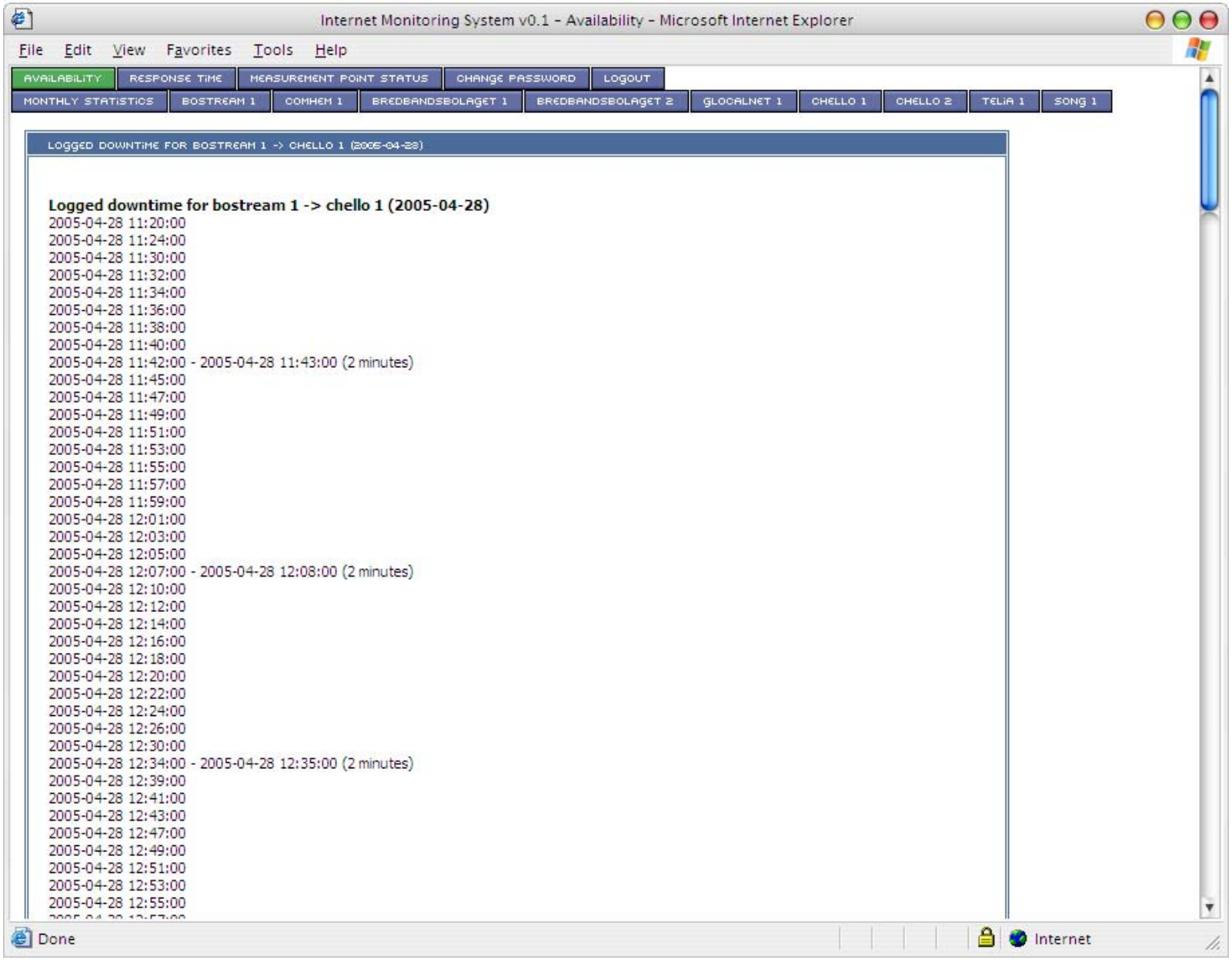
- Problems with peering and transit.
- Discovered when a measurement point has contact with some operators, but not others.
- These problems is most likely affecting a larger number of users.

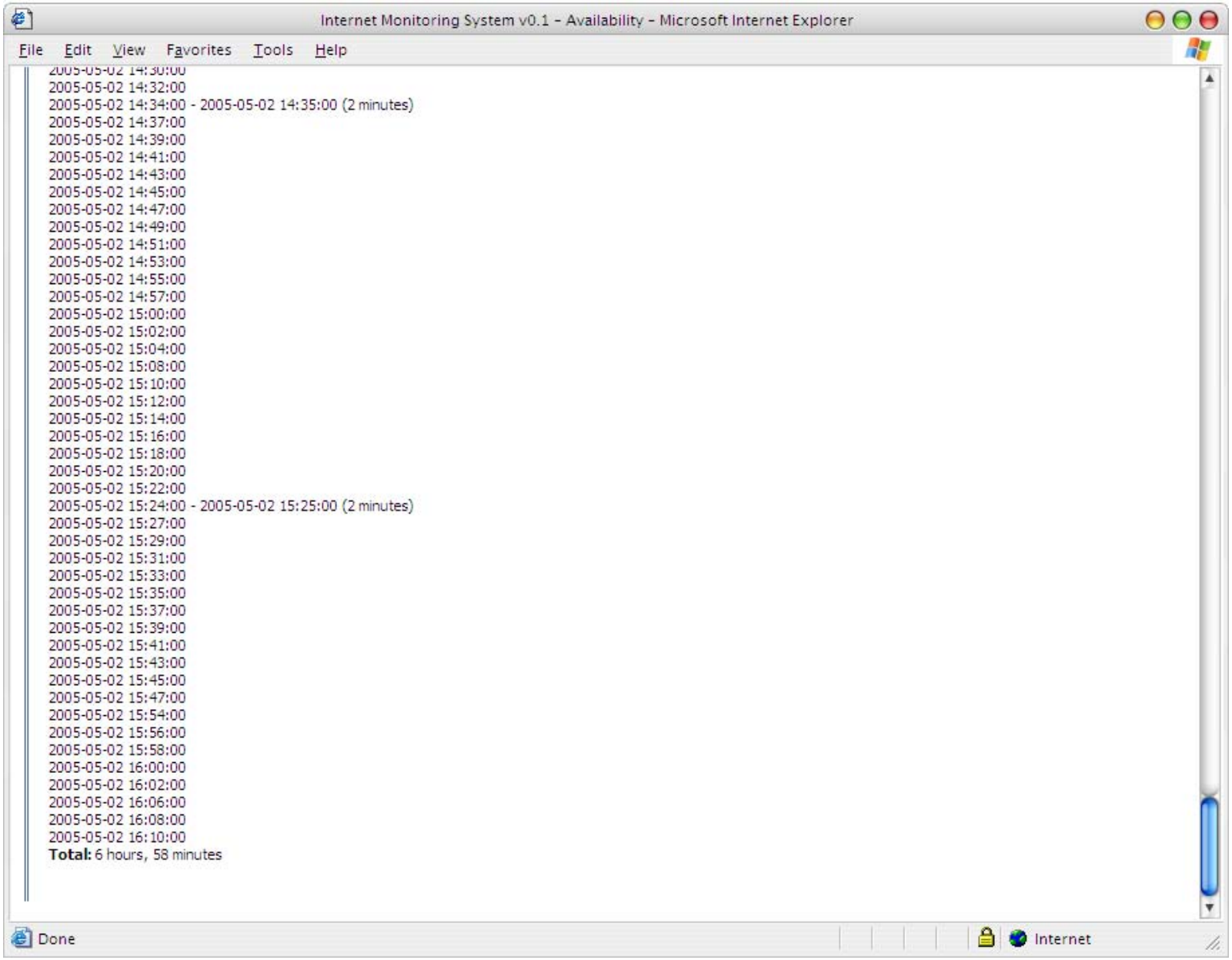

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
AVAILABILITY
RESPONSE TIME
MEASUREMENT POINT STATUS
CHANGE PASSWORD
LOGOUT
MONTHLY STATISTICS
BOSTREAM 1
COMHEM 1
BREDBANDSBOLAGET 1
BREDBANDSBOLAGET 2
GLOCALNET 1
CHELLO 1
CHELLO 2
TELIA 1
SONG 1
HISTORY - AVAILABILITY FOR THE LAST 62 DAYS PER DAY FOR MEASUREMENTS FROM CHELLO 1
BOSTREAM1 -> CHELLO1
COMHEM1 -> CHELLO1
BREDBANDSBOLAGET1 -> CHELLO1
Internet


Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
BREDBANDSBOLAGET1 -> CHELLO1
BREDBANDSBOLAGET2 -> CHELLO1
GLOCALNET1 -> CHELLO1
Internet


Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
GLOCALNET1 -> CHELLO1
CHELLO2 -> CHELLO1
TELIA1 -> CHELLO1
Internet


Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
TELIA1 -> CHELLO1
SONG1 -> CHELLO1
Internet

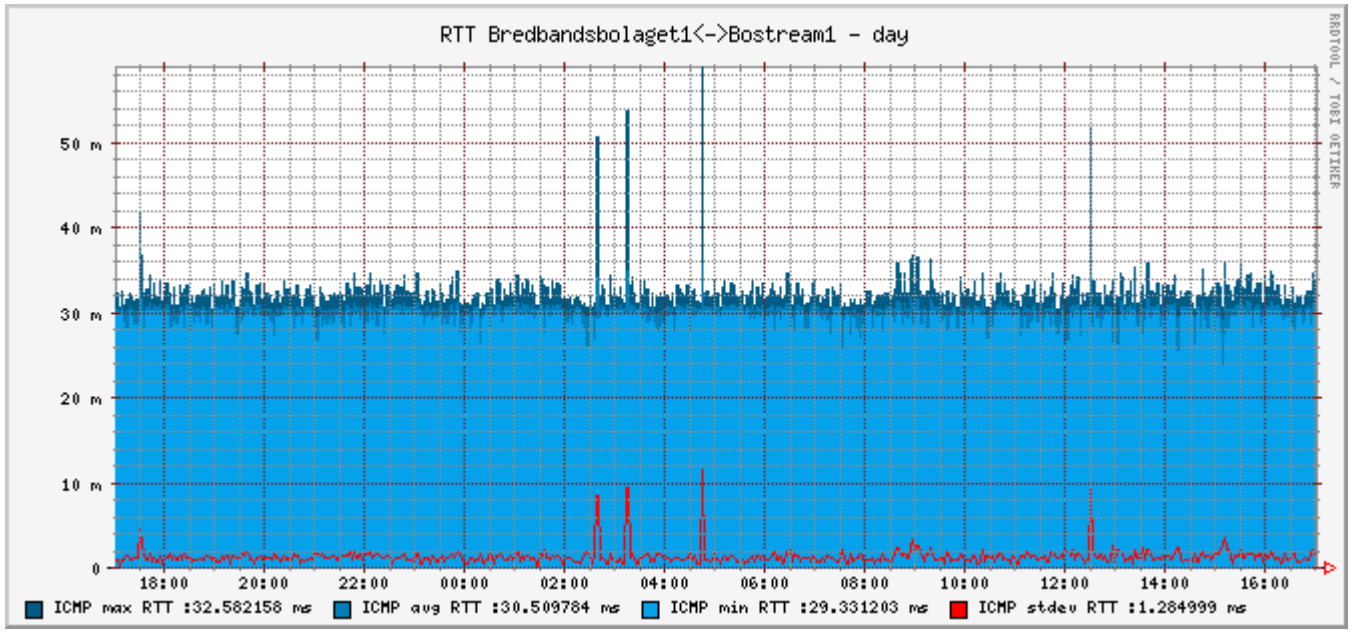

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
AVAILABILITY
RESPONSE TIME
MEASUREMENT POINT STATUS
CHANGE PASSWORD
LOGOUT
MONTHLY STATISTICS
BOSTREAM 1
COMHEM 1
BREDBANDSBOLAGET 1
BREDBANDSBOLAGET 2
GLOCALNET 1
CHELLO 1
CHELLO 2
TELIA 1
SONG 1
LOGGED DOWNTIME FOR BOSTREAM 1 -> CHELLO 1 (2005-04-28)
Logged downtime for bostream 1 -> chello 1 (2005-04-28)
2005-04-28 11:20:00
2005-04-28 11:24:00
2005-04-28 11:30:00
2005-04-28 11:32:00
2005-04-28 11:34:00
2005-04-28 11:36:00
2005-04-28 11:38:00
2005-04-28 11:40:00
2005-04-28 11:42:00 - 2005-04-28 11:43:00 (2 minutes)
2005-04-28 11:45:00
2005-04-28 11:47:00
2005-04-28 11:49:00
2005-04-28 11:51:00
2005-04-28 11:53:00
2005-04-28 11:55:00
2005-04-28 11:57:00
2005-04-28 11:59:00
2005-04-28 12:01:00
2005-04-28 12:03:00
2005-04-28 12:05:00
2005-04-28 12:07:00 - 2005-04-28 12:08:00 (2 minutes)
2005-04-28 12:10:00
2005-04-28 12:12:00
2005-04-28 12:14:00
2005-04-28 12:16:00
2005-04-28 12:18:00
2005-04-28 12:20:00
2005-04-28 12:22:00
2005-04-28 12:24:00
2005-04-28 12:26:00
2005-04-28 12:30:00
2005-04-28 12:34:00 - 2005-04-28 12:35:00 (2 minutes)
2005-04-28 12:39:00
2005-04-28 12:41:00
2005-04-28 12:43:00
2005-04-28 12:47:00
2005-04-28 12:49:00
2005-04-28 12:51:00
2005-04-28 12:53:00
2005-04-28 12:55:00
Done
Internet


Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer
File Edit View Favorites Tools Help
2005-05-02 14:30:00
2005-05-02 14:32:00
2005-05-02 14:34:00 - 2005-05-02 14:35:00 (2 minutes)
2005-05-02 14:37:00
2005-05-02 14:39:00
2005-05-02 14:41:00
2005-05-02 14:43:00
2005-05-02 14:45:00
2005-05-02 14:47:00
2005-05-02 14:49:00
2005-05-02 14:51:00
2005-05-02 14:53:00
2005-05-02 14:55:00
2005-05-02 14:57:00
2005-05-02 15:00:00
2005-05-02 15:02:00
2005-05-02 15:04:00
2005-05-02 15:08:00
2005-05-02 15:10:00
2005-05-02 15:12:00
2005-05-02 15:14:00
2005-05-02 15:16:00
2005-05-02 15:18:00
2005-05-02 15:20:00
2005-05-02 15:22:00
2005-05-02 15:24:00 - 2005-05-02 15:25:00 (2 minutes)
2005-05-02 15:27:00
2005-05-02 15:29:00
2005-05-02 15:31:00
2005-05-02 15:33:00
2005-05-02 15:35:00
2005-05-02 15:37:00
2005-05-02 15:39:00
2005-05-02 15:41:00
2005-05-02 15:43:00
2005-05-02 15:45:00
2005-05-02 15:47:00
2005-05-02 15:54:00
2005-05-02 15:56:00
2005-05-02 15:58:00
2005-05-02 16:00:00
2005-05-02 16:02:00
2005-05-02 16:06:00
2005-05-02 16:08:00
2005-05-02 16:10:00
Total: 6 hours, 58 minutes
Done
Internet

RTT/Jitter measurements

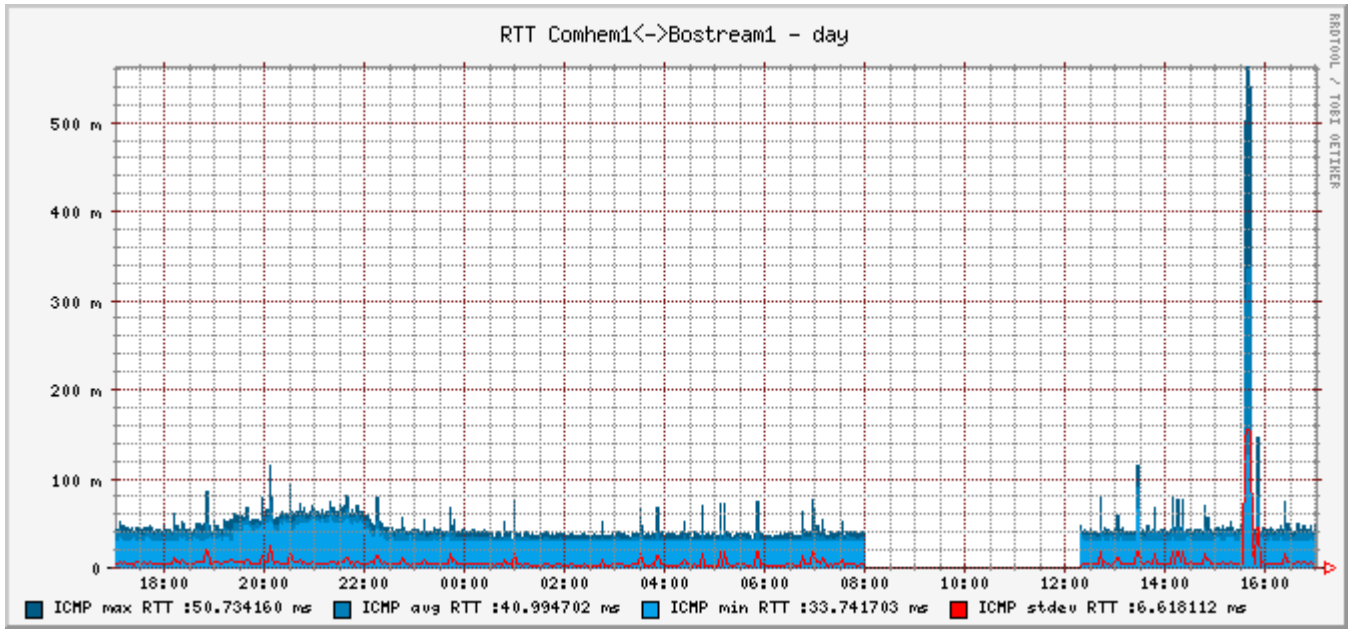
- Especially interesting for VoIP applications.
- Not a good idea for connections in use.
- Roundtrip times for what? ICMP, UDP, TCP??
- Tools, kernels and drivers?

Good RTT



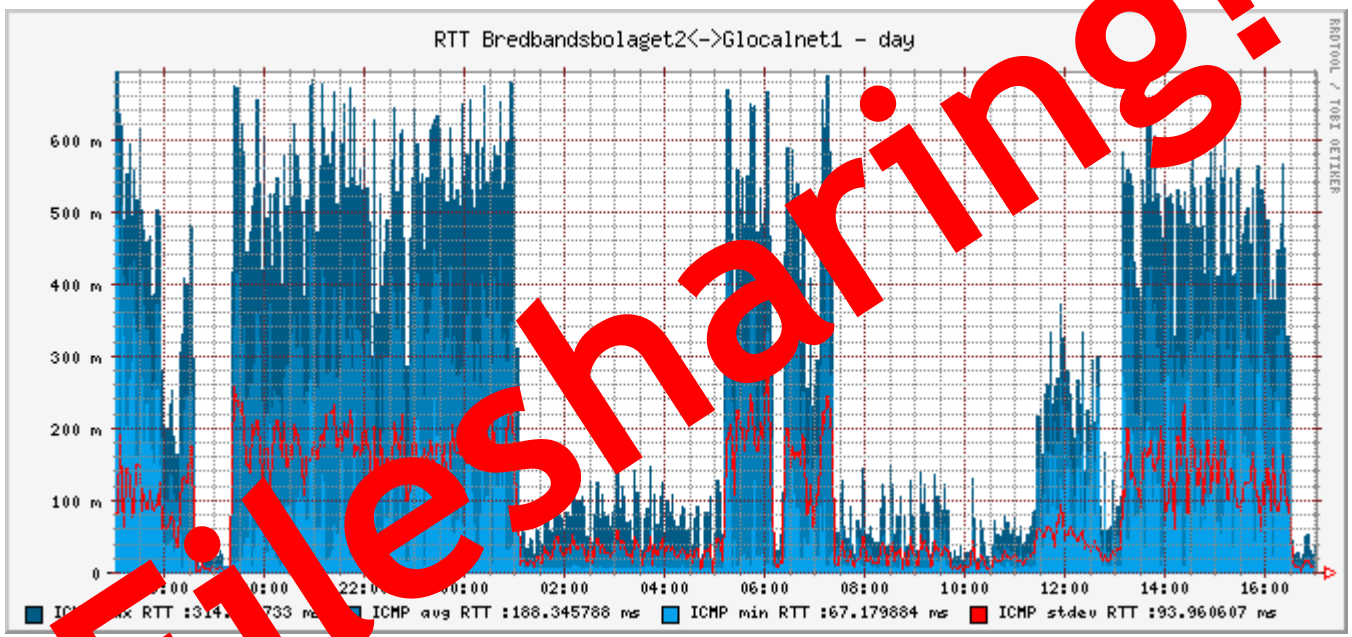
(Check the scale! 60 ms)

Bumb, downtime & peak



(Check the scale! 600 ms)

Bad RTT



Filesharing!

(Check the scale! 700 ms)

No problems with

- Operators with fiber infrastructure (~100% availability)
- Measurement point hardware (Really!)
- Server
- Scripts
- Vacuum cleaners!! (REALLY!)

Internet Monitoring System v0.1 - Availability - Microsoft Internet Explorer

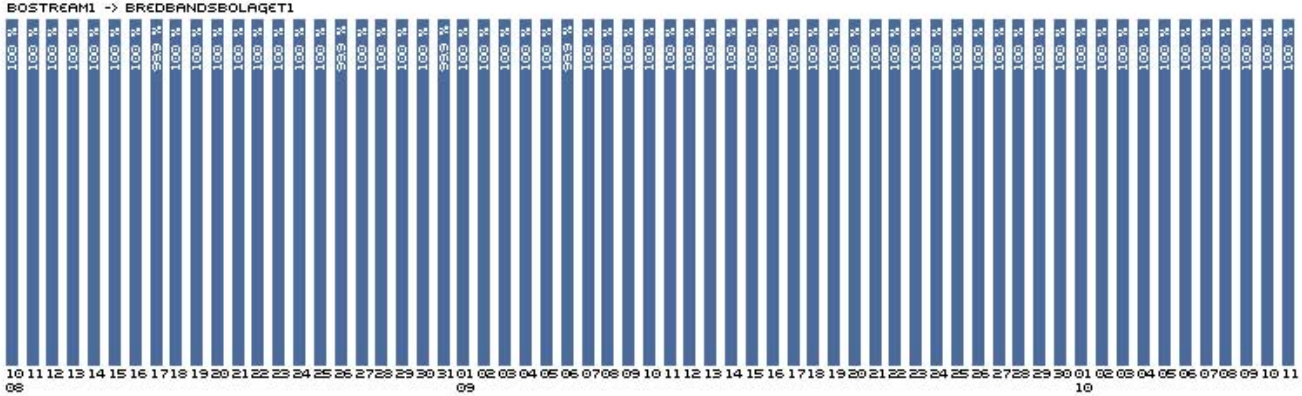
File Edit View Favorites Tools Help

AVAILABILITY | RESPONSE TIME | MEASUREMENT POINT STATUS | CHANGE PASSWORD | LOGOUT

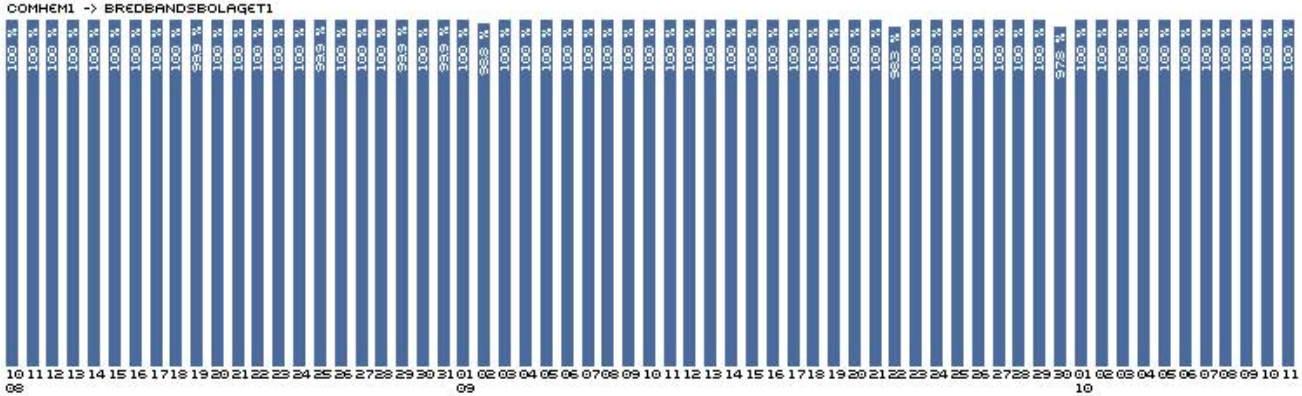
MONTHLY STATISTICS | BOSTREAM 1 | COMHEM 1 | BREDBANDSBOLAGET 1 | BREDBANDSBOLAGET 2 | GLOCALNET 1 | CHELLO 1 | CHELLO 2 | TELIA 1 | SONG 1

HISTORY - AVAILABILITY FOR THE LAST 62 DAYS PER DAY FOR MEASUREMENTS FROM BREDBANDSBOLAGET 1

BOSTREAM1 -> BREDBANDSBOLAGET1



COMHEM1 -> BREDBANDSBOLAGET1



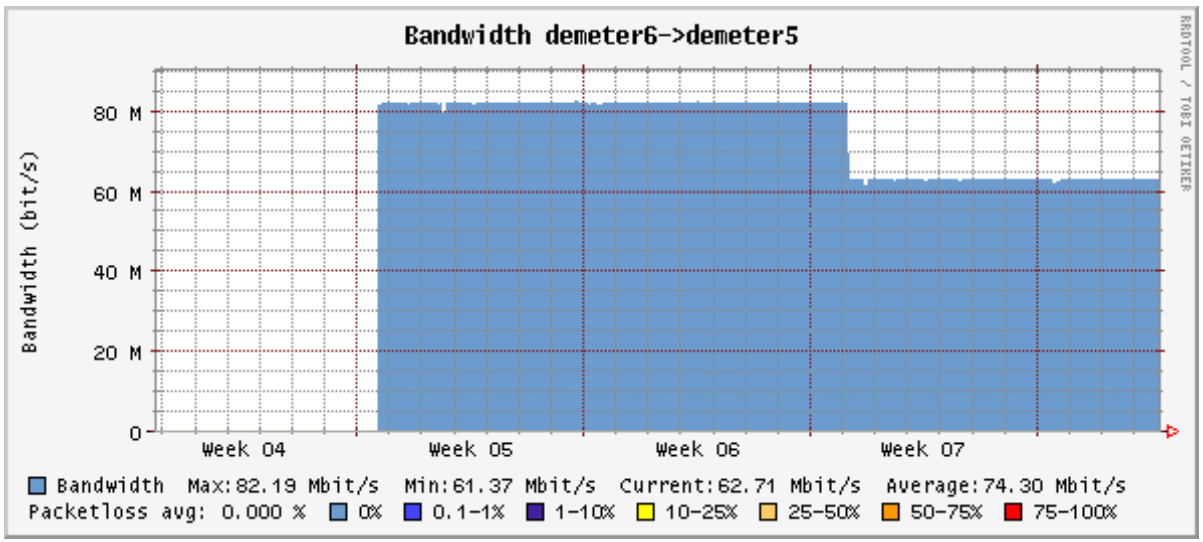
BREDBANDSBOLAGET2 -> BREDBANDSBOLAGET1

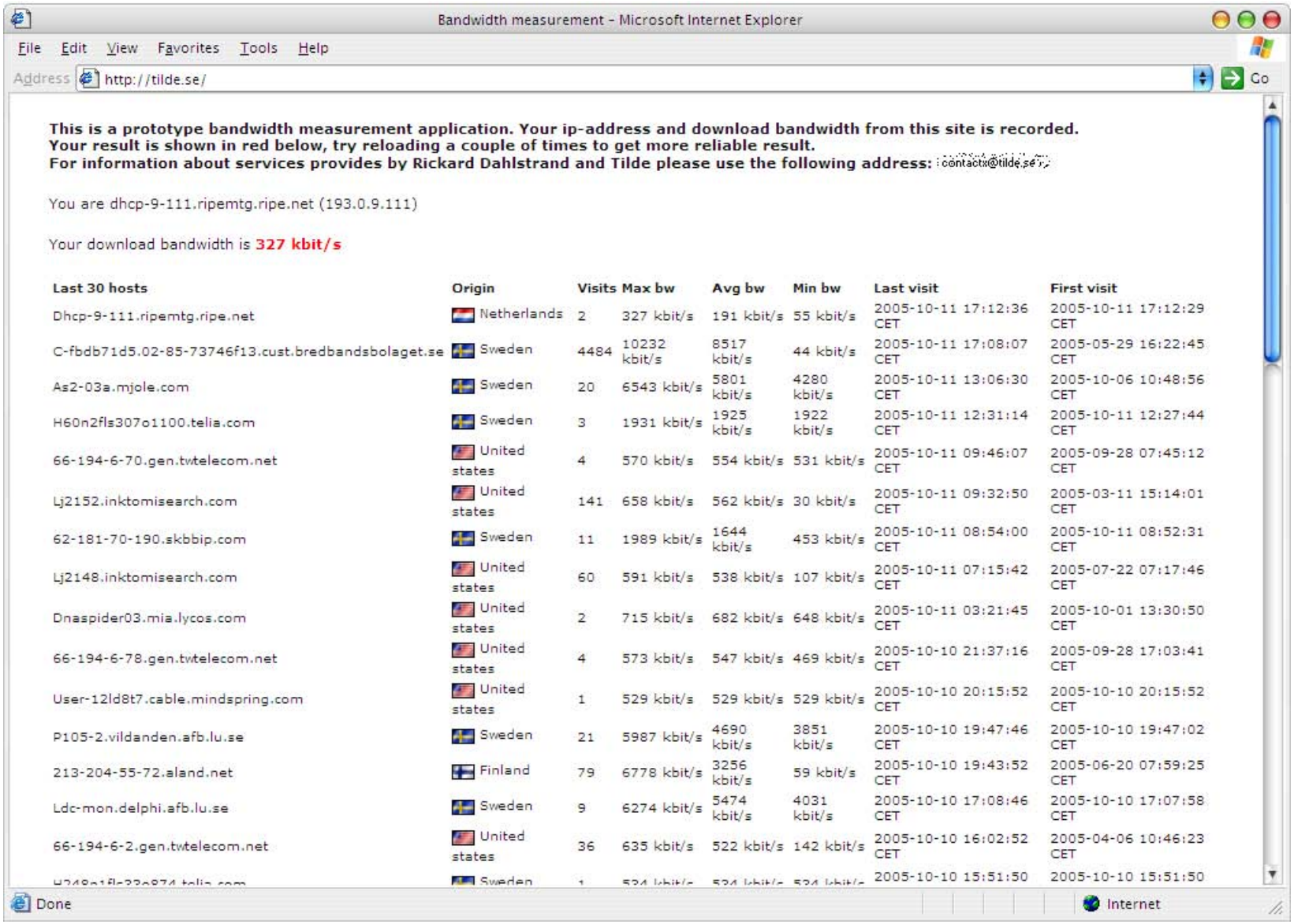
Done | Internet

Future measurements

Bandwidth measurements

- REALLY not a good idea for connections in use.
- Netperf/iperf
- Http download bw





This is a prototype bandwidth measurement application. Your ip-address and download bandwidth from this site is recorded.
Your result is shown in red below, try reloading a couple of times to get more reliable result.
For information about services provides by Rickard Dahlstrand and Tilde please use the following address: contact@tilde.se

You are dhcp-9-111.ripemtg.ripe.net (193.0.9.111)

Your download bandwidth is **327 kbit/s**

Last 30 hosts	Origin	Visits	Max bw	Avg bw	Min bw	Last visit	First visit
Dhcp-9-111.ripemtg.ripe.net	Netherlands	2	327 kbit/s	191 kbit/s	55 kbit/s	2005-10-11 17:12:36 CET	2005-10-11 17:12:29 CET
C-fbdb71d5.02-85-73746f13.cust.bredbandsbolaget.se	Sweden	4484	10232 kbit/s	8517 kbit/s	44 kbit/s	2005-10-11 17:08:07 CET	2005-05-29 16:22:45 CET
As2-03a.mjole.com	Sweden	20	6543 kbit/s	5801 kbit/s	4280 kbit/s	2005-10-11 13:06:30 CET	2005-10-06 10:48:56 CET
H60n2fls307o1100.telia.com	Sweden	3	1931 kbit/s	1925 kbit/s	1922 kbit/s	2005-10-11 12:31:14 CET	2005-10-11 12:27:44 CET
66-194-6-70.gen.twtelecom.net	United states	4	570 kbit/s	554 kbit/s	531 kbit/s	2005-10-11 09:46:07 CET	2005-09-28 07:45:12 CET
Lj2152.inktomisearch.com	United states	141	658 kbit/s	562 kbit/s	30 kbit/s	2005-10-11 09:32:50 CET	2005-03-11 15:14:01 CET
62-181-70-190.skbbip.com	Sweden	11	1989 kbit/s	1644 kbit/s	453 kbit/s	2005-10-11 08:54:00 CET	2005-10-11 08:52:31 CET
Lj2148.inktomisearch.com	United states	60	591 kbit/s	538 kbit/s	107 kbit/s	2005-10-11 07:15:42 CET	2005-07-22 07:17:46 CET
Dnaspider03.mia.lycos.com	United states	2	715 kbit/s	682 kbit/s	648 kbit/s	2005-10-11 03:21:45 CET	2005-10-01 13:30:50 CET
66-194-6-78.gen.twtelecom.net	United states	4	573 kbit/s	547 kbit/s	469 kbit/s	2005-10-10 21:37:16 CET	2005-09-28 17:03:41 CET
User-12ld8t7.cable.mindspring.com	United states	1	529 kbit/s	529 kbit/s	529 kbit/s	2005-10-10 20:15:52 CET	2005-10-10 20:15:52 CET
P105-2.vildanden.afb.lu.se	Sweden	21	5987 kbit/s	4690 kbit/s	3851 kbit/s	2005-10-10 19:47:46 CET	2005-10-10 19:47:02 CET
213-204-55-72.aland.net	Finland	79	6778 kbit/s	3256 kbit/s	59 kbit/s	2005-10-10 19:43:52 CET	2005-06-20 07:59:25 CET
Ldc-mon.delphi.afb.lu.se	Sweden	9	6274 kbit/s	5474 kbit/s	4031 kbit/s	2005-10-10 17:08:46 CET	2005-10-10 17:07:58 CET
66-194-6-2.gen.twtelecom.net	United states	36	635 kbit/s	522 kbit/s	142 kbit/s	2005-10-10 16:02:52 CET	2005-04-06 10:46:23 CET
H248n1fl-22o874.telia.com	Sweden	1	534 kbit/s	534 kbit/s	534 kbit/s	2005-10-10 15:51:50	2005-10-10 15:51:50

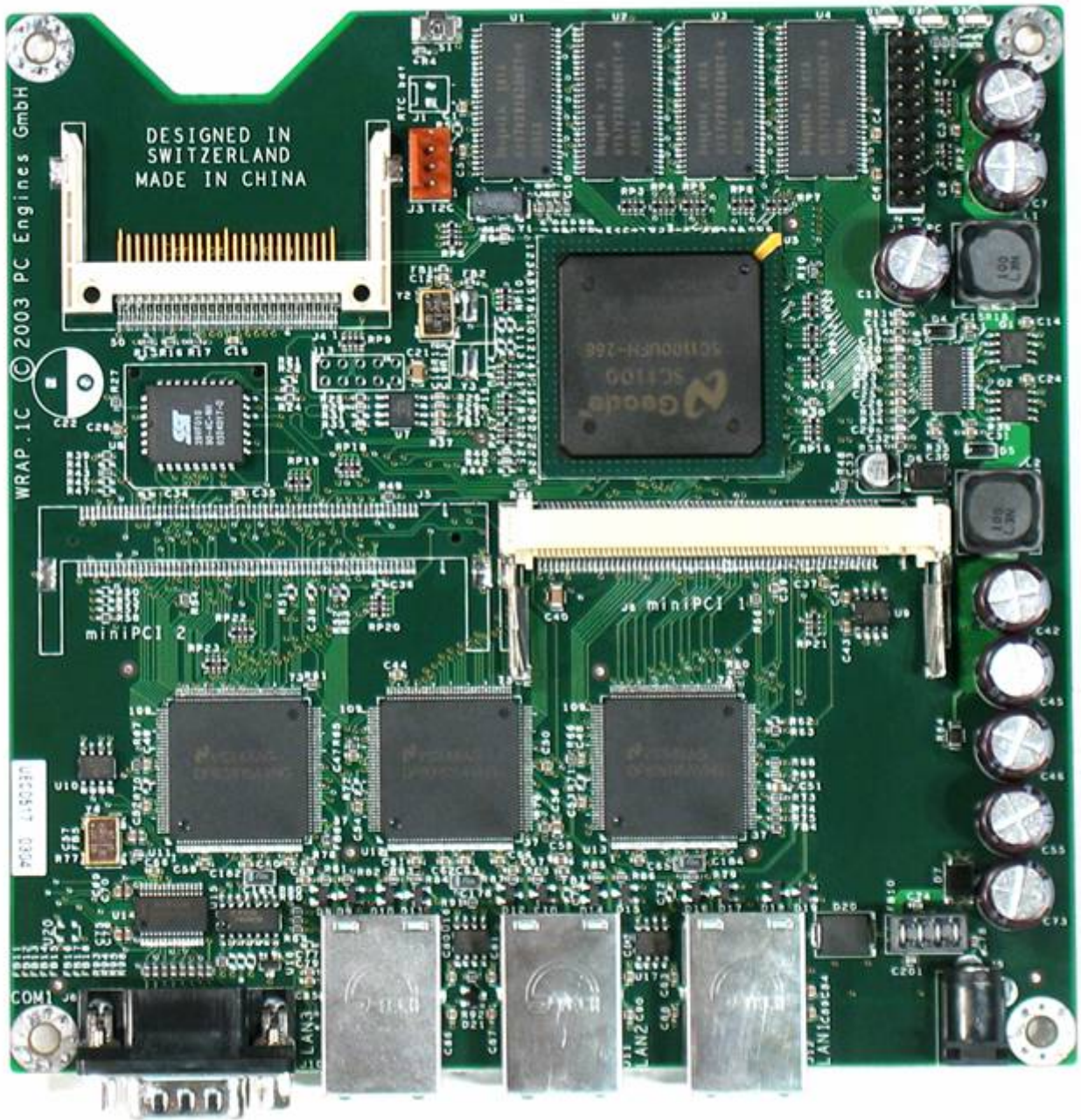
More crazy ideas

- RTT for other protocols? (UDP, TCP RTT)
- Hop-counts?
- Traceroutes? (Is this still a valid tool)

The neat stuff

Hardware

- PC Engines 6” WRAP system boards and boxes
- CPU: 266 MHz AMD Geode SC1100 CPU (x86)
- DRAM: 128 MB SDRAM
- Storage: 128 MB Compact Flash (Industrial grade are recommended!)
- OS: Any x86 OS are supported. (OpenBSD preferred)
- Power: 3-5W at 12 DC.
- LAN: 3 10/100 Ethernet port (National DP83816)
- Watchdog, LM77 temp monitor, serial console and 3 Leds you can flash and flicker!
- No keyboards, vga-ports, usb or power buttons!


DESIGNED IN
SWITZERLAND
MADE IN CHINA
© 2003 PC Engines GmbH
WRAP.1C
miniPCI 2
miniPCI 1
COM1
LAN3
LAN2
LAN1

Ramdisk-kernels

- Primary used for cd and floppy-based OS-installation, but perfect for flash-disk based systems!
- Limits the number of writes and reads to the flash which means longer lifespan and less corrupted flash.
- One kernel-file contains the kernel and a ramdisk image containing the full distribution.
- Means that an entire distribution can be upgraded at once. If you replace one file on flash you replace not only the kernel, but the entire installation.

OS

- Based on OpenBSD 3.7.
- No patches, just a custom built process.
- Follows releases (distribution and kernel)
- Uses PF as a firewall.
- DHCP and NAT on internal interfaces for use as a firewall.
- NTP for timesyncing
- Ram based round robin Syslog + centralized logging.
- OpenBSD rocks!

Remote Management using SSH

- It’s secure and can be scripted!
- All measurement points respond with SSH on a non-standard port
- Only public-key authentication allowed (a master key)
- Using ssh & scp you can basically do anything!
- Including OS-upgrades!

To check the temperature

```
[rd@demeterupdate]# execall "sysctl hw.sensors"
--------Probe1---------
hw.sensors.0=lmtemp0, TEMP, temp, 38.50 degC / 101.30 degF
--------Probe2---------
hw.sensors.0=lmtemp0, TEMP, temp, 37.00 degC / 98.60 degF
--------Probe3---------
hw.sensors.0=lmtemp0, TEMP, temp, 45.50 degC / 113.90 degF
--------Probe4---------
hw.sensors.0=lmtemp0, TEMP, temp, 37.00 degC / 98.60 degF
--------Probe5---------
hw.sensors.0=lmtemp0, TEMP, temp, 39.00 degC / 102.20 degF
--------Probe6---------
hw.sensors.0=lmtemp0, TEMP, temp, 44.00 degC / 111.20 degF
--------Probe7---------
hw.sensors.0=lmtemp0, TEMP, temp, 40.50 degC / 104.90 degF
--------Probe8---------
hw.sensors.0=lmtemp0, TEMP, temp, 39.50 degC / 103.10 degF
--------Probe9---------
hw.sensors.0=lmtemp0, TEMP, temp, 39.00 degC / 102.20 degF
[rd@demeterupdate]#
```

To verify NTP-functionality

```
[rd@demeterupdate]# execall date
--------Probe1---------
Tue Oct 11 14:09:54 CEST 2005
--------Probe2---------
Tue Oct 11 14:09:55 CEST 2005
--------Probe3---------
Tue Oct 11 14:09:56 CEST 2005
--------Probe4---------
Tue Oct 11 14:09:57 CEST 2005
--------Probe5---------
Tue Oct 11 14:09:59 CEST 2005
--------Probe6---------
Tue Oct 11 14:10:01 CEST 2005
--------Probe7---------
Tue Oct 11 14:10:02 CEST 2005
--------Probe8---------
Tue Oct 11 14:10:03 CEST 2005
--------Probe9---------
Tue Oct 11 14:10:04 CEST 2005
[rd@demeterupdate]#
```

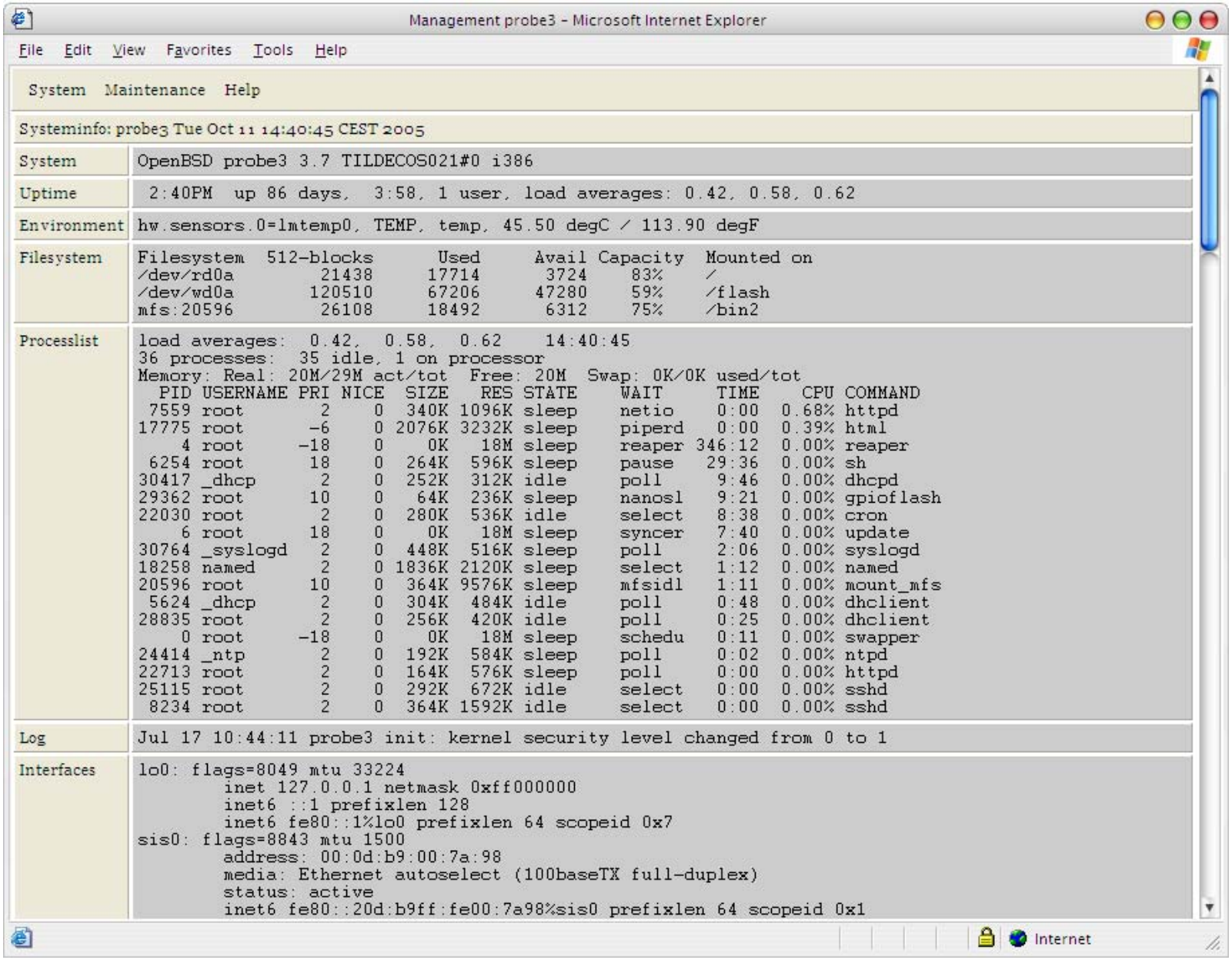
Or to upgrade

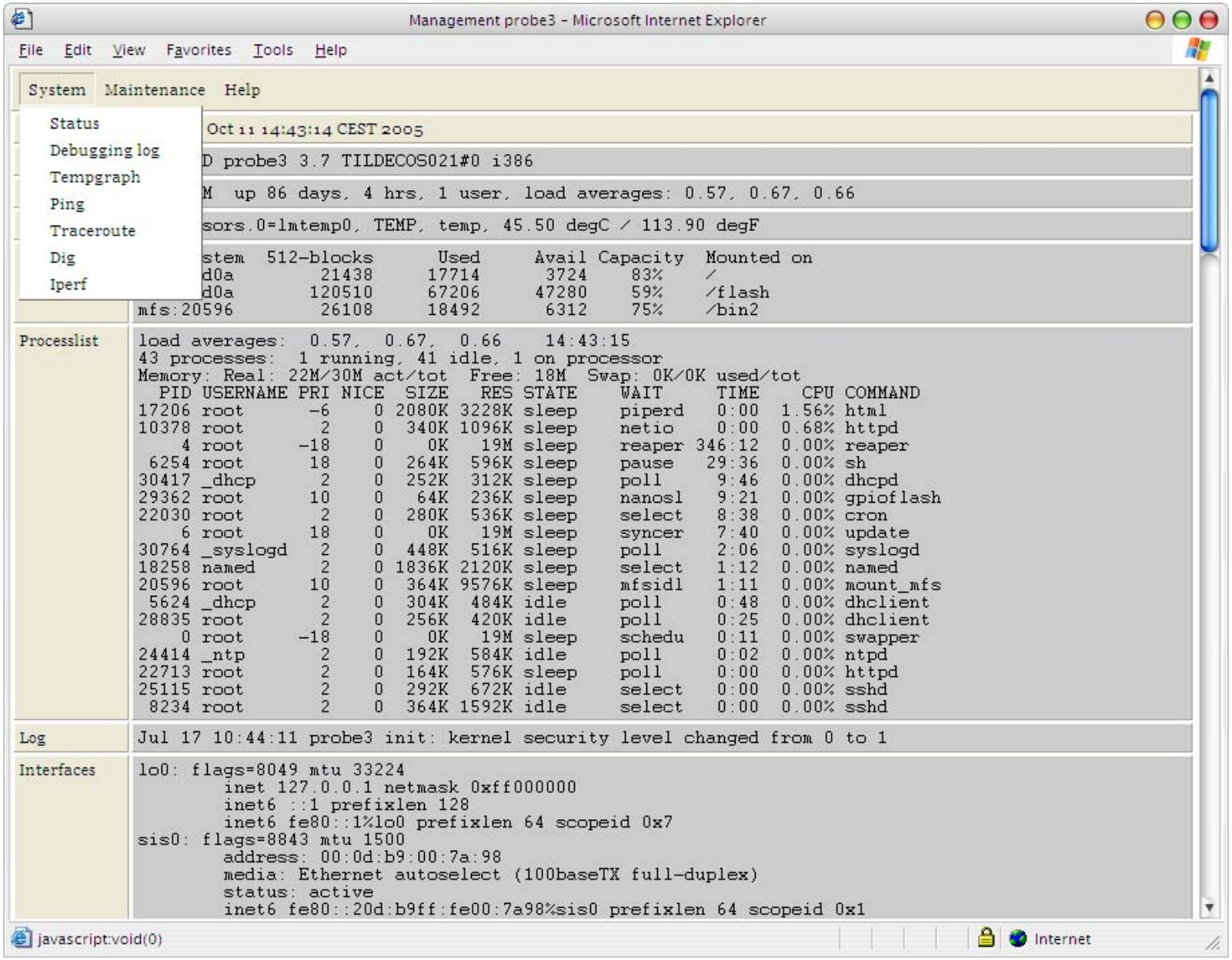
```
[rd@demeterupdate]# upgradeall bsd37.kernel
--------Probe1---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe2---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe3---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe4---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe5---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe6---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe7---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe8---------
bsd moved to obsd, new bsd moved to flash, rebooted
--------Probe9---------
bsd moved to obsd, new bsd moved to flash, rebooted
[rd@demeterupdate]#
```

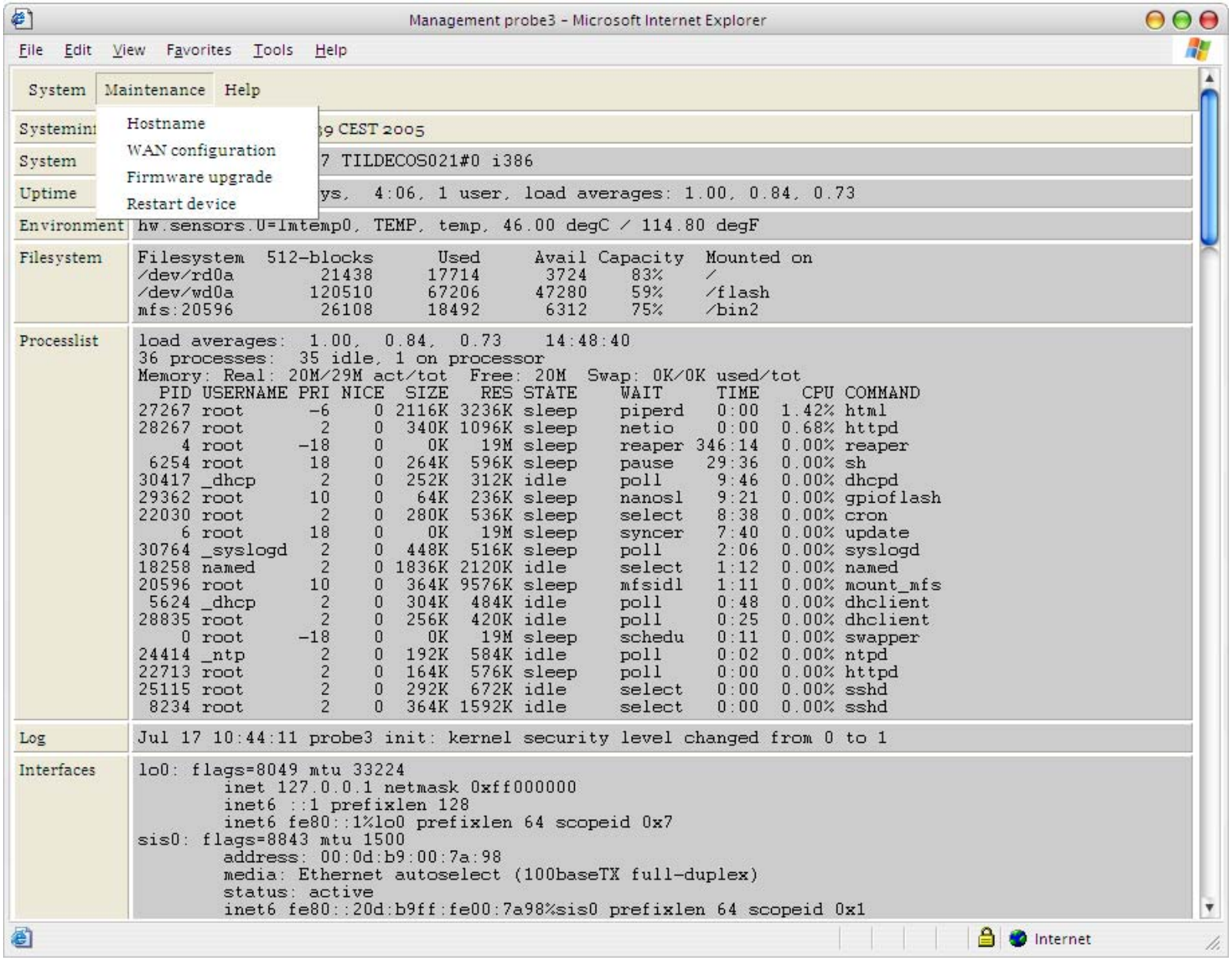
For those who don’t like SSH

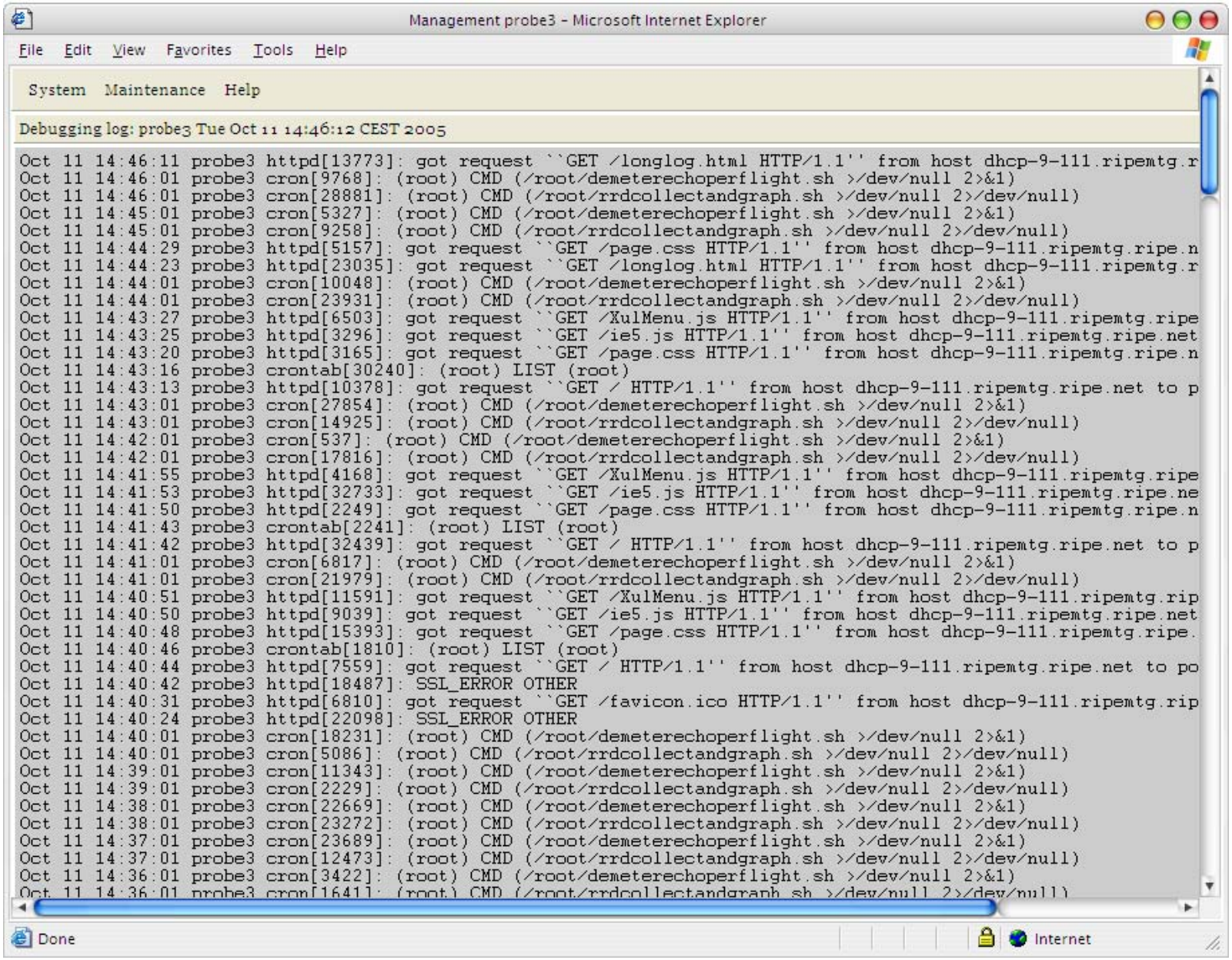
- A webbased management and troubleshooting interface accessible over https.
- Contains logs, ifconfig, netstat, firewall-config etc.
- Open on local ethernet ports and via Internet using a shell debugcommand:

```
[root@probe3 root]# openhttps
External management interface open from 193.0.9.111, now goto https://xxx.xxx.xxx.xxx/
[root@probe3 root]# closehttps
External management interface closed!
[root@probe3 root]#
```


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Systeminfo: probe3 Tue Oct 11 14:40:45 CEST 2005
System
OpenBSD probe3 3.7 TILDECOS021#0 i386
Uptime
2:40PM up 86 days, 3:58, 1 user, load averages: 0.42, 0.58, 0.62
Environment
hw.sensors.0=lmtemp0, TEMP, temp, 45.50 degC / 113.90 degF
Filesystem
Filesystem 512-blocks Used Avail Capacity Mounted on
/dev/rd0a 21438 17714 3724 83% /
/dev/wd0a 120510 67206 47280 59% /flash
mfs:20596 26108 18492 6312 75% /bin2
Processlist
load averages: 0.42, 0.58, 0.62 14:40:45
36 processes: 35 idle, 1 on processor
Memory: Real: 20M/29M act/tot Free: 20M Swap: 0K/0K used/tot
PID USERNAME PRI NICE SIZE RES STATE WAIT TIME CPU COMMAND
7559 root 2 0 340K 1096K sleep netio 0:00 0.68% httpd
17775 root -6 0 2076K 3232K sleep piperd 0:00 0.39% html
4 root -18 0 0K 18M sleep reaper 346:12 0.00% reaper
6254 root 18 0 264K 596K sleep pause 29:36 0.00% sh
30417 _dhcp 2 0 252K 312K idle poll 9:46 0.00% dhcpd
29362 root 10 0 64K 236K sleep nanosl 9:21 0.00% gpioflash
22030 root 2 0 280K 536K idle select 8:38 0.00% cron
6 root 18 0 0K 18M sleep syncer 7:40 0.00% update
30764 _syslogd 2 0 448K 516K sleep poll 2:06 0.00% syslogd
18258 named 2 0 1836K 2120K sleep select 1:12 0.00% named
20596 root 10 0 364K 9576K sleep mfsidl 1:11 0.00% mount_mfs
5624 _dhcp 2 0 304K 484K idle poll 0:48 0.00% dhclient
28835 root 2 0 256K 420K idle poll 0:25 0.00% dhclient
0 root -18 0 0K 18M sleep schedu 0:11 0.00% swapper
24414 _ntp 2 0 192K 584K sleep poll 0:02 0.00% ntpd
22713 root 2 0 164K 576K sleep poll 0:00 0.00% httpd
25115 root 2 0 292K 672K idle select 0:00 0.00% sshd
8234 root 2 0 364K 1592K idle select 0:00 0.00% sshd
Log
Jul 17 10:44:11 probe3 init: kernel security level changed from 0 to 1
Interfaces
lo0: flags=8049 mtu 33224
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x7
sis0: flags=8843 mtu 1500
address: 00:0d:b9:00:7a:98
media: Ethernet autoselect (100baseTX full-duplex)
status: active
inet6 fe80::20d:b9ff:fe00:7a98%sis0 prefixlen 64 scopeid 0x1
Internet


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Status
Debugging log
Tempgraph
Ping
Traceroute
Dig
Iperf
Oct 11 14:43:14 CEST 2005
D probe3 3.7 TILDECOS021#0 i386
M up 86 days, 4 hrs, 1 user, load averages: 0.57, 0.67, 0.66
sors.0=lmtemp0, TEMP, temp, 45.50 degC / 113.90 degF
stem 512-blocks Used Avail Capacity Mounted on
d0a 21438 17714 3724 83% /
d0a 120510 67206 47280 59% /flash
mfs:20596 26108 18492 6312 75% /bin2
Processlist
load averages: 0.57, 0.67, 0.66 14:43:15
43 processes: 1 running, 41 idle, 1 on processor
Memory: Real: 22M/30M act/tot Free: 18M Swap: 0K/0K used/tot
PID USERNAME PRI NICE SIZE RES STATE WAIT TIME CPU COMMAND
17206 root -6 0 2080K 3228K sleep piperd 0:00 1.56% html
10378 root 2 0 340K 1096K sleep netio 0:00 0.68% httpd
4 root -18 0 0K 19M sleep reaper 346:12 0.00% reaper
6254 root 18 0 264K 596K sleep pause 29:36 0.00% sh
30417 _dhcp 2 0 252K 312K sleep poll 9:46 0.00% dhcpd
29362 root 10 0 64K 236K sleep nanosl 9:21 0.00% gpioflash
22030 root 2 0 280K 536K sleep select 8:38 0.00% cron
6 root 18 0 0K 19M sleep syncer 7:40 0.00% update
30764 _syslogd 2 0 448K 516K sleep poll 2:06 0.00% syslogd
18258 named 2 0 1836K 2120K sleep select 1:12 0.00% named
20596 root 10 0 364K 9576K sleep mfsidl 1:11 0.00% mount_mfs
5624 _dhcp 2 0 304K 484K idle poll 0:48 0.00% dhclient
28835 root 2 0 256K 420K idle poll 0:25 0.00% dhclient
0 root -18 0 0K 19M sleep schedu 0:11 0.00% swapper
24414 _ntp 2 0 192K 584K idle poll 0:02 0.00% ntpd
22713 root 2 0 164K 576K sleep poll 0:00 0.00% httpd
25115 root 2 0 292K 672K idle select 0:00 0.00% sshd
8234 root 2 0 364K 1592K idle select 0:00 0.00% sshd
Log
Jul 17 10:44:11 probe3 init: kernel security level changed from 0 to 1
Interfaces
lo0: flags=8049 mtu 33224
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x7
sis0: flags=8843 mtu 1500
address: 00:0d:b9:00:7a:98
media: Ethernet autoselect (100baseTX full-duplex)
status: active
inet6 fe80::20d:b9ff:fe00:7a98%sis0 prefixlen 64 scopeid 0x1
javascript:void(0)
Internet


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Hostname
WAN configuration
Firmware upgrade
Restart device
Systemini 9 CEST 2005
System 7 TILDECOS021#0 i386
Uptime ys, 4:06, 1 user, load averages: 1.00, 0.84, 0.73
Environment hw.sensors.0=lmtemp0, TEMP, temp, 46.00 degC / 114.80 degF
Filesystem
Filesystem 512-blocks Used Avail Capacity Mounted on
/dev/rd0a 21438 17714 3724 83% /
/dev/wd0a 120510 67206 47280 59% /flash
mfs:20596 26108 18492 6312 75% /bin2
Processlist
load averages: 1.00, 0.84, 0.73 14:48:40
36 processes: 35 idle, 1 on processor
Memory: Real: 20M/29M act/tot Free: 20M Swap: 0K/0K used/tot
PID USERNAME PRI NICE SIZE RES STATE WAIT TIME CPU COMMAND
27267 root -6 0 2116K 3236K sleep piperd 0:00 1.42% html
28267 root 2 0 340K 1096K sleep netio 0:00 0.68% httpd
4 root -18 0 0K 19M sleep reaper 346:14 0.00% reaper
6254 root 18 0 264K 596K sleep pause 29:36 0.00% sh
30417 _dhcp 2 0 252K 312K idle poll 9:46 0.00% dhcpd
29362 root 10 0 64K 236K sleep nanosl 9:21 0.00% gpioflash
22030 root 2 0 280K 536K sleep select 8:38 0.00% cron
6 root 18 0 0K 19M sleep syncer 7:40 0.00% update
30764 _syslogd 2 0 448K 516K sleep poll 2:06 0.00% syslogd
18258 named 2 0 1836K 2120K idle select 1:12 0.00% named
20596 root 10 0 364K 9576K sleep mfsidl 1:11 0.00% mount_mfs
5624 _dhcp 2 0 304K 484K idle poll 0:48 0.00% dhclient
28835 root 2 0 256K 420K idle poll 0:25 0.00% dhclient
0 root -18 0 0K 19M sleep schedu 0:11 0.00% swapper
24414 _ntp 2 0 192K 584K idle poll 0:02 0.00% ntpd
22713 root 2 0 164K 576K sleep poll 0:00 0.00% httpd
25115 root 2 0 292K 672K idle select 0:00 0.00% sshd
8234 root 2 0 364K 1592K idle select 0:00 0.00% sshd
Log
Jul 17 10:44:11 probe3 init: kernel security level changed from 0 to 1
Interfaces
lo0: flags=8049 mtu 33224
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x7
sis0: flags=8843 mtu 1500
address: 00:0d:b9:00:7a:98
media: Ethernet autoselect (100baseTX full-duplex)
status: active
inet6 fe80::20d:b9ff:fe00:7a98%sis0 prefixlen 64 scopeid 0x1
Internet

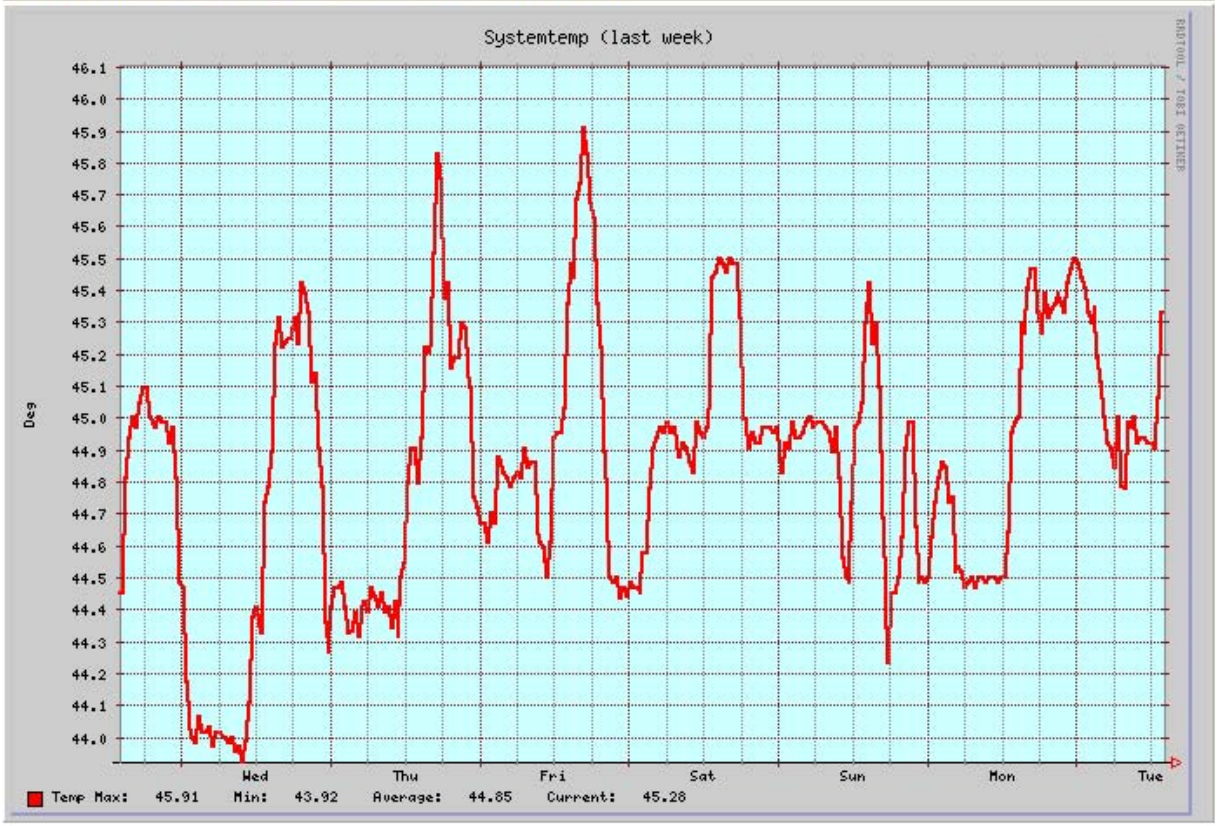

Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Debugging log: probe3 Tue Oct 11 14:46:12 CEST 2005
Oct 11 14:46:11 probe3 httpd[13773]: got request ``GET /longlog.html HTTP/1.1'' from host dhcp-9-111.ripemtg.r
Oct 11 14:46:01 probe3 cron[9768]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:46:01 probe3 cron[28881]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:45:01 probe3 cron[5327]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:45:01 probe3 cron[9258]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:44:29 probe3 httpd[5157]: got request ``GET /page.css HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.n
Oct 11 14:44:23 probe3 httpd[23035]: got request ``GET /longlog.html HTTP/1.1'' from host dhcp-9-111.ripemtg.r
Oct 11 14:44:01 probe3 cron[10048]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:44:01 probe3 cron[23931]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:43:27 probe3 httpd[6503]: got request ``GET /XulMenu.js HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe
Oct 11 14:43:25 probe3 httpd[3296]: got request ``GET /ie5.js HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.net
Oct 11 14:43:20 probe3 httpd[3165]: got request ``GET /page.css HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.n
Oct 11 14:43:16 probe3 crontab[30240]: (root) LIST (root)
Oct 11 14:43:13 probe3 httpd[10378]: got request ``GET / HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.net to p
Oct 11 14:43:01 probe3 cron[27854]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:43:01 probe3 cron[14925]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:42:01 probe3 cron[537]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:42:01 probe3 cron[17816]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:41:55 probe3 httpd[4168]: got request ``GET /XulMenu.js HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe
Oct 11 14:41:53 probe3 httpd[32733]: got request ``GET /ie5.js HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.ne
Oct 11 14:41:50 probe3 httpd[2249]: got request ``GET /page.css HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.n
Oct 11 14:41:43 probe3 crontab[2241]: (root) LIST (root)
Oct 11 14:41:42 probe3 httpd[32439]: got request ``GET / HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.net to p
Oct 11 14:41:01 probe3 cron[6817]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:41:01 probe3 cron[21979]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:40:51 probe3 httpd[11591]: got request ``GET /XulMenu.js HTTP/1.1'' from host dhcp-9-111.ripemtg.rip
Oct 11 14:40:50 probe3 httpd[9039]: got request ``GET /ie5.js HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.net
Oct 11 14:40:48 probe3 httpd[15393]: got request ``GET /page.css HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.
Oct 11 14:40:46 probe3 crontab[1810]: (root) LIST (root)
Oct 11 14:40:44 probe3 httpd[7559]: got request ``GET / HTTP/1.1'' from host dhcp-9-111.ripemtg.ripe.net to po
Oct 11 14:40:42 probe3 httpd[18487]: SSL_ERROR OTHER
Oct 11 14:40:31 probe3 httpd[6810]: got request ``GET /favicon.ico HTTP/1.1'' from host dhcp-9-111.ripemtg.rip
Oct 11 14:40:24 probe3 httpd[22098]: SSL_ERROR OTHER
Oct 11 14:40:01 probe3 cron[18231]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:40:01 probe3 cron[5086]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:39:01 probe3 cron[11343]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:39:01 probe3 cron[2229]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:38:01 probe3 cron[22669]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:38:01 probe3 cron[23272]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:37:01 probe3 cron[23689]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:37:01 probe3 cron[12473]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Oct 11 14:36:01 probe3 cron[3422]: (root) CMD (/root/demeterechoperflight.sh >/dev/null 2>&1)
Oct 11 14:36:01 probe3 cron[1641]: (root) CMD (/root/rrdcollectandgraph.sh >/dev/null 2>/dev/null)
Done
Internet

Management probe3 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

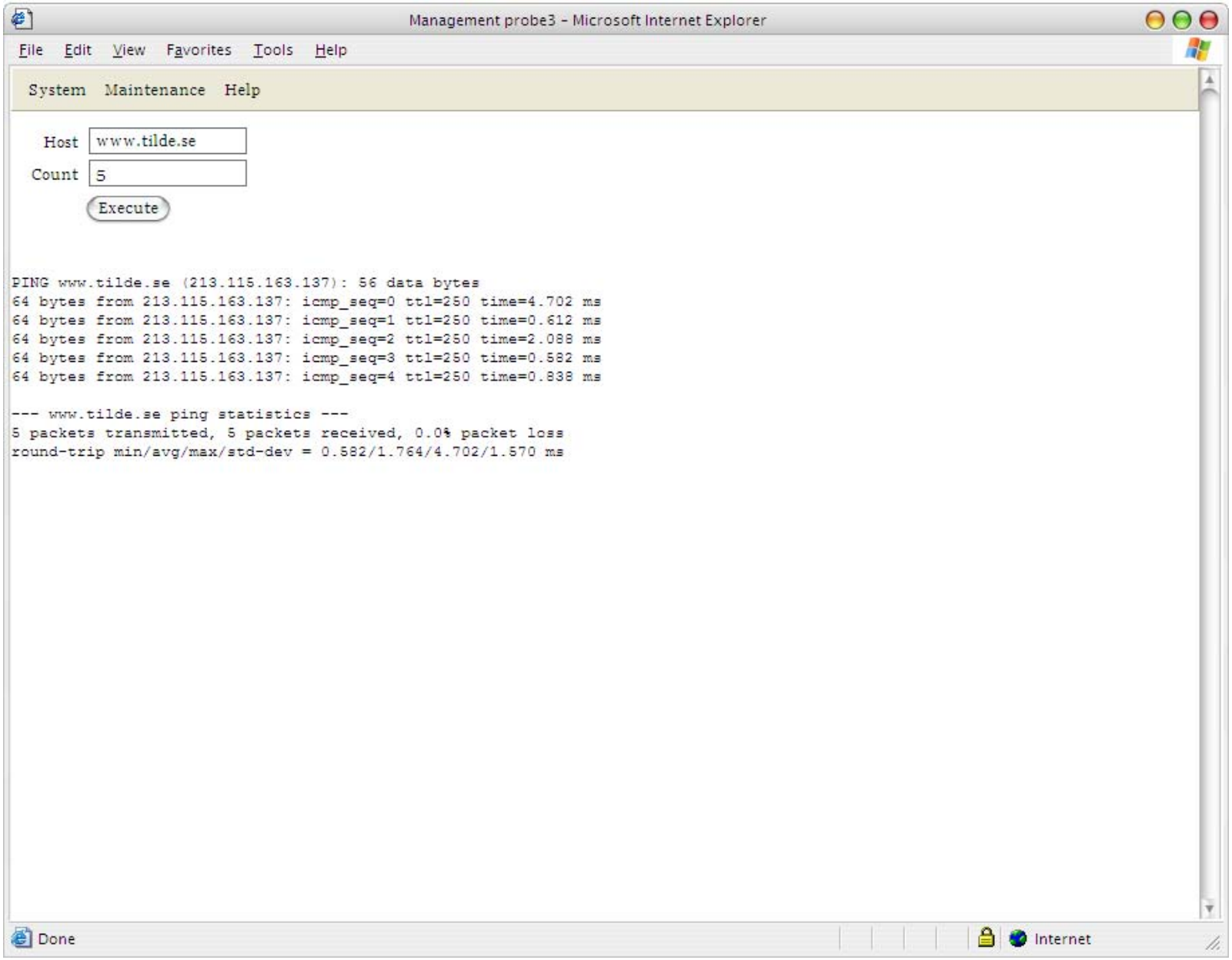
System Maintenance Help

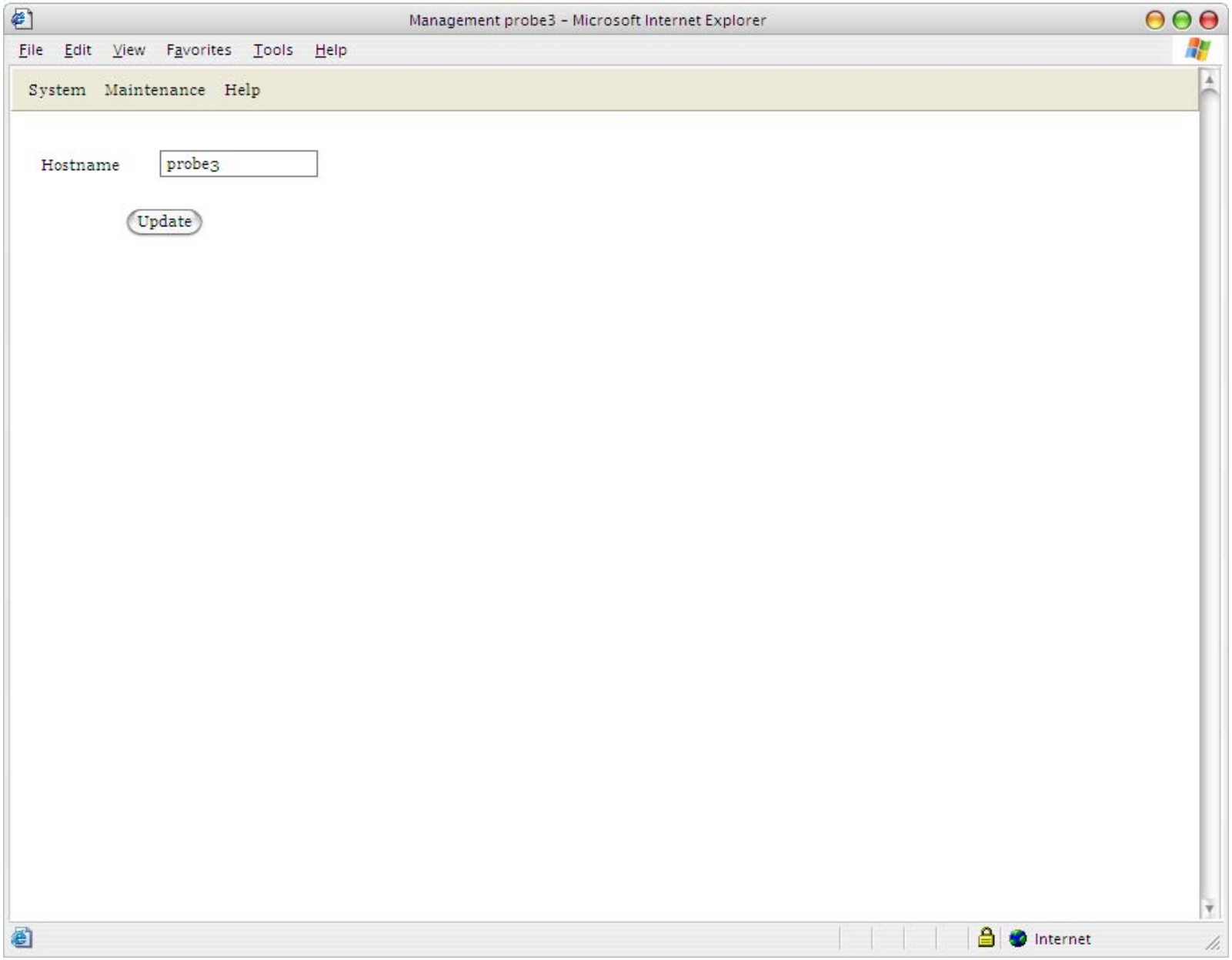
System Temperatur: probe3 Tue Oct 11 14:46:44 CEST 2005

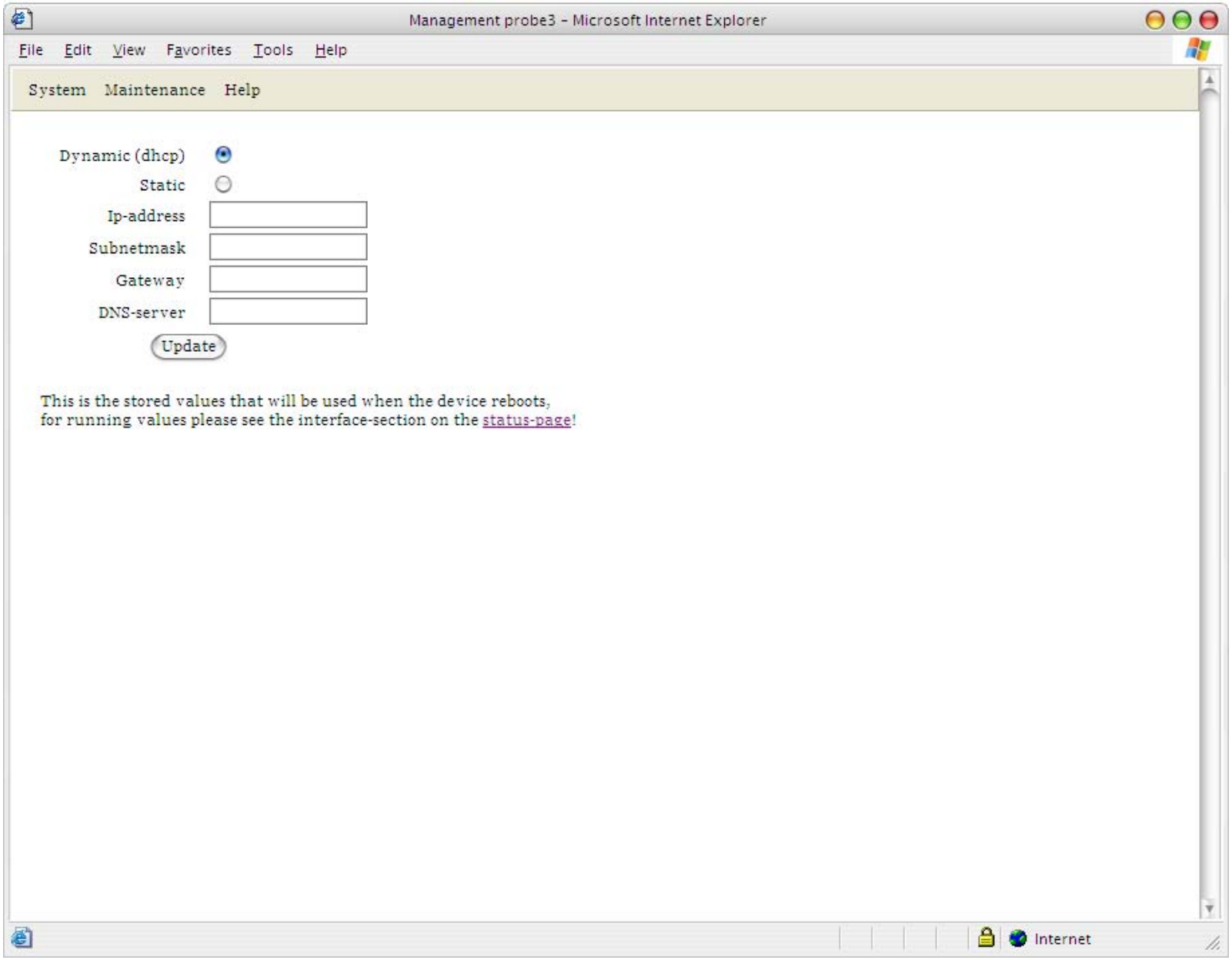


Done

Internet


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Host www.tilde.se
Count 5
Execute
PING www.tilde.se (213.115.163.137): 56 data bytes
64 bytes from 213.115.163.137: icmp_seq=0 ttl=250 time=4.702 ms
64 bytes from 213.115.163.137: icmp_seq=1 ttl=250 time=0.612 ms
64 bytes from 213.115.163.137: icmp_seq=2 ttl=250 time=2.088 ms
64 bytes from 213.115.163.137: icmp_seq=3 ttl=250 time=0.582 ms
64 bytes from 213.115.163.137: icmp_seq=4 ttl=250 time=0.838 ms
--- www.tilde.se ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.582/1.764/4.702/1.570 ms
Done
Internet


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Hostname
probe3
Update
Internet


Management probe3 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
System Maintenance Help
Dynamic (dhcp)
Static
Ip-address
Subnetmask
Gateway
DNS-server
Update
This is the stored values that will be used when the device reboots,
for running values please see the interface-section on the status-page!
Internet

Conclusion

Is it any good?

- Well, not really. It doesn't really answer any questions clearly!
- And you can't really draw any conclusions what caused a problem and where the problem was located.
- 9 measurement points really doesn't represent the Swedish Internet very well.
- People in Sweden need resources from other parts of the world as well.
- However, it will never give you a false positive! If a connection is up, it's working!

Problems

- Multi-operator infrastructure. (Where network owners and service providers are separated)
- Not enough measurement points.
- Measurement are made from consumer connections.
- Measurements are only made from Swedish parts of the Internet.

Who needs this?

- Consumers
  - Is a problem with my operator or my connection?
  - How is traffic working between my office and my home-connection?
  - Which operators/connection is the best?
- PTS
  - How is the Swedish part of Internet working?
- Operators (they just don’t know it yet)
  - Check how well their peering and transit is actually working

Questions