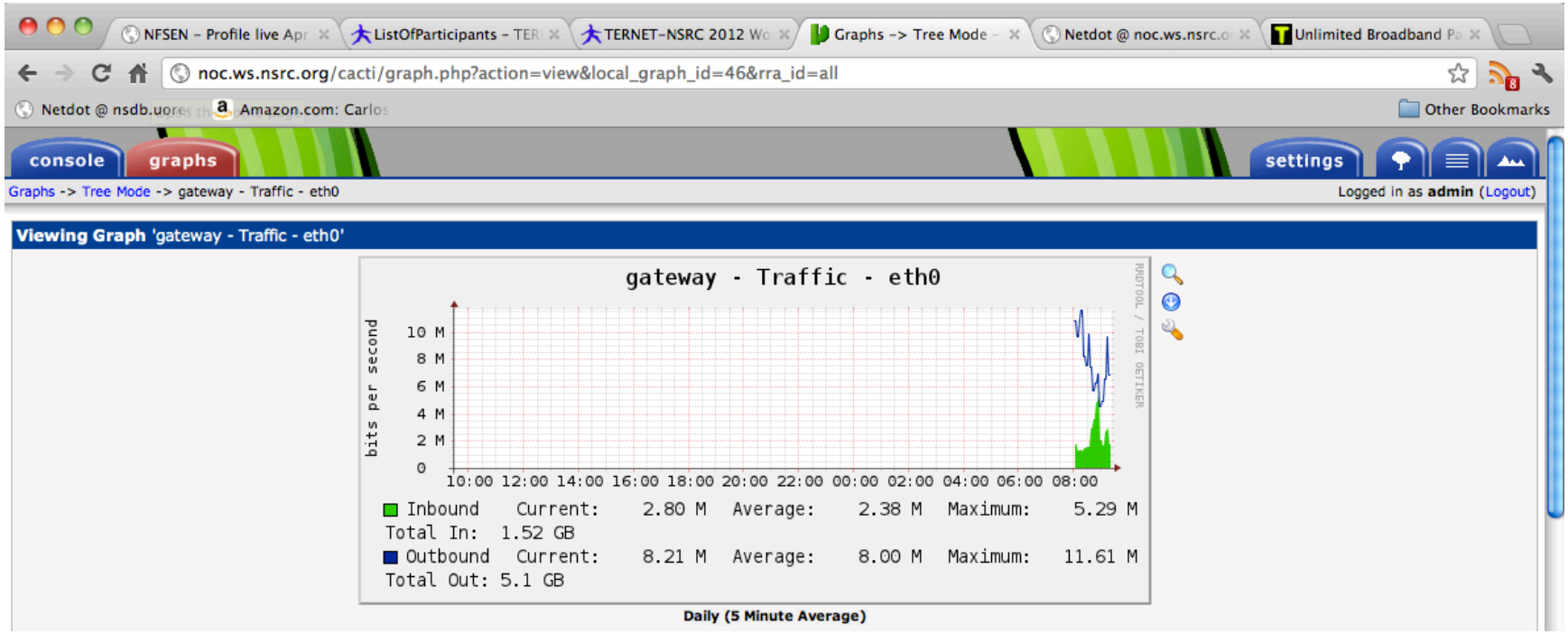
Security Analysis Process

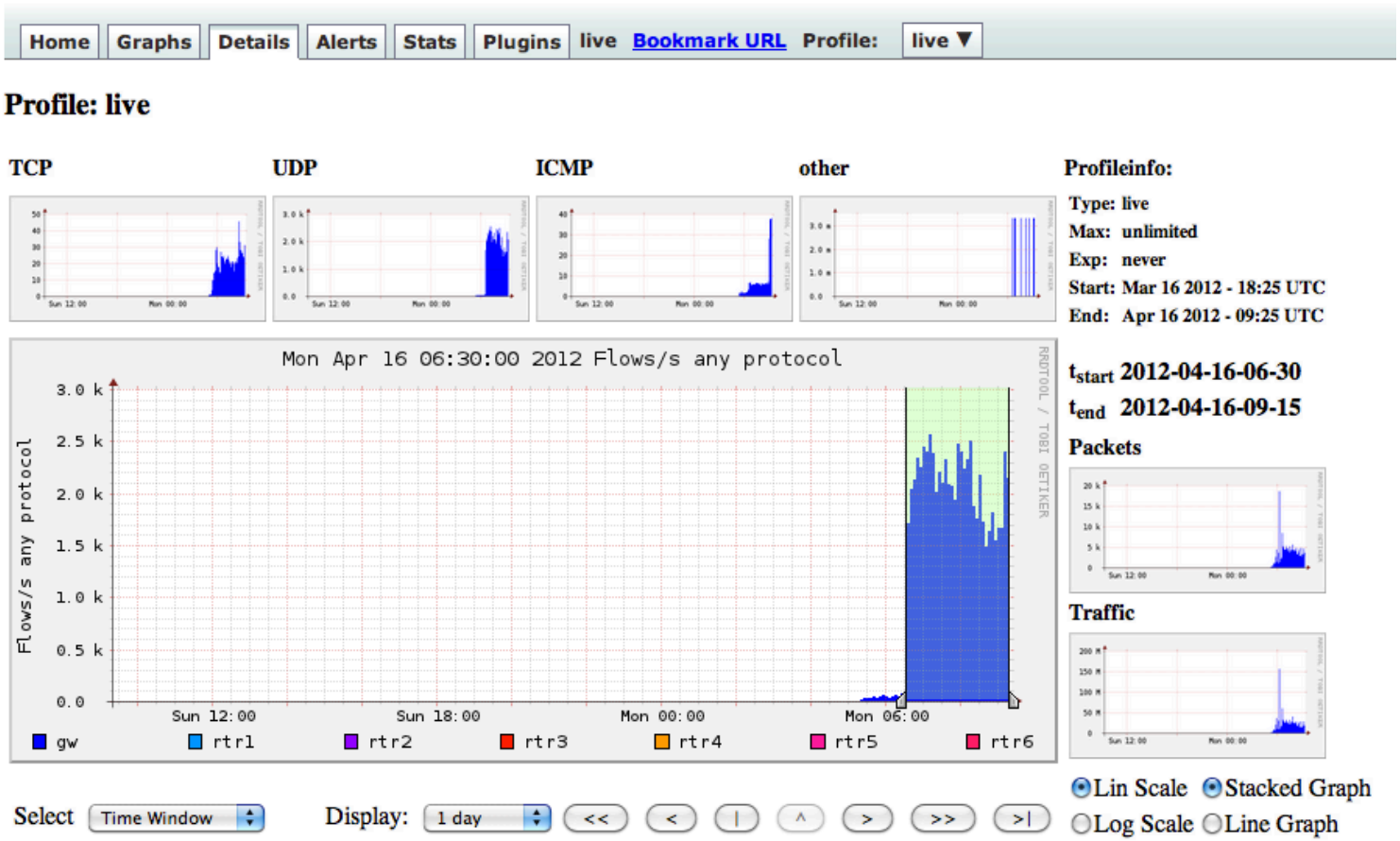
TERNET-NSRC 2012

Dar Es Salaam, TZ

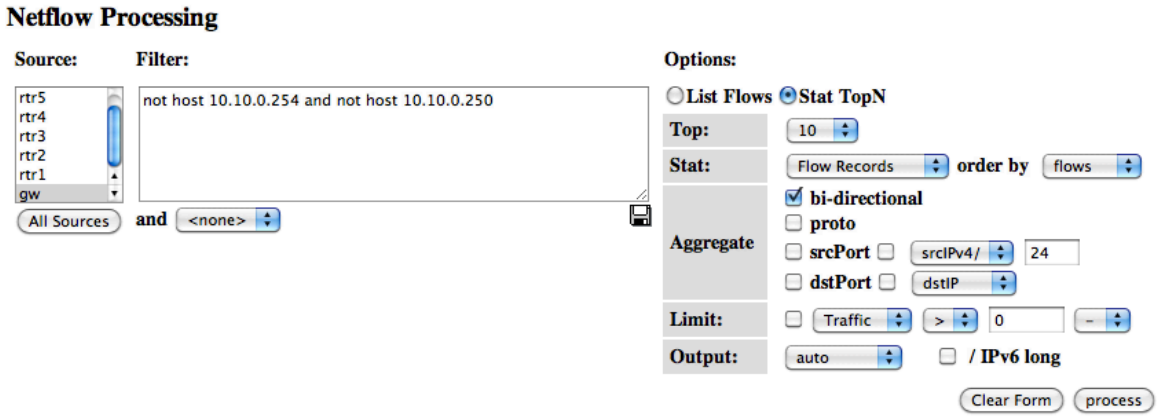
Traffic


NFSEN - Profile live Apr
ListOfParticipants - TER
TERNET-NSRC 2012 Wo
Graphs -> Tree Mode -
Netdot @ noc.ws.nsrc.o
Unlimited Broadband Pa
noc.ws.nsrc.org/cacti/graph.php?action=view&local_graph_id=46&rra_id=all
Netdot @ nsdb.uore
Amazon.com: Carlos
Other Bookmarks
console
graphs
settings
Graphs -> Tree Mode -> gateway - Traffic - eth0
Logged in as admin (Logout)
Viewing Graph 'gateway - Traffic - eth0'
gateway - Traffic - eth0
bits per second
10 M
8 M
6 M
4 M
2 M
0
10:00 12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00
Inbound Current: 2.80 M Average: 2.38 M Maximum: 5.29 M
Total In: 1.52 GB
Outbound Current: 8.21 M Average: 8.00 M Maximum: 11.61 M
Total Out: 5.1 GB
Daily (5 Minute Average)

Flow Statistics

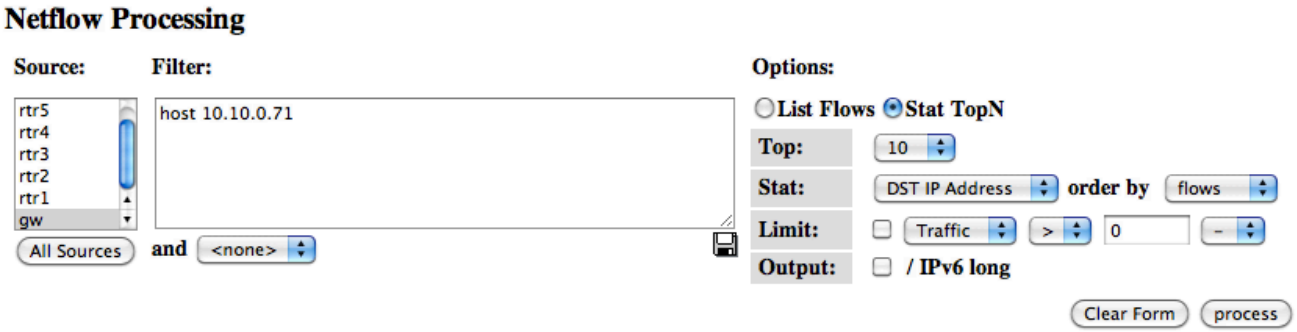


Flow Statistics – Top 10 by flows




```
** nfdump -M /var/nfsen/profiles-data/live/gw  -T  -R 2012/04/16/nfcapd.201204160630:2012/04/16/nfcapd.201204160915 -n 10 -s record/flows -B
nfdump filter:
not host 10.10.0.254 and not host 10.10.0.250
Command line switch -s overwrites -a
Aggregated flows 164911
Top 10 flows ordered by flows:
Date flow start          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Out Pkt   In Pkt Out Byte  In Byte Flows
2012-04-16 06:18:39.439 10858.930 UDP      2.103.215.118:13689 <->       10.10.0.71:18198    2.4 M   803913    3.5 G   42.3 M 1130514
2012-04-16 06:18:39.439 10858.930 UDP      2.103.215.118:13689 <->     41.93.45.100:1026     2.4 M   803913    3.5 G   42.3 M 1114129
2012-04-16 06:26:12.597 10426.874 UDP         10.10.0.71:18198 <->   99.187.121.189:43320   389319   818046   20.1 M    1.2 G 439935
2012-04-16 06:26:12.597 10426.874 UDP       41.93.45.100:1026  <->   99.187.121.189:43320   389319   818046   20.1 M    1.2 G 434416
2012-04-16 06:18:09.463  7406.277 UDP         10.10.0.71:18198 <->    89.164.210.89:56696   185733   408670    9.6 M  598.6 M 278629
2012-04-16 06:30:08.151 10191.625 UDP         10.10.0.71:18198 <->    24.11.138.190:41768   182866   385712    9.5 M  564.4 M 244056
2012-04-16 07:15:15.715  7484.128 UDP         10.10.0.71:18198 <->   196.206.160.119:56179  107461   239663    5.6 M  350.8 M 210626
2012-04-16 06:30:08.151  8714.881 UDP      24.11.138.190:41768 <->     41.93.45.100:1026    343131   163353  502.1 M    8.5 M 210479
2012-04-16 07:15:15.715  7484.128 UDP       41.93.45.100:1027  <->   196.206.160.119:56179  107461   239663    5.6 M  350.8 M 208417
2012-04-16 06:28:41.511  9895.920 UDP         10.10.0.71:18198 <->   207.47.177.245:20116   119966   246404    6.2 M  360.8 M 207522

Summary: total flows: 10524164, total bytes: 28.1 G, total packets: 29.1 M, avg bps: 14.5 M, avg pps: 1872, avg bpp: 965
Time window: 2012-04-16 05:01:10 - 2012-04-16 09:20:00
Total flows processed: 20632976, Blocks skipped: 0, Bytes read: 1072927764
Sys: 13.968s flows/second: 1477068.0  Wall: 14.327s flows/second: 1440067.8
```

Who is it talking to?




```
** nfdump -M /var/nfsen/profiles-data/live/gw  -T  -R 2012/04/16/nfcapd.201204160630:2012/04/16/nfcapd.201204160915 -n 10 -s dstip/flows
nfdump filter:
host 10.10.0.71
Top 10 Dst IP Addr ordered by flows:
Date first seen          Duration Proto       Dst IP Addr    Flows(%)     Packets(%)       Bytes(%)         pps      bps   bpp
2012-04-16 06:17:53.503 10926.500 any          10.10.0.71    2.0 M(39.9)    3.7 M(30.7)  206.8 M( 1.7)       340   151393    55
2012-04-16 05:35:06.244 13472.125 any       2.103.215.118   731400(14.2)    2.4 M(19.6)    3.5 G(29.0)       176    2.1 M  1465
2012-04-16 05:36:48.445 13391.026 any       99.187.121.189   288142( 5.6)   818094( 6.7)    1.2 G(10.0)        61   716027  1465
2012-04-16 06:13:37.457  7690.740 any        89.164.210.89   154877( 3.0)   408793( 3.4)  598.6 M( 5.0)        53   622721  1464
2012-04-16 06:13:34.469 11185.307 any        24.11.138.190   153858( 3.0)   387696( 3.2)  566.7 M( 4.7)        34   405315  1461
2012-04-16 06:23:19.497  5521.428 any       82.196.172.205   122027( 2.4)   296709( 2.4)  434.5 M( 3.6)        53   629602  1464
2012-04-16 07:15:15.715  7484.128 any      196.206.160.119   116056( 2.3)   244225( 2.0)  357.0 M( 3.0)        32   381556  1461
2012-04-16 05:52:35.339 12062.092 any       207.47.177.245   114577( 2.2)   246452( 2.0)  360.8 M( 3.0)        20   239297  1463
2012-04-16 06:13:38.506 11180.076 any         124.43.26.26    85361( 1.7)   170861( 1.4)  248.4 M( 2.1)        15   177765  1453
2012-04-16 06:47:24.596  4390.372 any        62.198.120.55    74230( 1.4)   162815( 1.3)  238.1 M( 2.0)        37   433870  1462

Summary: total flows: 5135393, total bytes: 12.0 G, total packets: 12.1 M, avg bps: 7.1 M, avg pps: 897, avg bpp: 990
Time window: 2012-04-16 05:34:50 - 2012-04-16 09:20:00
Total flows processed: 20632976, Blocks skipped: 0, Bytes read: 1072927764
Sys: 9.124s flows/second: 2261254.6  Wall: 11.931s flows/second: 1729259.6
```

Packet Capture

```
nsrc@noc:~$ sudo tcpdump -lnvvv -s 1500 host 10.10.0.71 -i eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 1500 bytes
10:12:34.773925 IP (tos 0x0, ttl 120, id 22451, offset 0, flags [DF], proto UDP (17), length 48)
    124.43.26.26.61219 > 10.10.0.71.18198: [udp sum ok] UDP, length 20
10:12:34.776858 IP (tos 0x0, ttl 128, id 21007, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 196.206.160.119.56179: [udp sum ok] UDP, length 1438
10:12:34.778948 IP (tos 0x0, ttl 128, id 21008, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 196.206.160.119.56179: [udp sum ok] UDP, length 1438
10:12:34.780878 IP (tos 0x0, ttl 128, id 21009, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 196.206.160.119.56179: [udp sum ok] UDP, length 1438
10:12:34.781285 IP (tos 0x0, ttl 128, id 21010, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 42.201.218.137.32555: [udp sum ok] UDP, length 1438
10:12:34.781821 IP (tos 0x0, ttl 111, id 10447, offset 0, flags [none], proto UDP (17), length 48)
    122.108.237.95.46237 > 10.10.0.71.18198: [udp sum ok] UDP, length 20
10:12:34.781850 IP (tos 0x0, ttl 111, id 10449, offset 0, flags [none], proto UDP (17), length 48)
    122.108.237.95.46237 > 10.10.0.71.18198: [udp sum ok] UDP, length 20
10:12:34.781869 IP (tos 0x0, ttl 111, id 10448, offset 0, flags [none], proto UDP (17), length 48)
    122.108.237.95.46237 > 10.10.0.71.18198: [udp sum ok] UDP, length 20
10:12:34.783115 IP (tos 0x0, ttl 128, id 21011, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 42.201.218.137.32555: [udp sum ok] UDP, length 1438
10:12:34.785825 IP (tos 0x0, ttl 111, id 10450, offset 0, flags [none], proto UDP (17), length 48)
    122.108.237.95.46237 > 10.10.0.71.18198: [udp sum ok] UDP, length 20
10:12:34.785867 IP (tos 0x0, ttl 128, id 21012, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 42.201.218.137.32555: [udp sum ok] UDP, length 1438
10:12:34.786239 IP (tos 0x0, ttl 128, id 21013, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 196.206.160.119.56179: [udp sum ok] UDP, length 1438
10:12:34.787715 IP (tos 0x0, ttl 128, id 21014, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 196.206.160.119.56179: [udp sum ok] UDP, length 1438
10:12:34.788080 IP (tos 0x0, ttl 128, id 21015, offset 0, flags [none], proto UDP (17), length 1466)
    10.10.0.71.18198 > 124.43.26.26.61219: [udp sum ok] UDP, length 1438
```

Identification - OS

nsrc@noc:~$ sudo nmap -sS -O 10.10.0.71

Starting Nmap 5.21 (http://nmap.org) at 2012-04-16 08:38 UTC
Nmap scan report for 10.10.0.71
Host is up (0.0021s latency).
Not shown: 991 closed ports
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1110/tcp open nfsd-status
2869/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
MAC Address: 00:1B:B1:E9:E1:21 (Wistron Neweb)
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate (build 7000)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 158.89 seconds

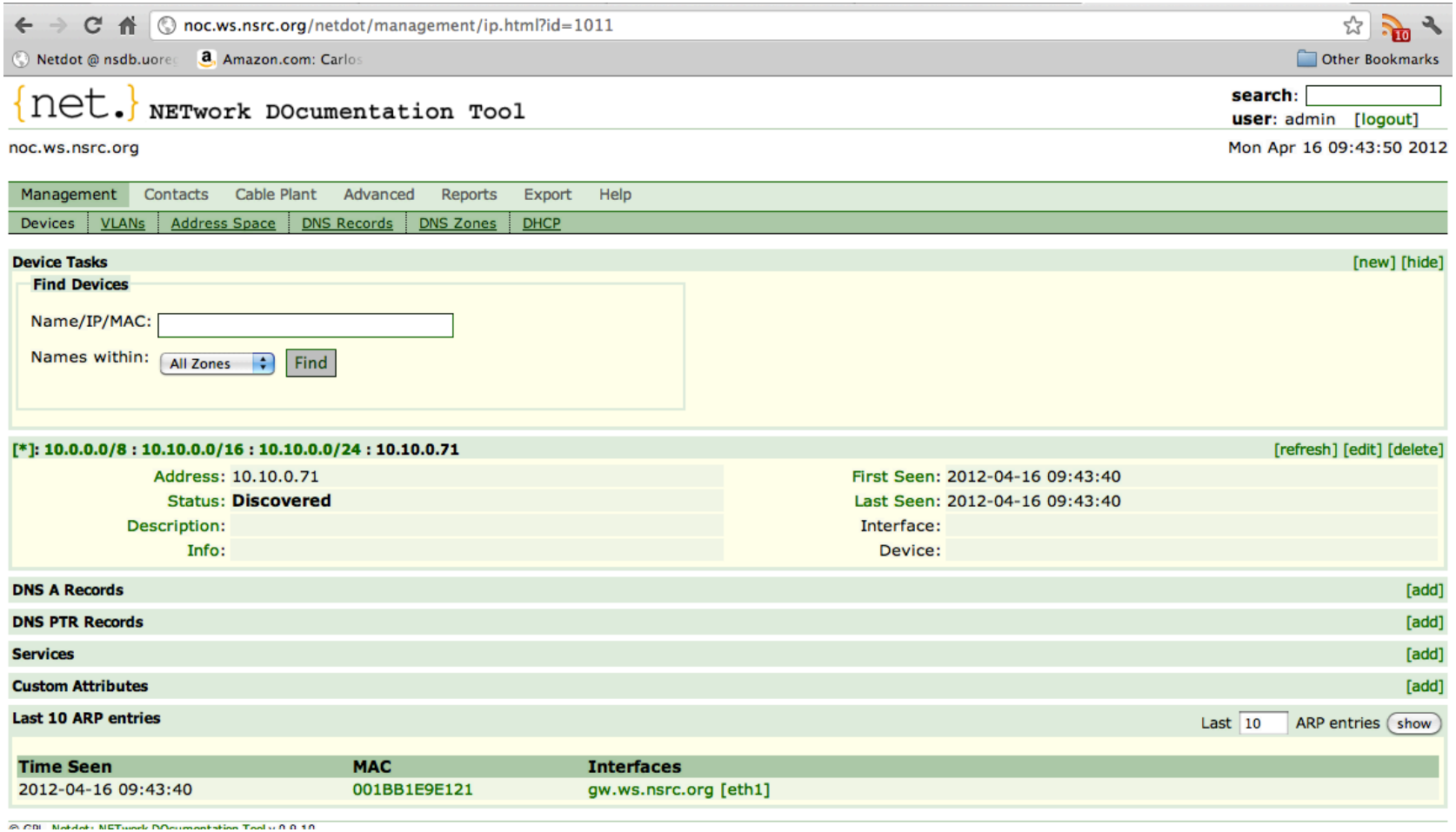
Identification – User?

```
nsrc@noc:~$ sudo nbtscan -hv 10.10.0.71
Doing NBT name scan for addresses from 10.10.0.71

NetBIOS Name Table for Host 10.10.0.71:

Incomplete packet, 173 bytes long.
Name            Service         Type
----------------------------------------
B2-IET-EMMANUEL  Workstation Service
WORKGROUP       Domain Name
B2-IET-EMMANUEL  File Server Service
WORKGROUP       Browser Service Elections

Adapter address: 00:1b:b1:e9:e1:21
----------------------------------------
```

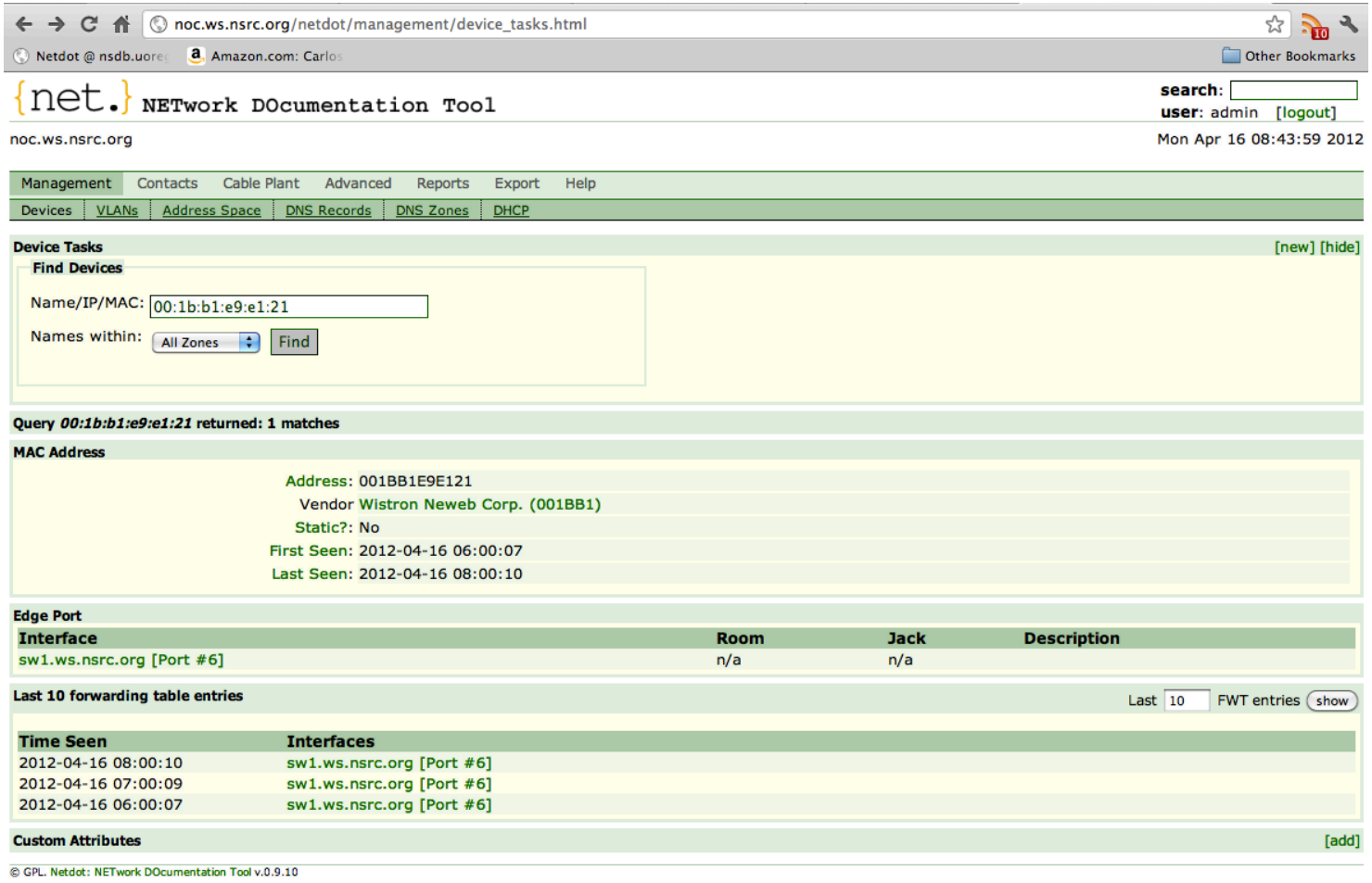
Identification - User

```
lease 10.10.0.71 {
  starts 1 2012/04/16 10:18:28;
  ends 1 2012/04/16 11:18:28;
  cltt 1 2012/04/16 10:18:28;
  binding state active;
  next binding state free;
  hardware ethernet 00:1b:b1:e9:e1:21;
  uid "\001\000\033\261\351\341!";
  client-hostname "B2-iet-EmmanuelJoseph";
}
```

Location


noc.ws.nsrc.org/netdot/management/ip.html?id=1011
Netdot @ nsdb.uore
Amazon.com: Carlos
Other Bookmarks
{net.} NETwork DOcumentation Tool
search:
user: admin [logout]
noc.ws.nsrc.org
Mon Apr 16 09:43:50 2012
Management
Contacts
Cable Plant
Advanced
Reports
Export
Help
Devices
VLANs
Address Space
DNS Records
DNS Zones
DHCP
Device Tasks
[new] [hide]
Find Devices
Name/IP/MAC:
Names within:
All Zones
Find
[*]: 10.0.0.0/8 : 10.10.0.0/16 : 10.10.0.0/24 : 10.10.0.71
[refresh] [edit] [delete]
Address: 10.10.0.71
Status: Discovered
Description:
Info:
First Seen: 2012-04-16 09:43:40
Last Seen: 2012-04-16 09:43:40
Interface:
Device:
DNS A Records
[add]
DNS PTR Records
[add]
Services
[add]
Custom Attributes
[add]
Last 10 ARP entries
Last 10 ARP entries show
Time Seen
MAC
Interfaces
2012-04-16 09:43:40
001BB1E9E121
gw.ws.nsrc.org [eth1]

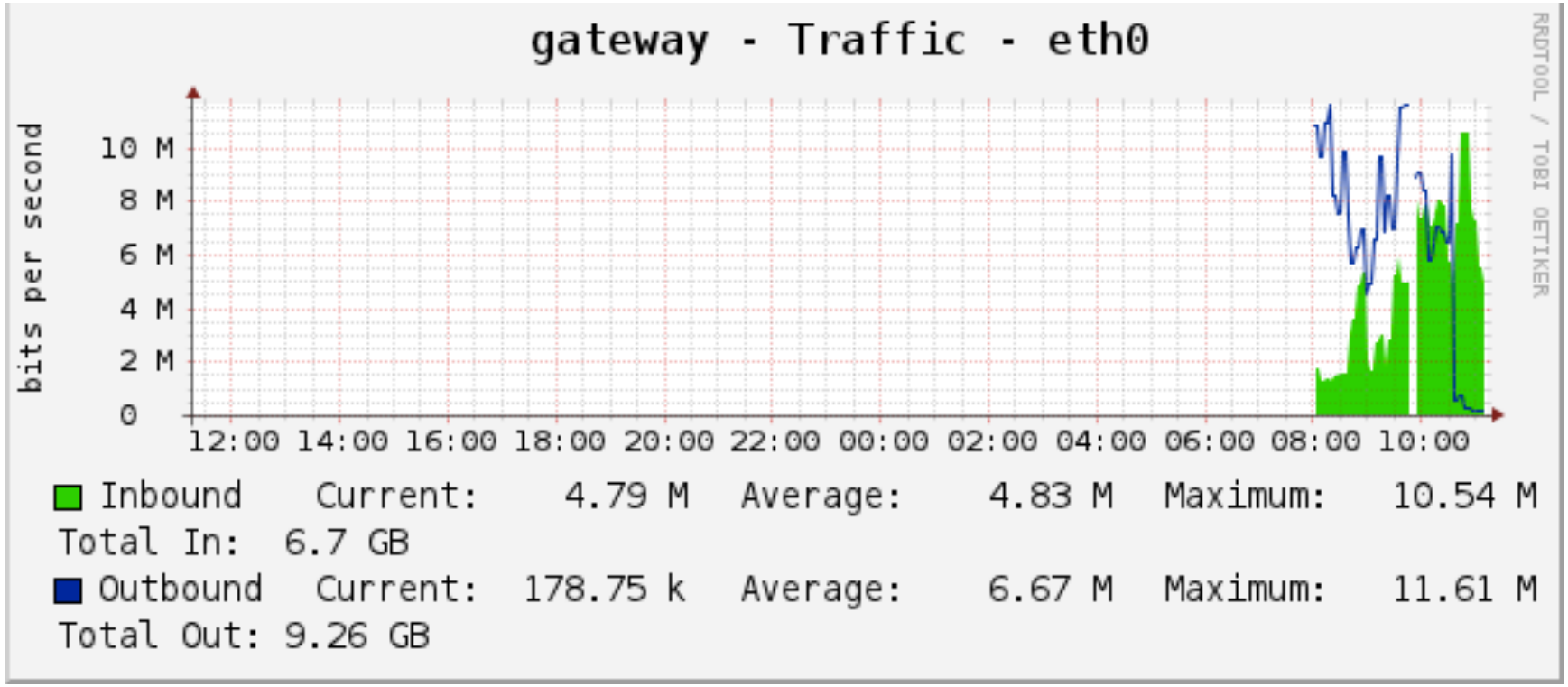
Location


noc.ws.nsrc.org/netdot/management/device_tasks.html
Netdot @ nsdb.uore
Amazon.com: Carlos
Other Bookmarks
{net.} NETwork DOcumentation Tool
search:
user: admin [logout]
noc.ws.nsrc.org
Mon Apr 16 08:43:59 2012
Management
Contacts
Cable Plant
Advanced
Reports
Export
Help
Devices
VLANs
Address Space
DNS Records
DNS Zones
DHCP
Device Tasks
[new] [hide]
Find Devices
Name/IP/MAC: 00:1b:b1:e9:e1:21
Names within: All Zones
Find
Query 00:1b:b1:e9:e1:21 returned: 1 matches
MAC Address
Address: 001BB1E9E121
Vendor Wistron Neweb Corp. (001BB1)
Static?: No
First Seen: 2012-04-16 06:00:07
Last Seen: 2012-04-16 08:00:10
Edge Port
Interface
Room
Jack
Description
sw1.ws.nsrc.org [Port #6]
n/a
n/a
Last 10 forwarding table entries
Last 10 FWT entries show
Time Seen
Interfaces
2012-04-16 08:00:10
sw1.ws.nsrc.org [Port #6]
2012-04-16 07:00:09
sw1.ws.nsrc.org [Port #6]
2012-04-16 06:00:07
sw1.ws.nsrc.org [Port #6]
Custom Attributes
[add]
© GPL. Netdot: NETwork DOcumentation Tool v.0.9.10

Resolution

- Talk to user. What are they running?
  - Peer-to-peer applicaction?
  - Malware infected?
  - Machine compromised?

After


gateway - Traffic - eth0
bits per second
10 M
8 M
6 M
4 M
2 M
0
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00
RRDTOOL / TOBI OETIKER
Inbound Current: 4.79 M Average: 4.83 M Maximum: 10.54 M
Total In: 6.7 GB
Outbound Current: 178.75 k Average: 6.67 M Maximum: 11.61 M
Total Out: 9.26 GB