

# Gestion y Monitorización

Importancia de la gestion y la monitorización

- Analizadores de tráfico

- Gestores SNMP

- Gestores QoS

- Otras herramientas

# Analizadores de tráfico

Analizadores de tráfico

#PTraf

NTOP

tcpdump □

# Analizadores. IPTraf I

## Iptraf. Estadísticas real-time

```
IPTraf
Statistics for eth1


```

	Total Packets	Total Bytes	Incoming Packets	Incoming Bytes	Outgoing Packets	Outgoing Bytes
Total:	21225	10179566	21225	10179566	0	0
IP:	21223	9836212	21223	9836212	0	0
TCP:	20663	9794868	20663	9794868	0	0
UDP:	136	17168	136	17168	0	0
ICMP:	341	20856	341	20856	0	0
Other IP:	83	3320	83	3320	0	0
Non-IP:	2	686	2	686	0	0

Total rates:	254.6 kbytes/sec	Broadcast packets:	0
	507.0 packets/sec	Broadcast bytes:	0
Incoming rates:	254.6 kbytes/sec		
	507.0 packets/sec		
Outgoing rates:	0.0 kbytes/sec	IP checksum errors:	0
	0.0 packets/sec		



# Analizadores. NTOP

Importancia del análisis de red

- Errores

- Malos usos

- Control de la red

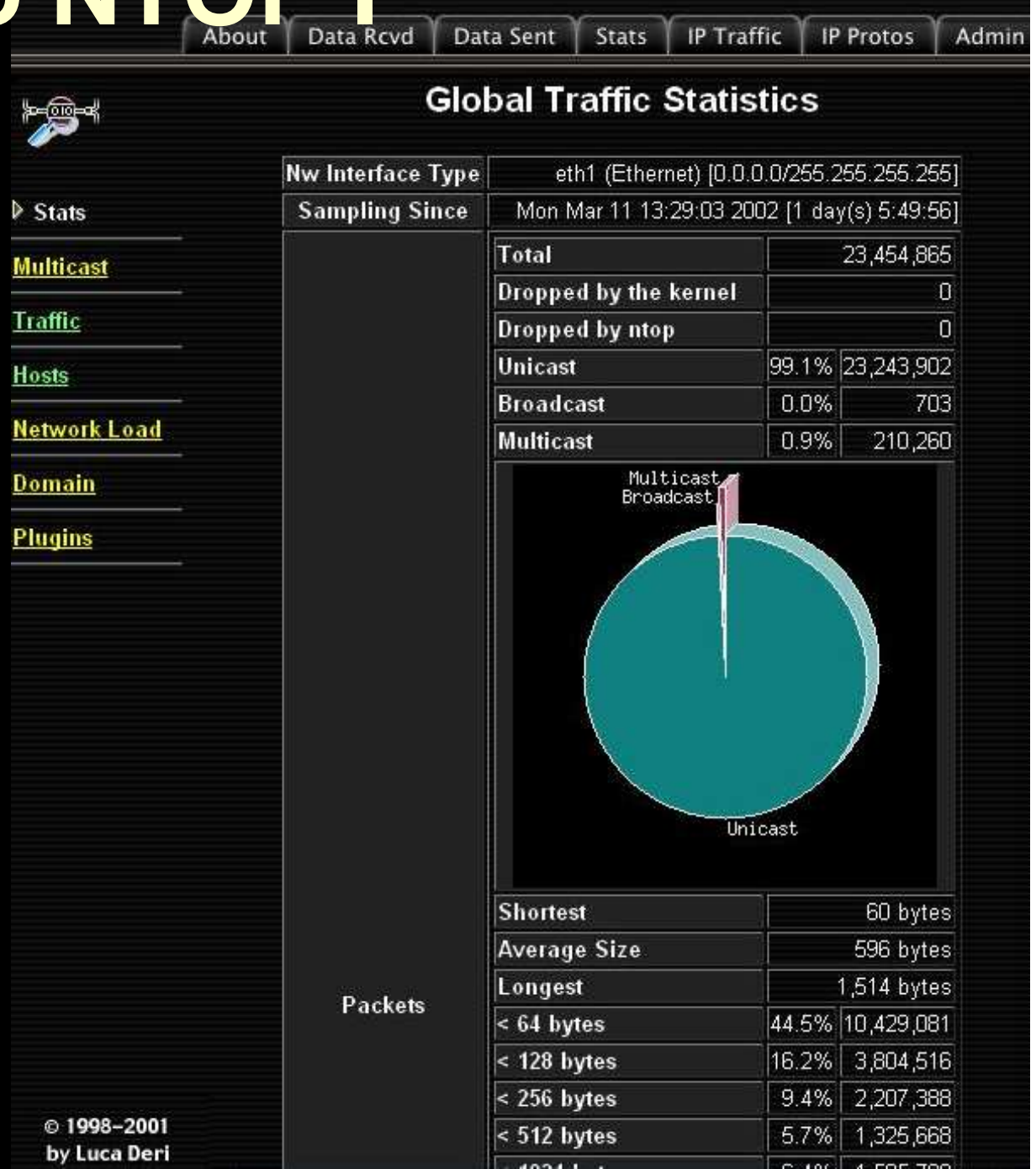
  - Hosts desconocidos

  - Trafico

  - Control de Carga

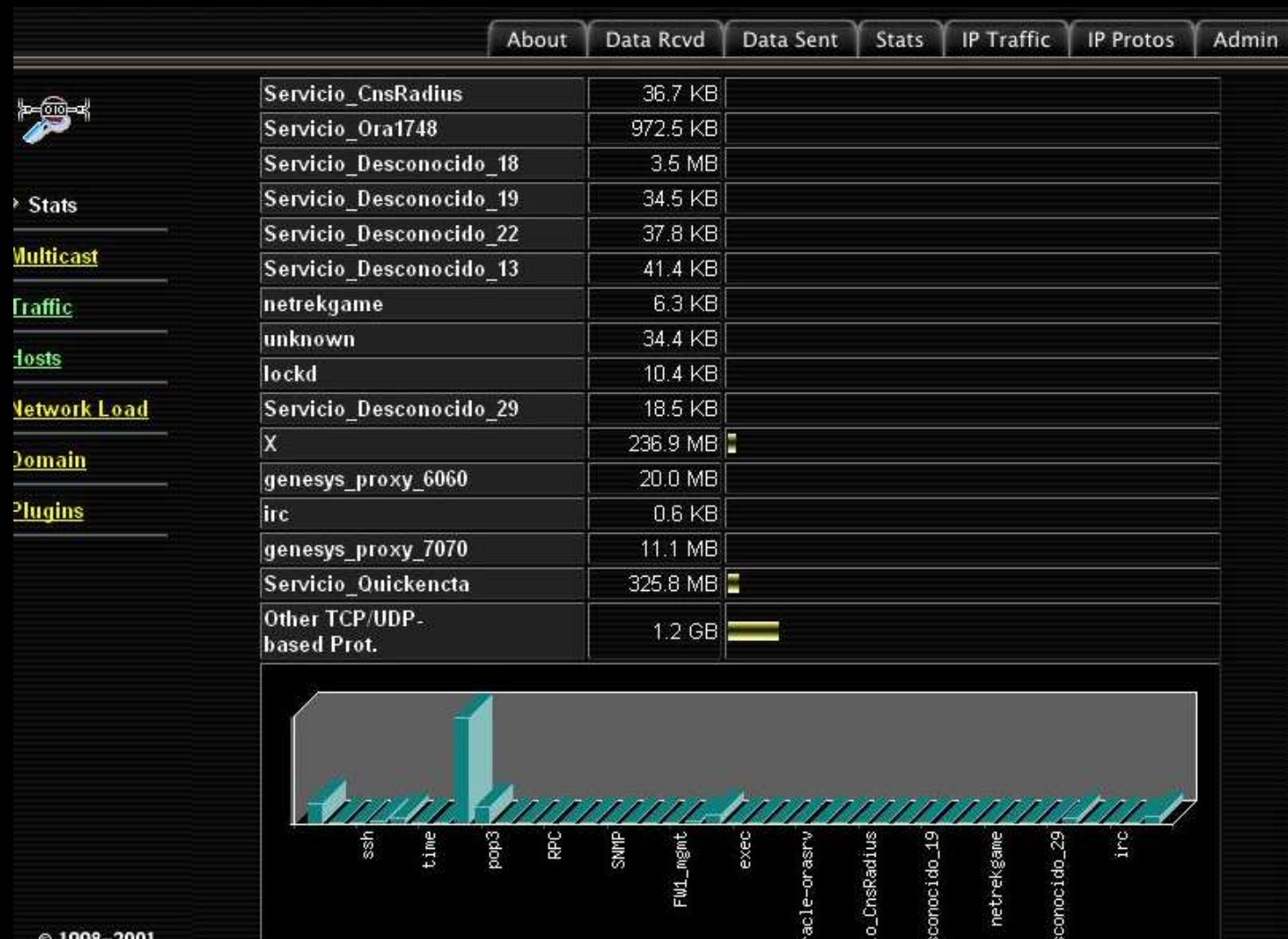
# Implementando NTOP I

Informacion global



# Implementando NTOP II


## Informacion de tráfico TCP/UDP



# Implementando NTOP III

Informacion de cada host

Navigation: About | Data Rcvd | Data Sent | Stats | IP Traffic | IP Protos | Admin

IP Address	216.52.146.227 [unicast]
First/Last Seen	03/12/02 19:04:40 - 03/12/02 19:04:40 [0 sec]
Last MAC Address/Router	00:00:5E:00:01:04
Host Location	Remote (outside specified/local subnet)
IP TTL (Time to Live)	125.234 hops
Total Data Sent	158/1 Pkts/0 Retran. Pkts [0%
Broadcast Pkts Sent	0 Pkts
Data Sent Stats	Remote (100 %)
Total Data Rcvd	77/1 Pkts/0 Retran. Pkts [0%
Data Received Stats	Remote (100 %)
Provided Services	Name Server
Host Physical Location	

Load

© 1998 Global Insight. 25 Km



# Implementando NTOP IV

## Informacion detallada de sesiones

[About](#) | [Data Rcvd](#) | [Data Sent](#) | [Stats](#) | [IP Traffic](#) | [IP Protos](#) | [Admin](#)

### Last Contacted Peers

Receiver Name	Receiver Address	Sender Name	Sender Address
<broadcast>			
10.0.0.1	10.0.0.1	10.0.0.1	10.0.0.1
10.0.0.2	10.0.0.2	10.0.0.2	10.0.0.2
10.0.0.3	10.0.0.3	10.0.0.3	10.0.0.3
10.0.0.4	10.0.0.4	10.0.0.4	10.0.0.4
10.0.0.5	10.0.0.5	10.0.0.5	10.0.0.5
10.0.0.6	10.0.0.6	10.0.0.6	10.0.0.6
10.0.0.7	10.0.0.7	10.0.0.7	10.0.0.7

### IP Service Stats: Client Role

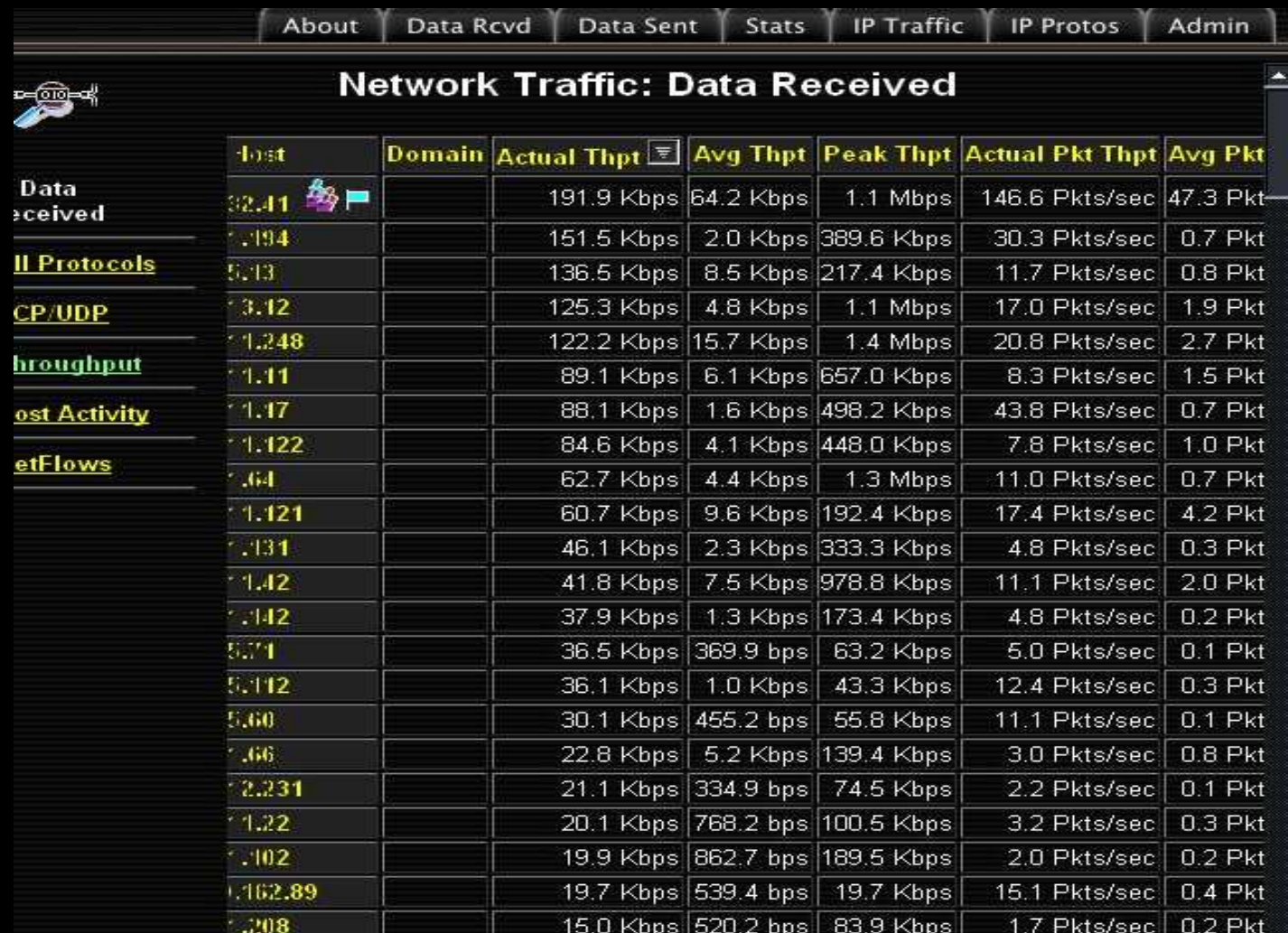
	# Loc. Req. Sent	# Rem. Req. Sent	# Pos. Reply Rcvd	# Neg. Reply Rcvd	Local RndTrip	Remote RndTrip
HTTP	0	153	0	0	0.0 ms - 0.0 ms	0.0 ms - 0.0 ms

### TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
ftp	21	468/313.3 KB	10.0.0.1		
smtp	25				
domain	53			220/37.0 KB	10.0.0.1
www	80			344/65.5 MB	10.0.0.1
pop3	110			695/3.4 MB	10.0.0.1
pop3	110			695/3.4 MB	10.0.0.1

# Implementando NTOP V

## Informacion general de hosts



The screenshot shows the Ntop V interface with a navigation bar at the top containing tabs for 'About', 'Data Rcvd', 'Data Sent', 'Stats', 'IP Traffic', 'IP Protos', and 'Admin'. The main content area is titled 'Network Traffic: Data Received' and features a table with the following columns: Host, Domain, Actual Thpt, Avg Thpt, Peak Thpt, Actual Pkt Thpt, and Avg Pkt. The table lists various hosts and their corresponding network statistics.

Host	Domain	Actual Thpt	Avg Thpt	Peak Thpt	Actual Pkt Thpt	Avg Pkt
192.168.1.1		191.9 Kbps	64.2 Kbps	1.1 Mbps	146.6 Pkts/sec	47.3 Pkt
192.168.1.194		151.5 Kbps	2.0 Kbps	389.6 Kbps	30.3 Pkts/sec	0.7 Pkt
192.168.1.13		136.5 Kbps	8.5 Kbps	217.4 Kbps	11.7 Pkts/sec	0.8 Pkt
192.168.1.3.12		125.3 Kbps	4.8 Kbps	1.1 Mbps	17.0 Pkts/sec	1.9 Pkt
192.168.1.248		122.2 Kbps	15.7 Kbps	1.4 Mbps	20.8 Pkts/sec	2.7 Pkt
192.168.1.11		89.1 Kbps	6.1 Kbps	657.0 Kbps	8.3 Pkts/sec	1.5 Pkt
192.168.1.17		88.1 Kbps	1.6 Kbps	498.2 Kbps	43.8 Pkts/sec	0.7 Pkt
192.168.1.122		84.6 Kbps	4.1 Kbps	448.0 Kbps	7.8 Pkts/sec	1.0 Pkt
192.168.1.64		62.7 Kbps	4.4 Kbps	1.3 Mbps	11.0 Pkts/sec	0.7 Pkt
192.168.1.121		60.7 Kbps	9.6 Kbps	192.4 Kbps	17.4 Pkts/sec	4.2 Pkt
192.168.1.131		46.1 Kbps	2.3 Kbps	333.3 Kbps	4.8 Pkts/sec	0.3 Pkt
192.168.1.12		41.8 Kbps	7.5 Kbps	978.8 Kbps	11.1 Pkts/sec	2.0 Pkt
192.168.1.12		37.9 Kbps	1.3 Kbps	173.4 Kbps	4.8 Pkts/sec	0.2 Pkt
192.168.1.71		36.5 Kbps	369.9 bps	63.2 Kbps	5.0 Pkts/sec	0.1 Pkt
192.168.1.12		36.1 Kbps	1.0 Kbps	43.3 Kbps	12.4 Pkts/sec	0.3 Pkt
192.168.1.60		30.1 Kbps	455.2 bps	55.8 Kbps	11.1 Pkts/sec	0.1 Pkt
192.168.1.66		22.8 Kbps	5.2 Kbps	139.4 Kbps	3.0 Pkts/sec	0.8 Pkt
192.168.1.231		21.1 Kbps	334.9 bps	74.5 Kbps	2.2 Pkts/sec	0.1 Pkt
192.168.1.22		20.1 Kbps	768.2 bps	100.5 Kbps	3.2 Pkts/sec	0.3 Pkt
192.168.1.102		19.9 Kbps	862.7 bps	189.5 Kbps	2.0 Pkts/sec	0.2 Pkt
192.168.1.162.89		19.7 Kbps	539.4 bps	19.7 Kbps	15.1 Pkts/sec	0.4 Pkt
192.168.1.208		15.0 Kbps	520.2 bps	83.9 Kbps	1.7 Pkts/sec	0.2 Pkt

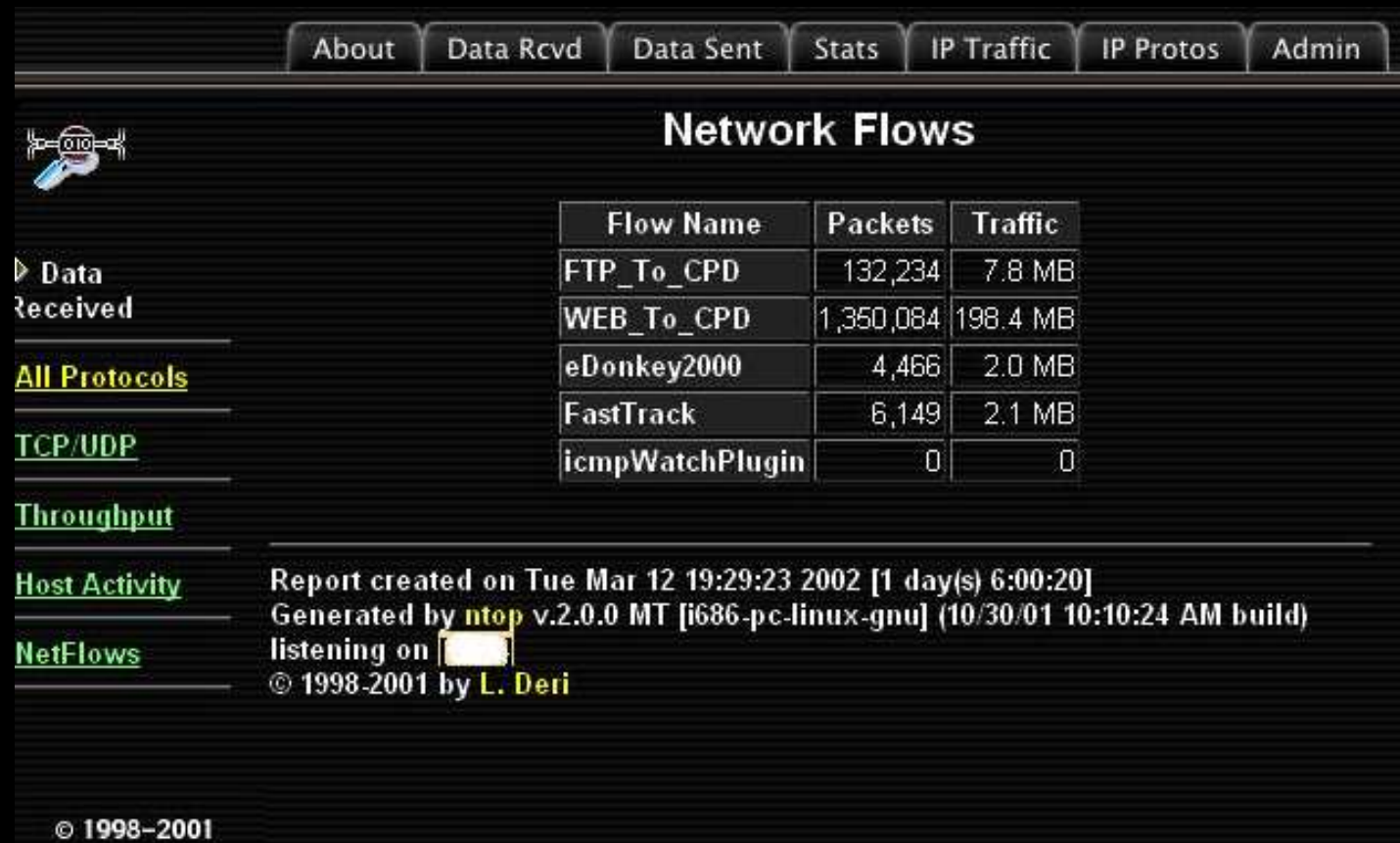
# Implementando NTOP VI

Monitorización continua de red, con históricos y logs.



# Implementando NTOP VII

## Definición de flujos de usuario



The screenshot displays the ntop Network Flows interface. At the top, there is a navigation bar with buttons for 'About', 'Data Rcvd', 'Data Sent', 'Stats', 'IP Traffic', 'IP Protos', and 'Admin'. Below this, the title 'Network Flows' is centered. A sidebar on the left contains a tree view with options: 'Data Received', 'All Protocols', 'TCP/UDP', 'Throughput', 'Host Activity', and 'NetFlows'. The main content area features a table with the following data:

Flow Name	Packets	Traffic
FTP_To_CPD	132,234	7.8 MB
WEB_To_CPD	1,360,084	198.4 MB
eDonkey2000	4,466	2.0 MB
FastTrack	6,149	2.1 MB
icmpWatchPlugin	0	0

Below the table, a report footer provides the following information:

Report created on Tue Mar 12 19:29:23 2002 [1 day(s) 6:00:20]  
Generated by ntop v.2.0.0 MT [i686-pc-linux-gnu] (10/30/01 10:10:24 AM build)  
listening on [redacted]  
© 1998-2001 by L. Deri

© 1998-2001

# Gestion y monitorización

- ▣ SNMP

- ▣ Herramientas

  - ▣ Netsaint

  - ▣ MRTG/RRD

# Gestion SNMP. MRTG I

## Carga de red

### FatalControl

### Firewalls

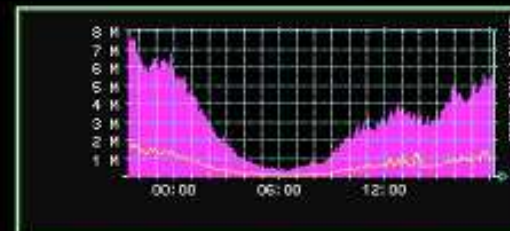
- FW-Ext1
- FW-Ext2
- FW-Ext3
- FW-Ext4
- FW-ExtGes1
- FW-ExtGes2
- FW-Int1
- FW-Int2
- FW-Int3
- FW-Int4
- FW-IntGes1
- FW-IntGes2

### Routers

#### Palma Albasanz

- Albasanz->Moraleja
- Albasanz->ParcBit
- Albasanz->Moraleja
- Moraleja->Albasanz
- Moraleja->ParcBit
- Moraleja->Castellana
- ParcBit->Moraleja
- ParcBit->Castellana
- ParcBit->Moraleja
- Castellana->Moraleja
- Castellana->ParcBit
- Castellana->Moraleja

Análisis de tráfico Router Albasanz/Tela (Serial)



Traffic Analysis for Retevision ALBASANZ -> Castellana

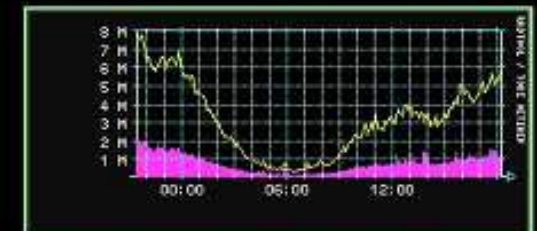


Traffic Analysis for Retevision ALBASANZ -> Palma



Traffic Analysis for Retevision Castellana -> Albasanz

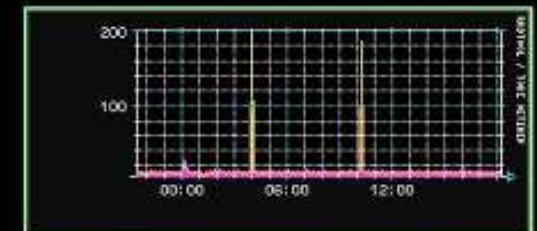
Análisis de tráfico Router Albasanz/Tela (Ethernet)



Traffic Analysis for Retevision ALBASANZ -> Moraleja



Traffic Analysis for Retevision Castellana -> Moraleja



Traffic Analysis for Retevision Castellana -> Palma

# Gestion SNMP. MRTG II

## Carga de firewalls

### TotalControl

#### Firewalls

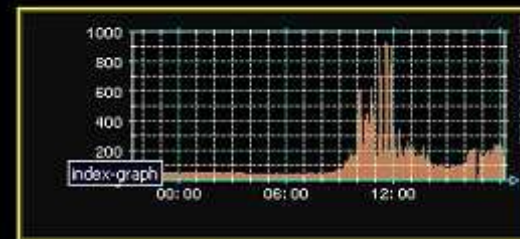
- FW-Ext1
- FW-Ext2
- FW-Ext3
- FW-Ext4
- FW-ExtGes1
- FW-ExtGes2
- FW-Int1
- FW-Int2
- FW-Int3
- FW-Int4
- FW-IntGes1
- FW-IntGes2

#### Routers

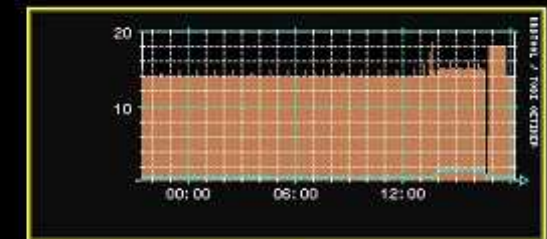
##### Telia Albasanz

- Albasanz->Moraleja
- Albasanz->ParcBit
- Albasanz->Moraleja
- Moraleja->Albasanz
- Moraleja->ParcBit
- Moraleja->Castellana
- ParcBit->Moraleja
- ParcBit->Castellana
- ParcBit->Moraleja
- Castellana->Moraleja
- Castellana->ParcBit
- Castellana->Moraleja

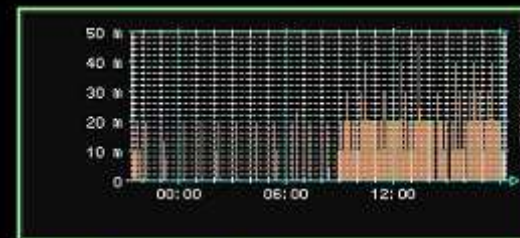
Trafico en FWExt-Gestion1 (Pag/Sec)



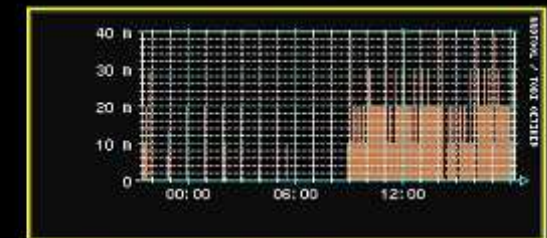
Trafico en FWExt-Gestion2 (Pag/Sec)



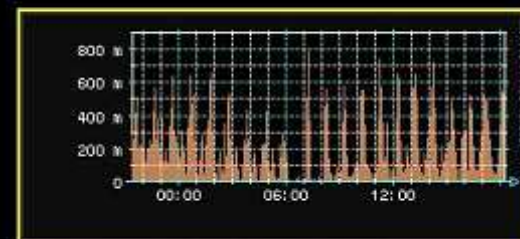
Trafico en FWINT-1 (Pag/Sec)



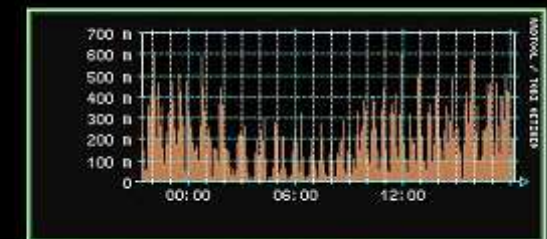
Trafico en FWINT-2 (Pag/Sec)



Trafico en FWINT-3 (Pag/Sec)



Trafico en FWINT-4 (Pag/Sec)



Trafico en FWINT-Gestion1 (Pag/Sec)

Trafico en FWINT-Gestion2 (Pag/Sec)

# Gestion SNMP. MRTG III

## Carga de llamadas en un RAS

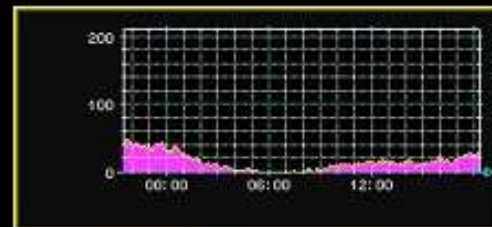
### totalControl

#### firewalls

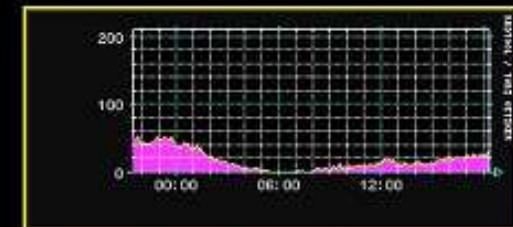
- ?W-Ext1
- ?W-Ext2
- ?W-Ext3
- ?W-Ext4
- ?W-ExtGes1
- ?W-ExtGes2
- ?W-Int1
- ?W-Int2
- ?W-Int3
- ?W-Int4
- ?W-IntGes1
- ?W-IntGes2

#### routers

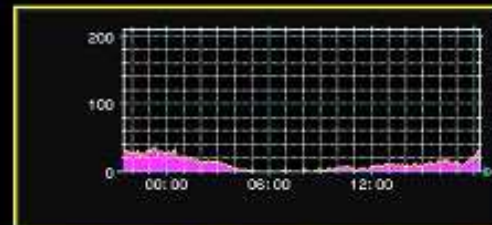
- ?alia Albasanz
- Ubasanz->Moraleja
- Ubasanz->ParcBit
- Ubasanz->Moraleja
- Arroleja->Albasanz
- Arroleja->ParcBit
- Arroleja->Castellana
- Arroleja->Moraleja
- Arroleja->Castellana
- Arroleja->Moraleja
- Castellana->Moraleja
- Castellana->ParcBit
- Castellana->Moraleja



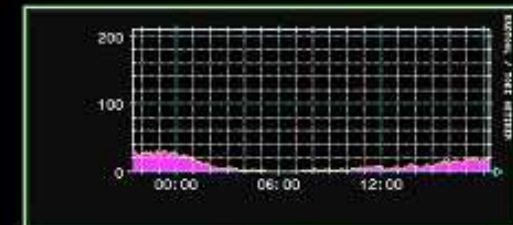
Llamadas entrantes en ARC-A TC 10



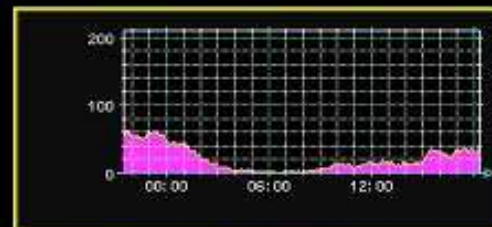
Llamadas entrantes en ARC-B TC 10



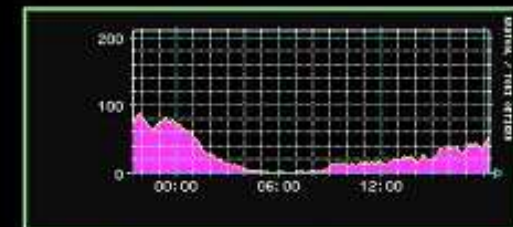
Llamadas entrantes en ARC-A TC 11



Llamadas entrantes en ARC-B TC 11



Llamadas entrantes en ARC-A TC 12



Llamadas entrantes en ARC-B TC 12