

# NETFLOW & MIKROTIK

1 **Monitoreando el tráfico  
de nuestra red**

# CUANTAS VECES NOS HA SUCEDIDO ESTO...?

- - Hola ...!?  
...hablo con CompuMundoHiperMega red !?....



- ¡¡ hace una semana que no “tengo internet”....!!

# NUESTRA REACCIÓN...



Y AHORA, QUE HACEMOS...?



- NET FLOW con MIKROTIK al RESCATE...!!



# ACERCA DE...

- Andres Gregori  
de Villa Mitre, Bahía Blanca, Argentina



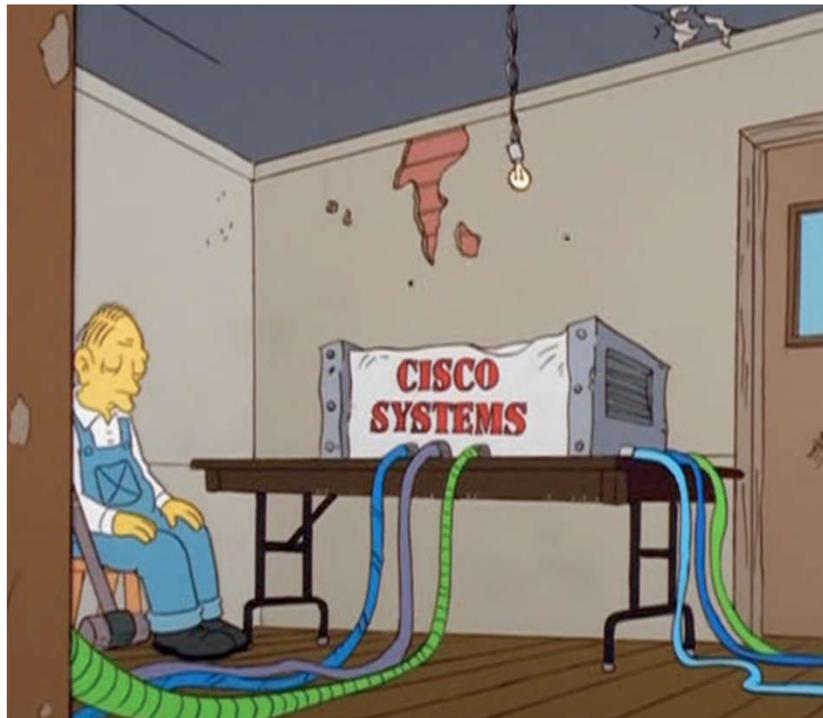
- Trabajando en ISP con Linux desde 1999
- y con Mikrotik desde 2003



- MTCNA, MTCTCE, MTCRE, MTCWE, UACA
- [www.netpro-ar.com](http://www.netpro-ar.com)

# QUE ES NETFLOW ?

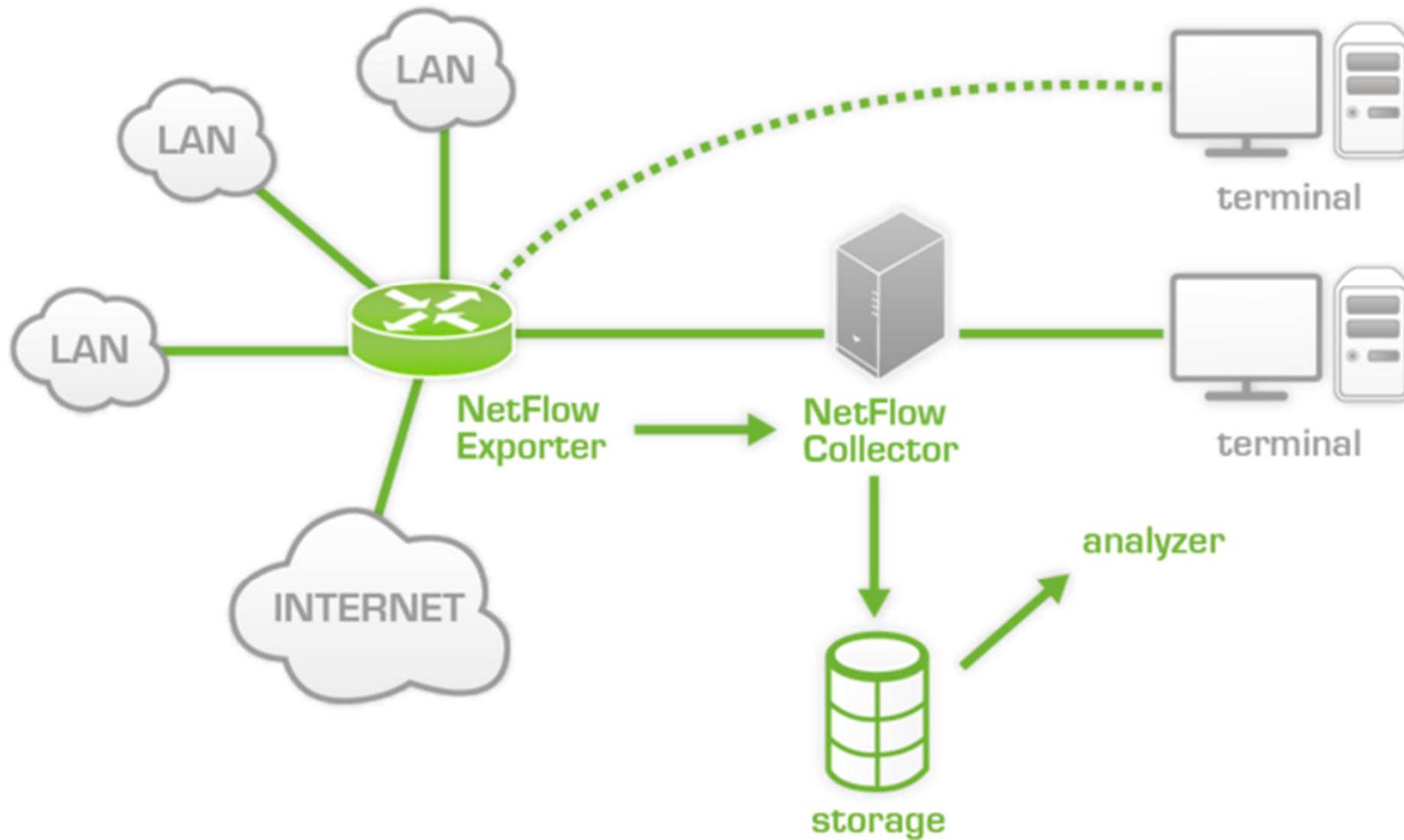
- NetFlow es un protocolo desarrollado por “Cisco Systems” para recolectar información sobre tráfico IP



# COMO FUNCIONA NETFLOW ... ??

- Normalmente un sistema de monitoreo basado en NETFLOW consta de:
  - Un Router , que soporte NetFlow (ejemplo cualquier RouterOS)
  - Un colector , que almacene la información producida por el router. Este colector puede ser una PC con Linux que guarda la información de los “flows” en el disco para su posterior análisis
  - Un Analizador: es una aplicación que revisa la información almacenada en el colector y la despliega en forma de “hermosos” gráficos.

# COMO FUNCIONA NET FLOW ?...



# SOBRE EL ROUTER (O “EXPORTER”)



- Lo ideal es que se encuentre ubicado en un punto de la red, de modo tal que todo el tráfico de la red “lo atraviese.”
- La información de todo el tráfico que pase por éste router será enviada al “colector”.
- Cada trozo de información que es enviado al colector, se denomina “flow”

HTTP Flow ●	Srdf Ge.1.1	Srd Padd 173.100.21.2	Dstif Ge.1.5	Dstl Padd 10.0.277.12	Protocol TCP	TOS 0x20	SPrt 4967	DPrt 80	...
Voice over IP ●	Srdf Ge.1.1	Srd Padd 173.100.21.2	Dstif Ge.1.3	Dstl Padd 20.0.100.10	Protocol UDP	TOS 0xA0	SPrt 6234	DPrt SIP	...
Voice over IP ●	Srdf Ge.1.1	Srd Padd 173.100.21.2	Dstif Ge.1.7	Srdf Padd 20.0.100.50	Protocol TCP	TOS 0x00	SPrt 21	DPrt 4623	...

# EL COLLECTOR

- Normalmente una PC con Linux,... aunque hay aplicaciones comerciales (y no muy accesibles).



- El almacenamiento de los Flows enviados por el router puede ser en una db (ej. Mysql), o en un sistema de archivos (ej. RRD = Round Robin Database)
- Lo habitual es que en el mismo “Colector” tengamos una aplicación de análisis y presentación de datos.

# EL ANALIZADOR

- Es una aplicación que lee los datos almacenados en el colector y las presenta al administrador de la red, de forma grafica
- Hay algunos analizadores muy interesantes como NF Sen o NTOP que permiten observar muy detalladamente el tráfico de la red, inclusive de forma histórica
- Ideal para revisar posibles eventualidades sucitadas en la red durante nuestra ausencia.



# NTOP

Welcome to ntop! - Microsoft Internet Explorer

Address: <https://10.222.222.117:3001>

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#) | [All Protocols](#) | [Local IP](#) | [FC](#) | [SCSI](#) | [Admin](#) | (C) 1998-2004 - L. Deri

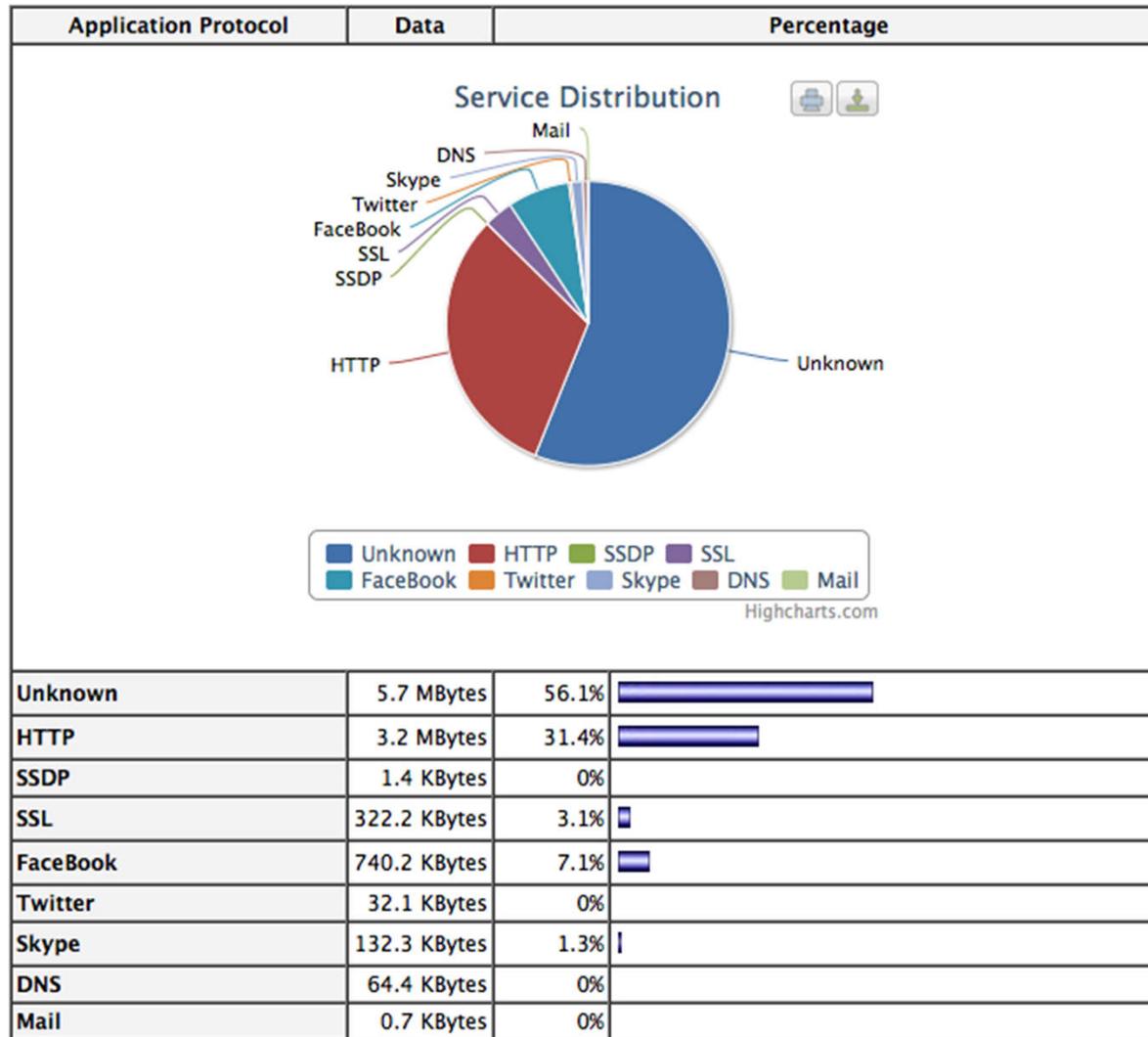
All Protocols: [Traffic](#) | [Throughput](#) | [Activity](#)

## Network Traffic [All Protocols]: All Hosts - Data Sent+Received

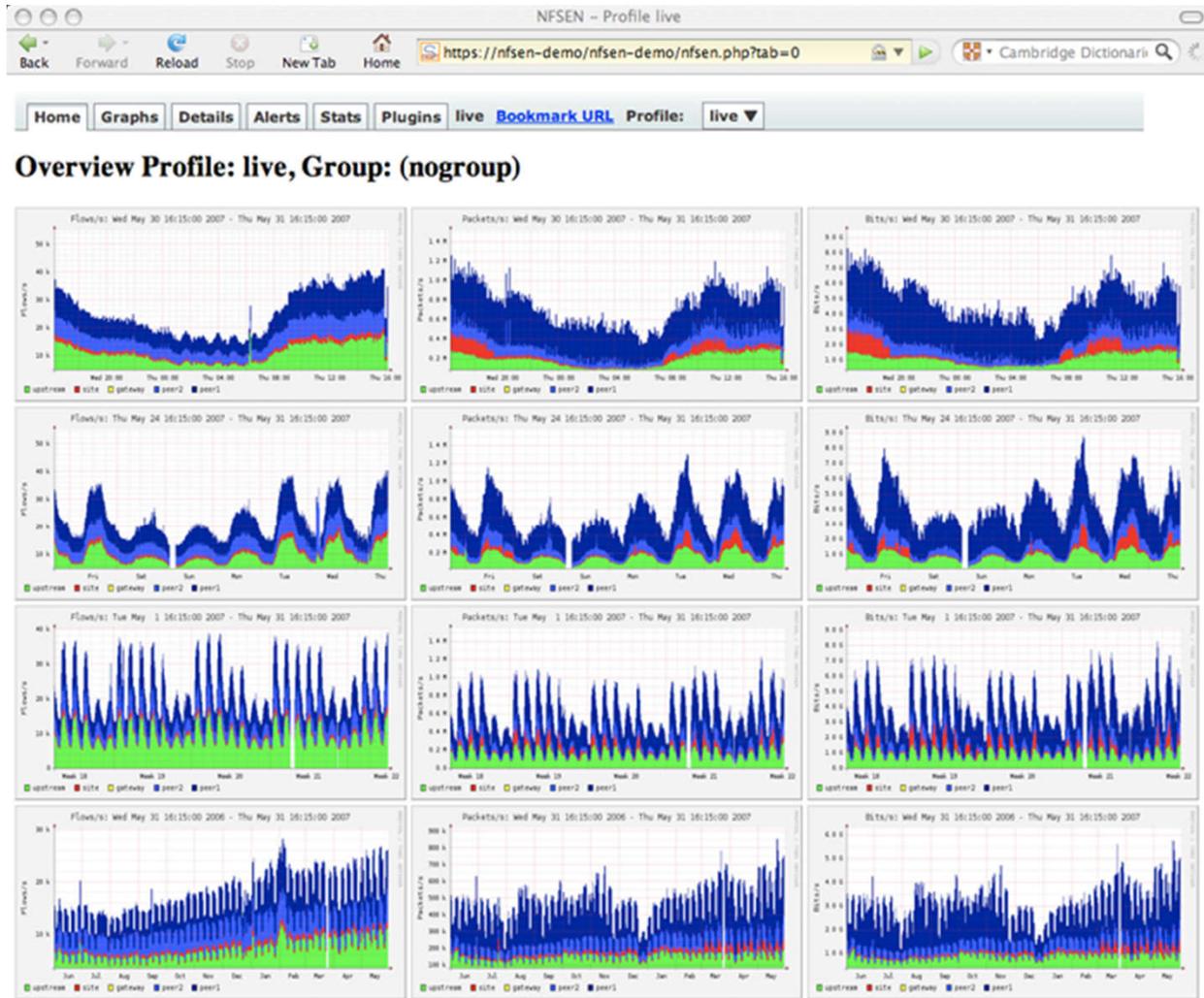
Hosts: [ All ] [ Local Only ] [ Remote Only ]      Data: [ All ] [ Sent Only ] [ Received Only ]

Host	Domain	Data	TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI
alb-24-29-56-1.nycap.rr.com		12.1 MB 35.0 %	0	0	0	0	0	0	0	12.1 MB	0	0	0
alb-24-194-134-127.nycap.rr.com		11.1 MB 32.0 %	10.8 MB	244.8 KB	13.3 KB	0	0	0	0	46	0	0	0
www.oasis-open.org		8.2 MB 23.7 %	8.2 MB	0	0	0	0	0	0	0	0	0	0
www.winnetmag.com		233.4 KB 0.7 %	233.4 KB	0	0	0	0	0	0	0	0	0	0
albyny-dns-cac-02-dmfe1.nyroc.rr.com		227.6 KB 0.6 %	0	227.6 KB	0	0	0	0	0	0	0	0	0
www.freeware-base.de		193.9 KB 0.5 %	193.9 KB	0	0	0	0	0	0	0	0	0	0
www.snort.org		189.4 KB 0.5 %	189.4 KB	0	0	0	0	0	0	0	0	0	0
ads.osdn.com		144.7 KB 0.4 %	144.7 KB	0	0	0	0	0	0	0	0	0	0
icons.wunderground.com		130.2 KB 0.4 %	130.2 KB	0	0	0	0	0	0	0	0	0	0
sourceforge.net		122.6 KB 0.3 %	122.6 KB	0	0	0	0	0	0	0	0	0	0
ms-pop-00.nycap.rr.com		115.2 KB 0.3 %	115.2 KB	0	0	0	0	0	0	0	0	0	0
www.juanso.com		111.6 KB 0.3 %	111.6 KB	0	0	0	0	0	0	0	0	0	0
www.wabbit1.homestead.com		102.6 KB 0.3 %	102.6 KB	0	0	0	0	0	0	0	0	0	0
205.188.12.16		102.4 KB 0.3 %	102.4 KB	0	0	0	0	0	0	0	0	0	0

# NTOP



# NFSEN



nfsen 1.3

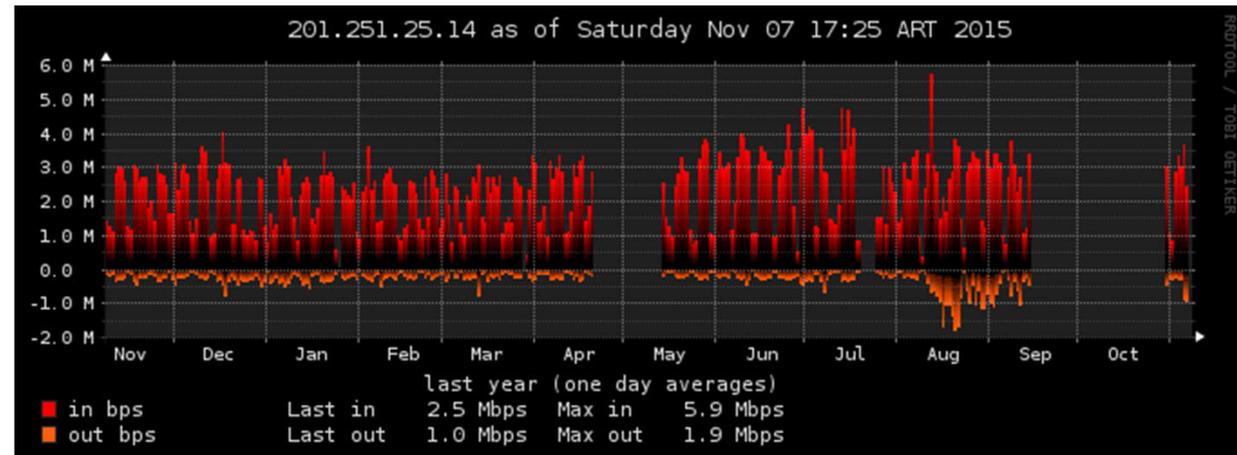
## PNRG – UN ANALIZADOR PLUG & PLAY !!

- El punto es que NTOP y NFSEN si bien son muy profesionales, requieren cierto tiempo de configuración y análisis, para extraer información que nos pueda ser útil sobre cada usuario de nuestra red. 
- Mas aun, si tenemos poco tiempo para configurar cada cliente nuevo que ingresa a nuestra red 
- Un hallazgo perdido en la red: PNRG es una pequeña app que se configura automáticamente.

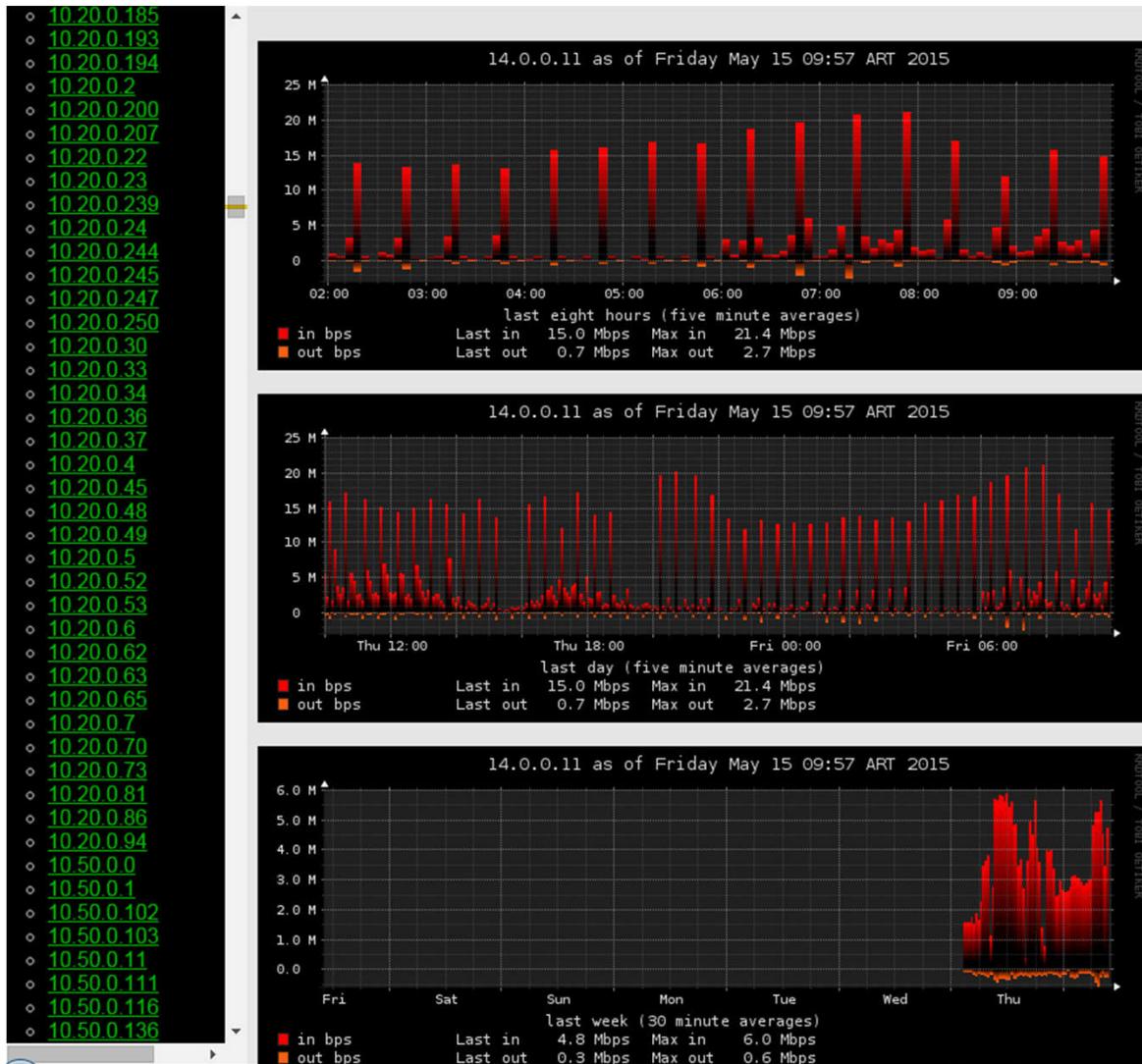
# PNRG EN ACCION

- Automáticamente se configura a medida que crece nuestra red de usuarios:

- 10.20.0.193
- 10.20.0.194
- 10.20.0.2
- 10.20.0.200
- 10.20.0.207
- 10.20.0.22
- 10.20.0.23
- 10.20.0.239
- 10.20.0.24
- 10.20.0.244
- 10.20.0.245
- 10.20.0.247
- 10.20.0.250

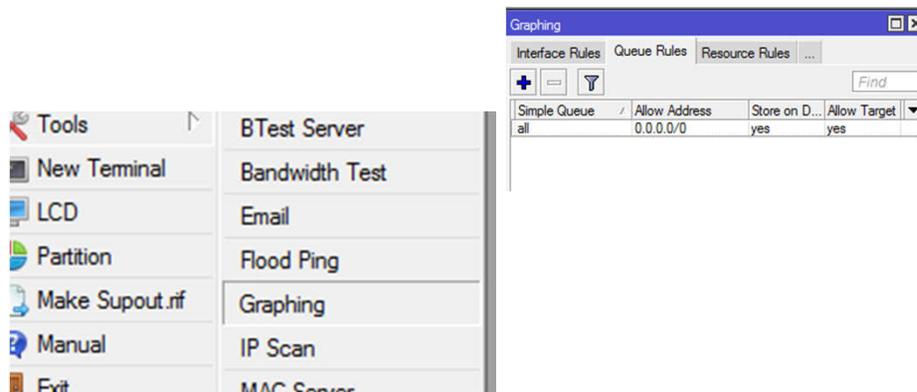


# PNRG: VISTAZO GENERAL



# ¿POR QUÉ USAR NETFLOW SI TENGO LAS GRAPHS DE MIKROTIK?

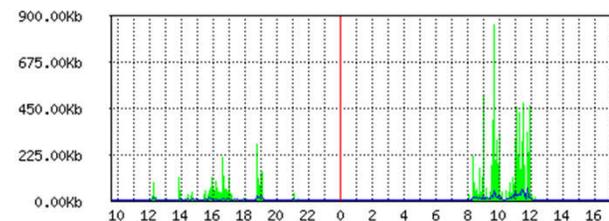
- Quizá no utilicemos *queues simples* (por ejemplo *queues tree*), o bien quizá usemos *queue simple* pero de modo distribuido en toda la red, y no todo concentrado en un solo router.
- Quizá no queramos sobrecargar al router procesando gráficos
- Quizá queramos tener un esquema de autenticación de acceso a las graficas (basado en apache web server por ejemplo),
- Muchas veces sucede que las gráficas generadas y almacenadas por la herramienta Graphs se pierden al reiniciarse el RouterOS.



## Queue <CPL> Statistics

- Source-addresses: 172.16.100.123
- Destination-address: ::/0
- Max-limit: 512.00Kb/1.02Mb (Total: unlimited)
- Limit-at: 512.00Kb/1.02Mb (Total: unlimited)
- Last update: Sat Nov 7 17:33:37 2015

## "Daily" Graph (5 Minute Average)

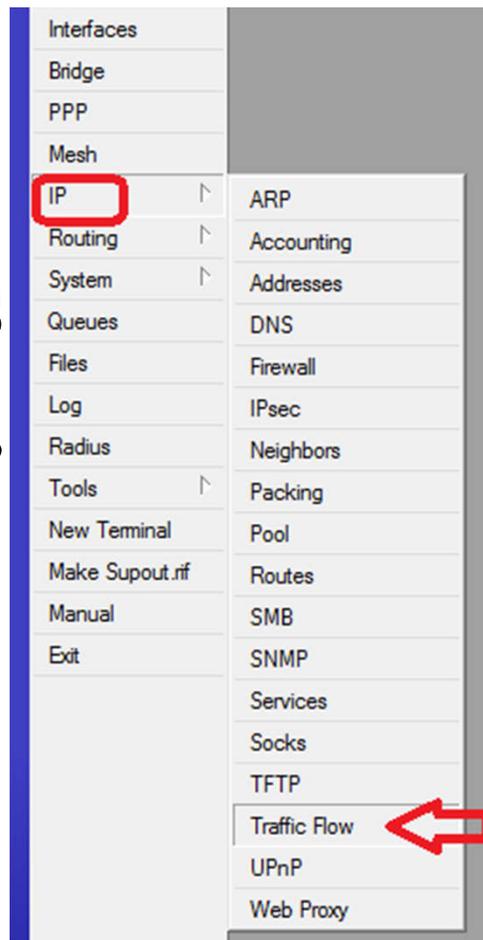


Max In: 857.71Kb (83.7%); Average In: 26.97Kb (2.6%); Current In: 4.24Kb (0.4%);  
Max Out: 58.97Kb (11.5%); Average Out: 2.66Kb (0.5%); Current Out: 680b (0.1%);

# PNRG: PUESTA EN MARCHA...!

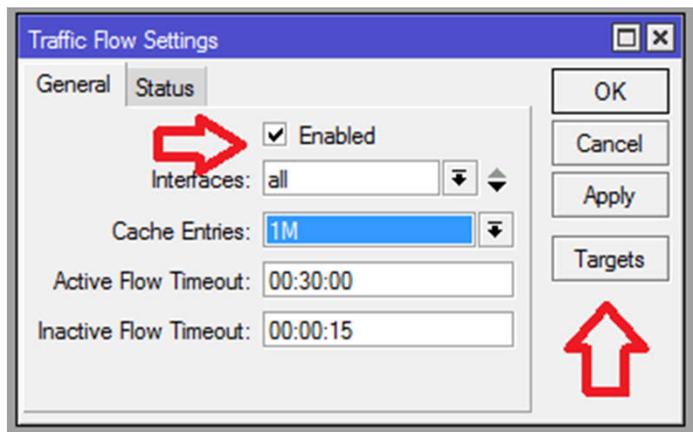
- Activamos el protocolo NetFlow en Router OS mediante:

- NetFlow en RoS se denomina *“Traffic Flow”*

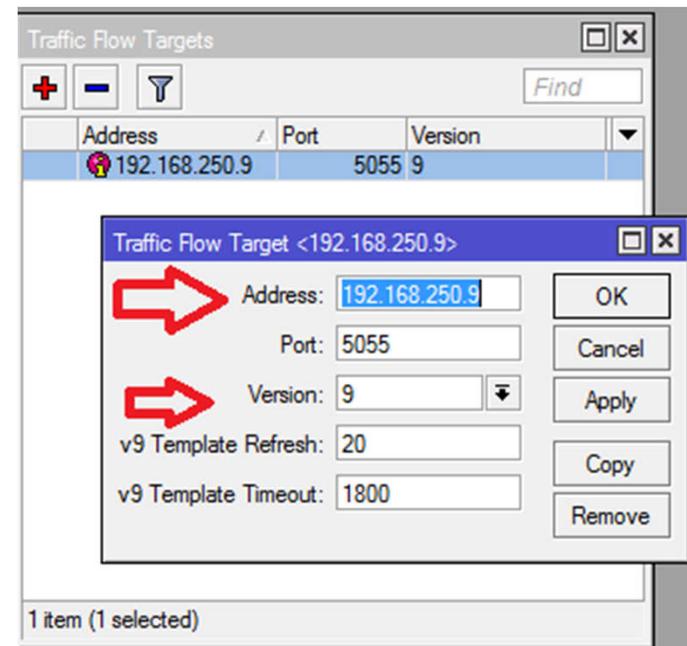


# PNRG: PUESTA EN MARCHA

- Activamos:

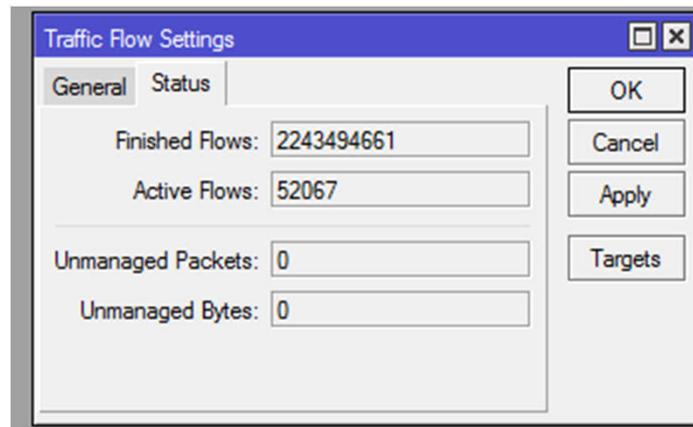


- Y seleccionamos la IP del colector:



## UNA VEZ ACTIVADO...

- Una vez activado NetFlow sobre RoS comenzara a enviar los Flows al Colector, y eso se verá reflejado en la pestaña “status”.



- Atención: según el puerto TCP seleccionado en el paso anterior, se deberá configurar el/los firewalls intermedios entre el router y el colector.

# PMACCT: “EL COLECTOR EN LINUX”

- Instalarlo en Linux simplemente con

```
aptitude install pmacct
```

(ejemplo basado en Linux Debian)



- Según la distro de Linux puede que tengamos que usar RPM, YUM, EMERGE, APT, etc....



# PMACCT: PAQUETE EN LINUX



- El paquete PMACCT incluye:
  - PMACCTD: Un daemon (no lo vamos a utilizar), que convierte al Linux en un NetFlow Exporter. Sin embargo, nuestro Exporter será RoS.
  - NFACCTD: el propio colector NetFlow
  - PMACCT: Un cliente de PMACCTD y NFACCTD que nos permitirá evaluar el funcionamiento del esquema.

# PMACCT: CONFIGURACIÓN:

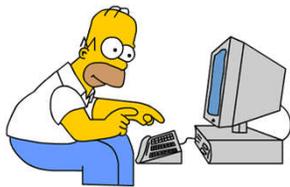
- Editamos el archivo de configuración, con nuestro editor favorito:

```
vim /etc/pmacct/nfacctd.conf
```



- Configuración básica....

# NFACCTD.CONF



```
!
! NFACCTD CONFIGURATION, ACEPTAR TRAFICO DESDE MIKROTIK
! TRAFFIC FLOW.
!
debug: false
daemonize: true
!
plugin_buffer_size: 80524
plugin_pipe_size: 18052324
!
networks_file: /etc/pmacct/hosts.def
!
! IMPORTANTE DEFINIR EL PUERTO QUE ESCUCHARA EL COLECTOR
! LUEGO EN EL MIKROTIK DEBEMOS INDICAR ESTE NUMERO DE PUERTO
!
nfacctd_port: 5055
!
! NOS INTERESA EL TRAFICO IN/OUT
!
plugins: memory[in], memory[out]
!
aggregate[in]: dst_host
aggregate[out]: src_host
!
! LA INFORMACION DE LOS FLOWS RECIBIDOS SE ALMACENARA
! EN LA MEMORIA, PARA LUEGO SER PROCESADA Y GRAFICADA
!
imt_path[in]: /tmp/pmacct_in.pipe
imt_path[out]: /tmp/pmacct_out.pipe
```

tamaño de los buffers en caso de que nuestra red sea más grande o pequeña

el archivo donde vamos a definir las subredes nuestras

el puerto definido en el router Mikrotik

sólo queremos monitorear el in/out de cada host

# HOSTS.DEF

- Elegimos nuestras redes locales a monitorear en el archivo `/etc/pmacct/hosts.def`

```
172.16.0.0/16  
10.0.0.0/8  
192.168.0.0/16  
Rangos de Ips publicas, etc...
```

- Reiniciamos el servicio ....

```
/etc/init.d/nfacctd stop  
/etc/init.d/nfacctd start
```

## VERIFICAMOS...

- Verificamos que el Colector este funcionando...

```
COLECTOR-SERVER:/etc/pmacct# pmacct -s -p /tmp/pmacct_out.pipe
SRC_IP PACKETS BYTES
11.0.1.234 2 238
11.0.3.168 2 238
11.0.0.42 2 238
11.1.2.196 2609 181636
11.1.4.130 208 34155
11.1.3.163 26 1664
11.1.1.229 53 5886
11.0.0.226 2 238
11.1.0.221 2978 1209665
11.1.3.122 732 138421
11.0.2.119 2 238
11.0.1.152 2 238
```

## POR ULTIMO: EL ANALIZADOR “PNRG”

- Pnrg era una aplicación open source prácticamente reconocida... al menos por mi
- Estuve mucho tiempo buscando en el foro de Mikrotik acerca de cómo monitorear el tráfico entrante y saliente de cada IP de nuestra red, de modo sencillo y nunca había encontrado una forma practica.
- Y un buen día encontré a PNRG, en el gigantesco mundo del open source. Un pequeño set de scripts escritos en “Perl”, que trabaja con RRD.



*PNRG es tan pequeña  
y desconocida que no  
posee logo*

# PNRG: INSTALACIÓN

- No tiene paquete de instalación: simplemente se deben copiar los archivos:
- Creación de los directorios

```
mkdir /usr/local/pnrg  
cd /usr/local/pnrg
```

- Descarga y descompresión:

```
wget http://www.pmacct.net/pnrg/pnrg-0.1.tar.gz  
  
tar zxvf pnrg-0.1.tar.gz  
mv pnrg-0.1/* .
```

- Instalación de la herramienta RRD TOOL

```
apt-get install rrdtool
```

- Le indicamos al CRON que actualice las graficas cada 5 minutos:

```
echo "*/5 * * * * root ( cd /usr/local/pnrg/; ./pnrg-wrapper.sh )" > /etc/cron.d/pnrg
```

# PNRG: INSTALACIÓN

- Creamos algunos symbolics links para facilitar la operación

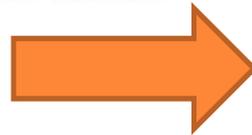
```
ln -s /usr/bin/pmacct /usr/local/bin/pmacct
mkdir -p /usr/local/rrdtool/bin/
ln -s /usr/bin/rrdtool /usr/local/rrdtool/bin/rrdtool
ln -s /usr/bin/rrdcgi /usr/local/rrdtool/bin/rrdcgi
```

- Y por último debemos configurar el servidor Web APACHE.

```
apt-get install apache2
```

```
ln -s /usr/local/pnrg/spool /var/www/pnrg
```

```
/etc/apache2/sites-enabled/000-default
```

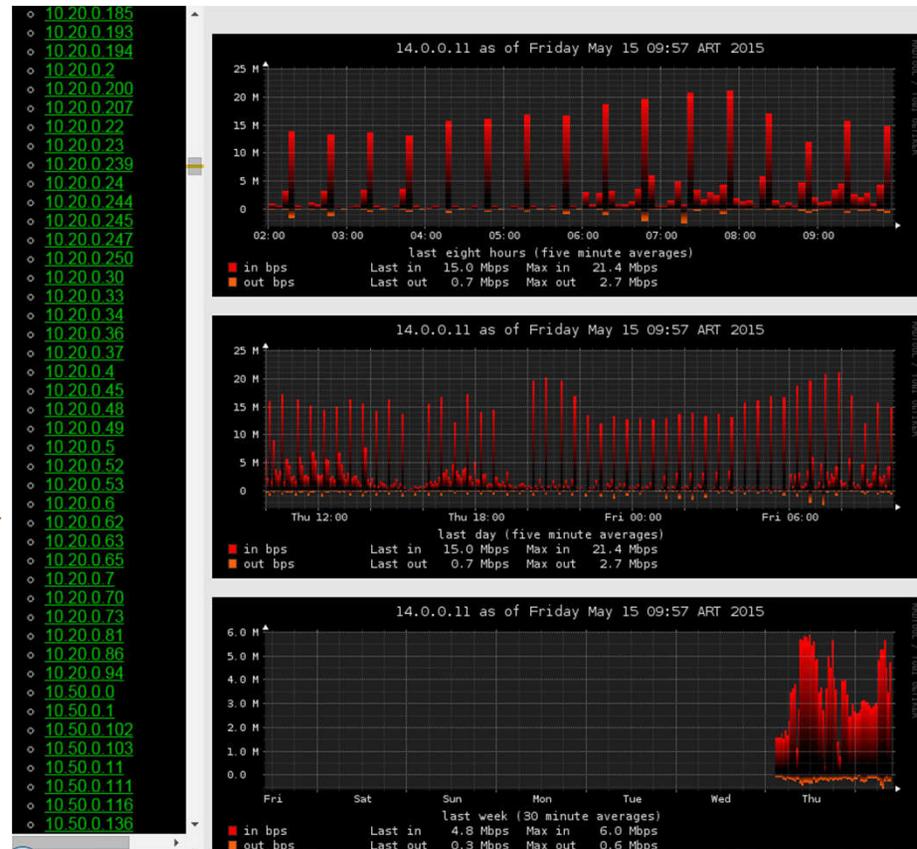


```
AddHandler cgi-script .cgi .pl
<Directory /var/www/pnrg/>
  Options Indexes ExecCGI
  AllowOverride None
  Order allow,deny
  Allow from all
</Directory>
```

# Y AHORA... MAGIA ...!!

- Si todo ha salido bien, podemos acceder a las graficas desde <http://IP.DEL.COLECTOR/pnrg>

Automáticamente PNRG detecta las direcciones IPs de nuestros clientes, y crea una sección con la grafica de cada uno de ellos...!!!



# MUCHAS GRACIAS ...!!!

- PREGUNTAS ... ?
- Pueden ver este tutorial y configuraciones en <http://www.netpro-ar.com/monitoreo-de-trafico-con-mikrotik-y-netflow/>

