









# NFSEN Exercise - 2

# What we will do

- 1 Your router should be sending flows to two PCs in your group. Confirm this!
- 2 Ensure NFSEN is running by browsing on the page and ensuring you can see the graphs with no errors indicated
- 3 We will now see what type of traffic is passing through the group router




# Create a Stat to graph specific traffic


- On the PC receiving flows, open the NFSEN page and click on 'live' on the top right of the page and select 'new profile' at the bottom
- Enter the name 'HTTP\_TRAFFIC' for the profile name and additionally create a new group called 'groupX' where X is your group number
- Select individual channels and shadow profile.
  - Individual channel – can create channels with own filters
  - Shadow profile – save hard disk space by not creating new data but instead analyses already collected data

<b>Profile:</b>	<input type="text" value="HTTP_TRAFFIC"/>	
<b>Group:</b>	<input type="text" value="New group ..."/> <input type="text" value="Group20"/>	
<b>Description:</b>	<input type="text"/>	
<b>Start:</b>	<input type="text"/> Format: yyyy-mm-dd-HH-MM	
<b>End:</b>	<input type="text"/> Format: yyyy-mm-dd-HH-MM	
<b>Max. Size:</b>	<input type="text" value="10G"/>	
<b>Expire:</b>	<input type="text" value="60 Days"/>	
<b>Channels:</b>	<input type="radio"/> 1:1 channels from profile live <input checked="" type="radio"/> individual channels	
<b>Type:</b>	<input type="radio"/> Real Profile <input checked="" type="radio"/> Shadow Profile	
<input type="button" value="Cancel"/> <input type="button" value="Create Profile"/>		







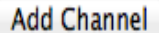
Click Create Profile at the bottom

## Profile: HTTP\_TRAFFIC

Group:	Group20	
Description:	<div style="border: 1px solid gray; height: 100px;"></div>	
Type:	Continuous / shadow	
Start:	2012-05-09-15-25	
End:	2012-05-09-15-25	
Last Update:	2012-05-09-15-20	
Size:	0 B	
Max. Size:	unlimited	
Expire:	never	
Status:	new	

▼ Channel List: 

Click on the plus sign next to 'Channel List' at the bottom of the page then fill the next page as below and click on 'Add Channel' at the bottom. The filter 'any' means ALL traffic

Channel name	TOTAL_TRAFFIC	
Colour:	Enter new value	#abcdef or Select a colour from 
Sign:	+ 	Order: 
Filter:	any	
Sources:	Available Sources	Selected Sources
	<div style="border: 1px solid gray; height: 100px;"></div>	gw-rtr
	 	
 		

**Channel name**

**Colour:** Enter new value  or

**Sign:**  **Order:**

**Filter:** `src port 80 and dst host 10.10.X.Y`

**Sources:**

Available Sources	Selected Sources
	gw-rtr



Add another channel by clicking the plus sign as before next to 'Channel List'. Fill the details as shown on the left. Replace Y with the pc number that is **NOT receiving flows in your pair!**

With this, we will track how much HTTP traffic is going to pcY ie how much he is actually downloading. In a HTTP download, source traffic is from port 80 always

Replace X with your Group number and ensure you change the color. You can use the color picker or enter the value shown in this example

Select the router as the source then click add channel

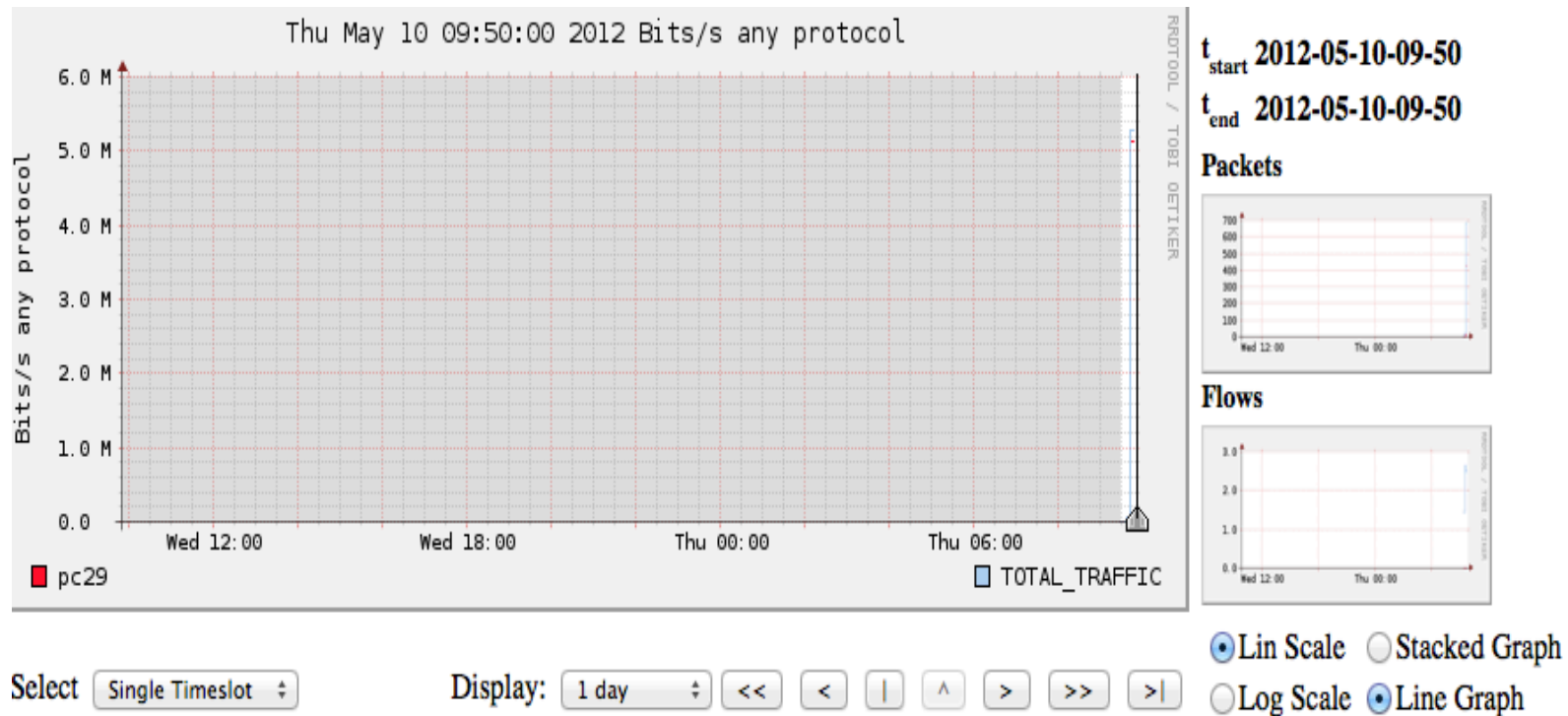
# Activate the profile

Start:	2011-11-17-11-10				
End:	2011-11-17-11-10				
Last Update:	2011-11-17-11-05				
Size:	0 B				
Max. Size:	unlimited				
Expire:	never				
Status:	new 				
▼ Channel List: +					
▼ User2 					
Colour:	#FF0000	Sign:	+	Order:	2
Filter:	dst host 10.10.0.139				

- Click the green tick to activate your new profile.
- The owner of pcY should now download over HTTP from the NOC server
- Click on Live then select the group you created and 'HTTP\_TRAFFIC' you will see your profile

# See the traffic

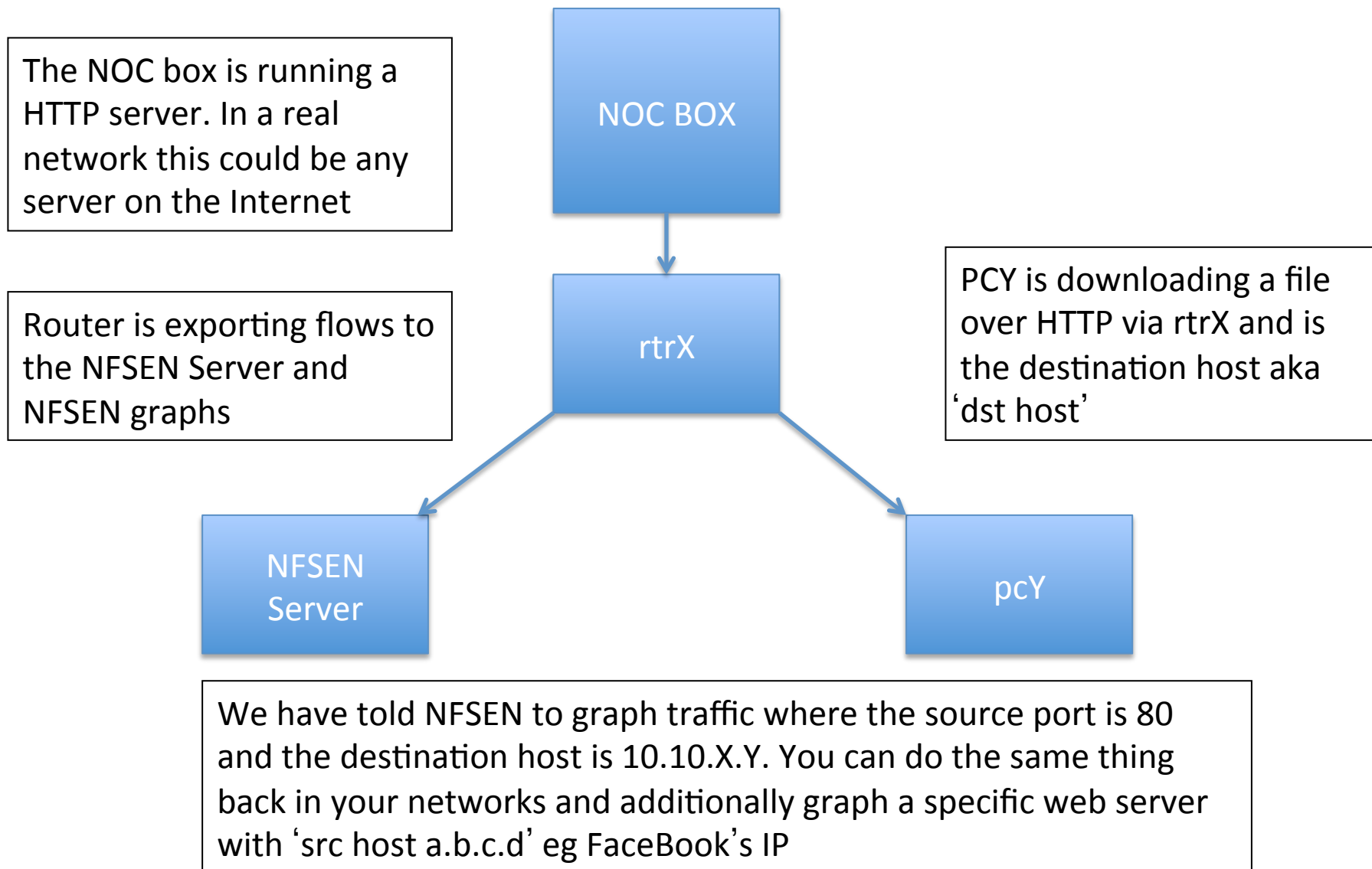
- Your graph will take 15min to update. Go to Graphs then Traffic. Then go to details and select 'Line Graph' at bottom



- This is a graph of the total traffic passing through the router vs the HTTP downloads that pcY is making



# STOP! What's happening here?



# See an FTP download from the NOC server

- Perform the exact same steps from slide number 5 but this time, change 'HTTP\_TRAFFIC' to 'FTP\_TRAFFIC'
- The FTP could randomize the ports so it may not be source port 20. We do know that it will be a port greater than 24 so the filter should read:
  - src port > 1024 and dst host 10.10.X.Y
- Now download the file from the noc box via <ftp://noc.ws.nsrc.org>

# Graph a specific interface on the router

- Go to cacti and identify the interface index number on your router that you want to graph
  - Click on Devices and select your router then at the bottom of the page, click on 'Verbose Query' under '**Associated Data Queries**'
- You will see something like
  - *Found item [ifDescr='FastEthernet0/0'] index: 1 [from value]*

```
- Located input field 'ifName' [walk]
- Executing SNMP walk for data @ '.1.3.6.1.2.1.31.1.1.1.1'
- Found item [ifName='Fa0/0'] index: 1 [from value]
- Found item [ifName='Fa0/1'] index: 2 [from value]
- Found item [ifName='Nu0'] index: 4 [from value]
- Located input field 'ifAlias' [walk]
```

- This is the index number 1. We can now use Nfsen to graph traffic for this specific interface
  - This interface must have 'ip flow egress' or ingress enabled
  - NB: You can also identify the index number with an snmpwalk
  - With 'snmp ifindex persist' the index number is maintained

# Add the interface on NFSEN

<b>Profile:</b>	<input type="text" value="Interface_FastEthernet_1"/>	?
<b>Group:</b>	<input type="text" value="Group20"/>	?
<b>Description:</b>	<div style="border: 1px solid gray; height: 40px;"></div>	
<b>Start:</b>	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
<b>End:</b>	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
<b>Max. Size:</b>	<input type="text" value="10G"/>	?
<b>Expire:</b>	<input type="text" value="60 Days"/>	?
<b>Channels:</b>	<input type="radio"/> 1:1 channels from profile live <input checked="" type="radio"/> individual channels	?
<b>Type:</b>	<input type="radio"/> Real Profile <input checked="" type="radio"/> Shadow Profile	?
<input type="button" value="Cancel"/> <input type="button" value="Create Profile"/>		

Give the Profile a suitable name and add it to the same Group you created

Choose individual channels and Shadow profile as before and select create profile. Then on the following screen click on the plus sign next to Channel list

<b>Status:</b>	<input type="text" value="new"/>
<b>Channel List:</b>	<input type="button" value="+"/> +

**Channel name**

**Colour:** Enter new value  or

**Sign:**  **Order:**

**Filter:**

**Sources:**

Available Sources	Selected Sources
	gw-rtr

**Channel name**

**Colour:** Enter new value  or

**Sign:**  **Order:**

**Filter:**

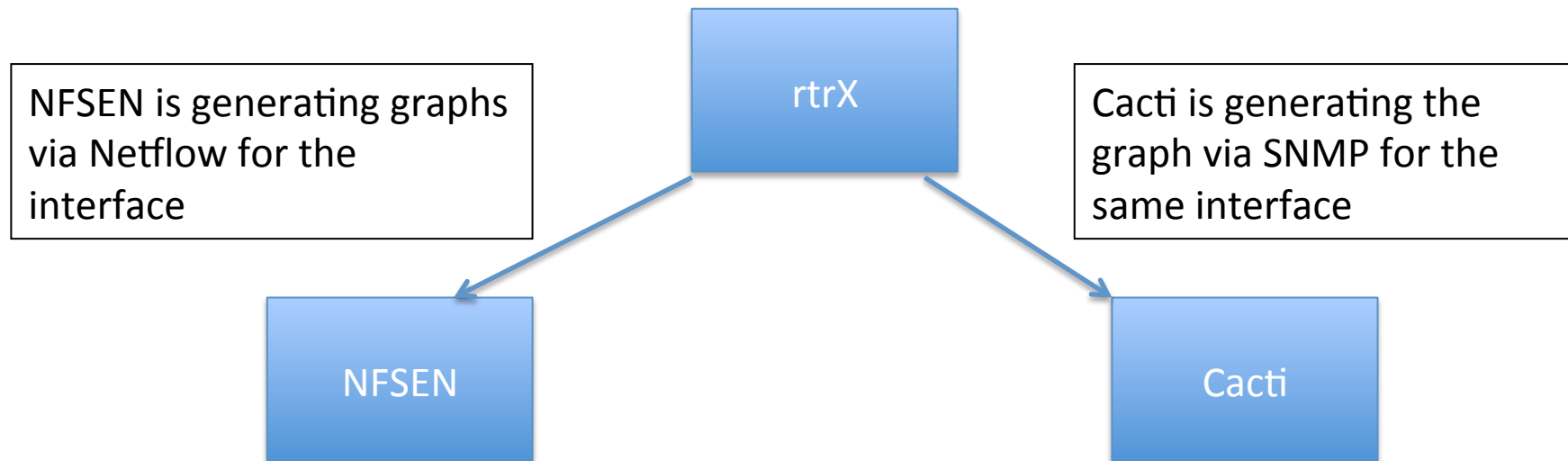
**Sources:**

Available Sources	Selected Sources
	gw-rtr

This means graph all traffic passing INTO interface 1. Click add channel and click plus to add a second channel

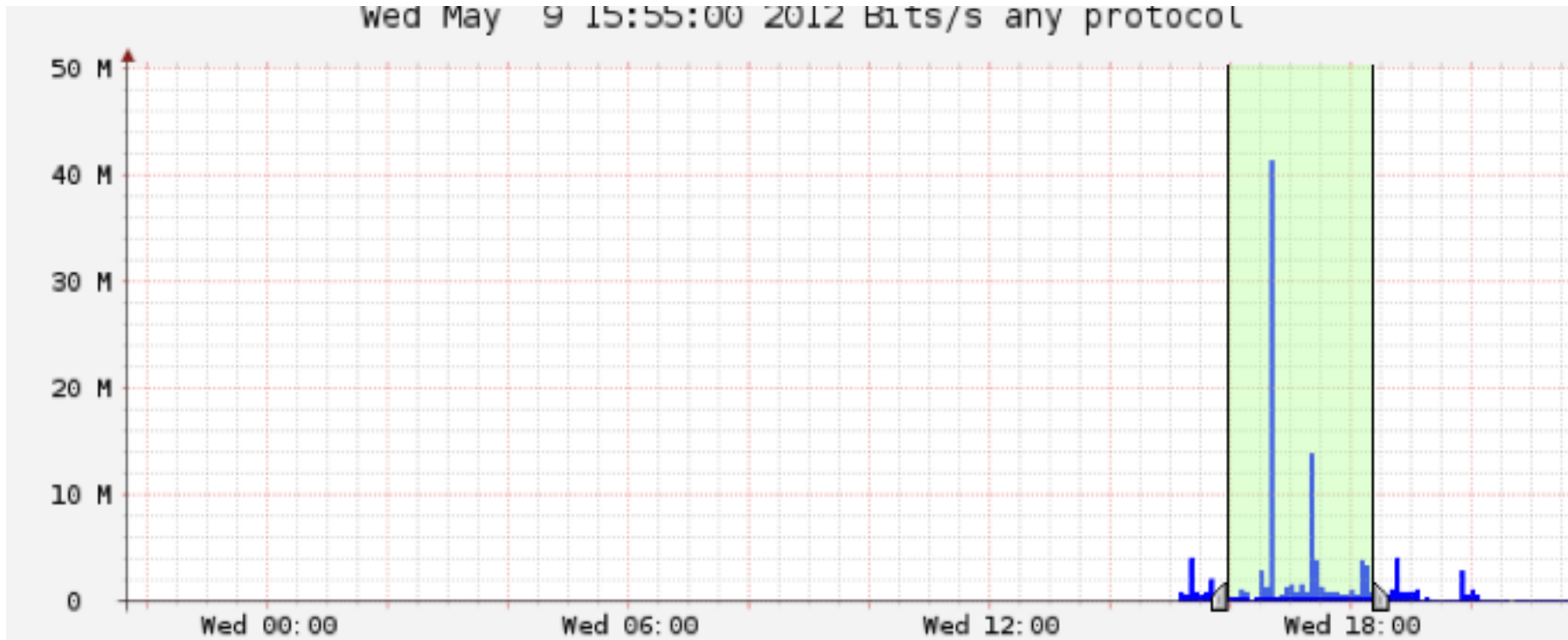
This means graph all traffic LEAVING/GOING OUT OF interface 1. Click add channel then activate the filter on the next screen. Give the graph time to generate. Compare the graph with Cacti's graph

# STOP! What's happening here?



With NFSEN, we can use the Netflow features to extract more data like which IP Addresses are active, what are the highest ports in use by bytes, what are the AS Numbers coming/leaving our network and so much more!

# Extended Netflow processing



Go to Profile, select the group you created then select 'HTTP\_TRAFFIC'. Then go to the 'Details' tab and select 'Time Window' instead of 'Time Slot' beneath the graph. Choose a part of the graph with activity as above

### Options:

List Flows  Stat TopN

**Top:** 10

**Stat:** Flow Records **order by** bytes

**Aggregate**

bi-directional

proto

srcPort  srcIP

dstPort  dstIP

**Limit:**  Packets > 0 -

**Output:** auto  / IPv6 long

Clear Form process

Select the options as on the left. This means, select the Top 10 Flows, Order them by Bytes from the highest to the lowest and display information of the source and destination ports and IPs. Then select 'Process'. Analyze the output you get which will look like the below screen.

Aggregated flows 53/73

Top 10 flows ordered by bytes:

Date flow start	Duration	Proto	Src IP Addr	Src Pt	Dst IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2012-05-09 16:31:43.481	664.018	TCP	10.10.0.60	53731	10.10.0.250	22	1.0 M	1.5 G	18.1 M	1482	1
2012-05-09 17:10:21.896	722.117	TCP	10.10.0.254	42499	10.10.8.29	22	310886	466.2 M	5.2 M	1499	47
2012-05-09 16:22:44.095	4108.913	TCP	208.117.226.27	80	10.10.0.77	49757	69250	103.7 M	201865	1497	2
2012-05-09 18:13:16.475	45.837	TCP	10.10.0.60	54946	10.10.0.250	22	66924	99.5 M	17.4 M	1487	1
2012-05-09 18:18:15.625	20.212	TCP	10.10.0.250	16617	10.10.0.60	51007	66230	80.3 M	20.3 M	1100	1



## Options:

List Flows  Stat TopN

Top:

Stat:  order by

Aggregate  bi-directional  
 proto  
 srcPort   
 dstPort

Limit:  Packets

Output:   / IPv6 long

## Netflow Processing

Source:

test  
pc29  
TOTAL\_TRAFFIC

Filter:

```
src port > 1024 and dst host 10.10.8.29
```

and

Try the same with the Bi-Directional traffic option. What do you see? Try playing with the different options and see what output you get. You can also add the same filters on the filter window next to the Options.

Try the following filters:

**src host 10.10.X.Y** – meaning look for flows for this host

**src port 22** – meaning flows where the source port is 21

**src port 22 or src port 80** – meaning flows of either port 22 or 80

**src port 80 and in if 1** – meaning flows of src port 80 that passed via interface 1

**dst net 10.10.0.0/16** – meaning all flows where the destination network is 10.10.0.0/16

**src port > 5000** – meaning all flows where the source port is greater than 5000

# Many more filters you could use

- If you want to see AS Number traffic for Google's AS 15169
  - `src as 15169`
- You can do the same for anyone's AS but your router should have the routing table installed and have *'ip flow-export version 9 origin-as'* configured
- You can then graph each of them using a Stat as in the earlier exercise
- More filters here:  
<http://nfsen.sourceforge.net/#mozTocId652064>

## **ADDITIONAL/OPTIONAL**

Monitor a specific host

Profile:	<input type="text" value="Troublesome_User"/>	?
Group:	<input type="text" value="New group ..."/> ▼ <input type="text" value="Hosts"/>	?
Description:	<input type="text"/>	
Start:	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
End:	<input type="text"/> Format: yyyy-mm-dd-HH-MM	?
Max. Size:	<input type="text" value="0"/>	?
Expire:	<input type="text" value="never"/>	?
Channels:	<input type="radio"/> 1:1 channels from profile live <input checked="" type="radio"/> individual channels	?
Type:	<input type="radio"/> Real Profile <input checked="" type="radio"/> Shadow Profile	?
<input type="button" value="Cancel"/> <input type="button" value="Create Profile"/>		

- When done click on 'Create Profile' at the bottom
- You will see a message “new profile created”
- Then click on the plus sign at the bottom to begin adding channels

# Monitor a Specific IP

Home Graphs Details Alerts Stats Plugins continuous / shadow [Bookmark URL](#) Pr

<b>Channel name</b>		<input type="text" value="User1"/>	
<b>Colour:</b>	Enter new value	<input type="text" value="#abcdef"/> or	
		Select a colour from ▾	
<b>Sign:</b>	<input type="button" value="+"/> ▾	<b>Order:</b>	<input type="button" value="1"/> ▾
<b>Filter:</b>	<input type="text" value="host 10.10.0.51"/>		
<b>Sources:</b>	<b>Available Sources</b>		<b>Selected Sources</b>
	<input type="text" value="rtr9"/>		<input type="text" value="noc"/>
		<input type="button" value="&lt;&lt;"/>	<input type="button" value="&gt;&gt;"/>
<input type="button" value="Cancel"/>		<input type="button" value="Add Channel"/>	

Replace  
10.10.0.51  
with your IP

# Add a second channel and start to accept

Last Update: 2011-11-17-11-05

Size: 0 B

Max. Size: unlimited

Expire: never

Status: new

**Channel List:**

**User1**

Colour: #abcdef Sign: + Order: 1

Filter: host 10.10.0.51

Sources: noc

Home Graphs Details Alerts Stats Plugins continuous / shadow !

Channel name: User2

Colour: Enter new value #FF0000 or Select a colour from

Sign: + | Order: 2 |

Filter: dst host 10.10.0.139

Sources:

Available Sources	Selected Sources
rtr9	noc

<< >>

Cancel Add Channel

# Filters

- Select a different color for the second channel so that the graphs can be distinguished
- Note that the two filters are different
  - The first filter will capture any flows pertaining to host one pc
  - The second filter will only capture flows where host the second pc is the DESTINATION host
- More attributes can be added here like src AS, dst AS, src ports etc based on the NFSEN filter syntax

[Home](#)[Graphs](#)[Details](#)[Alerts](#)[Stats](#)[Plugins](#)

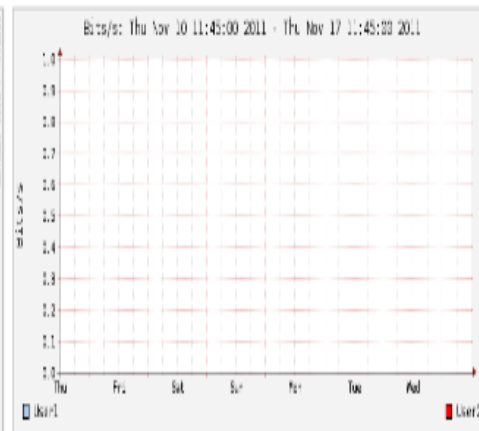
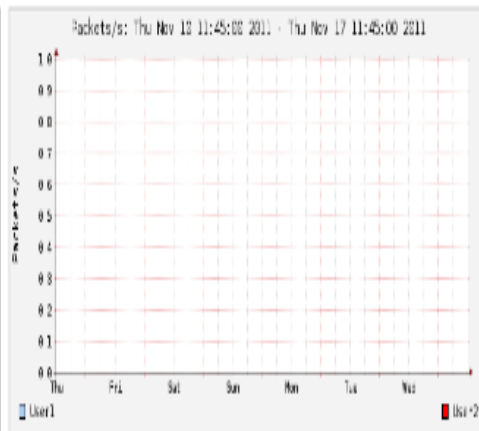
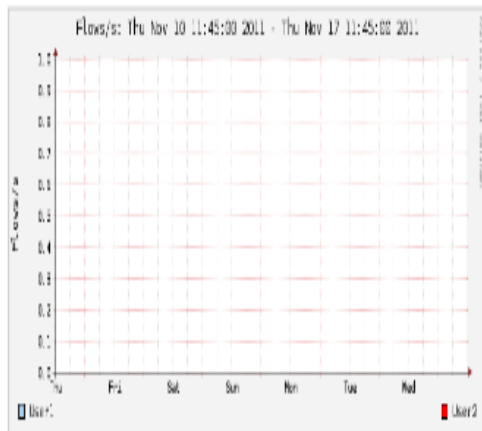
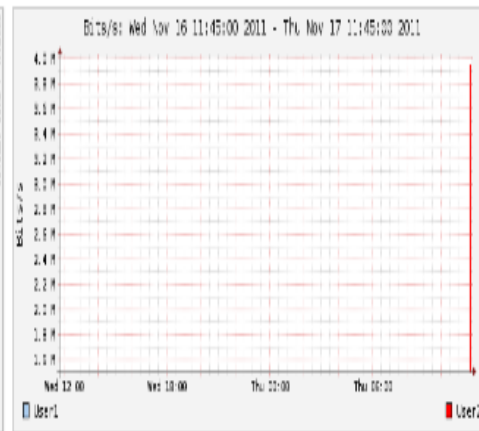
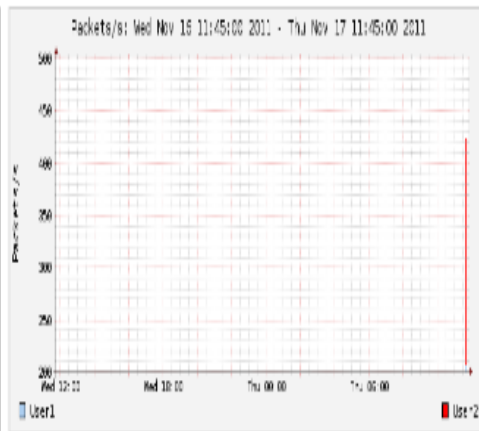
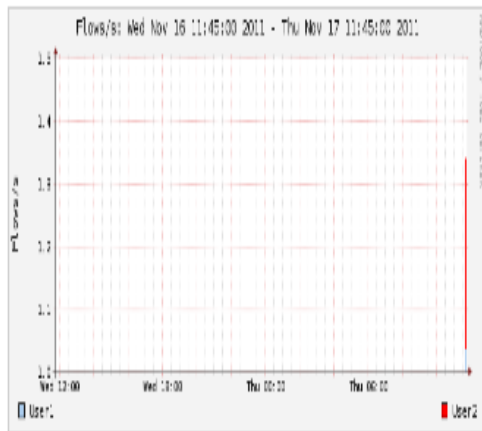
continuous / shadow

[Bookmark URL](#)

Profile:

Troublesome\_User ▾

## Overview Profile: Troublesome\_User, Group Hosts





**MOVE TO EXERCISE 3**