Campus Network Design Workshop

Introduction to NfSen

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

What is NfSen

- Is a graphical (Web Based) front end to NfDump
- NfDump tools collect and process netflow data on the command line
- NfSen allows you to:
  - Easily navigate through the netflow data.
  - Process the netflow data within the specified time span.
  - Create history as well as continuous profiles.
  - Set alerts, based on various conditions.
  - Write your own plugins to process netflow data on a regular interval.

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

NfSen structure

- Configuration file – nfsen.conf
- NfDump files – Netflow files containing collected flows stored in 'profiles-data' directory
  - NB: It is possible for other programs to read NFdump files but don't store them for too long as they can fill up your drive
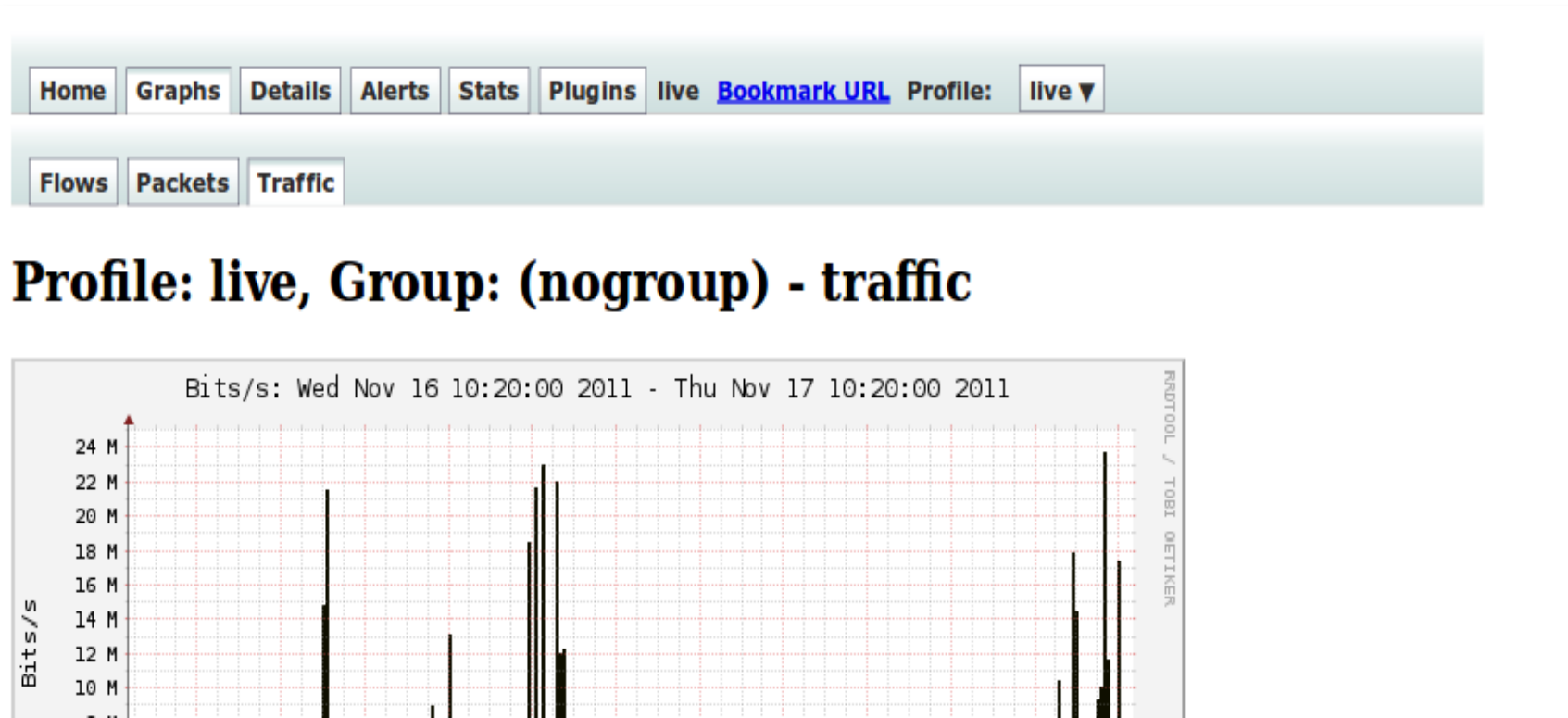- Actual graphs – stored in 'profiles-stat' directory
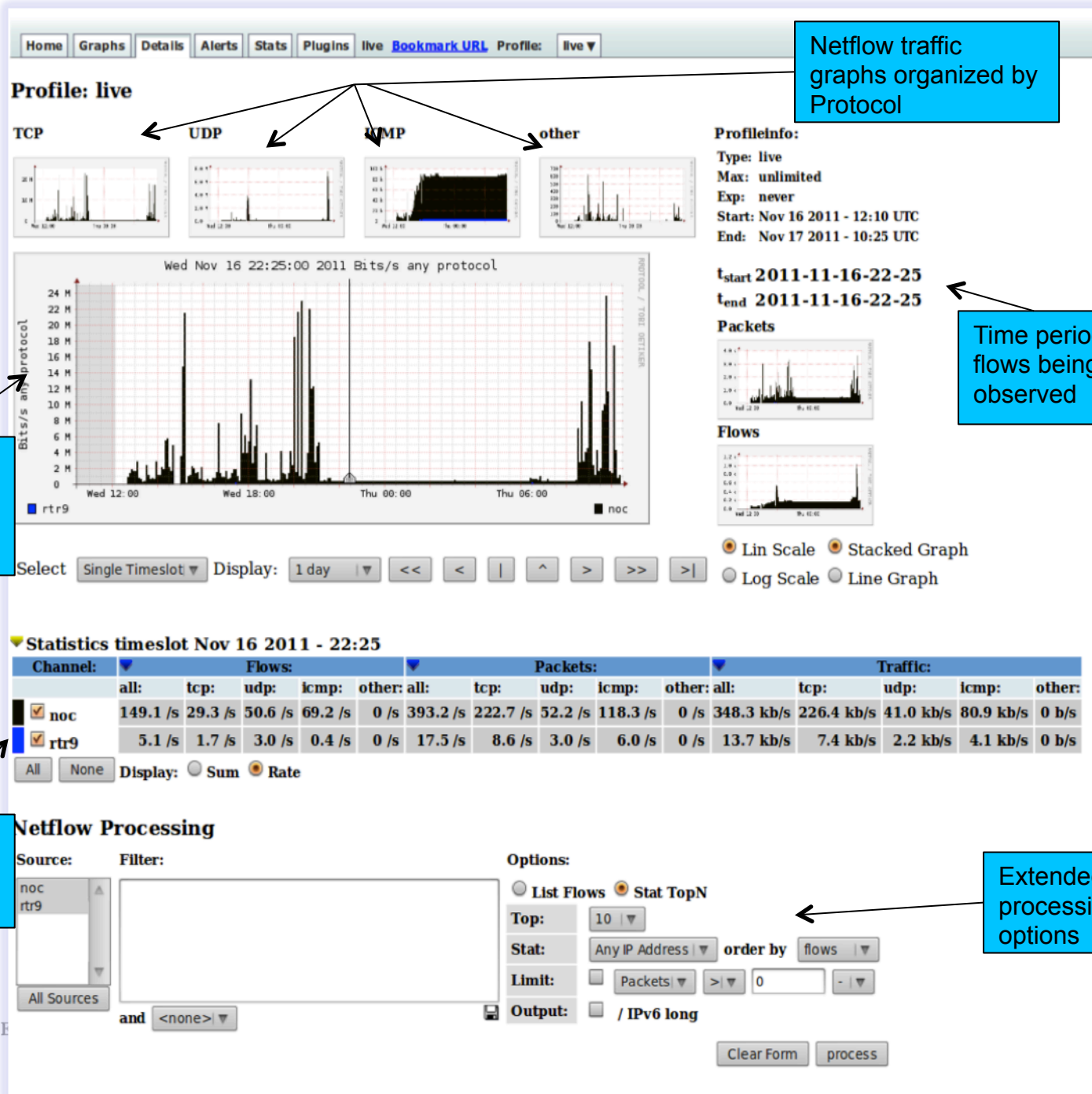
NfSen Home Screen
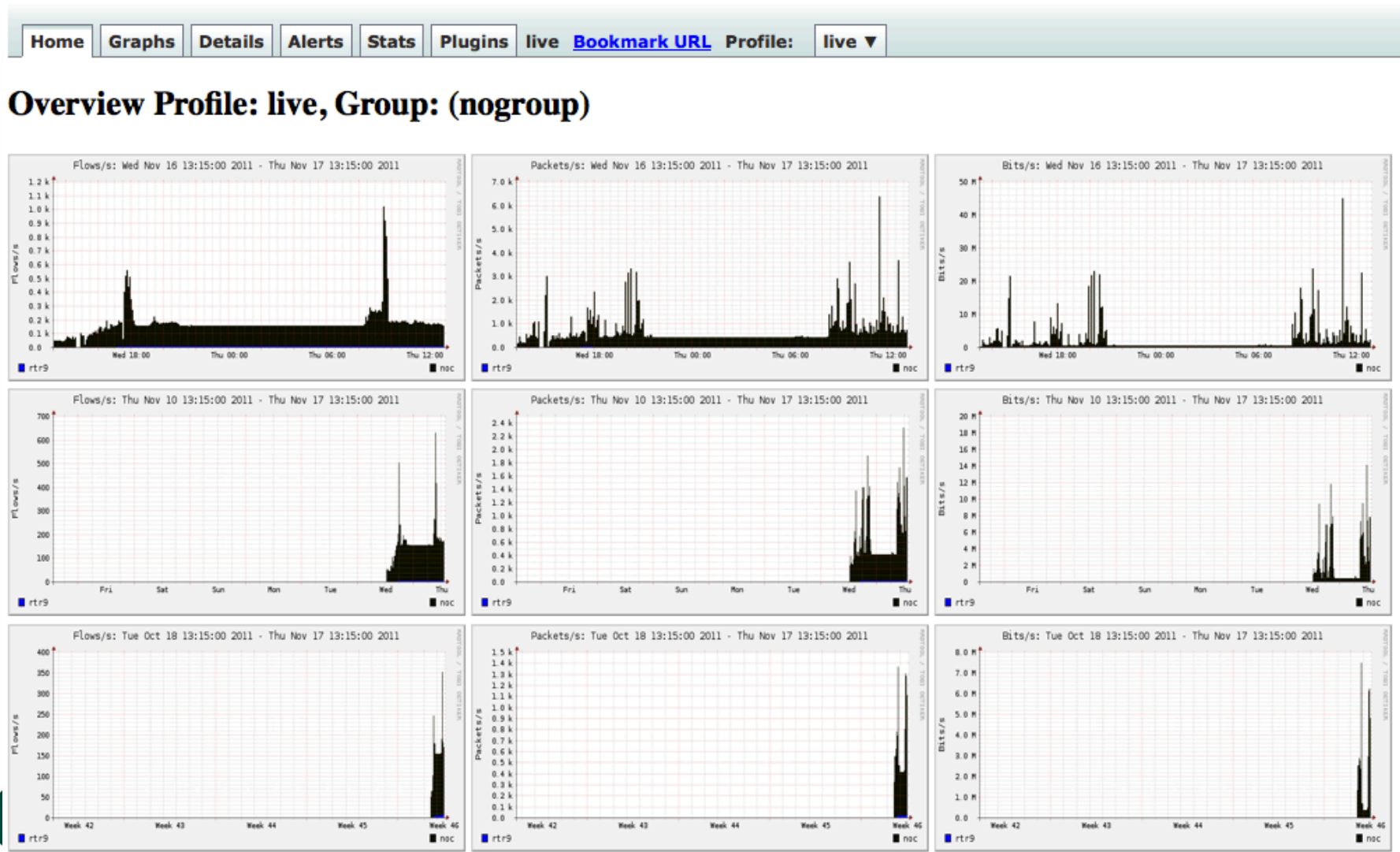
Graphs Tab

- Graphs of flows, packets and traffic based on interface with netflow activated
- NB: What is seen under Traffic should closely match what is under Cacti for the same interface

Details Page

- Most interesting page
- Can view present flow information or stored flow information
- Can view detailed Netflow information such as
  - AS Numbers (more useful if you have full routing table exported on your router)
  - Src hosts/ports, destination hosts and ports
  - Unidirectional or Bi-directional flows
  - Flows on specific interfaces
  - Protocols and TOS

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Home | Graphs | **Details** | Alerts | Stats | Plugins | live | **Bookmark URL** | Profile: | live ▼

Profile: live

TCP   UDP   ICMP   other

Netflow traffic graphs organized by Protocol

Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 10:25 UTC

t_{start} **2011-11-16-22-25**
t_{end} **2011-11-16-22-25**

Time period for flows being observed

Packets

Flows

Graph of Netflow traffic for all Protocols

Wed Nov 16 22:25:00 2011 Bits/s any protocol

○ Lin Scale ● Stacked Graph
○ Log Scale ○ Line Graph

Select [Single Timeslot ▼] Display: [1 day ▼] [<<] [<] [|] [^] [>] [>>] [>|]

▼ **Statistics timeslot Nov 16 2011 - 22:25**

Channel: ▼	Flows:				Packets:				Traffic:			
	all:	tcp:	udp:	icmp:	other: all:	tcp:	udp:	icmp:	other: all:	tcp:	udp:	icmp:	other:
☑ noc	149.1 /s	29.3 /s	50.6 /s	69.2 /s	0 /s 393.2 /s	222.7 /s	52.2 /s	118.3 /s	0 /s 348.3 kb/s	226.4 kb/s	41.0 kb/s	80.9 kb/s	0 b/s
☑ rtr9	5.1 /s	1.7 /s	3.0 /s	0.4 /s	0 /s 17.5 /s	8.6 /s	3.0 /s	6.0 /s	0 /s 13.7 kb/s	7.4 kb/s	2.2 kb/s	4.1 kb/s	0 b/s

[All] [None] **Display:** ○ Sum ● Rate

Routers being monitored

Netflow Processing

Source: **Filter:**   **Options:**

noc   ○ List Flows ● Stat TopN
rtr9   **Top:** [10 ▼]
                                                       Stat: [Any IP Address ▼] order by [flows ▼]
                                                       Limit: ☐ [Packets ▼] [> ▼] [0] [- ▼]
[All Sources]   **Output:** ☐ / IPv6 long
                and [<none> ▼]

Extended Netflow processing options

[Clear Form] [process]

UNIVE...

Alerts and Stats

- Alerts Page
  - Can create alerts based on set thresholds eg, increase or decrease of traffic
  - Emails can be sent once alarm is triggered

- Stats page
  - Can create graphs based on specific information
    - ASNs,
    - Host/Destination IPs/Ports
    - In/Out interfaces
    - Among others

Plugins

- Several plugins available:
  - Portracker tracks the top 10 most active ports and displays a graph
  - Surfmap displays country based traffic based on a Geo-Locator

- More plugins available here
  - http://sourceforge.net/apps/trac/nfsen-plugins/
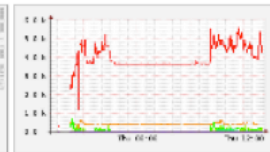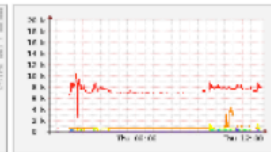
PortTracker
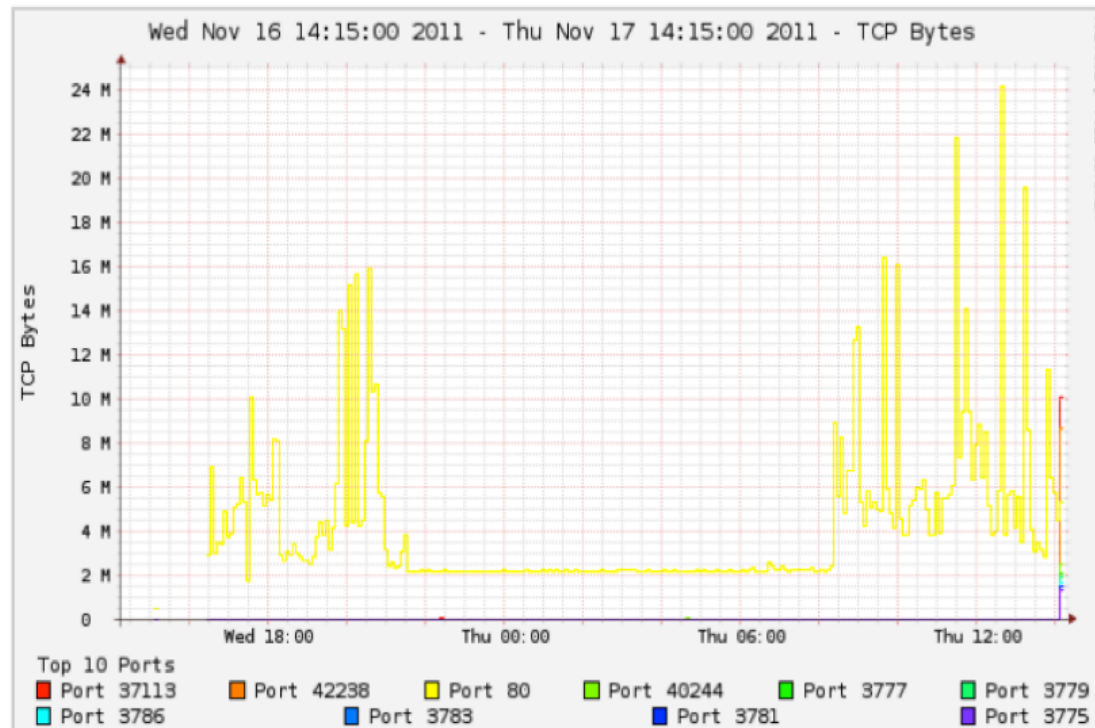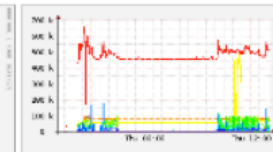
SurfMap

When to use NfSen

- Can be used for:
  - Forensic work: which hosts were active at a specific time
  - Viewing src/dst AS traffic, src/dst port/IP traffic among many other options
  - Identifying most active IPs or Protocols
- It is a tool to complement Cacti so that you can have more detailed info regarding the traffic
- With this information, you can make an informed decision eg:
  - You have a high amount of SMTP traffic, some machines could be sending out spam
  - 80% of your traffic is to ASN X. Perhaps its wise to connect directly with that network and save costs

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Bidirectional vs Unidirectional traffic as seen via NfSen

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Unidirectional and Bidirectional

- Unidirectional shows flows from host A to B and then host B to host A

- Bidirectional shows flows between Host A and B combined

- Can be used with any of the other filters (src port, src host plus many more)

- List of filters can be found here:
  - http://nfsen.sourceforge.net/#mozTocId652064

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Bidirectional

Unidirectional

References

- NfSen
  - http://nfsen.sourceforge.net

- NfDump
  - http://nfdump.sourceforge.net/

Questions?

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center