Ntop on Fedora Core 3 for Cisco Catalyst 6509 with Sup720

Tue Apr 19 11:03:19 PDT 2005
by Andrew Gristina
thanks to Luca Deri and the ntop team

This document specifically addresses a subset of interesting netflow export situations to an ntop netflow collector installed on Fedora Core 3 Linux.

Why ntop and netflow collection? There are many tools for gathering data for network troubleshooting. MRTG can monitor interfaces, bandwidth, and snmp counters such as CPU and memory usage. Nagios can monitor node availability. Syslog can give detailed information for troubleshooting. NBAR can help classify traffic. And network sniffing can give a very detailed profile of network traffic and captures are invaluable tools to help troubleshoot network problems. Netflow and Ntop can provide facets of several tools and can be implemented in situations where other tools can not reliably be used.

Ntop is excellent for summarizing netflow information. Ntop reports can give bandwidth summaries. Ntop can classify traffic and provide network profile. And Ntop can also allow you to get a detailed profile of network traffic. By using netflow, Ntop can help classify and profile network traffic on networks where spanning ports or sniffing may not be feasible due to scale or network architecture.

Installing ntop on a Fedora Core 3 Server

First, install ntop on a Fedora Core 3 server.

For ease of maintenance and installation, download the binary RPMs from Sourceforge:

```
http://sourceforge.net/project/showfiles.php?group_id=17233&package_id=
13248
```

The FC 2 RPMs will work on FC 3. Fedora should be binary compatible backward and forward one version (more than that and you are asking for trouble).

To install the rpm as root:

```
rpm –ivh ntop*
```

Then, copy the sample config to the location of the real config:

```
cp /etc/ntop.conf/sample /etc/ntop.conf
```

Edit the ntop.conf file.

If ntop is not capturing packets and is just being used as a netflow collector, change the interface listened on to none. Netflow only collection can help show the network traffic patterns when taps or spans aren't helping or available. Just copy the line "#? --interface none" and paste it in, then remove the "#?" that comments out the line:

```
––interface none
```

Next, change the "-m local subnets" to include the network addresses that ntop should regard as local. This example includes the 10.x.x.x network and multicast traffic as local:

```
–m 10.0.0.0/8,224.0.0.0/4
```

This should be all the changes needed to the config file. Check the config thoroughly to make sure it reflects the environment.

Before running ntop, setup the ntop admin user password. This password will be used for the web interface. Run the following command and follow the prompts:

```
/usr/bin/ntop –P /usr/share/ntop –u ntop –A
```

Document the password. Installation and initial configuration is now complete.

It is time to start ntop (these commands are Redhat/Fedora specific and may not be available on other linux variants):

```
/etc/init.d/ntop start
```

or

```
service ntop start
```

Next, make sure ntop starts at boot (these commands are Redhat/Fedora specific and may not be available on other linux variants):

```
chkconfig ntop on
```

If this succeeds, ntop is installed and running correctly. Check to see if the ntop web page is being served. Use a web browser to go to the ntop server's ip address or hostname and append port 3000 (if the port the webserver is listening is not 3000 in the configuration file, use the new port instead):

```
http://ntop.domain.local:3000
```

Configuring NTOP

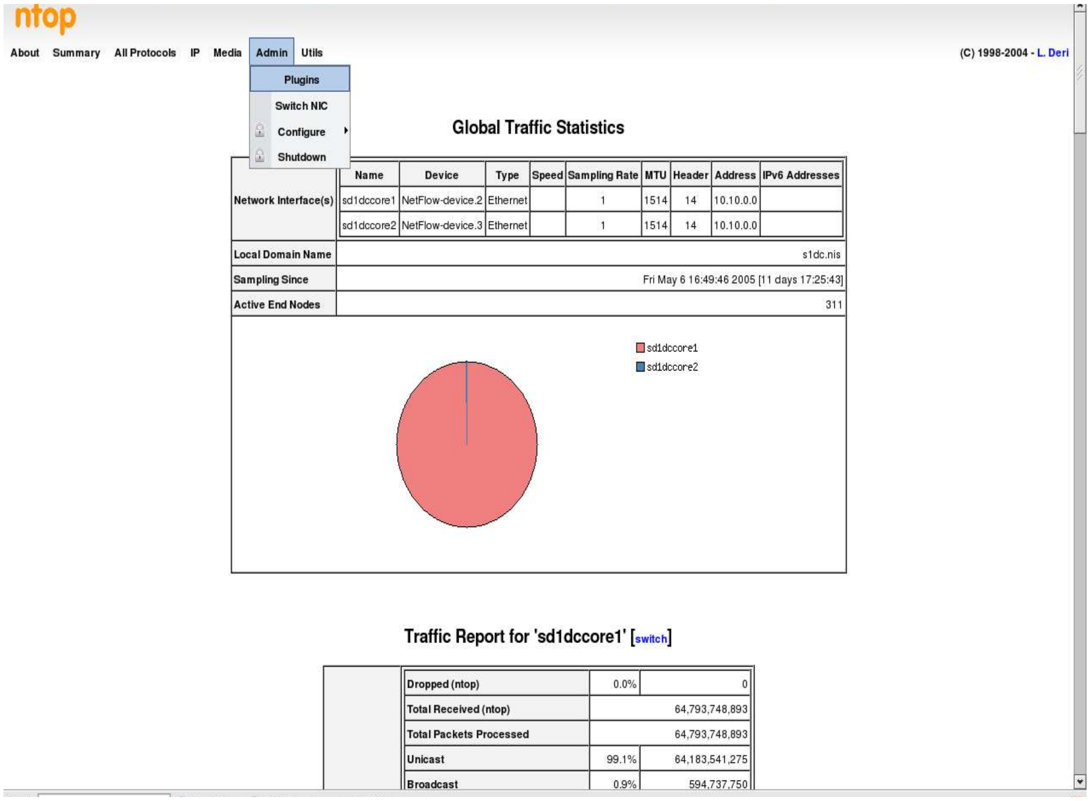
To configure ntop and netflow collection, use a web browser (firefox works) and connect to the ntop server:

```
http://ntop.domain.local:3000
```

As a pdf, this document includes pictures that will make it easier to understand than the text file version.

Click Admin: plugins (type in the web admin password).

Admin-plugins



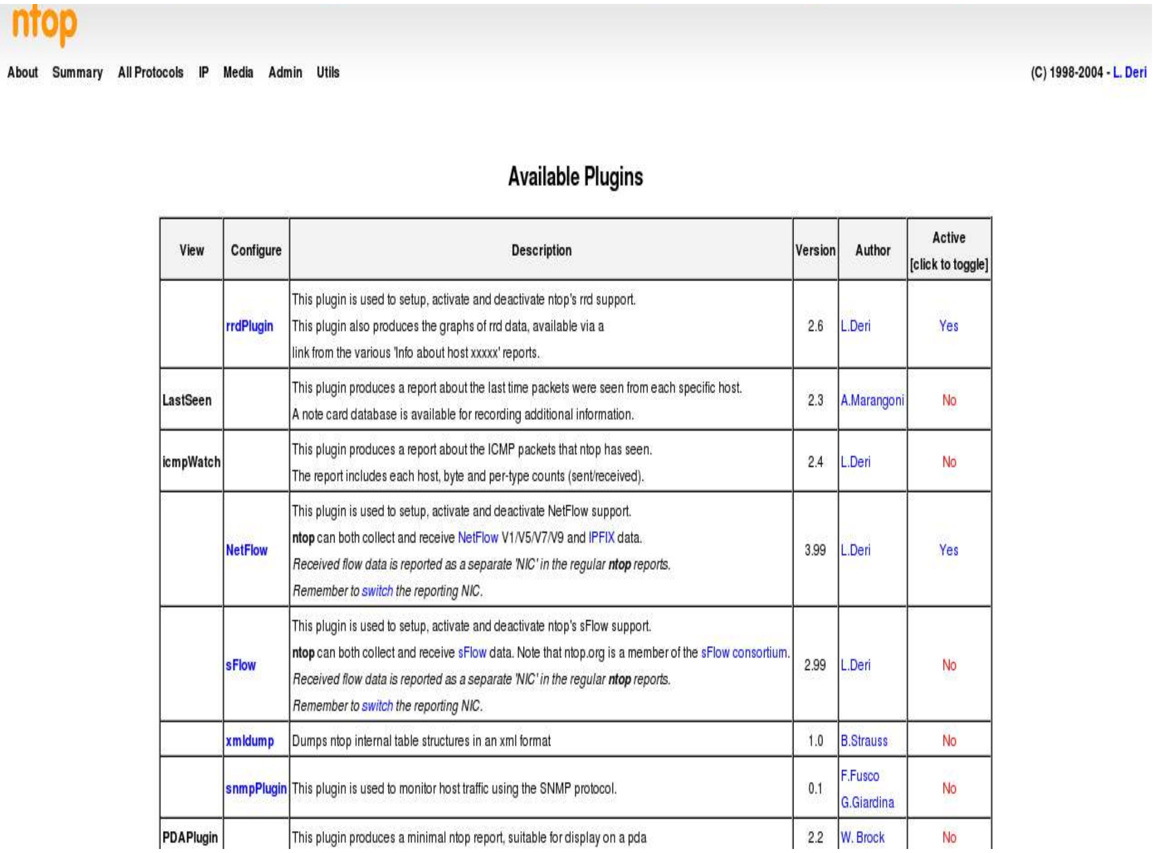
Global Traffic Statistics

	Name	Device	Type	Speed	Sampling Rate	MTU	Header	Address	IPv6 Addresses
Network Interface(s)	sd1dccore1	NetFlow-device.2	Ethernet		1	1514	14	10.10.0.0	
	sd1dccore2	NetFlow-device.3	Ethernet		1	1514	14	10.10.0.0	
Local Domain Name	s1dc.nis								
Sampling Since	Fri May 6 16:49:46 2005 [11 days 17:25:43]								
Active End Nodes	311								

Traffic Report for 'sd1dccore1' [switch]

Dropped (ntop)	0.0%	0
Total Received (ntop)		64,793,748,893
Total Packets Processed		64,793,748,893
Unicast	99.1%	64,183,541,275
Broadcast	0.9%	594,737,750

This should display the plugin page shown below:



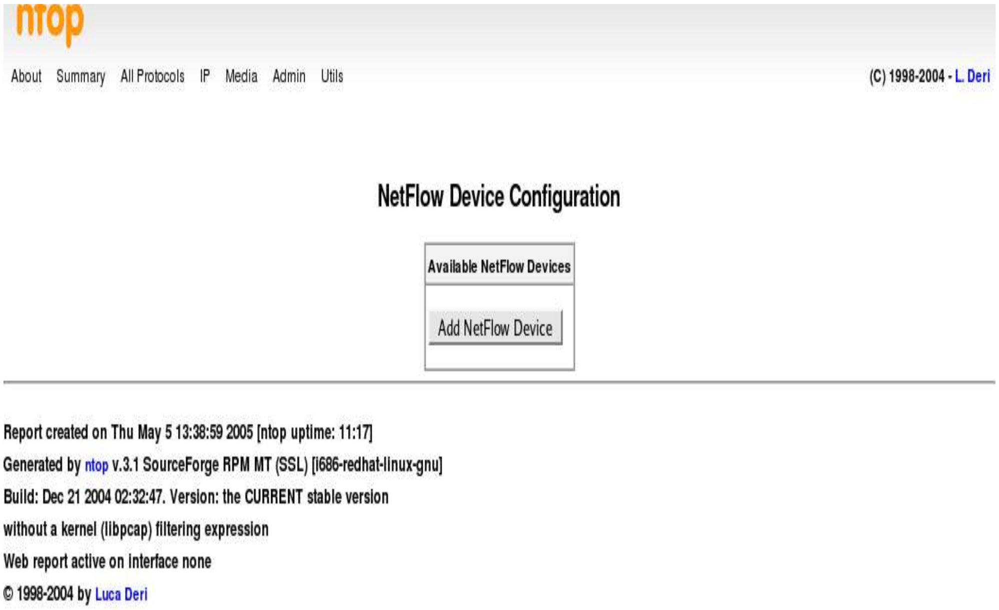
Available Plugins

View	Configure	Description	Version	Author	Active [click to toggle]
	rrdPlugin	This plugin is used to setup, activate and deactivate ntop's rrd support. This plugin also produces the graphs of rrd data, available via a link from the various 'Info about host xxxxx' reports.	2.6	L.Deri	Yes
LastSeen		This plugin produces a report about the last time packets were seen from each specific host. A note card database is available for recording additional information.	2.3	A.Marangoni	No
icmpWatch		This plugin produces a report about the ICMP packets that ntop has seen. The report includes each host, byte and per-type counts (sent/received).	2.4	L.Deri	No
	NetFlow	This plugin is used to setup, activate and deactivate NetFlow support. **ntop** can both collect and receive NetFlow V1/V5/V7/V9 and IPFIX data. *Received flow data is reported as a separate 'NIC' in the regular **ntop** reports.* *Remember to switch the reporting NIC.*	3.99	L.Deri	Yes
	sFlow	This plugin is used to setup, activate and deactivate ntop's sFlow support. **ntop** can both collect and receive sFlow data. Note that ntop.org is a member of the sFlow consortium. *Received flow data is reported as a separate 'NIC' in the regular **ntop** reports.* *Remember to switch the reporting NIC.*	2.99	L.Deri	No
	xmldump	Dumps ntop internal table structures in an xml format	1.0	B.Strauss	No
	snmpPlugin	This plugin is used to monitor host traffic using the SNMP protocol.	0.1	F.Fusco G.Giardina	No
PDAPlugin		This plugin produces a minimal ntop report, suitable for display on a pda	2.2	W. Brock	No

Then, in the column labeled “active click to toggle” where it meets the netflow row (where the second “yes” is in the figure above)- click the word “no” to toggle the plugin active. The screen should look like the picture above now and there should be a “Yes” in that square.

Then click netflow in the configure column.

This should display the following screen:



NetFlow Device Configuration

Report created on Thu May 5 13:38:59 2005 [ntop uptime: 11:17]
Generated by ntop v.3.1 SourceForge RPM MT (SSL) [i686-redhat-linux-gnu]
Build: Dec 21 2004 02:32:47. Version: the CURRENT stable version
without a kernel (libpcap) filtering expression
Web report active on interface none
© 1998-2004 by Luca Deri

On this screen, add a netflow device for each netflow router or switch. Click the button labeled “Add NetFlow Device” and then proceed to the following instructions.

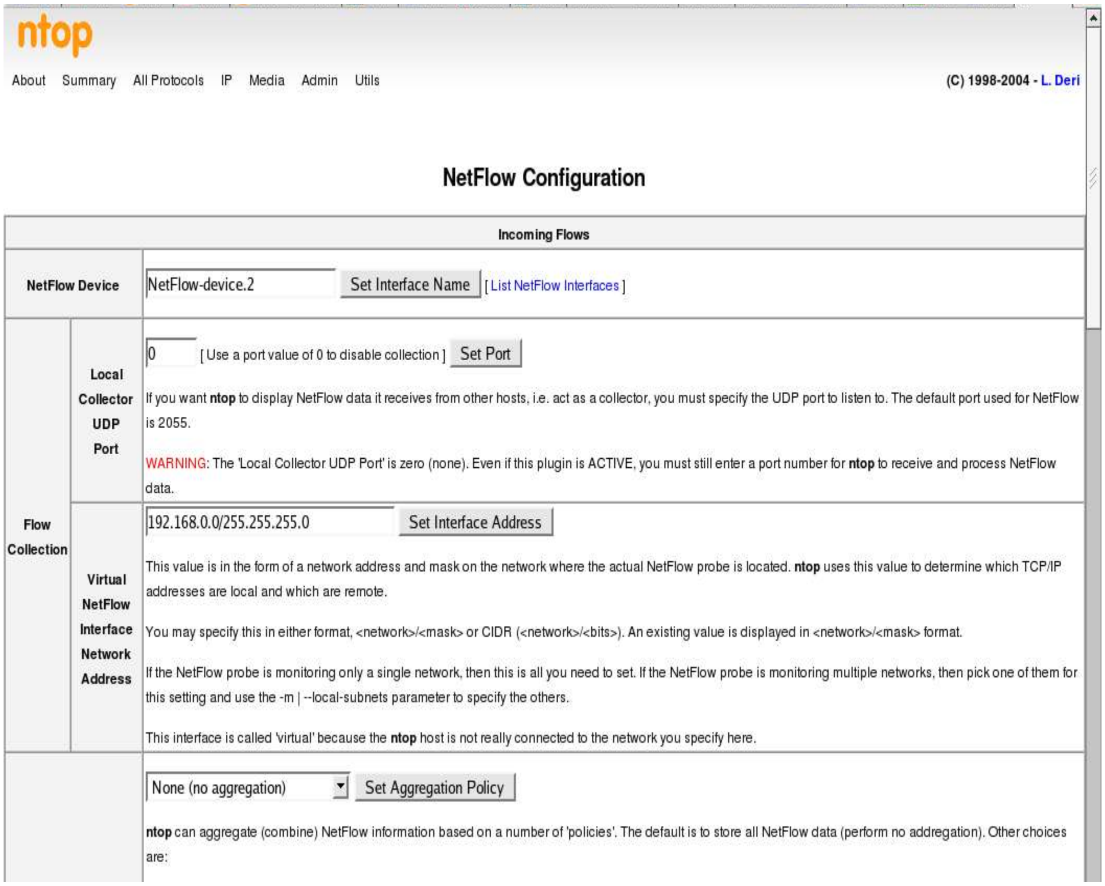
Fill in the following required fields. After filling in each field, click the set button following that field. If the set button is not clicked, that setting will be lost or not changed. Don't forget to click “set” after each field. The following are the minimum required fields:

Device: any useful name, the hostname of the netflow switch is recommended.

Port: 2055 is the normal netflow port, if there is only one device sending flows to ntop, use 2055. If you are having multiple devices that you want to keep separate, then use a different port for each one.

Netflow address: use the interface address, or just put in a subnet for what ntop should regard as local (192.168.1.0/24, 10.0.0.0/8 or whatever). This may be redundant with the -m in the config file.

The rest of the settings may need adjustment, but for a basic netflow collector, that is all that is needed. Example of configuring netflow plugin:



NetFlow Configuration

Incoming Flows		
NetFlow Device		NetFlow-device.2 [Set Interface Name] [List NetFlow Interfaces]
Flow Collection	Local Collector UDP Port	0 [Use a port value of 0 to disable collection] [Set Port] If you want **ntop** to display NetFlow data it receives from other hosts, i.e. act as a collector, you must specify the UDP port to listen to. The default port used for NetFlow is 2055. WARNING: The 'Local Collector UDP Port' is zero (none). Even if this plugin is ACTIVE, you must still enter a port number for **ntop** to receive and process NetFlow data.
	Virtual NetFlow Interface Network Address	192.168.0.0/255.255.255.0 [Set Interface Address] This value is in the form of a network address and mask on the network where the actual NetFlow probe is located. **ntop** uses this value to determine which TCP/IP addresses are local and which are remote. You may specify this in either format, <network>/<mask> or CIDR (<network>/<bits>). An existing value is displayed in <network>/<mask> format. If the NetFlow probe is monitoring only a single network, then this is all you need to set. If the NetFlow probe is monitoring multiple networks, then pick one of them for this setting and use the -m | --local-subnets parameter to specify the others. This interface is called 'virtual' because the **ntop** host is not really connected to the network you specify here.
		None (no aggregation) [Set Aggregation Policy] **ntop** can aggregate (combine) NetFlow information based on a number of 'policies'. The default is to store all NetFlow data (perform no addregation). Other choices are:

Cisco device configuration:

Check Cisco's latest document for the specific version IOS and hardware that netflow will be enabled on. Sup720 MSFCs are automatically in CEF mode. But to do netflow on other hardware such as routers, the equipment willl need to be in CEF mode. Here is a sample of configuration needed for a 6509 with sup720s:

```
ip flow-cache timeout active 5
ip flow-cache feature-accelerate
mls ip multicast flow-stat-timer 9
mls flow ip full
no mls flow ipv6
ip flow-export version 5
ip flow-export destination 10.10.10.10 2055
mls nde sender version 5
```

This will send flows to the ntop collector at 10.10.10.10 on port 2055. If a subset of the traffic is all that is required, use “mls flow ip ?” to display help on specifying subsets (not subnets). You can also limit netflow data to data from a certain interface:

```
int vlan 2
 ip route-cache flow
 mls netflow sampling
```

Router configuration:

On a router the NDE portion (network data export) is not needed. CEF however is required for netflow according to documentation for IOS 12.2 and 12.3. The following works on an 831 (and also on a 1750) running 12.2 train IOS:

```
ip cef
ip flow-cache timeout active 5
ip flow-export version 5
ip flow-export destination 10.10.10.10 2055
```

And then, if needed, turn netflow on the interface desired:

```
int s 0/0:0
ip route-cache flow

int fa 0/0
ip route-cache flow
```

If traffic is flowing through the devices, ntop should be reporting information. Check the webpage. If you have multiple netflow collectors, use the “Switch NIC” button to view the other collectors' statistics.

Confirmation and Troubleshooting

Once the netflow export is configured on the router or switch, test and verify that ntop is seeing flows correctly and that the server is receiving them. If ntop is not showing any data, verify receipt of the flow on the linux box. Assuming the netflow is going to port 2055, that is the default netflow port, you can use “tcpdump” to just show traffic to and from port 2055:

```
tcpdump udp port 2055
```

If “tcpdump” is installed, there should be plenty of data from the router or switch. If no data is shown, the netflow data is not reaching the linux box to be decoded. If you see data in the tcpdump output, but nothing in ntop, the netflow plugin is probably not configured properly, ntop is not running or you have an iptables/firewall blocking the traffic.

To check to see if ntop is running:

```
service ntop status
```

Then, make sure it is listening on the correct port :

```
netstat –an | grep 2055
```

Substitute any port you are sending to in place of 2055. It is beyond the scope of this document to troubleshoot iptables, but as a quick test disable the firewall if the security situation permits:

```
service iptables stop
```

or

```
/etc/init.d/iptables stop
```

Performance notes:

Monitoring gigabit networks with ntop (or monitoring on routers that are already cpu taxed) can cause performance issues on the network device and on the linux box. If you don't performance baseline your network equipment, it is a good idea to do so. Here are some easy steps to baseline just for the impact of ntop.

Run an application to measure performance like “top” on the linux box before you turn on ntop and again after you turn it on. Make some notes so you have a baseline for before and after. You can cause some CPU load on a box with too much netflow data going to it.

Likewise do a "show proc cpu hist" or “show proc” on the router (or similar) before and after turning netflow on. Make notes. Sending the netflow data takes a certain amount of CPU power and bandwidth, so baseline performance before and after starting it. Ignore these instructions if there already is a baseline for performance of the network equipment and linux boxes.

If ntop is using up too much ram and failing, which can happen when monitoring large networks or too many hosts (like keeping track of all internet connections), then tune the tracked hosts down by limiting tracking to local hosts (you can include non-local hosts in the local hosts statement to continue tracking interesting ip addresses).

In /etc/ntop.conf uncomment the line:

```
--track-local-hosts
```

Conclusion

Hopefully this guide helps implementation of netflow collection from Cisco IOS based products. Netflow can be an excellent tool for classifying and profiling networks. Ntop can help make sense of the netflow data, which can make troubleshooting and administration of a network easier.