# Network Flow Analyzer

Also known as ReporterAnalyzer

Using the NAST Tool

Presented by:
Stuart Weenig

CAIMGUC Communications Officer


NFA = Network Flow Analysis
pka: ReporterAnalyzer (or RA)


# NAST Tool = NFAParser

# Manual Method

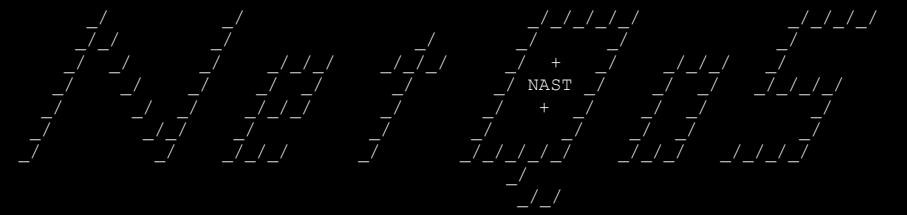
- Wireshark decode as CFLOW
- Find the v9 template (cflow.template_id) looking for:
  - IN_BYTES or 85 - IN_PERMANENT_BYTES
  - PROTOCOL
  - L4_SRC_PORT
  - IPV4_SRC_ADDR
  - INPUT_SNMP
  - L4_DST_PORT
  - IPV4_DST_ADDR
  - OUTPUT_SNMP
- https://communities.ca.com/docs/DOC-231149629

# Versions

| NFA Version | NAST/NFAParser Version |
|---|---|
| 9.1.3 & 9.2 | 13 |
| 9.1.2 | 11 |
| 9.0.161 | 10 |
| 9.0.118 | 9 |
| 8.3 or earlier | 8 |

# Usage

- Specify N minutes to analyze
- --batch = batch mode, requires N minutes as argument
- Outputs HTML file containing results




```
Type the number of NFA files (minutes) to process
Examples:
--> 1 = 1 minute
--> 10 = 10 minutes
--> 60 = 1 hour
--> 666 = 11 hours and 6 minutes
Additional options:[p|t|a|v|e]
--> p = output protocol stats
--> t = output ToS stats
--> a = output AS stats
--> v = verbose cmd output (doesn't change html
output)
--> e = external mode (not on a Harvester)
Tip: Just hit <Enter> to proceed using the default 5
minutes
```

Disclaimer - *FOR TROUBLESHOOTING PURPOSES ONLY*
Unlike Network Flow Analysis, NAST reports on raw netflow data as seen at the Harvester level.
The data presented in this report WILL NOT match the data in NFA.
Please do not compare the two.

# NAST v13 - CA Support

Time Span for this report: 2014-08-17 00:02:00 - 2014-08-17 00:12:00

10.00 Minutes | 7066761 Flows | 706676.10 Fpm | 4 Routers | 17 Total Interfaces

Routers in this report (number of active interfaces):

**10.210.160.1 - MRLAX01 (3)**
**10.251.248.1 - MRNYC01 (4)**
**10.130.195.1 - MRCHI01 (5)**
**10.130.196.1 - MRHOU01 (5)**

**The red list: Routers that may have incomplete flow data**
**(Some or all flows dropped by Harvester due to router reboot):**

10.173.254.248 ( 0 flows seen)
10.76.227.1 ( 16 flows seen)
10.253.10.133 ( 72 flows seen)
10.253.11.4 ( 79 flows seen)
10.253.119.3 ( 85 flows seen)

10.210.160.1 - MRLAX01:

Back to Top

| | | | | | |
|---|---|---|---|---|---|
| **Router Throughput:** | 52.70 GB | 702.62 Mbps | | | |
| **Router Flows:** | 359344 Flows | 35934 Fpm | | | |
| **Router Packets:** | 44 MPkts | 74.2 KPps | | | |
| Ifindex **4** bytes in: | 5.23 GB | 69.80 Mbps | 4126 Fpm | 6.8 KPps | |
| Ifindex **4** bytes out: | 7.76 GB | 103.41 Mbps | 4511 Fpm | 9.7 KPps | |
| Ifindex **339** bytes in: | 4.67 GB | 62.24 Mbps | 4782 Fpm | 6.9 KPps | |
| Ifindex **339** bytes out: | 6.32 GB | 84.26 Mbps | 4479 Fpm | 8.0 KPps | |
| TenGigabitEthernet1/7 (Ifindex **364**) bytes in: | 5.65 GB | 75.29 Mbps | 4212 Fpm | 11.0 KPps | 0.8 % |
| TenGigabitEthernet1/7 (Ifindex **364**) bytes out: | 8.96 GB | 119.49 Mbps | 4474 Fpm | 11.0 KPps | 1.2 % |

10.251.248.1 - MRNYC01:

**Unknown Netflow V9 Flow Set IDs detected - Parser couldn't read as many as 1574 flows due to missing netflow template(s).**

Back to Top

| | | | |
|---|---|---|---|
| **Router Throughput:** | 1.64 MB | 21.91 Kbps | |
| **Router Flows:** | 2818 Flows | 281 Fpm | (1244 V9 flows processed) |
| **Router Packets:** | 6 KPkts | 10.2 Pps | |
| Ifindex **243** bytes in: | 3.29 KB | 43.84 bps | 1 Fpm 0.1 Pps |

Routers sending flows during the sample period

Total Harvester Flow Rate

Number of interfaces detected

Routers that may have problems

Individual router & interface results

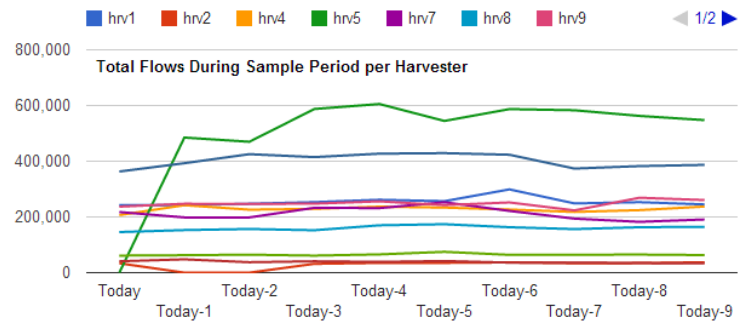
Possible v9 related errors

# The RED List: Possible Causes

- Bad SNMP response
- Bad sysUptime values in flows
- SEQ numbers out of order in flows
- v9 Template Missing
- Incorrect Netflow format (fields missing)

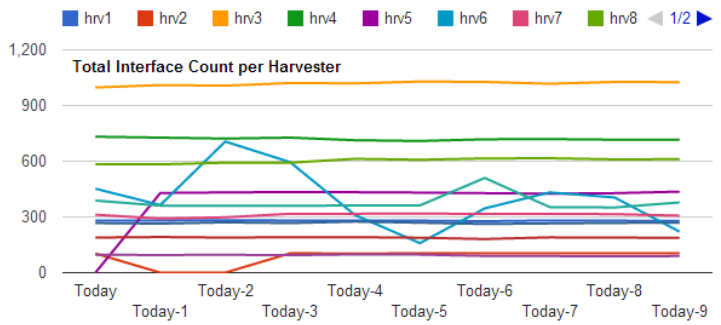
# Harvester 10 day Flow Count History

Show/Hide Data Table Export



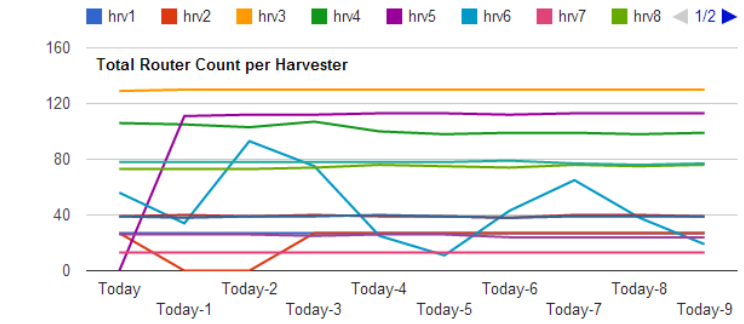

# Harvester 10 day Interface Count History

Show/Hide Data Table Export




# Harvester 10 day Router Count History

Show/Hide Data Table Export




# Top 5 Discarded Routers

View All

| Router | Flows discarded | Last Reported |
|---|---|---|
| 192.168.1.230 | 2207067 | 2014-08-18 00:02:00 |
| 192.168.1.234 | 1756460 | 2014-08-18 00:02:00 |
| 192.168.1.229 | 1754800 | 2014-08-18 00:02:00 |
| 10.0.7.1 | 1435720 | 2014-08-18 00:02:00 |
| 192.168.1.232 | 900616 | 2014-08-18 00:02:00 |

# Top 5 Inactive Routers

View All

| Router | Last Reported |
|---|---|
| 192.168.78.10 | 2014-08-18 00:05:00 |
| 192.168.133.252 | 2014-08-18 00:04:00 |
| 10.107.3.1 | 2014-08-18 00:04:00 |
| 172.20.3.1 | 2014-08-18 00:04:00 |
| 192.168.136.252 | 2014-08-18 00:04:00 |

# Resources (maintained by you)

- How To Enable NetFlow
  - https://communities.ca.com/docs/DOC-1061
- NAST Main Document
  - https://communities.ca.com/docs/DOC-231149079
- Verifying Netflow manually with Wireshark
  - https://communities.ca.com/docs/DOC-231149629

# Network Flow Analyzer

Also known as ReporterAnalyzer

Using the NAST Tool

Presented by:
Stuart Weenig

CAIMGUC Communications Officer

sweenig@gmail.com
http://stuart.weenig.com