nProbe: an Open Source NetFlow Probe for Gigabit Networks

Luca Deri
<deri@ntop.org>
NetFlow Traffic Monitoring

- Cisco NetFlow is a commercial standard for network monitoring and accounting.
- Many companies (e.g. Cisco, Juniper, Extreme) ship appliances with embedded NetFlow probes.
- Most commercial probes perform very poorly (~7-10’000 pkt/sec).
NetFlow: State of the Art [1/2]

• Several collectors available (both commercial and Open Source).
• Very little offering in the probe side.
• NetFlow monitoring cannot cope with Gbit speeds and above hence new mechanisms (e.g. sampled NetFlow) have been used to overcome this problem.
• sFlow, if more popular, could become a good alternative for high speeds and backbone monitoring.
NetFlow: State of the Art [2/2]

- NetFlow is supported only on high-end routers (no support or inability to use it on mid/low-end routers).
- Most people still rely on SNMP MIB II interface counters (no fine grained measurement at all).
- RMON is relatively used and difficult to both instrument and use.
Solution: nProbe+nTop [1/2]

• The community needed an open source probe able to bring NetFlow both into small and large networks.
• Ability to run at wire speed (at least until 1 Gb) with no need to sample traffic.
• Complete open source solution for both flow generation (nProbe) and collection (nTop)
Solution: nProbe+nTop [2/2]
nProbe: Main Features

- Ability to keep up with Gbit speeds on Ethernet networks handling thousand of packets per second without packet sampling on commodity hardware.
- Support for major OS including Unix, Windows and MacOS X.
- Resource (both CPU and memory) savvy, efficient, designed for environments with limited resources.
- Source code available under GNU GPL.
nProbe: Internals

• One thread captures packets, classifies, and stores them into a hash table
• A second thread periodically walks the table and emits expired flows.
• Static hash (dynamic hashes may loose packets during resize)
• No dynamic memory: everything is allocated at startup (no need to call malloc/free hence better performance).
nProbe: BGP Support

- NetFlow packets include information about ASs (Autonomous System) origin/peer.
- nProbe has no access to the BGP table (it is not running on a router).
- AS information is read from file.
- AS file can be produced reading the BGP table (e.g. via SNMP) from the local router or downloading it from public sites on the Internet.
nProbe: Performance [1/2]

• Tests performed using a traffic generator (Agilent RouterTester 900).

• nProbe run on a Dual Athlon, Intel Pro 1000 Gbit Ethernet card, GNU/Linux Debian 3.0, standard setup, no kernel tuning, Intel drivers (publicly available)
## nProbe: Performance [2/2]

<table>
<thead>
<tr>
<th>Packet Size</th>
<th>Network Load</th>
<th>nProbe Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>142 Mbit</td>
<td>277’340 packet/sec</td>
</tr>
<tr>
<td>64-1500 (random)</td>
<td>953.6 Mbit</td>
<td>152’430 packet/sec</td>
</tr>
</tbody>
</table>
Current Research Topics [1/2]

• nProbe-kernel: porting of nProbe into the Linux/BSD kernel for improving performance.
• nBox: Embedded nProbe-based appliance.
Current Research Topics [2/2]

• nFlow:
  – Security
  – Flow compression
  – MPLS/VLAN information
  – Payload information
  – Application/network performance.
Availability

• http://www.ntop.org/nProbe.html
• http://www.ntop.org/nBox.html
• http://www.nflow.org/