Passively Monitoring Networks at Gigabit Speeds Using Commodity Hardware and Open Source Software

Luca Deri
January 2003

Current Situation: Applications

- Most modern applications are bandwidth hungry (P2P).
- Exchanged files are getting large (from MP3 songs to movies).
- HTTP is no longer the most used protocol.
- End-users are exporting multimedia content.

Current Situation: Networks

- Most backbones are moving towards multi-Gbit networks (e.g. WDM, SDH).
- ATM is being replaced by MPLS-based networks (e.g. Gbit Ethernet on optical fibers).
- End-users are moving from 56K modems to ADSL lines.

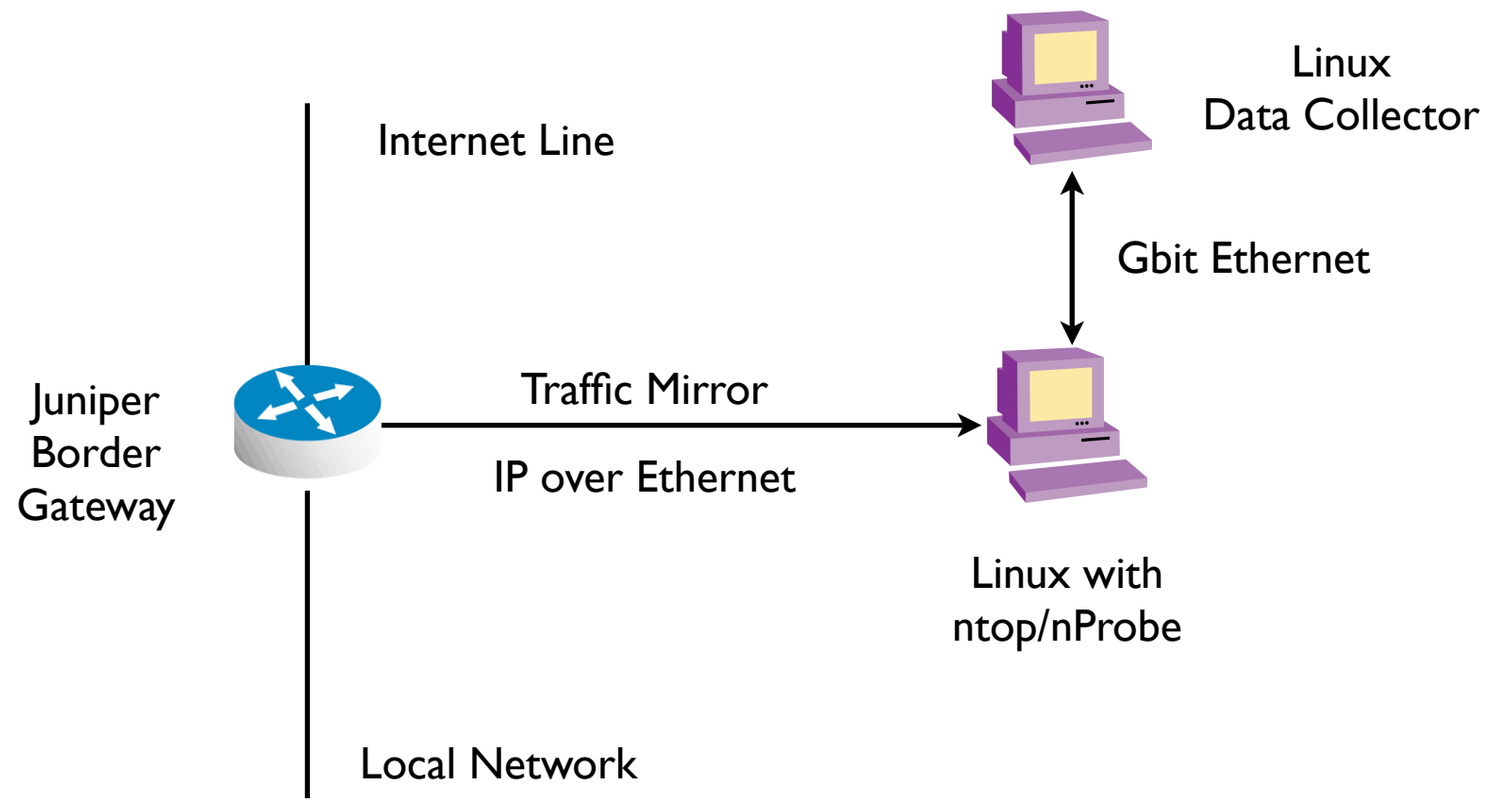
Current Situation: Network Management

- Most people still rely on SNMP MIB II and MRTG.
- Most NetFlow probes embedded on routers are not able to handle several thousand packets/sec.
- Slow, if any, major evolution of existing network monitoring tools.

Proposed Solution: Goals

- All hardware components must be available on the market at reasonable price.
- Software measurement applications must be open source or home grown.
- The architecture must be scalable and easily replicable on various environments.

Proposed Solution: Architecture



Proposed Solution: Motivation [1/3]

- Use the Juniper counters for accounting "easy to count" traffic (e.g. traffic volume), mirroring and filtering traffic (e.g. discard uninteresting packets).
- Use the PC for complex accounting (e.g. session tracking, attack detection, traffic matrix).

Proposed Solution: Motivation [2/3]

Juniper is used for:

- Natively mirroring traffic across different media.
- Filtering out “noise” traffic (e.g. non interesting protocols/networks) so less packets need to be analyzed by the Linux box.

Proposed Solution: Motivation [3/3]

The Linux box is used for:

- Running complex software that couldn't run on the Juniper (or that could significantly slow down the router).
- Be used both as a network probe and a collector for the Juniper-based counters.

Proposed Solution: Why Juniper? [1/2]

- Traffic filtering and accounting using a flexible configuration language.
- Ability to upload and run binary application on the switch.
- High performance filtering/mirroring implemented in ASIC.
- Accounting configurable via SNMP, CLI, and JunoScript (XML-RPC).

Proposed Solution: Why Juniper? [2/2]

- Cost savings: Junipers virtually cost nothing as they run the network and avoid the use of costly NPU-based cards.
- Monitoring Heterogeneous networks: mirror IP over ATM/Sonet networks on Gbit Ethernet.

Juniper-based Measurements [1/2]

- Spoofed packets (i.e. packets coming from the wrong interface).
- Traffic from/to suspicious ports (e.g. exec).
- Fragmented, broadcast (smurf) packets.
- Accounting of protocols using static (well-known) ports (e.g. http, smtp).

Juniper-based Measurements [2/2]

- Traffic on known DDoS-used ports.
- ICMP Traffic monitoring.
- Traffic on ports often used by trojans.
- Intra-AS, Internet traffic that should not be seen (e.g. DHCP, NetBIOS).

Proposed Solution: Linux PC

- Dual-CPU PC with 64 bit PCI Ethernet Gbit cards.
- Home grown software: ntop and nProbe (http://www.ntop.org/).
- Other Open Source Software: snort, Ethereal.

Linux-based Measurements

- RMON-like (top senders/receivers, protocols/IP distribution, traffic matrix).
- NetFlow-like (session tracking, duration, attempted connections, non-TCP/UDP/ ICMP protocol stats).
- Security (e.g. signature detection, ICMP traffic tracking, suspicious traffic detection).

Evaluation [1/2]

- Linux-based accounting works at Gb speeds and high packet rate (thousand packet/sec) if it's light (e.g. nProbe).
- Heavy monitoring software (e.g. ntop and SNORT) are not able to keep up at high packet rate.
- Preprocessing (e.g. nProbe exports preprocessed data to ntop) is a good way to run heavy software at high speeds.

Evaluation [2/2]

- Juniper-based accounting is very effective at Gbit speeds with no router performance degradation.
- Packet sampling can be used to reduce traffic on specific situations (e.g. under attack).
- Libpcap performance is not a bottleneck (instead application performance could be a problem).