The ntop Project: Open Source Network Monitoring

Luca Deri <deri@ntop.org>

Agenda

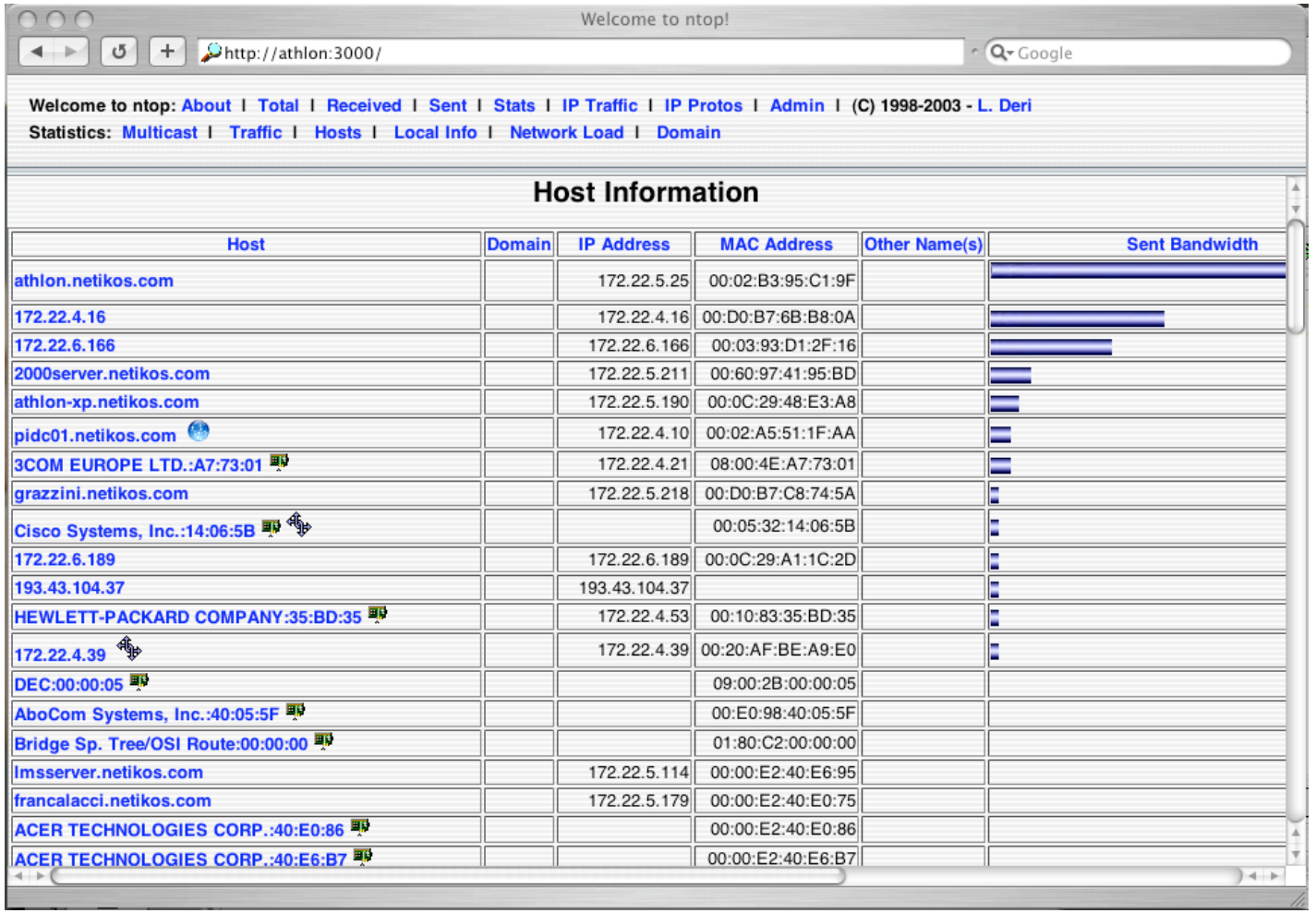
1. What can ntop do for me?
2. ntop and network security
3. Integration with commercial protocols
4. Embedding ntop
5. Work in progress

1. What can ntop do for me?

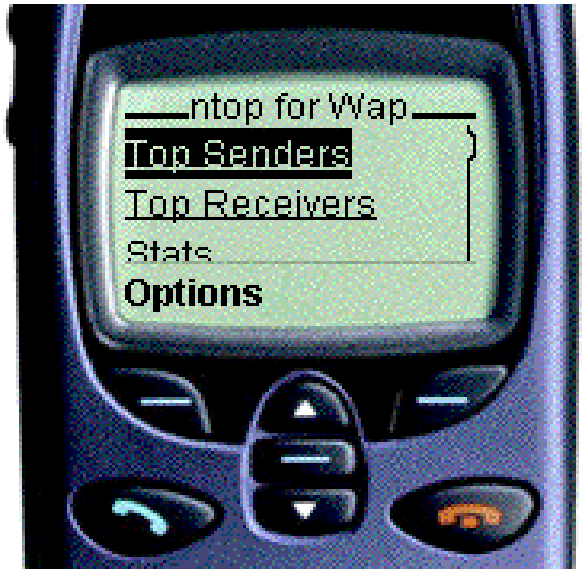
What's ntop ?

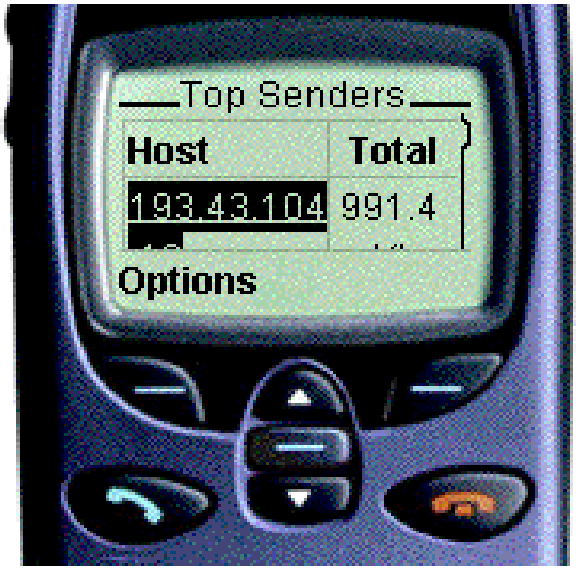
ntop is a simple, open source (GPL), portable traffic measurement and monitoring tool, which supports various management activities, including network optimization and planning, and detection of network security violations.

Welcome to ntop



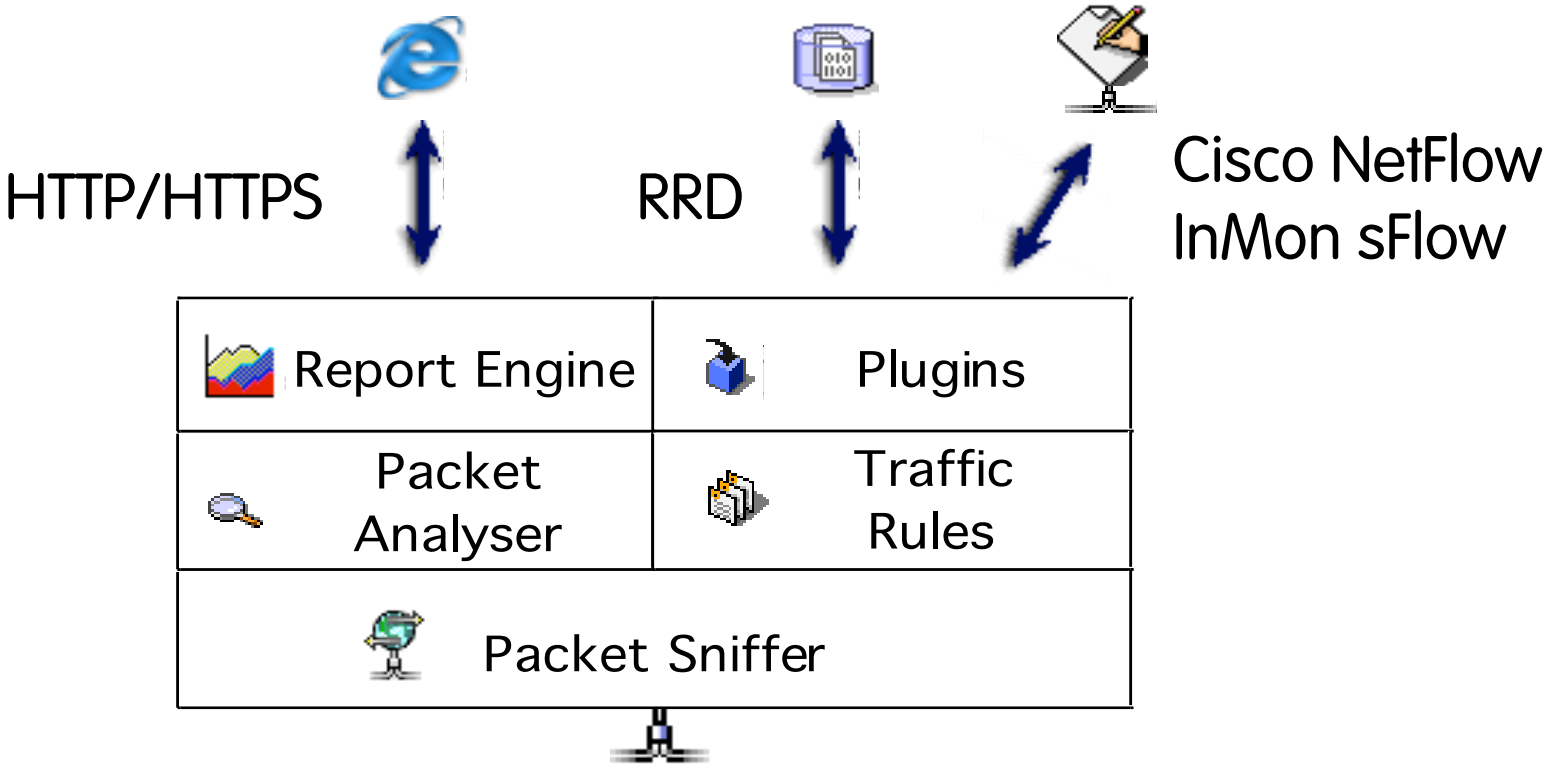
ntop for WAP


ntop for Wap
Top Senders
Top Receivers
Stats
Options


Top Senders
Host
Total
193.43.104
991.4
Options


Host 131.114.20.3
Name
ibook
Sent
312.5Kb

ntop Architecture



Network Management: Some Goals

- (No) Connectivity.
- Performance.
- Availability (Failure Detection).
- Responsiveness to Change and Growth.
- Inventory.
- Security.

What are the ntop Requirements ?

- Traffic measurement.
- Traffic characterisation and monitoring.
- Detection of network security violations.
- Network optimisation and planning.

What are the ntop Goals ?

- Fit end-user needs (no programming required).
- Easy to use and customize.
- Standard Interface (Web, SNMP).
- Open and Portable.
- Good performance and minimal resource requirements.

Traffic Measurement

- Data sent/received: Volume and packets, classified according to network/IP protocol.
- Multicast Traffic.
- TCP Session History.
- Bandwidth Measurement and Analysis.

Traffic Characterisation and Monitoring

- Network Flows
- Protocol utilisation (# req, peaks/storms, positive/negative repl.) and distribution.
- Network Traffic Matrix.
- ARP, ICMP Monitoring.

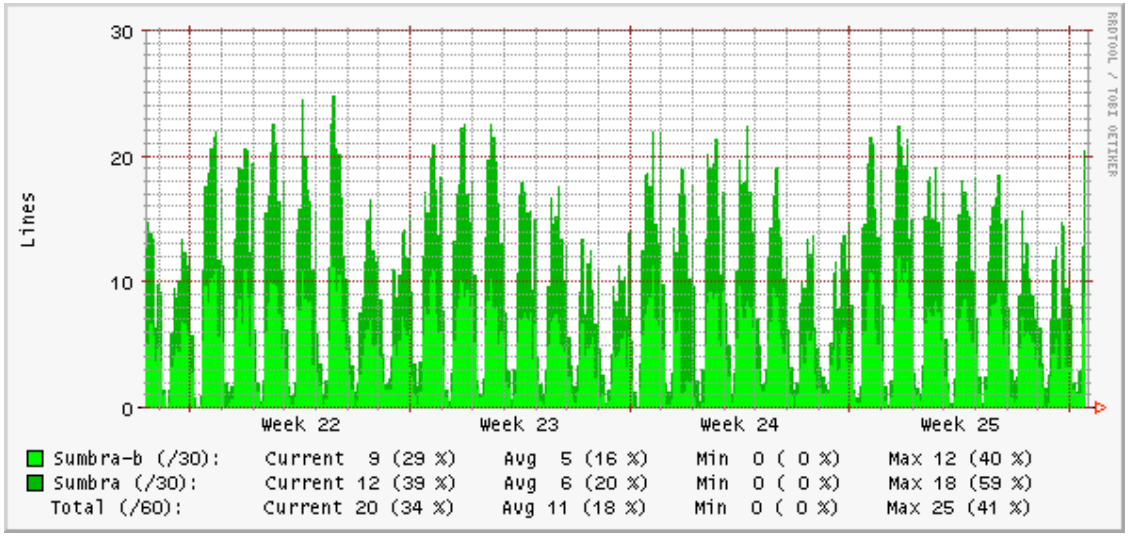
Network Optimisation and Planning

- Passive network mapping/inventory: identification of Routers and Internet Servers (DNS, Proxy).
- Traffic Distribution (Local vs. Remote).
- Service Mapping: service usage (DNS, Routing).

2. ntop and Network Security

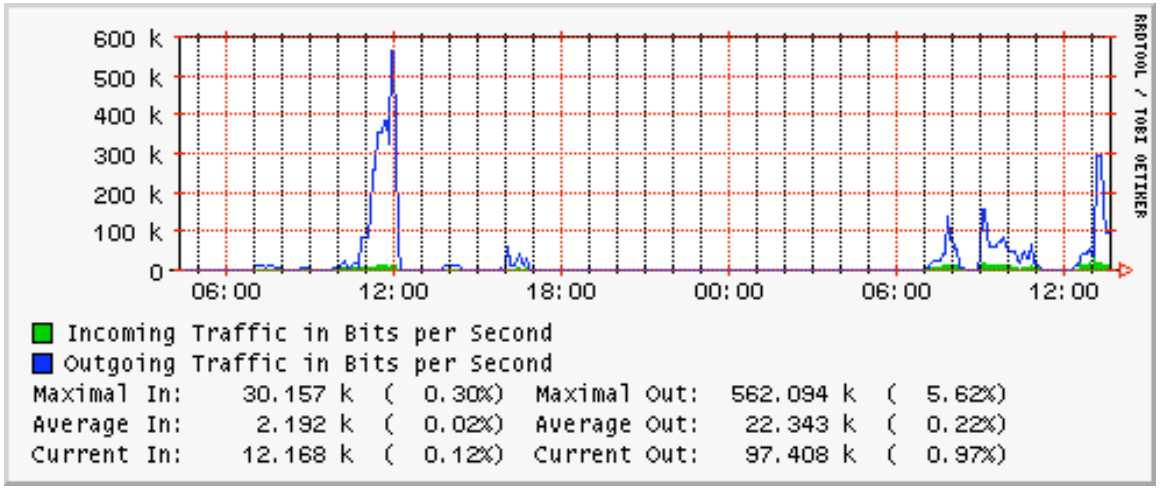
Defining a new Type of Anomaly Detection System [1/3]

- Various experiments performed on different networks confirmed the presence of some similarities on traffic.



Defining a new Type of Anomaly Detection System [2/3]

- Simple bytes/packets curves are not very reliable for detecting networks problems, as they can present some peaks caused by various reasons (e.g. a multicast transmission).



Defining a new Type of Anomaly Detection System [3/3]

The author decided to investigate whether it was possible to:

- Identify some selected traffic parameters that can be profitably used to model network traffic behaviour.
- Define traffic rules so that when such rules are violated there is necessarily a network anomaly (e.g. an abnormal network activity).

What is an Anomaly?

The deviation from the network's expected behaviour that is defined by considering two kinds of knowledge:

- IP protocol specifications contained in RFCs, that needs to be satisfied by every host and network (static knowledge).
- Statistical traffic analysis that varies according to network characteristics and type of users (dynamic knowledge).

ntop: Some Common Traffic Parameters

- ICMP ECHO request/response ratio
- ICMP Destination/Port Unreachable
- # SYN Pkts vs. # Active TCP Connections
- Suspicious packets (e.g. out of sequence)
- Fragments percentage
- Traffic from/to diagnostic ports (e.g. ident)
- TCP connections with no data exchanged

TCP/IP Stack Verification

- Network mapping: improper TCP three way handshaking (e.g. queso/nmap OS Detection).
- Portscan: stealth scanning, unexpected packets (e.g. SYN/FIN).
- DOS: synflood, invalid packets (ping of death, WinNuke), smurfing.
- IDS/Firewall elusion: overlapping fragments, unexpected SYN/ACK (sequence guessing).
- Intruders: peak of RST packets.

Intrusion Detection

- Trojan Horses (e.g. traffic at know ports BO2K).
- Spoofing: Local (more MAC addresses match the same IP address) and Remote (TTL Δ).
- Network discovery (via ICMP, ARP).
- Viruses: # host contacts in the last 5 minutes (warning: in this respect P2P apps behave as viruses/trojans!)

3. Integration with Commercial Network Monitoring Protocols

Cisco NetFlow

- Open standard for network traffic measurement defined by Cisco Systems
- Together with RMON (Remote MONitoring) is the industrial protocol for traffic measurement.
- Probes (usually on routers) send traffic flows (coded in NetFlow format) to collectors over UDP.

Why shall ntop support commercial network monitoring protocols?

- It is not always possible to capture traffic in the place we want (e.g. border gateway)
- Traffic reports used in industry are often trusted only if they are based on commercial products/protocols/probes
- Solution: let ntop be a NetFlow/sFlow probe and collector to ease its acceptance in the industry.

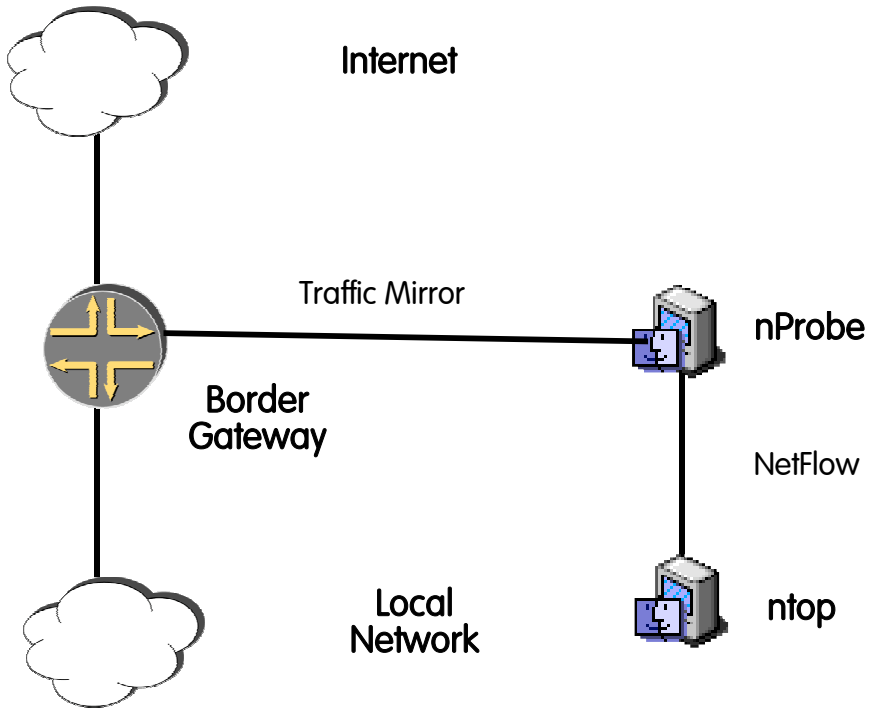
ntop: NetFlow and sFlow

- Currently ntop is able to collect/emit both NetFlow and sFlow flows.
- Due to ntop's original design, ntop is mostly a collector rather than a probe.
- Flows are very simple whereas ntop provides very complex statistics. Drawback: at high-speeds ntop looses packets due to all the calculations it has to perform.
- Solution: let an external probe feed ntop.

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 of NetFlow v5.
- 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: Performance

Packet Size	Network Load	nProbe Performance
64	142 Mbit	277'340 packet/sec
64-1500 (random)	953.6 Mbit	152'430 packet /sec

4. Embedding ntop

Why embedding ntop?

- In some cases it is easier to ship a simple appliance ready to use rather than provide a software application to install, configure, run.
- Modern embedded systems are based on OSs such as Linux, making easy the transition to them (no need to use proprietary/costly/ limited OSs such)
- Several manufacturers are selling cheap boxes suitable for this task.

nBox [1/2]

- Based on Cyclades TS/100 Appliance
- It runs nProbe 1.x
- Suitable for networks up to 10 Mbit of speed (e.g. xDSL, Frame Relay)

nBox [2/2]

- Easy configuration via the embedded web interface.
- Based on Linux/PPC
- Ability to export flows in NetFlow V5
- Ability to drive an LCD display

5. Work in Progress

nBox^3

- Embedded appliance based on a box with 3 Ethernet (1 GE+2x10/100 or 3x10/100)
- Ability to work in pass-through mode (bridge)
- Availability: September 2003.

nProbe 3.x

- Support of NetFlow v5/v9.
- Support of a new, open, flow format named nFlow (www.nflow.org)
- Ability to handle both IPv4 and IPv6 (NetFlow v9 only).
- Improved application performance with respect to current 2.x.
- Availability: snapshot at (www.ntop.org), final version (fall 2003)

Kernel-based nProbe

- Kernel traffic collector for improving performance (1 Gbit at full speed with 64 bytes packets and commodity hardware)
- Status: it currently runs on Linux 2.4.
- Availability: fall 2003 (with nProbe 3.x)
- Future Plans: port to FreeBSD based on NetGraph.

Wrap-up: ntop Availability

- Home Page: http://www.ntop.org/
- Platforms: Win32 and Unix.
- License: Gnu Public License (GPL).
- Distributions: Linux (Debian, Suse, RedHat, Slackware), BSD (MacOS X, OpenBSD, FreeBSD).