



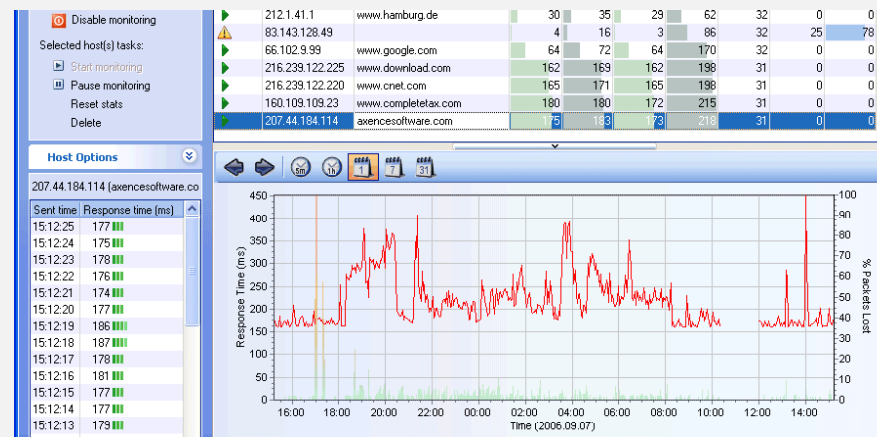
Network monitoring and IPv6 traffic information sharing via SNMP (pmacct, pmacct-snmp)

PSNC

Brussel, October 13th 2011

Implementing IPv6

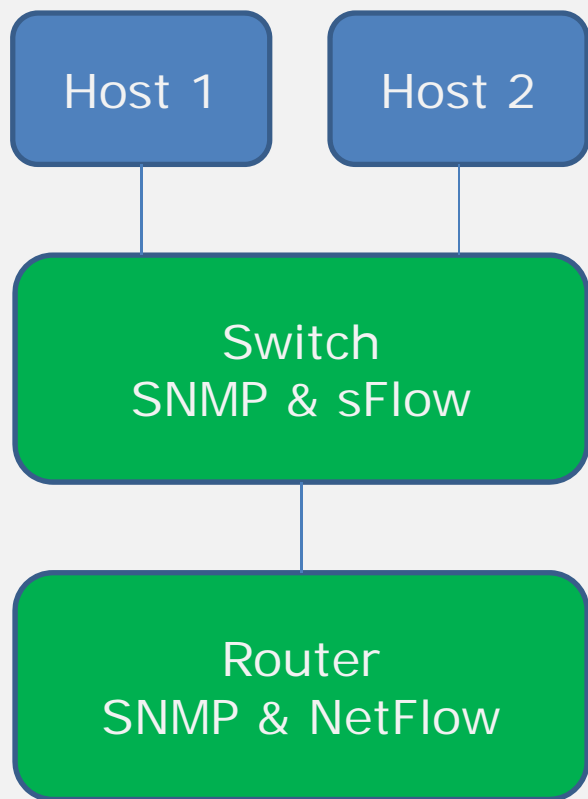
- Network monitoring:
 - Production networks have to be monitored and managed
 - Limitations of support for IPv6 in network management applications
 - Using SNMP for IPv6 could allow better and more effective network management and can cause popularization of IPv6



The Problem - Lack of Support for IPv6

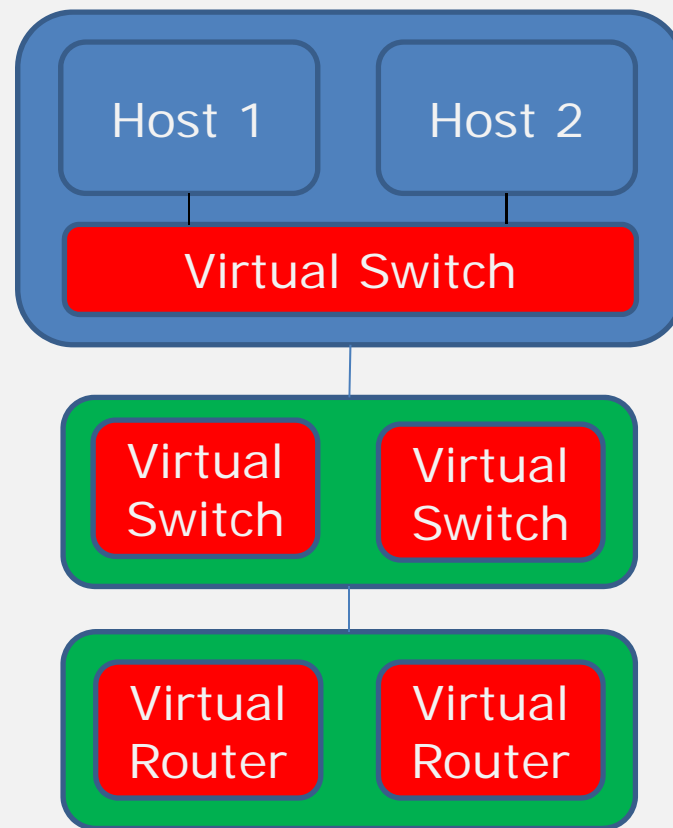
- Network management:
 - SNMP as currently the most popular network management protocol is used by many applications
 - Applications existing on the market provide only basic support for IPv6, many do not support it at all, eg:
 - CiscoWorks
 - HP OpenView

Real Environment vs Virtual Environment



Real

vs



Virtual

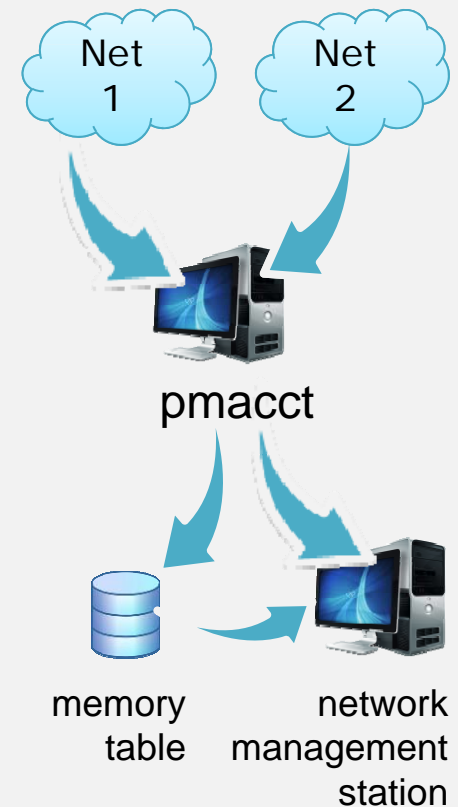
Proposed Solution

- Use pmacct and pmacct-snmp:
 - pmacct application is used to collect information about network and traffic aggregation and filtering of IPv6
 - Develop extension for Net-SNMP agent (pmacct-snmp) to support IPv6 traffic, adding the ability to support reports that contain network traffic data
- Profits:
 - possibility of reporting traffic information, both IPv4 and IPv6
 - ability to use tools that support so far only SNMP
 - detailed information about the network via SNMP

pmacct - Network Monitoring




● pmacct

- Set of passive network monitoring tools to measure, account, classify, aggregate and export IP traffic
- Support for both IPv4 and IPv6
- Collects data through libpcap, Netlink/ULOG, NetFlow v1/v5/v7/v8/v9, sFlow v2/v4/v5 and IPFIX
- Saves data to a number of backends including memory tables, MySQL, PostgreSQL, SQLite and BerkeleyDB
- Exports data to remote collectors through IPFIX, NetFlow v5/v9 and sFlow v5



pmacct - Advantages

Main advantages of pmacct:

- Runs on Linux , BSD , Solaris  and embedded systems
- Reports are created based on information such as VLAN, source and destination MAC addresses, hosts, networks, ASs, ports, IP protocol type field ToS / DSCP
- Supervises tunneled traffic
- It has easily extensible architecture that allows integration with other mechanisms
- Provides support for the packet sampling and its renormalization
- Open source (GNU GPL), actively developed

pmacct-snmp – Cooperation with SNMP

- pmacct-snmp:
 - Extension for Net-SNMP agent
 - Allows easy integration with information about IP traffic originating from pmacct
- The advantages of expanding the capabilities of SNMP pmacct
 - Information gathered can be used in many new applications
 - Generate summaries and graphs, on a specific network traffic
 - Notification of certain events
 - Create log files
 - Written in Perl
 - Created under open source license (GNU GPL)

pmacct-snmp

- The problem - lack of support IPv6 for pmacct-snmp - pmacct supports IPv6, but pmact-snmp does not
 - lack of support for the data obtained from pmacct
 - lack of support for configuration files

Work Progress

● Already done

- Preparing the hardware environment
- Installation and configuration software pmacct and extensions for SNMP agent - pmacct-snmp
- Testing the functionality of pmacct for IPv4 and IPv6 traffic
- Source Code Analysis pmacct-snmp (work in progress)
- Initial IPv6 support

Problem

- pmacct-snmp creates the branch for each IPv4 address within IP range
- how to solve it for IPv6 subnets? create a branch for each active IPv6 address? or summarize the traffic for the subnets?