Title:
6MoNPlus:Geographically distributed DualStack network monitoring

Authors:
Filippo Lauria, Claudio Porta, Andrea De Vita, Abraham Gebrehiwot, Alessandro Mancini

Author Affiliations: CNR - Instituto di Informatica e Telematica, Via G. Moruzzi 1, 56124, Pisa - Italy. Devision of "Telematic Network of CNR Pisa".

Keywords: Dual Stack (IPv4/IPv6), Geographically distributed Network Monitoring, Private Cloud, Network Address Translation traversal, real-time signaling protocol.

Abstract

Monitoring and controlling geographically distributed Dual Stack networks on the present Internet architecture is a complex task. The diffused use of Network Address Translation (NAT) and issues caused by border firewalls make remote network monitoring difficult. It is also necessary to physically be connected to the remote networks to sniff packets. There are several situations in which it is convenient to have an easy to use tool for monitoring and managing various networks, distributed in different locations, using a single management interface. This article is proposing a geographically distributed, scalable and extensible open tool for monitoring and controlling geographically distributed Dual Stack (IPv4/Ipv6) networks using a single management interface by solving the NAT traversal and firewall issues.

Using 6MoNPlus network administrators will be able to:

- *Detect, mitigate and notify rogue IPv6 router advertisements*
- *Monitor the network address utilization* by finding the associations between IPv4/IPv6/MAC/DUID/Username in a given range of time interval
- *Detect and notify the presence of unofficial DHCP servers*

The 6MoNPlus use a distributed architecture and is based on a back-end, a front-end and a DBMS.

The *back-end* is composed of a single central process called CORE and a number of geographically distributed processes called Probes. To install the tool in a private cloud, accessible from every location, the CORE and the front-end should be on a public Internet and may be installed in Virtual Machines while the Probes can be located behind NAT or firewall and should run on hardware based machines. The CORE, the DBMS, the front-end and the Probes can run on separate systems for scalability of the overall system. For a single and small network monitoring the overall system may be installed in a single hardware based machine. The CORE may use IPv4 or IPv6 protocols to communicate with the Probes. The communication between the CORE and the Probes uses a *control plane* and a *data plane* and is based on a finite state machine. The control plane uses a persistent TCP connection which is used for bidirectional signaling communication. It is used for controlling the functionalities of the Probes, the various modules running on the Probes and for event notification exchanges. The data plane is instead based on UDP protocol and is used to send Dual Stack network monitoring data from the Probes to the CORE. The Probes collects network monitoring data from remote sites, using specific modules, by listening various types of unicast, broadcast and multicast packets.

Broadcast and multicast packets are collected by putting the network interface of the Probes in a promiscuous mode and by listening both 802.1q tagged and non-tagged frames. The Probes also operate actively by sending requests to collect network monitoring data, such as SNMP requests and DHCP-Discover messages to detect the presence of a non official DHCP servers. Each monitoring module running on a Probe can be turned on/off separately by sending configuration commands from the front-end using the control plane. The back-end is developed using an efficient, flexible and low level C++ programing language and the overall libraries used for the development of 6MoNPlus are available for almost every Linux distribution.

The *front-end* is a web application used to configure and manage the overall functionalities of the CORE and the Probes. It provides a responsive GUI3 which allows to visualize the status of the CORE, the status of Probes and the status of each module running on the Probes. It is also used to visualize the remote network monitoring data collected by the Probes, by providing filters for custom searches, functions for address correlation and utilizzation, IPv4/IPv6 address management, DNS name lookup, MAC vendor lookup and a multi user management and configuration of the tool. The front-end is developed using both Django and Bootstrap WEB frameworks.

A working implementation of 6MoNPlus is used at the research Area of CNR of Pisa for monitoring and managing the whole campus Dual Stack network.

In this article we discuss the purpose and the internal logic of 6MoNPlus in details and show how it helps to monitor geographically distributed Dual Stack networks. We also show various measurement results and graphs to demonstrate the scalability and the efficiency of the 6MoNPlus by proving that we are able to monitor approximately 4000 Dual Stack active nodes using a single Probe installed on a low cost, credit card-sized single board computer such as Raspberry Pi.
As a future work, the proposed architecture will also being used for developing a framework for monitoring and controlling geographically distributed processes and objects. We are convinced that this communication framework will be useful for developing applications in the field of Internet of Things and Smart Cities.

This paper is an extension of our previous work [1] to which we have added many new features, with better algorithms to minimize both the processing power and the exchanged traffic between the distributed processes. The application have also been developed using an efficient and low level programing language in order to be able to run the various processes, particularly the Probes, on low power consumption and low cost computers such as Raspberry Pi.

6MoNPlus is developed by Devision of "Telematic Network of CNR Pisa" of Institute of Informatics and Telematics of CNR, Pisa - Italy.

Acknowledgements*:*

None

References:

1. *"6MON: Rogue IPV6 router advertisement detection and mitigation and IPV6 address utilization network monitoring tool"* presented on TERENA 2012 Networking Conference
2. RFC4861: Neighbor Discovery for IP version 6
3. RFC6104: Rogue IPv6 Router Advertisement Problem Statement

Author Biographies:

1. Filippo Lauria is a research fellow at the Institute of Informatics and Telematics of CNR in Pisa, Italy. He currently develops the back-end of 6MonPlus
2. Claudio Porta is a research fellow at the Institute of Informatics and Telematics of CNR in Pisa, Italy. He currently develops the front-end of 6MonPlus
3. Andrea De Vita is technician at the Institute of Informatics and Telematics of CNR in Pisa, Italy. He currently develops network monitoring tools and operates on multimedia cooperation applications.
4. Abraham Gebrehiwot is a technologist at the Institute of Informatics and Telematics of CNR in Pisa, Italy. He is the ***inventor of 6MoN*** and head of the division of "Telematics Network of CNR Pisa" and currently works on network management and developing of IPv6 network monitoring tools.
5. Alessandro Mancini is a technologist at the Institute of Informatics and Telematics of CNR in Pisa, Italy. He is currently involved in developing VoIP services and network management.