v6ops
Internet-Draft
Intended status: Informational
Expires: February 15, 2014

A. Servin
LACNIC
M. Rocha
Redes de Interconexion
Universitaria Asoc. Civil (ARIU)

August 14, 2013

Monitoring Dual Stack/IPv6-only Networks and Services
draft-ietf-v6ops-monitor-ds-ipv6-00

Abstract

This document describes a set of recommendations and guidelines to help operators to monitor dual stack and IPv6-only networks. The document describes how to monitor these networks using SNMP, Flow Analyzers and other means.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 15, 2014.

Table of Contents

1. Introduction 3
2. Network Monitoring 3
2.1. Transport vs. Data 3
2.2. Simple Network Management Protocol 4
2.3. Flow Analyzers 4
2.3.1. Netflow 4
2.3.2. Sflow 5
2.3.3. IPFIX 5
2.3.4. Network/Traffic Analyzers 5
2.4. Command line interface tools 5
2.5. Software Defined Networks 5
3. Addressing 6
4. Application Monitoring 6
4.1. Services 6
4.2. FQDN as connection discriminator 6
5. IPv6-Only Networks 7
6. Operational Challenges 7
7. Security Considerations 8
8. IANA Considerations 8
9. Acknowledgements 8
10. Informative References 8
Authors' Addresses 10

1. Introduction

Network and services monitoring become more important as we rely more on them for our critical operations. Depending of the complexity of our monitor solution we would be able to have more control and information from our network and services. Among other things, a good monitor solution allows to::

- Detect and avoid network incidents
- Determine which actions may solve a network incident
- Execute recovery and contingency plans

All these make sense when we monitor our network responsibly trying to cover all the variables. In the context of this memo, it means that we should monitor our services and networks running IPv6 as we have/had done in the IPv4 world..

There are many documents and guides explaining how to deploy IPv6 networks and services but there are so few that describe in detail how to monitor them. This document tries to encompass a set of recommendations and guidelines to help network and system administrators to monitor dual-stack/IPv6-only network and services.

2. Network Monitoring

In this section we describe SNMP and IPFIX as protocols able to manage IP devices and to monitor a variety of data from dual stack and IPv6-only networks. We also discuss traffic analyzers as other tools to monitor IP networks.

2.1. Transport vs. Data

It is important to understand the difference between IPv6 Transport vs. IPv6 data. In other words, protocols for monitor network infrastructure such as SNMP or IPFIX can send IPv6 collected data (e.g. the count of forwarded packets of an interface, flow information) using either IPv4 or IPv6 transport.

It is important to note that some node implementations would only send data (either IPv4 or IPv6) over IPv4 networks. Nevertheless these are implementation limitations not related to the monitoring protocol.

2.2. Simple Network Management Protocol

Simple Network Management Protocol (SNMP) defines the protocol suite to monitor and manage IP networks. SNMP works over UDP that allows it to work over IPv4 or IPv6 networks. However, the definitions that allow SNMP to collect data from IP devices know as "Management Information Base" (MIB) had to be modified from the original specifications. The most used versions of SNMP are Version 1 and Version 2 [RFC1441]. Version 3 is defined in [RFC3411].

SNMP MIB was defined in [RFC1156] and extended by [RFC1158]. Later it was modified by [RFC1213] in 1990 and in 1996 deprecated by RFCs [RFC2011], [RFC2012] and [RFC2013] that separated the MIB in IP, TCP and UDP. However all these modifications did not considered IPv6 yet. It was until [RFC2465] and [RFC2466] that MIB definitions were specified for IPv6 and ICMPv6. These RFCs described a dissociated definition for IPv4 and IPv6. The last MIB definitions came in 2006 when [RFC4292] (IP-Forwarding) and [RFC4293] (IP-MIB) defined an unified set of managed objects independent of the IP version.

Today there are many agent and collector implementations that support [RFC4292] and [RFC4293]. Nevertheless not all of them support them over IPv6 transport and IPv4 has to be used.

2.3. Flow Analyzers

Knowing the packet count that goes in and out from an interface it is very important but many times is not enough to detect faults or to get more detailed traffic information about the network. Netflow and IP Flow Information Export (IPFIX) [RFC5101] and [RFC5102] are protocols that monitor the IP flows passing through network devices. An IP flow is a sequence of packets identified by a common set of attributes such as IP Source Address, IP Destination Address, Source Port, Destination Port, Layer 3 protocol type, Class of service, etc.

2.3.1. Netflow

Netflow is a protocol developed by Cisco Systems and version 9 is described in the informational [RFC3594]. Other vendors have adopted equivalent technology such as Jflow (Juniper Networks), Cflowd (Alcatel-Lucent) and SFlow (sFlow.org consortium).

Netflow defines nine versions from which version 5 is the most common and only versions 9 and 10 support IPv6. Versions 9 and 10 are commonly known as the base of IPFIX. Although Netflow version 9 supports the collection of IPv6 flows, not all implementations of agents and collectors support IPv6 transport and IPv4 has to be used.

2.3.2. Sflow

Sflow is defined in [RFC3176] and it is very similar to netflow and IPFIX. It differs basically in the method to collect flow information. In the case of Sflow, it uses statistical packet-based sampling of switched flows and time-based sampling. The Sflow version described in [RFC3176] supports IPv4 and IPv6 address families.

2.3.3. IPFIX

IPFIX architecture and message format is defined in RFC5101 [RFC5101]and RFC5102 [RFC5102] defines its information model. From the operational standpoint of this document IPFIX and Netflow v9 are not very different and there is not much more to say besides that IPFIX as a relatively new protocol has not been widely implemented. For this reason finding an implementation supporting IPv6 transport may be hard to find.

2.3.4. Network/Traffic Analyzers

Besides SNMP and Flow analyzers IPv6 can be monitored using a variety of network/traffic analyzers. These devices come in a variety of flavors and some are open source or free and can be installed in commodity hardware, some other are expensive and run on specialized equipment. Commonly they are installed using promiscuous port that mirror all the network traffic or they are installed somewhere in the network where they can inspect most of the traffic.

Network/traffic analyzers are a quick way to inspect IPv6 traffic, however they may have scalability and privacy issues which make them unsuitable for large networks.

2.4. Command line interface tools

When SNMP and flow tools are not available in the network device and traffic analyzers are not suitable as a long term solution it may be possible to use in-house development or other tools to access networks devices and parse command line instructions that monitor IPv6 traffic. This solution could be used as well in IPv6 only networks when the device implementation does not support IPv6 transit to deliver monitoring data.

2.5. Software Defined Networks

TBD, In this section we will discuss the use of Software Defined Network (SDN) for the purposes of gathering data from the network.

3. Addressing

TBD. In this section we will discuss the implications to use of link-local, ULAs and Global Unicast Addresses for the purpose of monitor network infrastructure.

4. Application Monitoring

Beyond the traffic that goes through the network, network operators require to monitor other services such HTTP servers, email infrastructure, DNS, sensors, etc.

4.1. Services

Besides network information, network operators require to know other variables that could affect the good operation of the network. Dual stack networks pose an important challenge to network and system administrators. In principle we are talking about two different networks that may have different paths and users may perceive a difference in quality. Furthermore, thanks to Happy Eye Balls RFC6555 [RFC6555] that improves the user experience, service operators may have no idea to which protocol users are connected. This impose the need to monitor two networks and two set of services such as HTTP servers, email infrastructure, DNS, etc. to guarantee the service expectations from users.

In order to monitor service uptime and performance, it is common to use service probes that frequently poll a specific service to verify its reachability. Most of the time this probes are configured to access a service using a Fully Qualified Domain Name (FQDN) but sometimes literals are used as well.

To monitor services using FQDNs with A and AAAA records network/ system administrator must be aware that they do not have a guarantee that the probe is using IPv4 or IPv6 transport unless is forced to do so. Some tools provide configuration or execution flags to force the use of IPv4 or IPv6 transport. To guarantee a reliable monitoring strategy, we recommend using those flags to set up two monitor instances, one for each address family. Needless to say that in case of using literals instead of FQDNs, a new service monitor instance using an IPv6 address must be added.

4.2. FQDN as connection discriminator

We mentioned that one possible solution to discriminate between IPv4 and IPv6 services is to use some of the flags provided by the monitoring tool to force a connection either in IPv4 or IPv6.

Depending of the tool used, this option may not be always available. To address this restriction it is possible to use a special FQDN with only an A record to force an IPv4 connection and a different FQDN with only an AAAA record for IPv6.

For example suppose that the main organization website has the name www.example.com. The name www.example.com would have A and AAAA records as normally, however it would also contain an A record of the form www.v4-test.example.com pointing to its IPv4 address and an AAAA record www.v6-test.example.com point to the IPv6 address of the service. Other variants may be www.v6.example.com, www-v4.example.com, etc. As these FQDNs are meant to be only internally the selection of which to use is left to the network operator.

Bear in mind that using this alternative may introduce an extra overhead related to DNS management and should be used only when strictly necessary.

5. IPv6-Only Networks

The critical path to monitor IPv6 data on dual-stack networks is the device support of the IPv6 only MIBs ([RFC2465], [RFC2466], [RFC2452] and [RFC2454]), the unified MIBs ([RFC4293], [RFC4022], [RFC4113] and [RFC4292] or flow tools as Netflow 9 or IPFIX. As long as these protocols are supported, the device can be monitor using IPv4 or IPv6 transport. However, in IPv6-only networks supporting IPv6 data monitoring is not enough. In order to work it is critical for the device or collector to support the delivery or polling data using IPv6 transport.

For SNMP data there are a variety of agents and collectors that support IPv6 MIBs (IPv6 and Protocol Independent) using IPv6 transport. Nevertheless still exist devices that do not support neither IPv6 MIBs nor IPv6 transport of monitoring data.

With respect of flow tools, the authors of this document are aware of only a few implementations that support IPv6 transport.

6. Operational Challenges

Even though the end of IPv4 is near, there are still many network devices that cannot provide any type of IPv6 monitor data. In other cases the device can provide some sort of data through command line interfaces or in the best scenario through out the old IPv6 MIBs and using only IPv4 transit for delivery.

Still many network devices do not support to collect or send data related to IPv6. Also, some implementations are not widely tested and they may not support IPv6 monitoring correctly. For example, there were in the past cases where network devices did not correctly reported data collected from interface counters as they only counted packets that were process switched. Eventually this bug was fixed to include hardware-processed packets. It will still possible to find more of these types of bugs whilst IPv6 support mature. For that reason we recommend to network operators to always double check the IPv6 data retrieved from SNMP agents and interface counters at least for a short period of time. As the IPv6 support moves forward and matures, this practice would be less important in the future.

7. Security Considerations

From the security stand point, monitoring IPv4, IPv6 or Dual Stack networks is no different and the same preventions have to be taken. In order to protect SNMP agents, Network Monitoring Systems (NMS), flow collectors, network analyzers, etc. operators are advised to use a variety of methods such as access list, separate networks for management and monitoring, avoid the use of clear text access, etc.

8. IANA Considerations

None.

9. Acknowledgements

We would like to thank Humberto Galiza, Alejandro Acosta, Sofia Silva, Diego Lopez, Ariel Weher, and Christian O'Flaherty for their questions, suggestions, reviews and comments. Also we would like to thank the LACNOG community for the informal comments that gave us during the meetings.

10. Informative References

[RFC1156] McCloghrie, K. and M. Rose, "Management Information Base for network management of TCP/IP-based internets", RFC 1156, May 1990.

[RFC1158] Rose, M., "Management Information Base for network management of TCP/IP-based internets: MIB-II", RFC 1158, May 1990.

[RFC1213] McCloghrie, K. and M. Rose, "Management Information Base for Network Management of TCP/IP-based internets:MIB-II", STD 17, RFC 1213, March 1991.

[RFC1441] Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Introduction to version 2 of the Internet-standard Network Management Framework", RFC 1441, April 1993.

[RFC2011] McCloghrie, K., "SNMPv2 Management Information Base for the Internet Protocol using SMIv2", RFC 2011, November 1996.

[RFC2012] McCloghrie, K., "SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2", RFC 2012, November 1996.

[RFC2013] McCloghrie, K., "SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2", RFC 2013, November 1996.

[RFC2452] Daniele, M., "IP Version 6 Management Information Base for the Transmission Control Protocol", RFC 2452, December 1998.

[RFC2454] Daniele, M., "IP Version 6 Management Information Base for the User Datagram Protocol", RFC 2454, December 1998.

[RFC2465] Haskin, D. and S. Onishi, "Management Information Base for IP Version 6: Textual Conventions and General Group", RFC 2465, December 1998.

[RFC2466] Haskin, D. and S. Onishi, "Management Information Base for IP Version 6: ICMPv6 Group", RFC 2466, December 1998.

[RFC3176] Phaal, P., Panchen, S., and N. McKee, "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks", RFC 3176, September 2001.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3594] Duffy, P., "PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option", RFC 3594, September 2003.

[RFC4022] Raghunarayan, R., "Management Information Base for the

Transmission Control Protocol (TCP)", RFC 4022, March 2005.

[RFC4113] Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)", RFC 4113, June 2005.

[RFC4292] Haberman, B., "IP Forwarding Table MIB", RFC 4292, April 2006.

[RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.

[RFC5101] Claise, B., "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information", RFC 5101, January 2008.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, April 2012.

Authors' Addresses

Arturo Servin
LACNIC
Rambla Republica de Mexico 6125
Montevideo 11300
Uruguay

Phone: +598 2604 2222
Email: aservin@lacnic.net

Mariela Rocha
Redes de Interconexion Universitaria Asoc. Civil (ARIU)
Maipu 645 - 4to Piso
Buenos Aires
Argentina

Email: mrocha@riu.edu.ar