Practical IPv6 Monitoring–Challenges and Techniques

Matěj Grégr, Petr Matoušek, Miroslav Švéda
Brno University of Technology
Faculty of Information Technology
Božetěchova 2, 612 66 Brno, Czech republic
Email: igregr,matousp,sveda@fit.vutbr.cz

Tomáš Podermański
Brno University of Technology
Center of Computer and Information Services
Antonínská 1, 601 90 Brno, Czech republic
Email: tpoder@cis.vutbr.cz

***Abstract*—Network monitoring is an essential task of network management. Information obtained by monitoring devices gives a real picture of the network in production including transmitted data volumes, top hosts, a list of frequently used applications etc. Deep analysis of data collected by monitoring can reveal network attacks or detect misuse of network services. In addition, Data Retention Act requires each ISP to track user's activities. Protocol IPv6 puts new challenges for network administrators in the context of user identification. Unlike IPv4, an IPv6 address no longer uniquely identifies a user or PC. IPv6 address can be randomly generated and keeps changing in time. PCs with IPv6 stack can also communicate via predefined tunnels over IPv4 infrastructure. That tunneled traffic mostly bypasses network security implemented via firewalls. In this paper, we identify major monitoring and security issues of IPv6 connectivity and propose a solution based on SNMP and Netflow data that helps to uniquely identify users. The solution requires an extended set of monitoring data to be collected from network devices. We present a new data structure based on extended Netflow records. Feasibility of the approach is demonstrated on the Brno University of Technology (BUT) campus network.**

***Index Terms*—IPv6 monitoring, network security, IPv6 deployment, Netflow, SNMP, IPv6 data retention**

I. Introduction

The IPv6, a new version of the fundamental Internet Protocol, has been mainly developed to provide a larger address space. Today, the Internet is actively deploying not only IPv4, but also IPv6. IPv6 support is available for operating systems such as Unix, Mac OS, or Windows. Moreover, such operating systems as Windows 7 and Vista not only support IPv6, but also provide IPv6 connection by default. This fact exposes network users and organizations to additional vulnerabilities. Auto-configuration of IPv6 addresses creates a new challenge for network administrators. A host in a LAN cannot be easily identified by its IP address since there are several temporary IPv6 addresses in use. Unfortunately, many users are not aware of such intricacy. They unconsciously violate implemented security policy when they bypass standard IPv4 firewall rules and standard IPv4 addressing policy.

Traditional monitoring approaches are usually not applicable to IPv6 traffic because of temporary addresses, different types of encapsulation of IPv6 over IPv4, non-unique mapping between data link addresses and IP addresses, tunneling, etc.

So, new techniques using current tools need to be deployed. This paper shows current monitoring issues of IPv6 traffic and practical approaches how to solve these issues on the case as implemented at the BUT network.

Another challenge of IPv6 monitoring is tunneling IPv6 over IPv4. Tunnels encapsulate application data into tunneling protocols that have different IP headers and ports so the packets can bypass firewall rules. A real transition to the native IPv6 may last for months or years, so monitoring of tunneled traffic is actually required in order to detect stations that can be potentially sources of uncontrolled user traffic.

The paper describes an architecture of IPv4 and IPv6 monitoring and shows how user activities in IPv6 network can be identified and registered even when using temporary IPv6 addresses or tunneled connection. The proposed monitoring system can be generally deployed over both the IPv4 and IPv6 environment.

II. State-of-the-art

There are just few papers or studies discussing practical monitoring issues of IPv6 protocol like uniqueness of the IPv6 addressing, tunneling issues, etc. The very good overview of key security issues and challenges is given by [1] and [5]. Authors in [1] discuss IPv6 security challenges in comparison with IPv4 threats. They list autoconfiguration, DoS attacks on Neighbor Discovery (ND) protocol, and difficulties with packet filtering. Their approach is focused more on overview of security rather than on monitoring and tracking of user activities. The report [5] by NIST seems to be the most complex study of IPv6 security aspects in practical deployment with hints for network administrators. The report covers a wide area of IPv6 including security issues, tunneling, translation and new protocols. The report summarizes various techniques and hints for secure IPv6 deployment. However, several presented techniques like Secure ND (SEND) are not implemented yet. In our paper we focus on practical implementation of IPv6 monitoring with emphasis on identification of user behavior.

There are also several academic papers that deal with IPv6 monitoring. In [7], a novel architecture of IPv6 monitoring using SNMP is introduced. Authors propose monitoring data to be inserted and transmitted into IPv6 headers of a packet along the path. These information will be later processed on border routers. The approach brings an interesting idea,

978-1-4244-9220-6/11/$26.00 ©2011 IEEE

however it puts enormous additional computational effort on every router on the path which is definitely unfeasible for large networks. In [13] authors give only basic description of security issues of IPv6 while their monitoring is limited to three nodes using nmap tool. This approach cannot be applied for long-term monitoring of high volume transmission lines nor for gathering data about users connections.

These papers discuss security and monitoring issues in IPv6 networks. To our best knowledge we are not aware of the document comprising practical IPv6 monitoring like user identification and accounting in IPv6 networks which is nowadays a big problem for ISPs. This paper tries to cover this field omitted in other documents.

III. Contribution

Contribution of the paper includes two parts. At first, two major IPv6 monitoring issues from administrator's point of view are proposed: (i) automatically created tunnels of IPv6 traffic over IPv4 network that bypass standard security techniques, and (ii) randomly generated IPv6 addresses with temporary validity. In comparison with [1] or [5], practical experiences with IPv6 security implementation within current operation systems is presented.

In the second part of the paper (section V), we show what kind of information is needed for successful identification of an user in IPv4/IPv6 network and how these data can be obtained from active network devices using combination of ARP entries, SNMP data, Netflow records and Radius logs. Such further description was not given in any other work we observed. Based on this data, the proposed solution was implemented and deployed in the campus backbone network at Brno University of Technology (BUT). Current results prove that the proposed technique is viable in large networks and covers most of discussed security requirements of IPv6. In addition, the solution is independent on network topology or protocols and can be deployed in any network. Input data for the monitoring system are well described by open standards SNMP, ARP, or Netflow and can be easily obtained from active network devices.

IV. IPv6 Monitoring Issues

This section describes major monitoring issues enforced by IPv6 connectivity. From point of view of network management, IPv6 configured hosts on the IPv4 network can bypass defined security policy or hide their identity using temporary IPv6 addresses. These practical security issues has been the main motivation for the proposed solution presented later.

A. Tunneling IPv6 over IPv4

Tunneling is a transition technique [10] that connects IPv6 sites over IPv4 infrastructure. Routers, firewall, and security devices at the edge of the enterprise network may not be technically capable of inspecting IPv6 payload encapsulated within IPv4 packets entering or exiting the network. Three tunneling approaches are frequently applied—6to4 tunnels [2], Teredo [8], and ISATAP [4] . All these three tunneling mechanisms are enabled on Windows 7 and Vista by default. Thus, IPv4 can tunnel IPv6 traffic without security controls which can violate normal access control filtering. Problems with tunneling in IPv6 can be seen as similar to VPN tunneling in IPv4. However there are some differences. VPN are in generall used to connect a user from the Internet to his corporate network. Login and password are usually needed and endpoint of the tunnel is under control of network administrator. On the other hand IPv6 tunnels are created from inside the network to connect to the public Internet. It means that many devices which would be normally hidden and protected can be reachable on the network through public IPv6 address assigned by tunnel mechanism. IPv6 tunnels are also created automaticaly without user invention while VPNs have to be usually configured manually. An example how tunnels allow unauthorized use of service. Imagine border router blocking all outgoing SMTP traffic because of SPAM prevention. Only traffic from authorized SMTP servers are allowed to pass. Because the firewall does not inspect payload of tunneled packets like 6to4 or Teredo, host can distribute spam encapsulated in packets of protocol 41 (i.e., 6to4 tunnel) or UDP (i.e. Teredo tunnel).

B. IPv6 Addressing Issues

Temporary IPv6 Addresses Autoconfiguration is a new IPv6 feature that lets a node automatically generate an IPv6 address on its own.

Because of user privacy, IPv6 addresses with randomly generated 64-bits interface identifiers (so called privacy addresses) are preferred instead of EUI-64 identifier. Standard RFC 4941 [9] defines how to generate and change temporary addresses. The important requirement is that the sequence of temporary generated addresses on the interface must be totally unpredictable.

However, this requirement is in contradiction with the need of identification of the malevolent user. Private temporary addresses disrupt unique identification of a user/host connecting to a service as it was common for IPv4. This affects logging and prevents administrators from proper tracking what users are accessing which services.

Current implementation in Windows system enables Privacy extensions by default. Example: IPv6 address assigned to a host is eg. 2001:718:802:c0b1::1. Host has Privacy extension enabled so generates randomly address eg. 2001:718:802:c0b1:a197:8afe:5fe2:5106 and this is used for communication instead of assigned 2001:718:802:c0b1::1. The address is temporary so after several hours, a new random address is generated.

V. Integrated System for IPv6 Monitoring

This section describes how above discussed issues of IPv4 and IPv6 monitoring can be solved. The solution is presented on the case study of BUT campus network. The BUT campus network includes hundreds active devices on the backbone and thousands of connected users, mostly students. We will present what data and data sources are needed for monitoring and how they can be obtained. Preliminary results and statistics about IPv4 and IPv6 traffic are given at the end of this section.

A. Monitoring at IPv4 Networks

Today, ISPs identify their hosts based on the host's IPv4 addresses. Usually the ISP has a central Network Management System (NMS) that collects network statistics including a list of users with registered IPv4 and MAC addresses. MAC address is used in DHCP configuration to assign a corresponding IPv4 address. Registered MAC addresses together with system logs of DHCPv4 server and data from Radius server are sufficient enough to uniquely identify the user based on the IPv4 address.

B. Administration of IPv6 addresses—Current Techniques

User monitoring of IPv6 traffic is more complicated. The IPv6 address is no longer a unique identifier as it was with IPv4 address. That is mainly because of temporary address as described above. There are two ways how IPv6 addresses can be assigned. Practical experience at BUT shows that stateful configuration using DHCPv6 does not work properly , so only stateless configuration can be deployed.

Stateful IPv6 configuration uses DHCPv6 [11] to provide IPv6 addresses and other configuration parameters. Unfortunately, there are several DHCPv6 limitation cause, that it can not be used for stateful addressing. The main reason is, that default gateway can not be obtain via DHCPv6 so stateless configuration has to be deployed as well. This cause, that Windows systems use temporary address for communication instead of the address obtained through DHCPv6, because temporary addresses have higher priority. In addition, DHCPv6 client is not supported in Windows XP, which is still widely used. DHCPv6 also does not identifies hosts with MAC address as DHCPv4, but with DHCP Unique Identifier (DUID). This can not be easilly used as user identifier.

Stateless IPv6 configuration is using RA (Router Advertisement) messages. first part of the IPv6 address—network prefix—is assigned using RA messages together with default gateway and others options. The second part of the IPv6 address—interface ID—is generated using EUI-64 or privacy extensions. Because EUI generated with privacy extensions has higher priority than EUI-64, EUI also can not be used as a unique identifier.

Thus, neither stateful nor stateless configuration alone provide a unique ID needed for user identification. This can be achieved by combination of several techniques as discussed in the following section.

C. Data Structure for unique IPv6 host identification

As seen from the previous sections, a new unique identifier is needed to identify a host in the IPv6 network. One solution is to collect various sorts of data obtained from devices on the network. The information is listed in Table I.

All pieces of information together provide a complex view on the network and can help to identify a host. A tuple *(IPv6 address, MAC address, Login name)* is sufficient to identify a host/user. In practice, an extended tuple is built at BUT: *(Timestamp, IPv6 address, MAC address, Switch port, Login)*, see Fig. 1. Timestamp is added to track the communication time that is missing in SNMP records. Switch port number is used to control if a user is blocked or if unregistered MAC address appeared on a port. In addition to these values, VLAN number and interface statistics are stored, however, these data are not necessary for host identification.

TABLE I
INPUT DATA FOR IPV6 INTEGRATED MONITORING SYSTEM

OSI layer	Data Source	Information Obtained
L2	Radius log (using 802.1x)	Login, MAC address
L2	Switching table	Switch port, MAC address
L3	Router Neighbor Cache	IPv6 address, MAC address
L3	Router ARP table	IPv4 address, MAC address
L4-7	Netflow records	IPv4/IPv6 addresses, ports

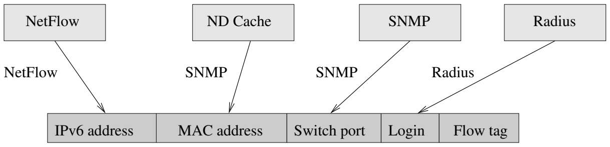

Fig. 1. Data collections in Integrated Monitoring System

Timing of downloading these information is crucial for right work of the system. The presented data records are not created at once but the record items are filled in progressively as data become available.

D. Getting Monitoring Data–Protocols, Times, Devices

Monitoring data are collected using SNMP protocol and stored in the central database. Network administrator can search database using IPv6, IPv4 or MAC address as keys. SNMP pools data from switches every 15 minutes.

1) Mapping: between the IPv6 address and its correspondent MAC address is downloaded from the router's neighbor cache. Port, VLAN number and other information comes from the switch's FDB (Forwarding Database) table[1] Traffic statistics are obtained by Netflow. Netflow records themselves are not sufficient for user surveillance and activity tracking because of IPv6 temporary addresses. Therefore, Netflow records are extended by additional information called *a flow tag*. The flow tag is added to a flow record after its creation, usually when the information is received and stored at the main database. The tag is a unique identifier of the user since Netflow records are generated for every single connection of one user even with different IPv6 addresses! The flow tag can be used as a key to identify any user activity stored in the system.

2) Devices: Combination of Netflow records with SNMP, ND cache and Radius fills the gap and makes the central monitoring system applicable for both IPv4 and IPv6. The

[1] Since older devices support different MIB standards, ipNetToPhysical table [12] is used to get these data.

system is depicted on Fig. 2. It is composed of L2 and L3 switches, Netflow probes, routers, and integrated monitoring systems running as application on the server.

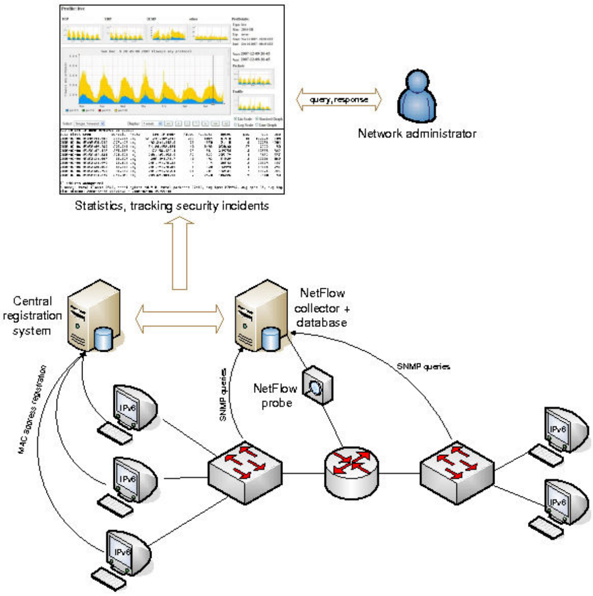

Fig. 2. Integrated monitoring system for IPv4 and IPv6

At BUT, there is a huge amount of monitoring data. Daily Netflow data reaches 9 GB of compressed data (18 GB of uncompressed). So, the size of database grows rapidly. For example, data from routers at student dormitories are taken every 15 minutes. Considering several thousands of students at six dormitories, it makes about 600,000 entries to be added to the database every week.

E. Practical IPv6 Monitoring—Statistics

Following statistics deal with BUT university campus network having 2.500 staff and more than 23.000 students. The top utilization is seen at student dormitories where more than 6.000 students is connected via 100 Mbps links. The core of BUT network is based on 10 Gbps technology with 10 Gbps external connection to CESNET (Czech Academic Network). The IPv6 connectivity at the campus is implemented according to the Internet Transition Plan [3]. Some parts of university already provide native IPv6 connectivity. Table II shows proportion of tunneling protocols at BUT networks. These statistics are different in comparison with Google [6], where tunneling traffic is bigger than native IPv6 traffic. That is mainly because BUT offers native IPv6 connectivity that has higher priority in operation systems than tunneling However tunneling techniques are still used. 6to4 tunneling is used most because every node in BUT network has a public IPv4 address, so NAT is not needed. As discussed above, 6to4 tunneling mechanism is in this case used as the first.

VI. Conclusion

IPv6 brings new monitoring challenges due to temporary addresses and tunneling. The main issue is how to identify a host/user. The solution presented here is based on Netflow, SNMP and other data records. These data are gathered into the integrated monitoring system where user activities are preserved. The proposed solution was implemented and deployed at BUT campus network. The paper discusses the architecture of the system and preliminary results of its deployment. The results prove viability of the approach for monitoring of larger networks. There are still open challenges for IPv6 monitoring. One is reliability of transmission of monitoring data because Netflow and SNMP use UDP. When network is under attack, important data can be lost and monitoring statistics become incomplete. There is also a challenge to built a new Netflow collector optimized for high-volume data. Current systems based on MySQL databases are suitable for small networks. Effective algorithms and data structures for fast lookup will be needed for data processing and information retrieval in more demanding network environments.

TABLE II
IPv4, IPv6 native and tunneling connection

Protocol	Bytes sent	%	Packets sent	%
protocol 41	13.918 GB	0.21	27.074 M	0.3
udp 3544	32.087 MB	0.00047	0.4 M	0.0045
native IPv6	120.849 GB	1.83	131.82 M	1.45
IPv4	6450,225 GB	97.478	8.910 G	98.23
total	6617.079 GB	100	9.070 G	100

VII. Acknowledgments

The research is supported by the Czech Ministry of Education grant MSM 0021630528: Security-Oriented Research in Information Technology, by ESF project CZ.1.07/2.3.00/09.0067 ”TeamIT—Building Competitive Research Teams in IT” and by BUT FIT grant FIT-S-10-2.

References

[1] C. E. Caicedo, J. B. Joshi, and S. R. Tuladhar. IPv6 Security Challenges. *Computer*, 42:36–42, 2009.

[2] B. Carpenter and K. Moore. *Connection of IPv6 Domains via IPv4 Clouds*. RFC 3056, February 2001.

[3] J. Curran. *An Internet Transition Plan*. RFC 5211, July 2008.

[4] D. T. F. Templin, T. Gleeson. *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*. RFC 5214, March 2008.

[5] S. Frankel, R. Graveman, and J. Pearce. Guidelines for the Secure Deployment of IPv6 (Draft). Technical Report 800-119, National Institute of Standards and Technology, 2010.

[6] S. H. Gunderson. Global IPv6 statistics. Measuring the current state of IPv6 for ordinary users. In *Proc. of 73 IETF*, 2008.

[7] E. Hofig and H. Coskun. Intrinsic Monitoring Using Behaviour Models in IPv6 Networks. *LNCS*, 5844:86–99, 2009.

[8] C. Huitema. *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*. RFC 4380, February 2006.

[9] T. Narten, R. Draves, and S. Krishnan. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. RFC 4941, September 2007.

[10] E. Nordmark and R. Gilligan. *Basic Transition Mechanisms for IPv6 Hosts and Routers*. RFC 4213, October 2005.

[11] R.Droms, J.Bound, B.Volz, T.Lemon, and C.Perkins. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)* . RFC 3315, July 2003.

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

[13] D. Źagar, K. Grgić, and S. Rimac-Drlje. Security aspects in IPv6 networks - implementation and testing. *Comput. Electr. Eng.*, 33(5-6):425–437, 2007.