DEPLOYING IPV6 - PRACTICAL PROBLEMS FROM THE CAMPUS PERSPECTIVE

Tomas Podermanski
Brno University of Technology, Božetěchova 1/2, 612 66 Brno, Czech Republic,
e-mail: tpoder@cis.vutbr.cz

Matěj Grégr
Brno University of Technology, Božetěchova 1/2, 612 66 Brno, Czech Republic,
e-mail: igregr@fit.vutbr.cz

Miroslav Švéda
Brno University of Technology, Božetěchova 1/2, 612 66 Brno, Czech Republic,
e-mail: sveda@fit.vutbr.cz

Paper type

Technical paper

Abstract

On February 2011, IANA has run out of IPv4 addresses. On April 2011, APNIC pool reached the final /8 IPv4 address block. Projected address pool exhaustion for other RIRs varies from the beginning of the 2012 to the end of 2014. This situation pushes organizations to think about transition to IPv6. Unfortunately IPv4 and IPv6 are incompatible protocols that make the transition more difficult and raise new security issues. This paper shares experiences of deploying IPv6 in the university campus network, describes the most significant troubles that we have been faced with and describes the best practices in the practical IPv6 deployment. The article discusses differences in IPv6 and IPv4 networks with focus on the first hop security, autoconfiguration (SLAAC, DHCP, DHCPv6) and different clients' support.

Keywords

IPv6, security, campus network, transition

1. Introduction

The idea of IPv6 deployment proposed by RFC 5211 [1] expected that the Internet would be fully migrated to IPv6 in these days. Unfortunately, it seems that all deployment strategies defined in either political [2],[3] or technical documents were too optimistic. IANA IPv4 address pool is already depleted, more than 10% autonomous systems (AS) announces IPv6 prefix in global BGP table [4] and most of operating systems support IPv6. However, the content providers still indicate that less than 0.5% [5] of clients is being able to use IPv6 connectivity. What is worse, there are statistics showing that IPv6 connectivity in some networks might be broken or less stable comparing to IPv4 [6]. As the result, most of content providers are afraid to announce IPv6 for their services in fear of losing customers.

Observing the global IPv6 infrastructure and deployment, we believe there are no significant problems to have a good IPv6 connectivity for servers in data centers. Many transport networks can deliver IPv6 traffic today as well. We believe that the key problem of the low IPv6 penetration is on the side of ISPs providing last mile to customers. ISP must ensure a positive user experience, thus if the IPv6 is deployed, it is important that the deployment is secure and a service quality is the same as in IPv4 network. Unfortunately, there are not many devices able to implement IPv6 first hop security that is equivalent to IPv4 security. Ordinary user does not care about protocol used for connection, but does care if the connection is broken or unstable, which is sometimes a problem with IPv6 connection.

This article comprises experience with deploying IPv6 at the campus network at the Brno University of Technology (BUT) which is one of the biggest universities in the Czech Republic. Currently, the core of the network has fully enabled support for the dual-stack and the IPv6 network completely follows topology of IPv4 network. University also has own provider independent (PI) IPv6 address space to be able to use multihomed IPv6 connections in future. The university campus network connects more than 2,500 staff users and more than 23,000 students. The top utilization is present at student dormitories where more than 6,000 students are connected via 100 Mb/s and l Gb/s links.

In the following sections we will describe the most significant issues that we have been faced with during the deployment of IPv6 protocol in the campus network. The deployment started at the university in 2002. At the beginning, the experimental network on dedicated devices and links was created. Currently, the IPv6 and IPv4 share the same infrastructure that is operated as a dualstack network. Most of the network services support both protocols. However, the process of transition to IPv6 at the university has not been finished yet, and it would take a lot of time and effort to move all services to IPv6 with the equivalent stability and reliability as we have in IPv4.

2. Addressing issues

One of the main issues is address assignment for clients. The mixture of various OSs in a network requires automatic address assignment that is supported by most of the systems. Assigning addresses with a DHCP server became de-facto standard for IPv4. However, DHCPv6 protocol is different.

DHCPv6 features two basic modes. In practice, the first mode, stateless DHCPv6, is a layer on top of the autoconfiguration mechanism (SLAAC) and is used to provide recursive DNS server addresses. Two special flags are used for this purpose in the Router advertisement (RA) message: *M* – managed, *O* – other. These flags tell the client that it should ask a DHCPv6 server for more information related to the connection parameters. If the *M* flag is set, statefull DHCPv6 is used. If the *O* flag is set, SLAAC will be combined with stateless DHCPv6. The strong binding between SLAAC and DHCPv6 brings several problems.

- It is not possible to pass all necessary configuration options (e.g. option for default route) via DHCPv6 server. Authors of DHCPv6 protocol stated that because SLAAC has to be used anyway, default route is not necessary – client learns a default route from RA message. However, this forces to use both autoconfiguration mechanisms together and increases the complexity.
- When a client sees an RA with *M* flag on, a client sends a DHCPv6 Solicit message looking for a DHCPv6 server. A DHCPv6 server responds with appropriate configuration for the client. However, if the client has a DHCPv6 derived address, and receives an RA with *M* flag off, the client will release that DHCPv6 derived address. Unfortunately, RA messages can be easily spoofed so the attacker can force all clients in a local network to release their IPv6 addresses just with one packet. This can be solved by proper filtering on access layer; however this is sometimes a problem. The filtering possibilities are discussed later in the paper.

Using DHCPv6, we do not get the same results as with DHCPv4 server (MAC to IPv6 address binding). DHCPv6 does not use a MAC address to identify the client; instead, it uses a specially created unique identifier called a DUID (DHCP Unique Identifier). The main idea behind this identifier is to release the clients from dependence on hardware and on a specific network interface. The advantage is that a change of a network adapter or a connection through another interface (such as WiFi instead of Ethernet) would mean that the user always obtain same IPv6 address. Unfortunately, there are several issues connected with the DUID identifier.

- DUID is controlled by software, thus it is not as stable as it should. E.g., if the client has dual boot, every OS will have different DUID.
- DUID is changed, after OS is reinstalled.
- If the administrator clones an OS image and copy it to another computer, two computers will have the same DUID.
- It is impossible to tie DUID with the host identification that is used in DHCP(v4) – host's MAC address which complicates assigning address especially in a dualstack environment. Solution is either to extend existing systems for address management to support DUIDs or to use workarounds like MAC address option specified in RFC 6221. Unfortunately, vendors have not included the support for the RFC 6221 yet.

Moreover, statefull autoconfiguration using DHCPv6 is very difficult to be used today because of lack of support on many platforms including Windows XP, which is still very widespread OS. Most of mobile devices has not implemented support for DHCPv6 yet and some OSs (e.g. MAC OSX) must be updated to the latest version, which is a problem if the devices are not managed by an ISP.

The operational experience shows that according to these issues, the DHCPv6 protocol and its implementations are still not mature enough to be used in a production network and moreover, it is not feasible to use it for address assignment in networks where the hosts' identification is required.

Another choice for address assignment available in IPv6 is to use the *stateless autoconfiguration* (SLAAC). Unfortunately, the stateless autoconfiguration in some OSs turns on privacy extensions. This means that devices generate a random end user identifier (EUI) - temporary IPv6 Address. This is a brand new IPv6 feature that allows a node to automatically generate a random IPv6 address on its own without the control of a network administrator.

However, this contradicts the need to identify a malevolent user. Private, temporary addresses hinder the unique identification of users/hosts connecting to a service. This prevents logging and tracking users based on IPv6 address. However, the knowledge of relation between an address and a device (or user) that has been used is necessary for solving security incidents and is required by law in several countries.

The Table 1 summarizes the autoconfiguration techniques in IPv6 protocol.

	DHCP (v4)	DHCPv6	SLAAC
Handle default route to a client	√		√
Handle address of DNS servers to a client	√	√	*[1]
Privacy extension or EUI64 address created by a client			√
Assignment IP address based on client's MAC address	√		
Assignment IP address based on client's DUID address		√	

Table 1: Autoconfiguration techniques for IPv4 and IPv6

If a security policy requires better control, either fixed IPv6 addresses must be centrally assigned and logged, which is not a feasible option for a large network, or statefull configuration using DHCPv6 has to be deployed.

Before the deployment of IPv6 in a local network, a network administrator must decide whether:

- Addresses will be assigned by DHCPv6 – the advantage is better control over hosts with, but many devices will not be able to use IPv6.
- Hosts will create own address based on SLAAC – all hosts will be able to use IPv6, but an administrator either gives up to have control over user identification in the network or a new mechanism must be deployed to identify the users [21]. Example of our implementation is described later on.

The Table 2 summarizes the IPv6 autoconfiguration support among the OSs.

	DHCP (v4)	IPv6	DHCPv6	SLAAC	RFC 6106	SEND
Windows XP	√	√		√		
Windows Vista / 7 / 8	√	√	√	√		*[2]
MAC OSX	√	√	√	√		
MAC OSX prior to Lion (2011)	√	√		√		
Linux	√	√	√	√	√	*[3]
Android	√	√		√		
Windows phone	√					
iOS (iPhone, iPad, iPod)	√	√		√		

Table 2: Autoconfiguration techniques supported by various OS in default configuration

First hop security in IPv4

IP address autoconfiguration process might be perceived as a honey pot for a hacker. If the hacker is able to interfere the configuration process, the whole user's traffic can be rerouted to the attacker's PC. In many cases it does not need to be a targeted attack, but simply an accident, where a user connects a Wi-Fi router with a preconfigured DHCP server to the network and causes a network malfunction for other users. This problem, as the other problems with first hop security, is known in IPv4 world for quite long time. For this reason some mechanisms were created in the IPv4 world which would prevent or at least complicate some of these attacks. The best place to implement protection for end users is on the end-user switch access port that the user is connected to. Different vendors use slightly different terminology for individual types of protection but generally we can meet the following ones:

DHCP Snooping: Some ports are explicitly defined in the switch configuration so port is able to receive DHCP

[1] Handling address of DNS server was standardized in RFC 6106, but major OS have not implemented the standard yet.

[2] Only experimental implementation not available for download yet [26].

[3] An experimental implementation available for Linux [25].

responses from DHCP (so called trusted port). It is assumed that somewhere behind the trusted port is a DHCP server. If a reply from a DHCP server arrives to a port not defined as trusted, the response is discarded. Any DHCP server running on the client system (whether intentionally or by accident) does not threaten other clients on the network because the answers will not reach further than the access port for which this protection has been activated. DHCP snooping is usually prerequisite for other protection mechanisms such as IP lockdown or ARP protection as described below.

Dynamic ARP protection, ARP inspection: DHCP snooping database contains MAC address - IP address - switch port combination. This database is then used on untrusted ports to inspect ARP packets. Other MAC addresses not recorded in the database are discarded. This eliminates attacks focused on creating fake records in the ARP table (poisoned ARP cache). Another often-appreciated feature of this mechanism is the fact that the client cannot communicate over the network unless an IP address from the DHCP server is obtained. That forces user to use DHCP instead of configuring static address.

Dynamic IP Lockdown, IP source guard: Another degree of protection is achieved by inspecting source MAC and IPv4 address on untrusted ports for all packets entering the port. This eliminates spoofing a source IPv4 or MAC address.

The Table 3 describes different attacks and techniques available for mitigating the attacks in IPv4 network.

	DHCP snooping	Dynamic ARP inspection, ARP protection	Dynamic IP lockdown, IP source guard
Rogue DHCP server	√		
ARP poisoning		√	
Forces users to use DHCP		√	√
Source IPv4 address spoofing			√
Source MAC address spoofing			√
Require support on access port	√	√	√

Table 3: First hop security threads and protection features in IPv4

3. First hop security in IPv6

The above described solutions for mitigating attacks in IPv4 networks are implemented in various access switches on the market. As we wrote previously, the autoconfiguration techniques are different in IPv6 so new solutions are necessary. Security mitigation techniques in IPv6 networks are described below.

Source Address Validation Improvements (SAVI): The set of techniques that complement ingress filtering with finer-grained, standardized IP source address validation [11]. Framework has option for DHCP servers and tries to solve a mechanism similar to the one we described with DHCP snooping for IPv4. It is limited to DHCPv4 and DHCPv6 and does not deal with the problems of rogue Router Advertisement messages. SAVI is mainly supported in devices produced by Hewlett Packard - A series. Very similar technique called *ND inspection* is implemented in Cisco devices.

Secure Network Discovery (SEND): This method tries to deal with autoconfiguration problem in a totally different way. SEND is based on signing packets with cryptographic methods [15]. Apart from a router it does not require support on the access switches. The validity verification itself through message certificate takes place at the end-user system. IPv6 address of the end-user system is a result of a cryptographic function (see, we have another auto configuration method). Using SEND directly excludes using static, EUI 64 and Privacy Extensions Address. However SEND provides great advantage - it not only solves the autoconfiguration problem but also other safety problems of the Network Discovery protocol (RFC 2461). Another advantage is independent infrastructure; hence it can also be used in the same way in the either wired or Wi-Fi networks.

The main shortcoming of SEND is the requirement for public key infrastructure according to X.509. To make the SEND works properly, a certificate of the certification authority have to be installed on each client that wants to use SEND. The certificate has to be issued for each router as well. So it grows the costs of the management of the network – certificates have to be reissued or replaced before they expire.

SEND is a patented Cisco technology (US patent number 20080307), therefore no one would be surprised that it is implemented especially on some devices of this company. Presence of the patent raised several discussions especially with SEND and RA Guard integration. According to Cisco statement, Cisco will however not assert any patents against any party that implements the standard [17].

Considering the SEND deployment, a network administrator will face the problem that the protocol is not supported on any operation system yet. There are only some basic Linux and Windows implementations; however thay cannot be used in a production environment. Windows OS, as the most widespread system, nor Mac OS do not support the SEND protocol even in the most recent versions. SEND protocol could potentially solve security problems of NDP protocol; however, it cannot be deployed and there are no indications that this should change in the near future.

Router Advertisement Guard (RA Guard): Another alternative, which unfortunately deals only with the issue of fake router advertisements, is IPv6 Router Advertisement Guard [9]. It is similar technique as DHCP snooping, but determined for Router Advertisement packets. It tries to block fake router advertisements on an access user port. Apart from tools that should ease the initial switch configuration (learning mode), it opens the path to integration with SEND. In this mode the switch works as a so called node-in-the-middle, where the switch with activated RA Guard uses information from SEND to verify packet validity and for the connected end-user system it appears as normal Router Advertisement packet. As you could guess from the title RA Guard does not solve DHCP or DHCPv6 issues in any way. We can already find an implementation in some Cisco devices.

Access Lists on the switch (ACL/PACL):. If a network device supports ACL or PACL (Port access list) it is possible to configure an ACL blocking the malevolent traffic. A network administrator can configure ACL that will block all ICMPv6 messages type 134 (RA messages) and also block traffic to the UDP target port 546 (dhcpv6-c1ient). The rules are subsequently applied to the inputs of ports to which the c1ients are connected. This can eliminate instances of rogue routers and DHCPv6 servers. A required condition to use this mechanism is IPv6 ACL support on the relevant switch. The problem of this solution is that very few access switches supports creation of IPv6 access-lists today. Also price of that switches is usually two or three times higher comparing to the switches where IPv6 PACL and other IPv6 security features are not implemented.

The solution with RA-Guard and ACL/PACL has however big disadvantage. It works very well for accidently announced RA messages but can be easily avoided using combination of fragmented packets and extension header in the RA message [18]. Existing protection for the targeted IPv6 attack does not exist today. There are some proposed solutions how to solve the problem [19],[20], but all of them are only drafts and it will take a long time before support will be added to operating systems and network devices.

The most undesired option is **blocking or disabling whole IPv6** traffic. It is obvious that this step protect a host against all attack related to IPv6, however it is against the idea of deploying IPv6. That solution can be used only as a short-term solution when the other possibilities are not available. IPv6 protocol can be suppressed on the client by disabling o uninstalling IPv6 protocol or blocking the whole IPv6 traffic on the access port by filtering out all Ethernet packets identified with Ether Type 0x86DD (Ether type for IPv6 protocol).
The Table 4 summarizes first hop security threads and protection in IPv6 network.

	RA-Guard	ACL/PACL	SAVI, ND inspection	SEND	Disabling IPv6	Blocking IPv6
Rogue DHCPv6 server		√	√		√	√
Accidently rogue router advertise	√	√		√	√	√
Intentional rouge router advertise				√	√	√
ND cache poisoning			√	√	√	√
Source IPv6 address spoofing			√	√	√	√
DAD DOS attack			√		√	√
Neighbour cache overload			√		√	√
Source MAC address spoofing			√		√	√
Requires support on access switches	√	√	√			√
Requires support or configuration on client side				√	√	

Table 4: First hop security threads and protection features in IPv6

4. First hop security in IPv6 – current situation

Thinking about IPv6 deployment and security, network administrators will face the fact, that all of the above mentioned techniques can be used rather theoretically today. Either they are not implemented on client's side or device support is missing. Another issue is that if the protective devices are to be truly purposeful they must be placed as close to the end-user system as possible. This could often mean a complete replacement of network infrastructure that is a job that few will want afford just to implement IPv6.
To summarize our experience, after two years of operating the IPv6 network in production environment and several more years of testing the IPv6 protocol, we did not observe a targeted attack to our IPv6 network. The main problems, we have to solve are above described problems with autoconfiguration, bogus router advertisements together with missing monitoring tools for IPv6 network.

Many rogue advertises are generated by Windows computers. This is a serious issue because computers propagate their own interface as a default gateway. Unfortunately this behaviour can be in some conditions caused by properly used Internet connection sharing service. The Figure 1 shows the number of rogue advertises on the network with approximately 2000 of connected hosts.

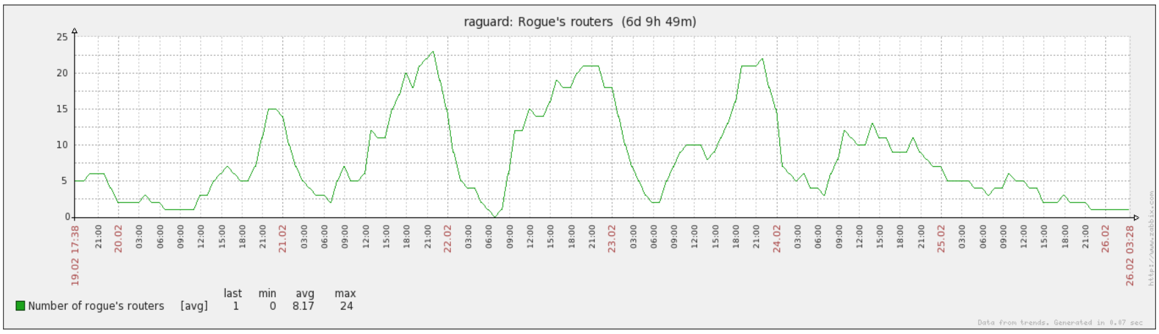

Figure 1: Number of rogue advertises detected in the network

As we mentioned earlier, because of missing implementation of mitigation techniques on switches, more affordable solution that would at least alleviate efforts to paralyze the IPv6 autoconfiguration mechanism is detection of fake Router Advertisements. This will not protect the network from a well-crafted and targeted attack but it can at least detect incorrectly configured c1ients. For many networks it would be the only usable solutions for a long time. All tools for detection of rogue Router Advertisements work based on the same principle. They connect to the FF02::1 multicast group where the router advertises messages are sent and thus are able to monitor all RA messages appearing on the network. The monitoring tool can then inform the administrator about the undesirable status, call an automated action (Ndpmon [22], Ramond [23]), or even send a message cancelling the validity of fake Router Advertisements (rafixd [24]).

5. User tracking, monitoring and accounting

Long-term network monitoring, accounting and backtracking of security incidents is often achieved in IPv4 networks using NetFlow probes and collectors. This can be a problem if IPv6 is deployed and privacy extensions are allowed in the network. The same user can than communicate with different addresses. That means that address cannot be used as a unique identifier anymore. As the part of deploying IPv6 we tried to develop extension to existing monitoring systems to allow easier tracking users in an IPv6 network.

The main idea of the extension is collecting and putting together data obtained from differed parts of the network. A neighbour cache database on routers and forwarding databases on switches can provide information about relation between an IPv6 address port on a switch and a MAC address used by a user. In the next step the MAC address can be used for identifying a user in a database provided by radius server.

These pieces of information, together, provide a complex view of the network and can help to identify a host. A tuple (lPv6 address, MAC address, Login name) is sufficient to identify a host/user. In practice, an extended tuple is built: (Timestamp, IPv6 address, MAC address, Switch port, Login) as depicted in the following Figure 2.

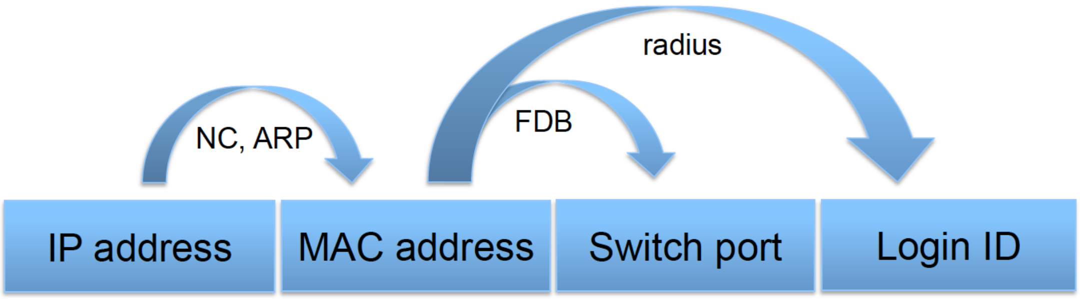

Figure 2: Items in the extended flow record and relations amongst them

Timestamp is added to provide a history of communication. Switch port is necessary if the user is blocked or if an unregistered MAC address is used on a port. In addition to these values, the VLAN number and interface statistics are stored; however, these data are not necessary for host identification.

It is important to note that this data structure is not created at once, but it is filled in when data are available. For instance, NetFlow data are taken from the NetFlow probe when they are sent to the collector. However, there is no information about MAC addresses yet. The address is downloaded later from the switch's ND cache. Login data from RADIUS can also be added. However, RADIUS data are not available for every user - only for those who are connected using 802.1x authentication. For other users, only the IPv6 address and the switch port number and MAC address are used for identification.

Data are collected using the SNMP protocol and stored in the central database where the network administrator can search data using the IPv6, IPv4 or MAC addresses as keys. Useful tool for polling and storing information from switches and routers is Network Administration Visualized (NAV) [12]. SNMP polls the data from switches every fifteen minutes. The mapping between the IPv6 address and its corresponding MAC address is downloaded from the router's neighbour cache. Port, VLAN number and other information comes from the switch's FDB (Forwarding Database) table. Traffic statistics are obtained from NetFlow. NetFflow records alone are not sufficient for user surveillance and activity tracking because of the temporary IPv6 addresses as described in previous sections.

The time dependency of gathering different data is crucial when accessing the ND Cache. This temporary memory at the router stores information needed to build the link between the IPv6 address and the MAC address. Because IPv6 addresses change in time and have limited validity, if the ND entry is lost, there is no way to link the IPv6 address and the user/host. To ensure that all information is stored properly in the monitoring system, the SNMP polling interval has to be shorter than the expiration timeout of the ND Cache. Otherwise, some entries in the ND Cache could expire without being downloaded into the central system. Typical timeouts for collecting SNMP and RADIUS data are fifteen minutes. The ND Cache expiration timeout is usually set to more than one hour.

6. Conclusion

This paper presents security and addressing issues in IPv4 and IPv6 protocol environment and solutions how to solve them. Nowadays, the IPv6 traffic volume is low, but this is caused by the lack of IPv6 sources (web pages, servers) on the Internet. Also widespread operation systems such as Windows XP support IPv6 but IPv6 is not enabled by default.

Next generation Windows systems together with Linux, Mac OS and Unix systems have however IPv6 protocol enabled by default and penetration of these systems is growing every day. Security and addressing issues discussed in this paper present the overview of problems we encountered when we deployed IPv6 protocol in BUT campus network. Addressing issues and problems with user tracking in IPv6 protocol introduce the necessity for a new monitoring system that is able to overcome the specific problems in IPv6 address assignment. Solutions, how to solve these issues, are proposed. We discussed possibilities, how we are able to limit the impact of security problems in IPv6 network together with monitoring and tracking system that is able to identify and track a host in IPv4 and IPv6 network.

References

[1] J. Curran: An Internet Transition Plan, [online], url: http://tools.ietf.org/html/rfc5211

[2] Commission of the European Communities: Action Plan for the deployment of Internet Protocol version 6 (IPv6) in Europe, [online], url: http://ec.europa.eu/information_society/policy/ipv6/action_plan/

[3] Transition Planning for Internet Protocol Version 6 (IPv6), [online], url: http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-22.pdf

[4] IPv6 CIDR REPORT, [online], url: http://www.cidr-report.org/v6/as2.0/, http://bgp.potaroo.net/index-bgp.html

[5] Lorenzo Colitti, Steinar H. Gunderson, Erik Kline, Tiziana Refice, Evaluating IPv6 Adoption in the Internet, [online], url: http://www.google.com/intl/en/ipv6/statistics/

[6] Geoff Huston: Flailing IPv6, [online], url: http://www.potaroo.net/ispcol/2010-12/6to4fail.html

[7] S.Thomson, T.Narten, and T.Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862, September 2007, [online], url: http://tools.ietf.org/html/rfc4862

[8] J. Curran: An Internet Transition Pian, RFC 5211, July 2008, url: http://tools.ietf.org/html/rfc5211

[9] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi: IPv6 Router Advertisement Guard, RFC 6105, February 2011, [online], url: http://tools.ietf.org/html/rfc6105

[10] S. Frankel, R. Graveman, and J. Pearce. Guidelines for the Secure Deployment of IPv6. Technical Report 800-119, National Institute of Standards and Technology, 2010, [online], url:http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[11] J. Bi, J. Wu, G. Yao, F. Baker: SAVI Solution for DHCP (work in progress) July 2011, [online], url: http://tools.ietf.org/html/draft-ietf-savidhcp-l0

[12] UNINETT and Norwegian University of Science and Technology: NAV, [online], 2011-03-15, [online], url: http://metanav.uninett.no/

[13] J. Bi, G. Yao, J. Wu, F. Baker.: Savi solution for Stateless Address - work in progress, April 2010, [online], url: http://tools.ietf.org/html/draft-bi-savi-stateless-OO

[14] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi.: IPv6 Router Advertisement Guard. RFC 6105, February 2011. [online], url: http://tools. ietf. org/html/rfc6105

[15] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander: SEcure Neighbor Discovery (SEND). RFC 3971, Febuary 2011, [online], url: http://tools. ietf. org/html/rfc3971

[16] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogl: Source Address Validation Improvement Framework", draft-ietf-saviframework-04 (work in progress), March 2011.

[17] R. Albright, Cisco System's Statement of IPR related to draft-ietf-v60ps-ra-guard-02, April 2009, [online], url: http://www.ietf.org/ietfftpIlPR/cisco-ipr-draft-ietf-v60ps-ra-guard-02.txt

[18] F. Gont, IPv6 Router Advertisement Guard (RA-Guard) Evasion, December 2011, [online], url: http://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01

[19] F. Gont, Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard), Febuary 2012, [online], url: http://tools.ietf.org/html/draft-gont-v6ops-ra-guard-implementation-01

[20] F. Gont, Security Implications of the Use of IPv6 Extension Headers with IPv6, January 2012, [online], url: http://tools.ietf.org/html/draft-gont-6man-nd-extension-headers-02

[21] Grégr, M., Podermański, T., Šoltés, M., Žádník, M.: Design of Data Retention System in IPv6 network, December 2011, [online], http://www.fit.vutbr.cz/~igregr/pubs.php?id=9840

[22] Frederic Beck, Ndpmon, August 2009, [online], url:http://ndpmon.sourceforge.net/

[23] Ramond, [online], url: http://ramond.sourceforge.net/

[24] Rafixd, [online], url: https://github.com/strattg/rafixd

[25] Tony Cheneau, Ndprotector, March 2012, [online], http://amnesiak.org/NDprotector/

[26] Meinel Ch.: Winsend, March 2012, [online], url:http://www.hpi.uni-potsdam.de/meinel/forschung/security_engineering/ipv6_security/winsend.html

Biographies

Tomas Podermanskí - works as a backbone network administrator, research developer and PhD student at Brno University of Technology. Participates in several research projects focused on security, monitoring and IPv6. Professional experiences shares as an active member oft he European project in the activity GÉAN3 Campus Best Practice.

Matěj Grégr - PhD student at Brno University of Technology. He teaches network related courses and his research concerns IPv6 security, monitoring and deployment. He works also as a network administrator at Brno campus network and participates in the European project - GÉAN3 Campus Best Practice.

Miroslav Švéda works since 2002 as professor in Computer Science and Engineering at Brno University of Technology. His research includes embedded systems, formal verification, Engineering of Computer-Based Systems, Computer networks and communication protocols.