Security Issues of IPv6 Network Autoconfiguration

Maciej Rostański, Taras Mushynskyy

Security issues of IPv6 network autoconfiguration

Maciej Rostański, Taras Mushynskyy

Academy of Business in Dąbrowa Górnicza, Faculty of Computer Science,
Cieplaka 1C, 41-300 Dąbrowa Górnicza, Poland
mrostanski@wsb.edu.pl
http://www.wsb.edu.pl

Abstract. IPv6 is a new version of IP protocol, which was defined in the series of RFC documents at the end of previous century. Although developments and improvements are conducted for many years already, a new standard still did not get such distribution as IPv4. The useful innovation and one of basic advantages of IPv6 protocol is a possibility of automatic assignment of addresses to the network devices. Such mode got the name SLAAC (StateLess Address AutoConfiguration). However, there are tasks, for implementation of which greater control is needed. In this case it is necessary to use the static addressing or DHCPv6 server for IPv6 protocol (stateful autoconfiguration). The aim of this work was to visualize an IPv6 network using stateless and stateful addressing modes and to reveal the features and security issues of the specific configurations. Those security issues need to be reminded to the administrators, as the big IPv6 migration is coming for small and medium businesses.

Keywords: IPv6, Computer Networks, Network Security, SLAAC, DHCPv6

1 Introduction. On the verge of the Internet of Things

Networks are growing endlessly and more and more data is being processed every day. For example, only by utilizing the amount of sensors gathering data, the Internet is becoming huge infrastructure for aggregation and delivery of constant data for the end-systems. The concept of this, called The Internet of Things, is a bit futuristic expression created by K. Ashton (see [1]). The idea is that not only typical computers, smartphones or tablets will use network for communication - but any device will. This is very relevant to the IPv6 adoption - as the IPv6 major feature is a huge addressing space and simplified network configuration, supporting massive scalability of networks, at the same time enabling end-to-end communication with devices connected to internetwork. Once enabled, this concept creates endless possibilities - such as the Talking Tree Project[1], a very interesting idea of equipping a tree with sensors, cameras, etc. and utilizing complex software allowing a tree to literally tweet about the weather, noises, wind changes.

[1] Talking Tree Project Website: http://www.talking-tree.com/

Migration to IPv6 protocol with its vast address space is a step forward into those and many other possibilities for innovative services. This is a major IPv6 adoption driver for innovative enterprises, and many of small and medium organizations are considering migration. Although the dynamics of IPv6 protocol deployment is not as high as expected, experts assume it is going to grow for a couple of next years [2]. There is an overall impression, that only legacy applications hold back the migration for many organizations, especially when they learn about many advantages of IPv6, such as simple autoconfiguration mechanisms. This article shows a different perspective on this matter.

1.1 IPv6 is not about bigger address space only

IPv6 protocol, being a successor to the most popular network layer protocol, is thoroughly described in RFCs and in numerous literature, such as [3], [4] or [5]. There are many advantages of IPv6 over IPv4 protocol, which, among many benefits, include:

- multi-addressing, which basically means, the node may have many IPv6 addresses, related to its function and connectivity, as well as address scope
- simplified network configuration, relying on automatic host addressing and routers sending the prefixes in router advertisements,
- directed data flows, utilizing multicast rather than broadcast transmission - in addition, IPv6 header includes Flow Label field for identifying packets within the same flow,
- simplified packet header, meaning more efficient packet processing - for example, there is no IP-level checksum,
- true end-to-end connectivity, restored by eliminating the need for Network Address Translation,
- authentication and privacy capabilities, built into protocol itself.

For many years, there is a discussion still active, whether it is a good time to migrate to IPv6. As years went by, it was becoming clearer that IPv4 is not going to vanish entirely in a fast manner; some even predict that a dual IP protocol coexistence is going to last a very long time. The organizations are reluctant in IPv6 adoption. Arbor Networks study cited in [6] indicates that possible obstacles to adoption include lack of economic incentives, lack of existing IPv6 content and technical and design hurdles.

On the other hand, the IPv4 address space is shrinking rapidly; on September 2012, RIPE NCC ran out of IPv4 addresses[2]. Technical problems diminish: most of modern operating systems are fully IPv6 capable, the network equipment is IPv6 ready, and IPv6 knowledge is becoming more and more common.

According to the Author, the best thing about IPv6 protocol is the most surprising one: IPv6 is in fact simpler in configuration and more efficient in deployment than IPv4. Many administrators would disagree and point out the

[2] Further information: `http://arstechnica.com/information-technology/2012/09/europe-officially-runs-out-of-ipv4-addresses/`

complexity of IPv6 address compared to IPv4, however considering other features, like stateful and stateless autoconfiguration of network nodes, mobility support, mandatory security protocols support, the above statement is quite defendable.

1.2 About this paper

Myths and benefits of IPv6 deployment are very well described by Van Beijnum in [3]. The ease of configuration creates risks - some administrators would just plug the network equipment in and, while it works, won't bother with security checks. That's why this article is important - it focuses on the presentation of autoconfiguration mechanisms risks in IPv6. The protocols and messages used during autoconfigurations are described in section 2; section no. 3 presents several security issues related to the autoconfiguration protocols. Section 4 presents a real-life case scenario and the results of field testing.

2 About automatic address configuration in IPv6

The useful advantage of IPv6 protocol, most relevant to the subject of this paper, is allowing network nodes to address themselves on their own or with Neighbor Discovery Protocol is called SLAAC (Stateless address autoconfiguration).

Although there are tasks, for implementation of that greater control is needed besides addressing in LAN networks. At that case it is necessary to use the static addressing or DHCP server for IPv6 protocol (DHCPv6).

As the first step, every host configures link-local address on every IPv6-enabled interface. In early IPv6 documentation, the address should almost everytime be derived from layer 2 address (e.g. MAC address) - now, it is not the case (see [7]), for example Microsoft Windows 7 or 8 configures its host address portion randomly. In any case, the IPv6 host is supposed to perform a DAD (Duplicate Address Detection) operation. Once link-local address is configured, the autoconfiguration operation commences. The entire process is described in [8]. Just to provide short overview, the process relies on:

a) IPv6 router sending out RAs (Router Advertisements) periodically and on-demand (as a response to RS message - Router Solicitation),
b) Hosts sending RS messages and obtaining RA information, such as an address prefix and a lease lifetime.

Fig. 1 provides the lifecycle of an autoconfigured IPv6 address.

In simple terms, stateful configuration utilizes an updated version of DHCP for IPv4. The DHCP protocol for IPv6 (DHCPv6) is slightly different because it relies on the client sending RS messages, thus detecting the presence of the routers on the link. The steps that follow include [9]:

a) If a router is found (RA is received), the RA message is examined for flags indicating whether DHCP can or should be used,

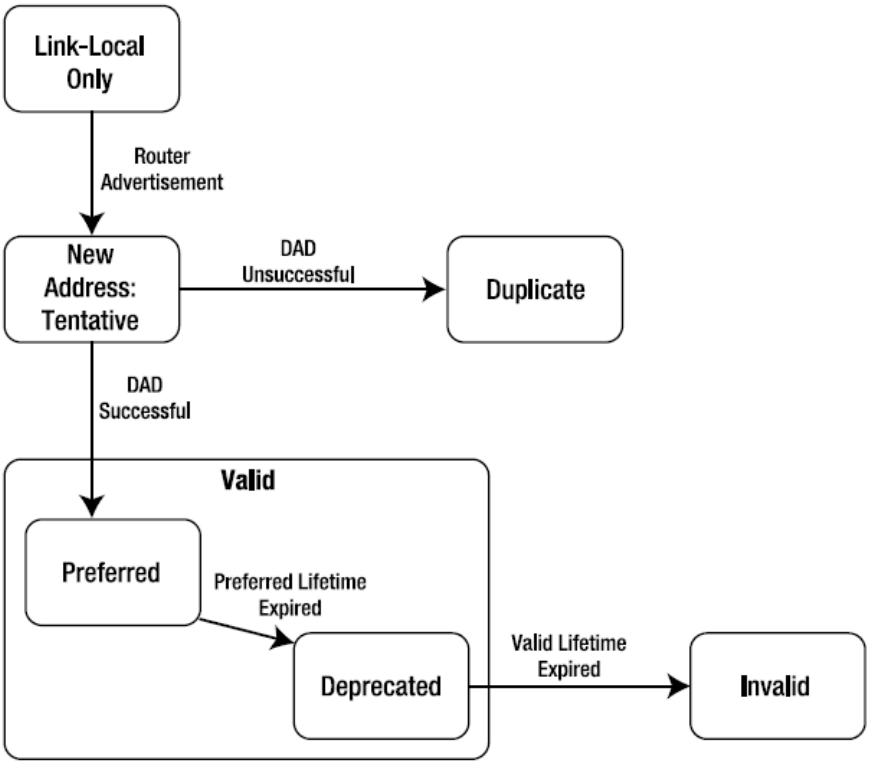

Fig. 1. The state-diagram of the life cycle of an IPv6 address. Source: [3]

b) If no router is found or DHCP can be used, host sends DHCP Solicit message to All-DHCP-Agents multicast address (this is somewhat deprecated due to lack of default gateway specification, see [10] for details).

The overview of DHCPv6 operation is presented on Fig. 2.

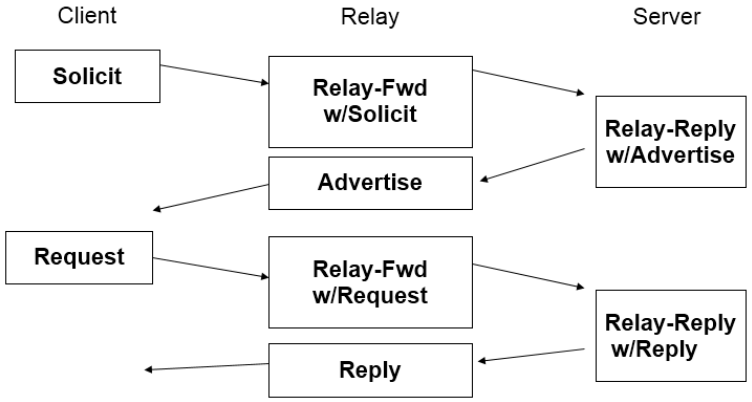

Fig. 2. The state-diagram of DHCPv6 operation. Source: [4]

3 Automatic configuration security issues

Unfortunately, IPv6 configurations may impose a vulnerability threats in many situations, when improperly used. An example of such problems involve using fragmentation for attacks on IPv6 network, such as overlapping fragments, Paxson/Shankar model [11] or Rose attack [12], as well as 6to4 tunneling, quoting [3]: "allowing people to create packets with spoofed IPv6 addresses and encapsulate them in legitimate IPv4 packets, thereby passing anti-spoofing filters that may be in effect". Other examples include using tunneling for attacks, DNS advertising or neighbor discovery. As shown before, the stateless configuration allows any IPv6 device to communicate with other IPv6 devices in the same LAN, by advertising its presence, so it can be located by Neighbor Discovery Protocol. NDP protocol however, cannot be left without supervision; it may allow an attacker to gather network devices data, for example. Further data on this subject is thoroughly described in [13].

3.1 State-of-the-art

The autoconfiguration mechanisms of an IPv6 protocol are subject to huge research indicating its vulnerabilities, as [14], [7], [15] or [16]. There is also well known literature pointing to techniques of securing network behavior, especially:

- Secure Neighbor Discovery (SEND) [17];
- IPv6 Router Guard [18];
- Autoconfig filtering on Ethernet switches [19];
- Implications for Network Scanning [20].

Such techniques and mechanisms have been recognized as more or less effective, but are also difficult to configure. With autoconfiguration in mind, the common practice (for example when setting up a conference network) is to configure the edge router for IPv6 and let the modern operating systems autoconfigure themselves. The most dangerous fact is, modern operating systems attempt IPv6 autoconfiguration by default and use IPv6 stack with higher priority than IPv4 [21]. This is extremely probable for example if BYOD (Bring Your Own Device) strategy is deployed without sufficient configuration and/or monitoring. The point of this article is to present vulnerability of such scenario and show yet another security flaw - the DHCP 'flapping' on an autoconfigured network.

The malicious behavior scenarios possibilities are discussed in IPv6 related documentation, such as [22] or [17]. Mitigating such risks is by all means possible and doesn't mean that IPv6 features are flawed; the administrator just has got to have knowledge of such threat and be aware of the conditions imposing a vulnerability. Several techniques for securing IPv6 local traffic are considered canonical, such as SEND (SEcure Neighbor Discovery, see [17]), other methods are possible but deployed rarely, e.g. IPv6 Router Advertisement Guard [18]. The problem is, those solutions are, quoting Levy-Abegnoli, 'non-trivial to deploy' ([18]). In case of non-prepared administrators or low budget for security testing, those techniques won't even be considered. This is sadly a typical experience in small and medium enterprises.

In this section, several autoconfiguration security issues for default-configured network devices and hosts are described. An administrator should be able to recognize such conditions in his own network and prepare for those situations accordingly.

3.2 Typical autocofiguration scenarios and associated threats

Following scenarios are possible if the attacker has access to local network and the IPv6 devices are configured with default security measures. The network doesn't have to be configured for IPv6, all modern devices support IPv6 and the IPv6 stack is turned on by default.

Stateless autoconfiguration with rogue station: This security risk scenario assumes that following conditions are fulfilled:

a) The original network node is autoconfigured using SLAAC mode with address A1,
b) The malicious node is trying to set its address to A1 repeatedly ignoring DAD (Duplicate Address Discovery) messages.

The outcome should be IPv6 stack disabled on the second node. However, because of the malicious nature, should the second node continue to send packets, the original node's operating system operation may vary, depending on its manufacturer and version. This is a situation that should be tested for systems used in organization's network.

Stateless autoconfiguration with rogue router: This security risk scenario assumes that following conditions are fulfilled:

a) The network nodes are using SLAAC autoconfiguration. For this purpose, an original router node is configured to send RAs containing network prefix,
b) Every node is configured with network prefix and default gateway through RA messages,
c) The malicious router is being introduced to the network, sending RAs on his own.

In the outcome, an administrator would want the nodes to ignore other RAs and this is achievable through specific configuration and network security devices introduction; but the question is: how would default configured equipment behave? This is interesting research subject for various operating systems and versions.

Stateful autoconfiguration with rogue DHCP server: Scenario conditions include:

a) Configuring network nodes and DHCPv6 server for a stateful configuration of any device,
b) Introducing a malicious DHCPv6 server, competing with an original one.

Desired network behavior would be ignoring new DHCP server, until lease expiration time. The device should then ask legitimate server for another lease, choosing another DHCP only in the situation of denial or absence of legitimate DHCP server.

Stateful autoconfiguration with rogue router: Scenario conditions include:

a) Configuring network nodes and DHCPv6 server for a stateful configuration of any device,
b) Introducing a malicious IPv6 router, sending RAs on his own.

Desired network behavior would be ignoring malicious router, until lease expiration time. The device should then ask legitimate server for another lease, choosing RA information only in the situation of denial or absence of legitimate DHCP server.

4 Field study. Rogue SLAAC server vs. legitimate DHCP server example

For the study of security issues, the last and most interesting scenario was chosen for field testing. The scenario consisted of:

a) Configuring a typical internetwork with DHCP server,
b) Introducing an IPv6 rogue router advertising RAs for stateless autoconfiguration.

The aim of this work was to create an IPv6 network using DHCP addressing mode and revealing the features of the network equipment's work.

4.1 Research topology

For the project we used the following equipment:

- Routers: Cisco 1841 with IOS operating system,
- Switches: Cisco 2950T with IOS operating system,
- PCs with Microsoft Windows7 Enterprise SP1 operating system,
- PCs with Microsoft Windows Server 2008 R2 Enterprise SP1 operating system.

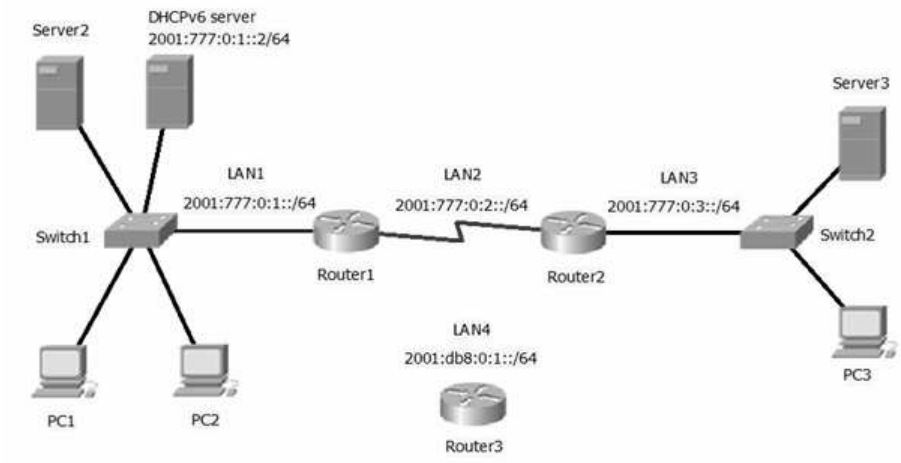

Fig. 3. Test topology. Source: own work

Schematic representation of the networks and their connection to each other is shown in Figure 3. DHCP server has been deployed on the Windows server 2008 r2 enterprise sp1. In order for a computers to receive addresses from the DHCP server, Router1 and Router2 were configured for the *dhcp-relay* mode with the commands:

```
Router1:
ipv6 dhcp relay destination 2001:777:0:1::2
ipv6 nd managed-config-flag
ipv6 nd prefix 2001:777:0:1::/64 no-advertise

Router2:
ipv6 dhcp relay destination 2001:777:0:1::2 Se0/0/0
ipv6 nd managed-config-flag
ipv6 nd prefix 2001:777:0:3::/64 no-advertise
```

As a result of configuration, all computers obtained dynamic addresses from DHCP server. DHCP server and routers were assigned static IP addresses. Moreover, the server gave out addresses for both networks LAN1 and LAN2.

4.2 Rogue SLAAC router scenario

After verification, it was decided to connect router3 to switch1. Router3 was configured with these commands:

```
ipv6 unicast-routing
ipv6 address 2001:db8:0:1::1/64  (on the interface FastEthernet0/0)
ipv6 enable
```

That is, router3 had IPv6 mode enabled and assigned an IPv6 address to the FastEthernet interface. Accordingly, the automatic address assignment SLAAC was activated, which was enabled by default.

Connecting the router3 to switch1 had significant effects on the computers in the network LAN1. First, the computer was running using the address obtained from the DHCP server. Then, after a while, the computer received the SLAAC address from Router3. After a few minutes the computer again received address from a DHCP server, but different from the first one. The address lease time at DHCP server was 8 days by default. On the average, changing of IP address occurred in 6-9 minutes. Fig. 4 shows the result of observation, which was carried out using Wireshark sniffer application.

Fig. 4 shows that the command "ping 2001:777:0:3::6" was executed on computer with IP address 2001:777:0:1::d. After changing of addressing in SLAAC mode and returning back to the DHCP provisioned address, IP address of the computer became 2001:777:0:1::c.

This change in the DHCP address happened every time, going through all the addresses from scope, thus depleting the available pool. This problem occured on all computers in the network with both Microsoft Windows Server 2008 and Microsoft Windows 7.

A similar experiment was done in the network LAN3 (Router3 was connected to Switch2). The results of computers behavior were the same as in the network LAN1. Routing protocol RIP was used on routers 1 and 2. If RIP protocol was enabled on Router3, then during IP address change, the computer was still able

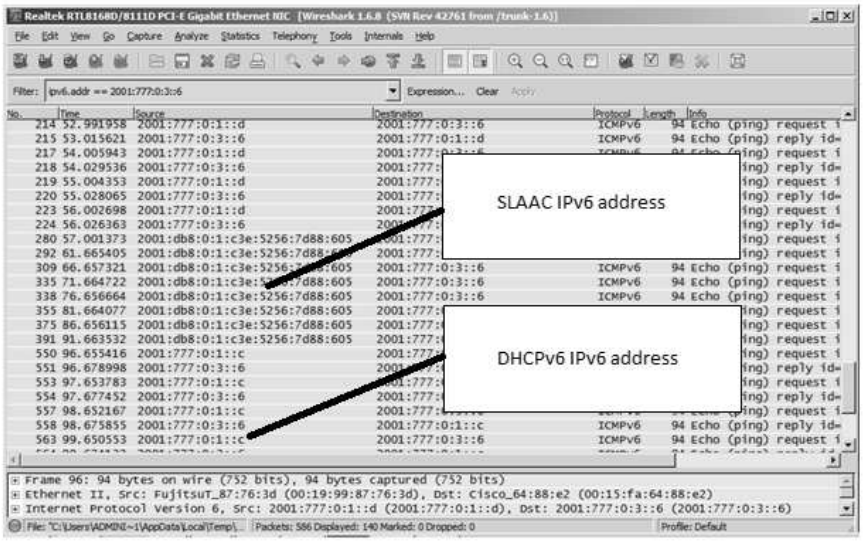

Fig. 4. Traffic during experiment - the 'flapping' between stateless and stateful address. Source: own work

to ping the devices in the other network. If the Router3 was not assigned the static unicast address during configuration phase, then the computers received only link-local addresses from Router3, but everything else followed the same erratic scenario. Rogue router's RAs may result in change of the default route on affected hosts - this is another vulnerability as described in [14].

5 Conclusion

In this article, given security risk scenarios are described as potentially dangerous; field testing confirming the most interesting scenario was presented as case study. As a result of this work it was shown that two autoconfiguration methods (one of which is the stateful mode, and the other is a SLAAC mode) would work in IPv6 network with the same priority and hinder the work of each other. This in turn can lead to serious disturbances in the functioning of DHCP servers - the basic service of corporate networks.

This article shows one of many vulnerabilities of an autoconfigured IPv6 network. Important fact is, given latest BYOD strategies, such autoconfiguration may occur without administrator's knowledge - modern operating systems support IPv6 by default. This is not indication of a flaw - just a reminder, that in IPv6 networks, careful administration of autoconfiguration must (!) be applied, for example using SEND [17].

Acknowledgement

Presented work is a part of ongoing research "IPv6 role in High Availability and Redundant Networks of Small and Medium Organisations", being conducted in Academy of Business in Dabrowa Gornicza.

References

1. Ashton, K.: That 'Internet of Things' Thing. In: RFID Journal, 22 July 2009
2. Curtis S., Niedzielewski D.: Internet of Things: miliardy urządzeń, czujników i liczników podłączonych do sieci. Networld polish ed. 01/2013, Miller Druk, Warszawa 2013
3. Van Beijnum I.: Running IPv6, Apress New York, 2006, ISBN: 1-59059-527-0
4. Odom W.: CCNP Route 642-902 Official Certification Guide 4th ed., Cisco Press, Indianapolis, 2011
5. Deering S., Hinden R.: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, IETF 1998
6. Burkhalter M.: Study: IPv6 adoption remaining slow, Perle Industry News, 2011, http://www.perle.com/articles/Study-IPv6-adoption-remaining-slow-800490443.shtml
7. Narten T. et al.: Privacy Extensions for Stateless Address Autoconfiguration in IPV6, (RFC 4941), IETF 2007
8. Thomson S., Narten, T., Jinmei T.: IPv6 Stateless Address Autoconfiguration (RFC 4862), Draft Standard, IETF 2007
9. Droms R. et al.: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), (RFC 3315), IETF 2003
10. Droms R., Narten T.: Default Router and Prefix Advertisement Options for DHCPv6, IETF 2009 http://tools.ietf.org/html/draft-droms-dhc-dhcpv6-default-router-00
11. Novak J.: Target-Based Fragmentation Reassembly, Sourcefire, Columbia, MD 2005
12. Hollis K.: Rose Attack Explained, http://digital.net/~gandalf/Rose_Frag_Attack_Explained.htm, retrieved: 16.02.2013
13. Narten T. et al: Neighbor Discovery for IP version 6 (IPv6) (RFC 4861), Draft Standard, IETF 2007
14. Chown T., Venaas Sl.: IPv6 Router Advertisement Problem Statement, (RFC 6104), IETF 2011
15. Chown T.: Dynamic Host Configuration Protocol(DHCP): IPv4 and IPv6 Dual-Stack Issues, (RFC 4477), IETF 2006
16. Durand A. et al.: Operational Considerations and Issues with IPv6 DNS, (RFC 4472), IETF 2006
17. Arkko J.: (Ed.): SEcure Neighbor Discovery (SEND), (RFC 3971), IETF 2005
18. Levy-Abegnoli E. et al.: IPv6 Router Advertisement Guard, (RFC 6105), IETF 2011
19. Ward N.: IPv6 Autoconfig Filtering on Ethernet Switches, Internet Draft, IETF 2009
20. Chown T.: Implications for Network Scanning, (RFC 5157), IETF 2008
21. Chown T.: Default Address Selection for Internet Protocol Version 6 (IPv6), (RFC 6724), IETF 2012

22. Nikander P. (Ed.): IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756, IETF 2004
23. Mankin A.: Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6, Internet Draft, IETF 2002