PD.TVZ.HR
POLYTECHNIC & DESIGN Vol. 13, No. 3, 2025.
Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995
DOI: 10.19279/TVZ.PD.2025-13-3-15

SIMULACIJA SIGURNOSNIH PRIJETNJI U IPV6 MREŽAMA: NAPADI PREPLAVLJIVANJEM RA I NS PORUKAMA

SIMULATION OF SECURITY THREATS IN IPV6 NETWORKS: RA AND NS FLOODING ATTACKS

Miran Dorčec[1], Dunja Bjelobrk Knežević[2], Nikolina Kasunić[2], Ognjen Staničić[2]

[1] Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia, Student
[2] Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia

SAŽETAK

Iako IPv6 donosi brojne prednosti u odnosu na IPv4, uključujući prošireni adresni prostor i poboljšane mehanizme automatizirane konfiguracije, istovremeno uvodi i nove sigurnosne izazove. Rad analizira sigurnosne rizike dva karakteristična napada na IPv6 mreže - napad preplavljivanjem Router Advertisement porukama i napad preplavljivanjem Neighbor Solicitation porukama. Napad preplavljivanjem RA porukama temelji se na slanju velikog broja lažnih RA poruka, što može rezultirati pogrešnom konfiguracijom mrežnih sučelja žrtve. Napad preplavljivanjem NS porukama koristi preopterećenje mreže putem velikog broja Neighbor Solicitation zahtjeva, koji opterećuju memoriju i procesor žrtvinog sustava. Cilj rada bio je demonstrirati takve napade u kontroliranom laboratorijskom okruženju, utvrditi njihov utjecaj na žrtvu te ukazati na slabosti IPv6 sigurnosnih mehanizama i važnost implementacije učinkovitih zaštitnih mjera. Testno okruženje bazirano je na virtualnim strojevima, uz upotrebu alata Scapy za generiranje paketa te alata Wireshark za analizu mrežnog prometa. Dobiveni rezultati pokazuju da su navedeni napadi lako izvedivi te da mogu imati ozbiljan utjecaj na IPv6 mrežu, što naglašava potrebu za odgovarajućim sigurnosnim mjerama i mitigacijskim tehnikama.

Ključne riječi: *IPv6, NDP ranjivosti, sigurnosni napadi, SLAAC ranjivosti*

ABSTRACT

Although IPv6 offers numerous advantages over IPv4, including an expanded address space and improved automated configuration mechanisms, it also introduces new security challenges. This paper analyses security risks associated with two common attacks on IPv6 networks - Router Advertisement and Neighbor Solicitation flooding attacks. The RA flooding attack is based on sending a large number of forged RA messages, potentially resulting in incorrect configuration of the victim's network interfaces. The NS flooding attack overloads the network by generating a high volume of Neighbor Solicitation requests, placing excessive load on the memory and processor of the victim's system. The objective of this study was to demonstrate such attacks in a controlled laboratory environment, assess their impact on the victim, and highlight the weaknesses in the IPv6 security along with the importance of implementing effective protective measures. Testing environment was based on virtual machines and utilized tools such as Scapy for packet generation, as well as Wireshark for network traffic analysis. The results indicate that these attacks are easily executable and can have a significant impact on IPv6 networks, underscoring the need for appropriate security measures and mitigation techniques.

Keywords: *IPv6, NDP vulnerabilities, Security attacks, SLAAC vulnerabilities*

1. UVOD
1. INTRODUCTION

Limitations of existing network protocols are becoming more apparent as Internet use and infrastructure grows by day. The IPv4 protocol, which served as the backbone of internet communication for many years, faces well-documented limitations, such as a shortage of available IP addresses and increasing difficulty in its security management. IPv6 protocol was developed to address these challenges. It offers a larger address space, simpler configurations, and potentially greater security, as it was designed to include security features that were not standard in IPv4. One key advantage of IPv6 is the optional integration of IPsec, which ensures encrypted and authenticated communication, although its adoption in practice remains limited [1]. Despite these improvements, IPv6 is still not immune to security threats. New mechanisms such as Neighbor Discovery Protocol (NDP) introduce new attack vectors not present in IPv4 environments. [2]

The Neighbor Discovery Protocol replaces several functions that was in IPv4 handled by ARP, ICMP Redirect, and router discovery. It is responsible for several IPv6 functions, including router discovery, address resolution, and neighbour reachability detection. Router Solicitation (RS) messages are sent by hosts to request configuration information, while Router Advertisement (RA) messages are used by routers to announce their presence and provide network parameters. Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages support address resolution and reachability verification.

NDP also enables automatic configuration through the Stateless Address Autoconfiguration (SLAAC) mechanism without the need for centralized services like DHCP. [3]

However, although IPv6 offers many benefits, its design and operation can introduce significant vulnerabilities. Unlike IPv4, which uses broadcast-based mechanisms, IPv6 Neighbor Discovery uses multicast communication. While this approach reduces unnecessary network traffic, it also introduces new attack surfaces at the local network level. Attacks exploiting fake RA messages and vulnerabilities in SLAAC represent serious security challenges [4]. The following chapter discusses fundamental vulnerabilities of IPv6, focusing on SLAAC and NDP. In Chapter 3 we describe the research methodology and experimental setup used to simulate RA and NS flooding attacks. In Chapter 4 we discuss results and provide recommendations for minimizing the risks associated with IPv6 deployment.

2. RANJIVOSTI U OSNOVNIM IPV6 MEHANIZMIMA
2. SECURITY VULNERABILITIES IN FUNDAMENTAL IPV6 MECHANISMS

While IPv6 functionalities can significantly ease network administration and improve scalability, they simultaneously open up the network to various types of attacks, particularly within local networks where a certain degree of trust between devices is often assumed. Many vulnerabilities do not result from design flaws, but rather from a lack of additional security layers to protect open mechanisms like NDP and SLAAC. Common attacks include RA spoofing, NA spoofing, and different forms of Denial-of-Service (DoS) through RA, NS, and NA flooding. [4]

2.1. SLAAC RANJIVOSTI
2.1. SLAAC VULNERABILITIES

SLAAC allows IPv6-enabled devices to autonomously generate addresses using RA messages and locally available data, such as their MAC addresses [5]. While this provides significant administrative ease, particularly in large-scale networks, it also introduces privacy and security issues related to automatic configuration. These vulnerabilities arise from the trust devices place in incoming RA messages, which attackers can exploit by sending forged RA messages. This can result in incorrect configuration and potential on-path attacks (formerly known as MitM - Man-in-the Middle). [4]

In addition to the configuration threat, SLAAC poses a privacy risk. Since the MAC address is

often used to generate the host portion of the IPv6 address, devices become easily trackable over extended periods and across different networks. Privacy Extensions address this by modifying the SLAAC address generation process to use temporary, randomized interface identifiers instead of stable, MAC-based ones. These temporary addresses periodically change, which reduces long-term device tracking and improves privacy. However, this mechanism is not always implemented or properly configured, exposing devices to tracking. [6]

While SLAAC is one method for IPv6 address configuration, DHCPv6 [7] also exists and provides a more centralized alternative, similar in concept to DHCP in IPv4. This centralized and controlled address management reduces risks from rogue routers or misconfigurations. Nevertheless, DHCPv6 is known to be susceptible to attacks such as DHCP spoofing.

2.2. ROUTER ADVERTISEMENT (RA) NAPADI

2.2. ROUTER ADVERTISEMENT (RA) ATTACKS

Router Advertisement messages are an integral part of SLAAC, as routers use them to communicate network information to devices. Attackers can exploit this mechanism by sending fake RA messages to manipulate network configurations. There are primarily two types of RA-based attacks: RA flooding and RA spoofing.

RA flooding is a specific DoS attack in IPv6 networks, where attackers flood the network with fake RA messages. These confuse devices, forcing them to constantly update their configurations, which can congest the network and disrupt internet access. The constant state of reconfiguration causes severe instability and impairs communication between devices. As a result, services may become unavailable, and network performance drops.

In contrast, RA spoofing is more targeted. It involves sending a smaller number of fake RA packets posing as legitimate routers to redirect traffic and manipulate network configurations. In a typical RA spoofing scenario, the attacker advertises itself as a default router by sending RA messages with routing parameters designed to influence router selection to its advantage. After the victim selects the attacker as its primary gateway, its IPv6 traffic is forwarded through the attacker's system. This traffic redirection enables MitM attacks and unauthorized data interception, allowing the attacker to inspect od modify traffic without victim's awareness.

Defence mechanisms include implementing RA Guard on network switches, which filters unauthorized RA messages [8], [9]. However, RA Guard can be bypassed by advanced techniques. Additional protections include filtering ICMPv6 messages, segmenting networks to limit the injection of new RA messages, SEND - Secure Neighbor Discovery, ACLs on switches, etc.

2.3. NEIGHBOR DISCOVERY (ND) NAPADI

2.3. NEIGHBOR DISCOVERY (ND) ATTACKS

IPv6 relies on the Neighbor Discovery Protocol to identify adjacent devices and maintain up-to-date neighbor tables, but the lack of authentication in NDP messages makes it vulnerable. Two common attack types are NS/NA flooding and NA spoofing attacks.

In flooding attacks, attackers send a massive number of NS and NA messages, overloading neighbor tables (Neighbor Table Overflow). Once full, legitimate NS and NA messages are ignored, disrupting device communication.

In Neighbor Spoofing, the attacker claims ownership of an IPv6 address by sending fake NA messages, misleading devices to route traffic to the attacker - causing traffic redirection or loss.

NDP attacks can destabilize networks similarly to how ARP spoofing affects IPv4 networks. Mitigation includes Secure Neighbor Discovery (SEND), which uses cryptographic protections to prevent fake NDP messages, and limits on the number of neighbors per device [10]. While SEND offers strong protection, its complexity and cost hinder widespread adoption. SLAAC Monitoring tools can also be used

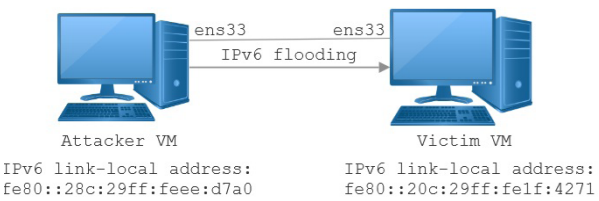
by administrators to detect abnormal changes indicative of attacks.

Previous studies consistently report that these types of attacks can be easily executed in local networks without advanced protections like RA Guard or SEND. These findings have been demonstrated through security assesment [4], vendor analyses [9], and experimental evaluations [11], [12].

3. METODOLOGIJA I TESTNO OKRUŽENJE

3. METHODOLOGY AND TESTING ENVIRONMENT

The testing environment consisted of two virtual machines, one representing the attacker and the other the victim, both configured within VMware Workstation Player 17 [13] and running the Ubuntu 20.04 LTS as the operating system [14]. Both virtual machines have a network interface ens33, which was automatically assigned by the Ubuntu operating system during installation process. Usage of virtual machines enabled controlled experimentation and isolation of the test network. When setting up the virtual machines, the NAT networking mode was used only to provide an isolated virtual network in which both virtual machines were within the same Layer 2 broadcast domain. Figure 1 shows network topology used in this experiment.



Slika 1 *Mrežna topologija eksperimentalnog okruženja s virtualnim strojevima napadača i žrtve unutar iste Layer 2 mreže*

Figure 1 *Network topology of the experimental setup, illustrating the attacker and victim virtual machines in the same Layer 2 network*

NAT gateway in this scenario does not participate in IPv6 SLAAC and does not generate RA messages. This enables simulation of local IPv6 attacks without exposing external networks. Figures 2 and 3 show the network interface configuration of the attacker's and victim's virtual machines, respectively, including the IPv6 addresses assigned to their ens33 interfaces.

```
ubuntu@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.130  netmask 255.255.255.0  broadcast 192.16
        inet6 fe80::20c:29ff:feee:d7a0  prefixlen 64  scopeid 0x20<l
        ether 00:0c:29:ee:d7:a0  txqueuelen 1000  (Ethernet)
        RX packets 3615  bytes 4743287 (4.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1617  bytes 170323 (170.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Slika 2 *Ispis konfiguracije mrežnog sučelja ens33 na računalu napadača*

Figure 2 *Network configuration output for the ens33 interface on the attacker's computer*

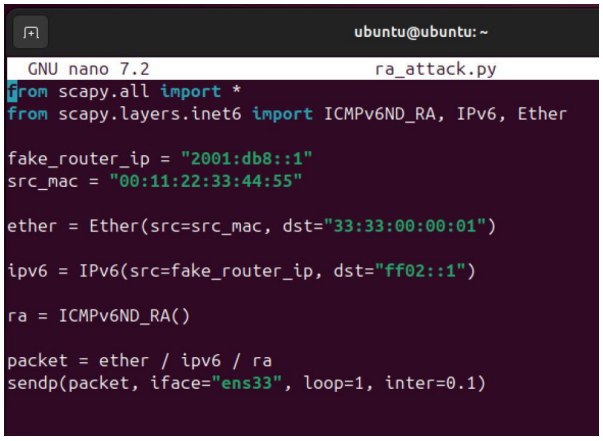
```
ubuntu@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.129  netmask 255.255.255.0  broadcast 192.168
        inet6 fe80::20c:29ff:fe1f:4271  prefixlen 64  scopeid 0x20<li
        ether 00:0c:29:1f:42:71  txqueuelen 1000  (Ethernet)
        RX packets 62445  bytes 91926166 (91.9 MB)
        RX errors 0  dropped 15  overruns 0  frame 0
        TX packets 5429  bytes 415704 (415.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Slika 3 *Ispis konfiguracije mrežnog sučelja ens33 na računalu žrtve*

Figure 3 *Network configuration output for the ens33 interface on the victim's computer*

The attacker's machine was equipped with tools used for generating and analyzing IPv6 traffic. Scapy is an open-source Python library for creating and manipulating network packets [15]. In this experiment, Scapy was used to create forged RA messages that were sent to the victim's interface. These messages simulated a rogue router within the network. Scapy was also used to generate a large number of NS messages. Wireshark, a network protocol analyzer [16], was used on both the attacker's and victim's computers for capturing IPv6 traffic during both attacks, providing a visual confirmation of abnormal packet rates.

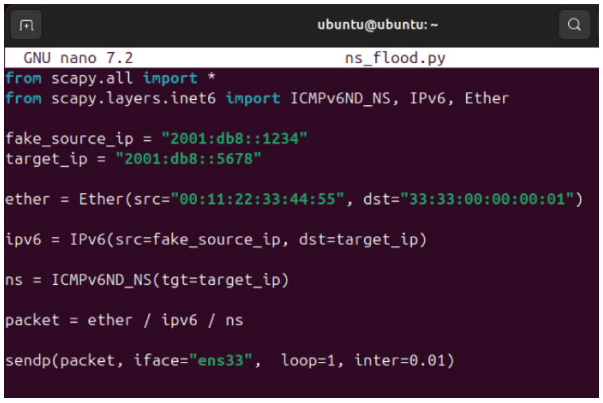
The Router Advertisement (RA) flooding attack was the first simulated attack, carried out using prewritten script based on the Scapy library, as shown in Figure 4. The script generates forged RA messages in which the attacker advertises itself as a router in the local IPv6 network, by using a fake IPv6 address (2001:db8::1) and spoofed source MAC address (00:11:22:33:44:55). These RA messages are sent to the IPv6 all-nodes multicast address (ff02::1) and packets are continuously sent through the ens33 interface.



Slika 4 *Skripta za pokretanje RA napada s virtualnog stroja napadača*

Figure 4 *Script for launching RA attack from attacker's VM*

The Neighbor Solicitation (NS) flooding attack was also carried out using prewritten script based on the Scapy library, as shown in Figure 5. The script generates a high volume of NS messages using a spoofed source IPv6 address (2001:db8::1234) and unicast IPv6 address as a target address (2001:db8::5678). Similar as in the previous attack, a spoofed source MAC address (00:11:22:33:44:55) is used and NS packets are continuously sent through the ens33 interface.



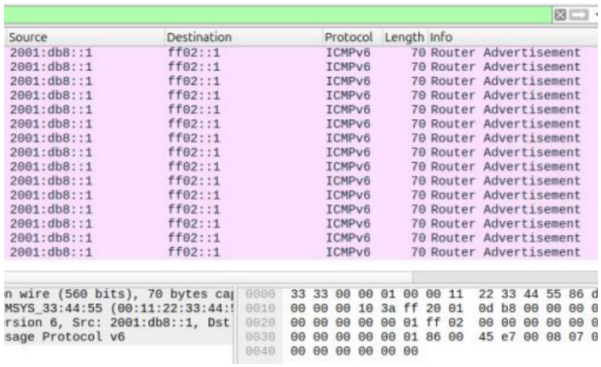
Slika 5 *Skripta za pokretanje NS napada s virtualnog stroja napadača*

Figure 5 *Script for launching NS attack from attacker's VM*

4. REZULTATI I ANALIZA
4. RESULTS AND ANALYSIS

This section presents the results obtained from the simulated RA and NS flooding attacks.

The goal of the RA flooding attack was to overwhelm the victim with a large number of RA messages with the purpose of disrupting the normal router discovery process and creating unstable routing conditions leading to tricking the victim into accepting the fake router as legitimate. During the experiment, Wireshark was used to capture traffic on the victim's machine during the attack, providing a visual confirmation of abnormal RA message rates (Figure 6).



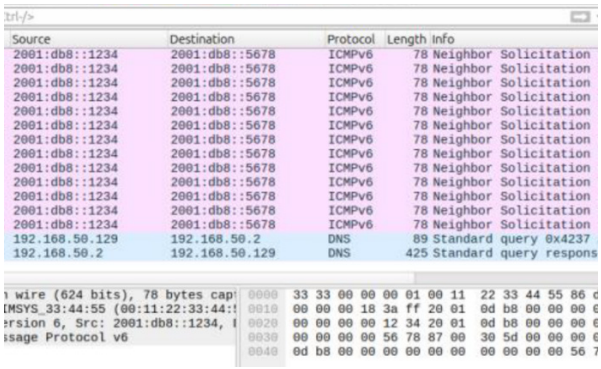
Slika 6 *Wireshark – snimka prometa na računalu žrtve koja pokazuje neuobičajeno veliku količinu RA poruka*

Figure 6 *Wireshark - captured traffic on victim's computer showing unusually high volume of RA messages*

Impact on the network:

- The victim received a large number of forged RA messages
- The continuous influx of RA messages containing false network information indicates unstable router behaviour and network conditions that are not normal, suggesting the presence of an attack
- In a real network environment with a legitimate IPv6 router present, the RA flooding attack could cause clients to prioritize the rogue router as a default gateway, resulting in traffic redirection, loss of connectivity, or man-in-the-middle scenarios. Continuous reconfiguration may also lead to temporary loss of default routes.

The second attack executed was the Neighbor Solicitation (NS) flooding attack. The goal of the NS flooding attack was to overwhelm a host with a large number of NS messages, leading to disruption of the usual behaviour expected from the IPv6 NDP process and overloading networking equipment and the victim's machine. During the experiment, Wireshark was used to capture traffic on the victim's machine during the attack, providing a visual confirmation of abnormal NS message rates (Figure 7).



Slika 7 *Wireshark - snimka prometa na računalu žrtve koja pokazuje neuobičajeno veliku količinu NS poruka*

Figure 7 *Wireshark - captured traffic on victim's computer showing unusually high volume of NS messages*

Impact on the network:

- The victim machine received a large number of NS requests, resulting in abnormal network traffic conditions, observable at the network interface
- The continuous influx of NS messages indicates abnormal behaviour of Neighbour Discovery mechanism and unstable network conditions, suggesting the presence of the attack
- In the conducted experiment, the impact of the NS flooding attack was observed as a increase in ICMPv6 traffic. In a real network environment, if the targeted IPv6 address belonged to a legitimate host, such behaviour would force that host to continuously respond which would in turn lead to exhaustion of the neighbour cache or increased processing, causing denial-of-service conditions on this targeted host.

Although different in execution, both attacks shared a common goal—to destabilize the IPv6 network and disrupt or degrade the victim's network communication. The RA flooding attack focused on altering the victim's network configuration and routing logic, causing frequent changes, whereas the NS flooding attack aimed to exhaust neighbour table resources.

The simulation results indicate a potentially significant impact of both attacks on the victim's system performance. Both attacks were executed with minimal resources and without the need for escalation of privilege, making them a serious threat in unsecured network environments. The results demonstrate that IPv6 Neighbor Discovery mechanisms can be exploited to generate abnormal network conditions in unsecured environments, highlighting the need for additional security mechanisms.

5. ZAKLJUČAK
5. CONCLUSION

IPv6 introduces several improvements over IPv4, including larger address space, support for automatic configuration, and integrated support for security such as IPsec. However, despite offering more advanced features, it also introduces new security consideration, especially in the local network environment.

Security risks associated with Router Advertisement attacks have demonstrated that IPv6 networks using automatic address configuration can be vulnerable to serious attacks. RA flooding attacks can influence client behaviour through the router discovery process, leading to network destabilization.

The simulations conducted in this study demonstrate the vulnerability of IPv6 networks to basic attacks exploiting weaknesses in the Neighbor Discovery Protocol mechanisms. By using forged Router Advertisement messages, RA attacks can cause unauthorized changes in network configurations, while NS flooding attacks overwhelm the victim's system resources by generating large volumes of unnecessary Neighbor Solicitation requests. Both attacks exploit the fact that IPv6 does not provide authentication for the source of such messages by default, enabling attackers to successfully impersonate devices on the network. The findings indicate the importance of implementing additional non-default security measures in IPv6 environments, such as RA Guard (which filters unauthorized RA messages) and Secure Neighbour Discovery (SEND), which uses cryptographic signatures to validate messages.

This study confirms that using simple tools can threaten the stability of IPv6 networks, highlighting the need for a proactive approach in designing and configuring IPv6 infrastructure to mitigate security risks. The key to securing IPv6 networks lies in the correct application of security technologies and standards, as well as proactive monitoring of potential security threats.

6. REFERENCE

6. REFERENCES

[1.] IPv6 Implementation Guide, Cisco IOS Release 15.2S - Implementing IPsec in IPv6 Security [Cisco IOS 15.2S]', Cisco. Accessed: Jan. 17, 2026. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2s/ipv6-15-2s-book/ip6-ipsec.html

[2.] S. E. Deering and B. Hinden, 'Internet Protocol, Version 6 (IPv6) Specification', Internet Engineering Task Force, Request for Comments RFC 8200, Jul. 2017. doi: 10.17487/RFC8200.

[3.] W. A. Simpson, T. Narten, E. Nordmark, and H. Soliman, 'Neighbor Discovery for IP version 6 (IPv6)', Internet Engineering Task Force, Request for Comments RFC 4861, Sep. 2007. doi: 10.17487/RFC4861.

[4.] F. Gont, 'Results of a Security Assesment of the Internet Protocol version 6 (IPv6)', 2012.

[5.] T. Narten, T. Jinmei, and S. Thomson, 'IPv6 Stateless Address Autoconfiguration', Internet Engineering Task Force, Request for Comments RFC 4862, Sep. 2007. doi: 10.17487/RFC4862.

[6.] A. Cooper, F. Gont, and D. Thaler, 'Security and Privacy Considerations for IPv6 Address Generation Mechanisms', Internet Engineering Task Force, Request for Comments RFC 7721, Mar. 2016. doi: 10.17487/RFC7721.

[7.] T. Mrugalski et al., 'Dynamic Host Configuration Protocol for IPv6 (DHCPv6)', Internet Engineering Task Force, Request for Comments RFC 8415, Nov. 2018. doi: 10.17487/RFC8415.

[8.] G. V. de Velde, J. Mohácsi, E. Levy-Abegnoli, and C. Popoviciu, 'IPv6 Router Advertisement Guard', Internet Engineering Task Force, Request for Comments RFC 6105, Feb. 2011. doi: 10.17487/RFC6105.

[9.] 'Security Configuration Guide, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches) - Configuring IPv6 RA Guard [Support]', Cisco. Accessed: Jan. 17, 2026. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst1000/software/releases/15_2_7_e/configuration_guides/sec/b_1527e_security_c1000_cg/configuring_ipv6_ra_guard.html

[10.] J. Kempf, J. Arkko, B. Zill, and P. Nikander, 'SEcure Neighbor Discovery (SEND)', Internet Engineering Task Force, Request for Comments RFC 3971, Mar. 2005. doi: 10.17487/RFC3971.

[11.] F. Najjar, Q. Bsoul, and H. Al-Refai, 'An Analysis of Neighbor Discovery Protocol Attacks', Computers, vol. 12, no. 6, p. 125, Jun. 2023, doi: 10.3390/computers12060125.

[12.] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. B. Omar, 'SADetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network', Informatica, vol. 46, no. 9, 2022, doi: 10.31449/inf.v46i9.4441.

[13.] 'VMware Workstation Pro 17.0'. Accessed: Jan. 18, 2026. [Online]. Available: https://techdocs.broadcom.com/us/en/vmware-cis/desktop-hypervisors/workstation-pro/17-0.html

[14.] '20.04 LTS', Ubuntu. Accessed: Jan. 18, 2026. [Online]. Available: https://ubuntu.com/blog/tag/20-04-lts

[15.] 'Welcome to Scapy's documentation! — Scapy 2.7.0 documentation'. Accessed: Jan. 18, 2026. [Online]. Available: https://scapy.readthedocs.io/en/latest/

[16.] 'Wireshark User's Guide'. Accessed: Jan. 18, 2026. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/

AUTORI · *AUTHORS*

• Dunja Bjelobrk Knežević - (Zagreb, 1985) graduated in 2009 from the Faculty of Electrical Engineering and Computing, University of Zagreb, majoring in Telecommunications and Informatics. The same year she was employed as an assistant at the professional studies of Computer Science and Informatics at the Zagreb University of Applied Sciences. Since 2014, she has been working as a lecturer, and then as a senior lecturer, with a teaching focus on courses in the field of computer networks and unconventional computing procedures. She is particularly interested in contemporary topics in the field of network technologies and network security.

Korespondencija · *Correspondence*

dbk@tvz.hr

• Nikolina Kasunić - The unchanged biography can be found in Polytechnic & Design Vol. 10, No. 2, 2022.

Korespondencija · *Correspondence*

nkasunic@tvz.hr

• Ognjen Staničić - He graduated in 2010 as a graduate engineer in electrical engineering at the Faculty of Electrical Engineering and Computing, University of Zagreb, was elected to the associate title of assistant in 2011, to the title of lecturer in 2015, and to the title of senior lecturer in 2021 at the Zagreb University of Applied Sciences. He teaches the courses Interactive Web Programming and Advanced JavaScript Programming at the Faculty of Informatics and Computer Science at the Zagreb University of Applied Sciences. His primary work and education interests are the development of modern web applications primarily using the JavaScript programming language and its frameworks (Angular, Node.js).

Korespondencija · *Correspondence*

ostanicic@tvz.hr