Bachelor Thesis

February 4, 2026

From Security by Obscurity to Imminent Exposure:

Security Risks for IoT Devices in the IPv6 Transition

Jorge Miguel Angel Vite Espinosa

of University of Zurich, Switzerland (23-746-399)

supervised by

Prof. Dr. Ivan De Oliveira Nunes

University of Zurich[UZH]

Bachelor Thesis

From Security by Obscurity to Imminent Exposure:

Security Risks for IoT Devices in the IPv6 Transition

Jorge Miguel Angel Vite Espinosa

University of Zurich[UZH]

Bachelor Thesis

Author: Jorge Miguel Angel Vite Espinosa, jorgemiguelangel.viteespinosa@uzh.ch

URL: https://github.com/Vite04/ThesisCode

Project period: 2026-01-15 - 2026-07-01

Security and Privacy of Information, Networks, and Systems (SPINS)
Department of Informatics (IfI), University of Zurich

Acknowledgements

Abstract

Contents

1. Introduction

This thesis explores how global IPv6 addressing increases the attack surface of the Internet of Things (IoT) environment. The study combines not only a comprehensive literature review but also an empirical assessment of default system configurations through controlled laboratory demonstrations, highlighting how the adoption of new network standards can potentially affect the security of millions of end devices.

The IPv4 to IPv6 Transition is the result of an inherent limitation in the design of IPv4's address space, which only supports 2^{32} unique addresses. A boundary already exceeded by the estimated 16 billion IoT devices alone in 2024 **iotanalytics2024**. IPv6 mitigates this limitation by implementing a 128-bit architecture, offering a virtually infinite address space. Despite its technical advantage, the global adoption has been gradual due to the current scale of IPv4-based infrastructures and the cost of migration. Therefore, technologies such as Network Address Translation (NAT) were adopted to extend the lifetime of IPv4 **rfc3022**.

In practice, NAT allows multiple internal hosts within a private local-area network (LAN) to share a single IPv4 address by translating internal IP addresses and TCP/UDP port numbers to a public address and port at the network boundary. This translation process is stateful and connection-oriented, meaning that the address mappings are created only for outbound traffic initiated by hosts within the LAN **rfc3022**, **rfc4787**. Consequently, unless explicitly allowed through static port-forwarding rules, any unsolicited inbound traffic that does not match an existing mapping entry is discarded by default **rfc4787**. Nonetheless, the use of NAT translation tables violates the original end-to-end connectivity principle of the Internet architecture **saltzer1984end**, and simultaneously provides a form of perimeter protection by preventing direct external access to internal hosts.

Loss of NAT and IoT Exposure

Research Objectives & Questions

Contributions

Thesis Structure

2. Background and Related Work

IPv6 Architecture vs. IPv4

The IoT Security Landscape

Network Perimeter Security

3. Methodology

Research Design

Experimental Setup

Ethical Considerations

4. Configuration and Risk Analysis

Default Router Configurations

IPv6 Attack Vectors

5. Experimental Demonstration

Scenario: Global Accessibility of an IoT Device

Scanning and Enumeration Results

Vulnerability Exploitation

6. Mitigation Strategies

Recommendations for Network Administrators

Recommendations for Manufacturers

End-User Best Practices

7. Discussion and Limitations

Interpretation of Results

Limitations

Threats to Validity

8. Conclusion and Future Work

A. First Appendix

B. Second Appendix