THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

Wire-speed FPGA packet filter with Ethernet MAC and web server using a RISC-V softcore processor

Project Proposal

Matthew Gilpin

45801600

Semester 1, 2023

The University of Queensland

School of Information Technology and Electrical Engineering

List of Abbreviations

Abbreviations	
IoT	Internet of Things
FPGA	Field Programmable Gate Array
pf	Packet Filter
MAC	Medium Access Control
ISA	Instruction Set Architecture

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter provides the necessary background and reasoning behind the proposed project.

1.1 Background

In a technology age of growing numbers of cyber attacks and record number of connected devices, it's paramount to ensure these devices operate safely and securely. The Australian Cyber Security Center (ACSC) received in excess of 76,000 cybercrime reports and growing in the 2021-22 financial year [1]. The growing trend of Internet of Things (IoT) will provide more opportunity for black hats (malicious attackers). IHS Markit estimates 125 billion IoT devices will be connected by 2030 [2].

To cope with the increase in IoT devices, a common shift to edge computing has evolved in favour over the traditionally more centralised cloud computing architecture. The core principals behind the paradigm is to move the data processing closer geographically to its origin to not only decrease the central load, but to improve latency [3]. Due to the distributed load, smaller and more efficient computers can be used at the edge/perimeter of these networks [3]. Just like any other computer connected to the broader network, these edge networks also need to be protected from bad actors.

1.2 Topic

While there is no single solution that will fully protect an edge network, a common and effective way to reduce the unauthorised/unwanted network traffic is by simply filtering out the potentially malicious packets. While this may seem overly complex, in reality a few simple rules can be followed to decide on whether to forward or deny/drop/block packets from entering or exiting a network. These packet filters (pf) are a type of firewall that do not follow any complex rules and keep state between packets or use deep packet inspection to check the contents of the payload to ensure it's not malicious.

Packet filters are considered as stateless and traditionally only filter based on the fields in the headers at the network (layer 2) and transport (layer 3) layers [4]. Such fields include IP addresses, port numbers and protocol type.

The proposed project consists of making a hardware implementation of a pf with custom Ethernet Media Access Controllers (MAC) connected to a hardware based filtering block which is all controlled by a RISC-V softcore processor. This will then also have a web interface so that a user can configure the rules for the pf.

1.3 Aims

The aims of the proposed FPGA Ethernet controller and web interface on a RISC-V processor are:

- Increase security to edge IoT networks,
- Increase the power efficiency for wire-speed firewalls, and
- Decrease the latency for packet filter firewalls.

1.4 Establishing Exclusions

While the proposed project will reduce the likelihood of network based attacks it is not a *'one size fits all'* solution. By the nature of the IoT and edge network ecosystem, there are a myriad of different attack vectors where not all of them will be detectable at the network level.

The proposed project will **not**

- Protect against all attacks,
- Be able to protect against all IoT devices, or
- Perform routing

Chapter 2

Background

Some of the concepts behind the proposed project, such as an Ethernet MAC or RISC-V processor are not new, there is a variety of previous works in these areas. This part of the proposal will explore the prior work related to the project.

2.1 Custom MAC

The decision in creating a custom MAC might be considered as insteresting given the range of pre-existing Intellectual Property (IP) cores for Ethernet on FPGAs. The issue with the pre-existing solutions only have a single output to connect to something like a softcore processor. To create a firewall, the network traffic would need to pass through the processor. To decrease latency, a second interface can be added to the MAC to allow traffic to flow through a hardware-based firewall. This is analogous to the direct memory access (DMA) controller on most modern microprocessors.

2.2 Packet Filter Firewall

Usually, the first line of defence against bad actors, it is a vital component in a computer network and can become vastly complex. There are several types of Firewalls such as packet filters (pf), stateful packet firewalls and application firewalls [4]. Firewalls can also perform other tasks and employ other techniques to secure a network, however, in this project the most basic pf-style firewall will be implemented. Packet filters are considered as stateless and traditionally only filter on the fields in the headers in the network (layer 2) and transport (layer 3) layers [4]. Such fields include IP addresses, port numbers and protocol type.

More advanced firewalls can perform deep packet inspection and explore the contents of the higher layers to better evaluate a packets true intention. While there is provision to add this functionality on an FPGA based firewall, this will not be explored in this project due to its significant increase in complexity.

2.3 RISC-V processor

The IEEE 802.3 standard [5], more commonly known by the name of 'Ethernet' defines the *'Medium Access Control'* (MAC) protocol amongst other things for two or more devices to communicate over a network. This standard is just one part in the layered network models such as the OSI model and TCP/IP models.

RISC-V, a reduced instruction set computer architecture, is an open and royalty free instruction set architecture (ISA). As a result, a plethora of soft-core processors have been made. The specific core proposed in this project is the 'NEORV32' RISC-V processor. It's a highly configurable microcontroller like system on chip (SoC) written purely in VHDL.

Chapter 3

Timeline and Plan

This section of the report details the plan and timeline of the proposed project. It also details the necessary risk assessment.

3.1 Milestones

Table 3.2 shows the tasks and expected durations of the proposed project.

Task	Details	Duration
Create MAC	Create custom Layer 2 Ethernet hardware based on the IEEE 802.3 standard	3-4 Weeks
Wishbone Interface	Connect the Ethernet MAC to the NEORV32 RISC-V Processor using the wishbone interface and access it via software	2 Weels
Webserver	Create and Get the webserver working on the NEORV32 Processor. Web page should be accessed from another computer	5-6 Weeks
Firewall Hardware	Create the hardware between 2 Ethernet MACs to filter out packets based on rules	3-4 Weeks
Integration with software	Add functionality to the server to be able to configure the firewall rules	1 Week
Measure and Compare	Compare to pre-existing solutions	1 Week

Table 3.1: Milestones for the proposed project

3.2 Project Risk Assessment

The majority of the work compeleted in the proposed project is digital and poses little risk outside of the standard office sitting.

Risk	Severity	Likelyhood	Mitigation
Licensing	Minor	Moderate	Avoid software/hardware that requires a specific license.
Data loss	Catastrophic	Unlikely	Ensure all items are backed-up to the cloud and use services such as GitHub where appropriate. Employ a 3 2 1 backup strategy
Hardware Failure	Moderate	Unlikely	Double check all connections to the FPGA board before powering. Reduce excessive handling where necessary to minimise risk of damaging the equiptment
Illness	High	Likely	Take breaks periodically to avoid being over-worked, and take necessary recovery steps if sick.
Missed Deadlines	Major	Likely	Ensure plans are followed and compelete tasks as soon as possible. If behind, spend extra time on project to catch up.

Table 3.2: Risk assessment of proposed project

Chapter 4

Conclusion

Conclude your thesis.

Bibliography

[1] A. C. S. Center, "Acsc annual cyber threat report, july 2021 to june 2022," Nov 2022.

[2] IHS, "The internet of things: a movement, not a market," tech. rep., IHS Markit, 2017.

[3] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge computing perspectives: Architectures, technologies, and open security issues," in *2019 IEEE International Conference on Edge Computing (EDGE)*, pp. 116–123, IEEE, 2019.

[4] E. W. Fulp, "Chapter e74 - firewalls," in *Computer and Information Security Handbook*, pp. e219–e237, Elsevier Inc, third edition ed., 2017.

[5] "IEEE Standard for Ethernet," standard, The Institute of Electrical and Electronics Engineers, Inc., New York, USA, Dec. 2012.

Appendix A

Appendix

Write your appendix here. Following two are examples.

A.1 Name of Appendix-1

A.2 Name of Appendix-2