WWW.MWFTR.COM

Network Packet Inspection and Intrusion Detection

Team

Laurence Wilson (CE)
Tolu Onibiyo (CE)
Marlon Winder (CE)
Idris Ozoya (EE)
Hassan Ayinde (EE)

Background

Customer needs:

- Extremely fast packet† processing
- Detect malicious behavior that compromise security of a computer system
- Improve packet inspection and enhance intrusion detection

† A packet is a block of data transmitted over the network

On July 19, 2001 more than 359,000 computers were infected with the code red worm in less than14hours

Contents

- Background
- Problem Formulation
- Functional Requirements
- Approach
  - Alternative designs
  - Adopted solution
- Cost Analysis
- Ethics and Standards
- Conclusion
- Acknowledgements

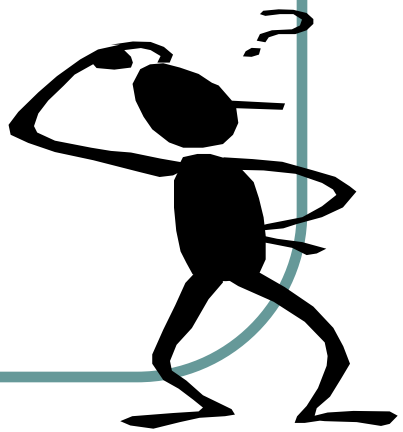
Problem Formulation

Definition:

Design a packet processor that will reduce the processing time of network intrusion detection

Design Requirements:

- Performance
- User friendly
- Enhance intrusion detection for the end user (typically network administrators).



Functional Requirements

Hardware

- Process packets at line speed (100mbps)
- Search for “don’t care” bytes
- Support of relational operations (i.e. =, !=, <, > est..)
- Search for matches given data input at a rate in excess of 1Gb/s

Software

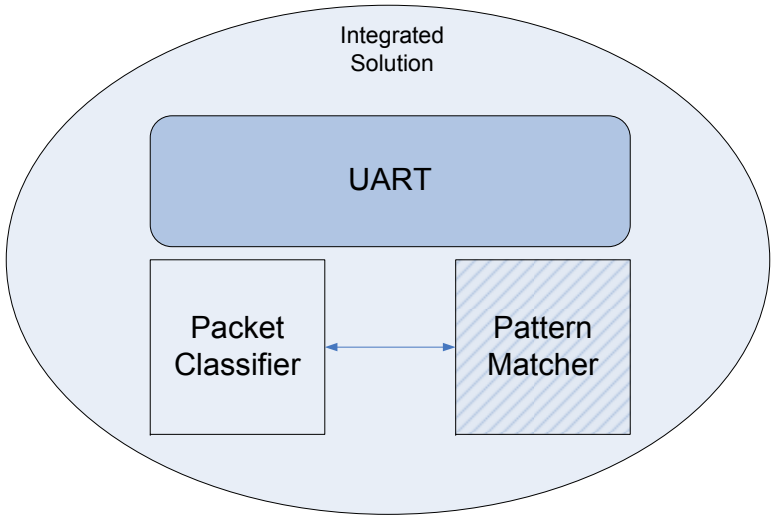
- Configuration and manipulation of search patterns
- Receive signals from the hardware device
- Provide statistics regarding match count

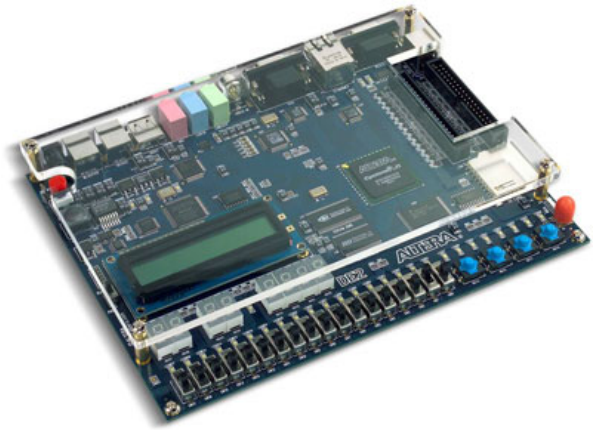
Approach

Alternative Designs

- Pure software based approach
  - Enhanced Parallel Processing
  - Snort Algorithm
- Hardware Based Approach
  - PIC16F877
  - Motorola 68000
  - Custom FPGA
- Hybrid Approach
  - Software
  - Hardware

Adopted Solution



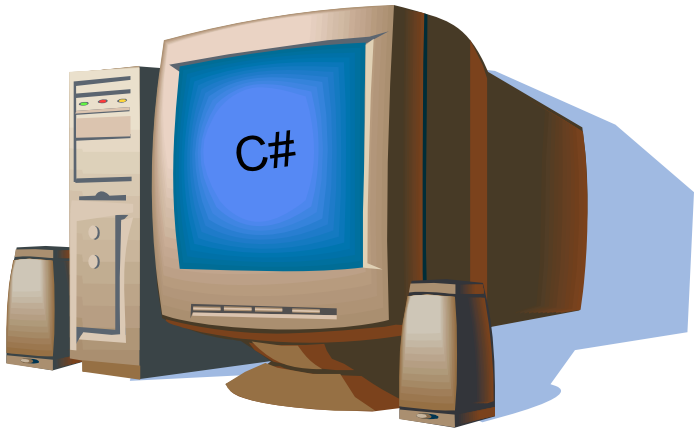


- **Friendly User Interface**
- **Process and Identify Packets**
- **Identifies Information of Interest**
- **Implemented on an FPGA † Board**

† An FPGA (Field Programmable Gate Array) is a semiconductor device used to evaluate the design

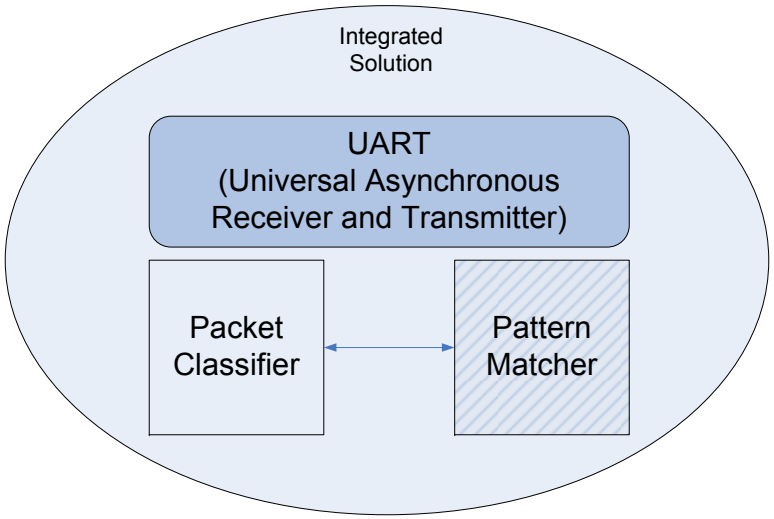
System Components

Front-End



Client (C#)

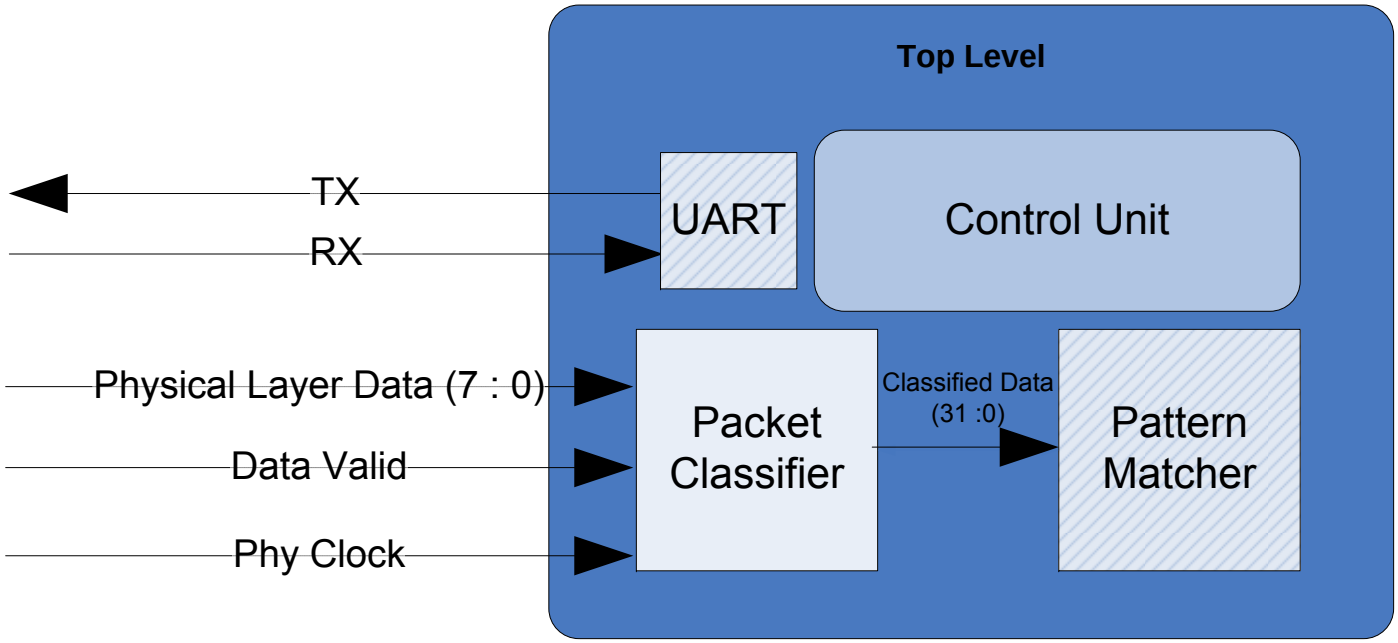
Back-End Processing



Hardware (VHDL)

Top-Level System Schematic

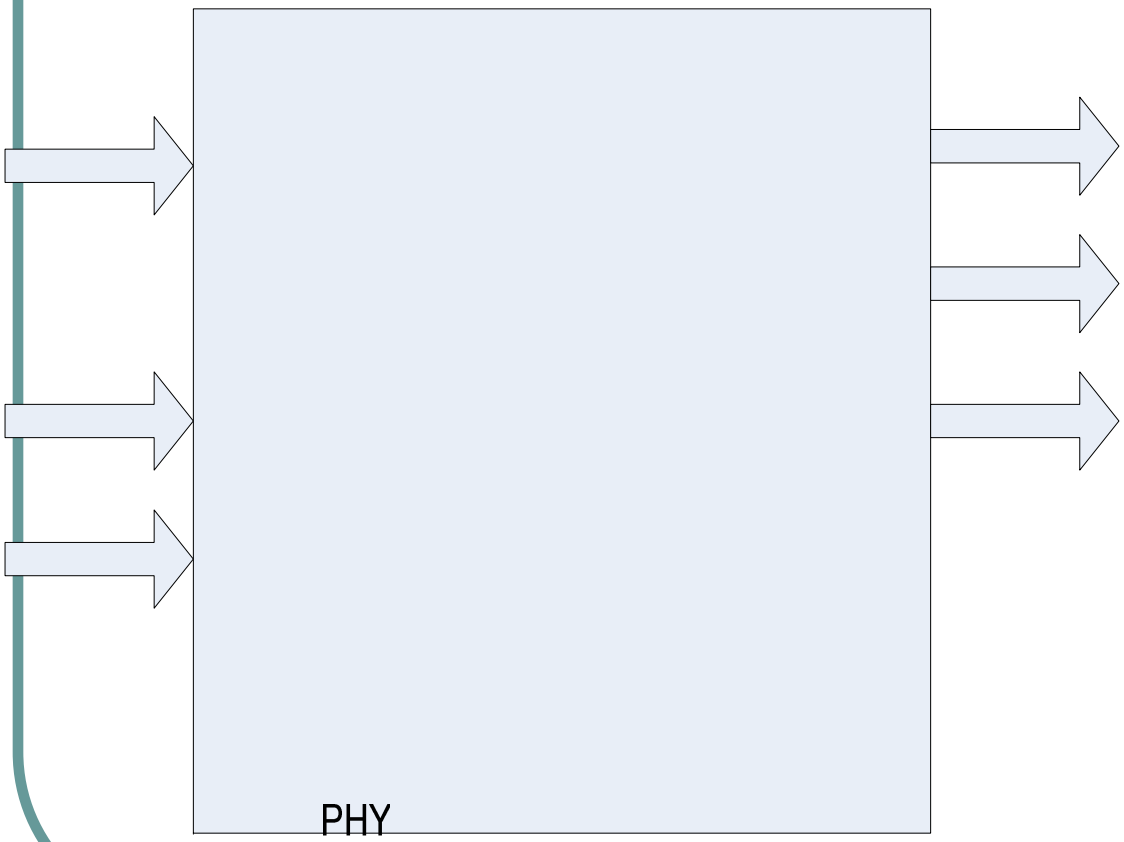
Top Level Diagram



TX – Transmit Data

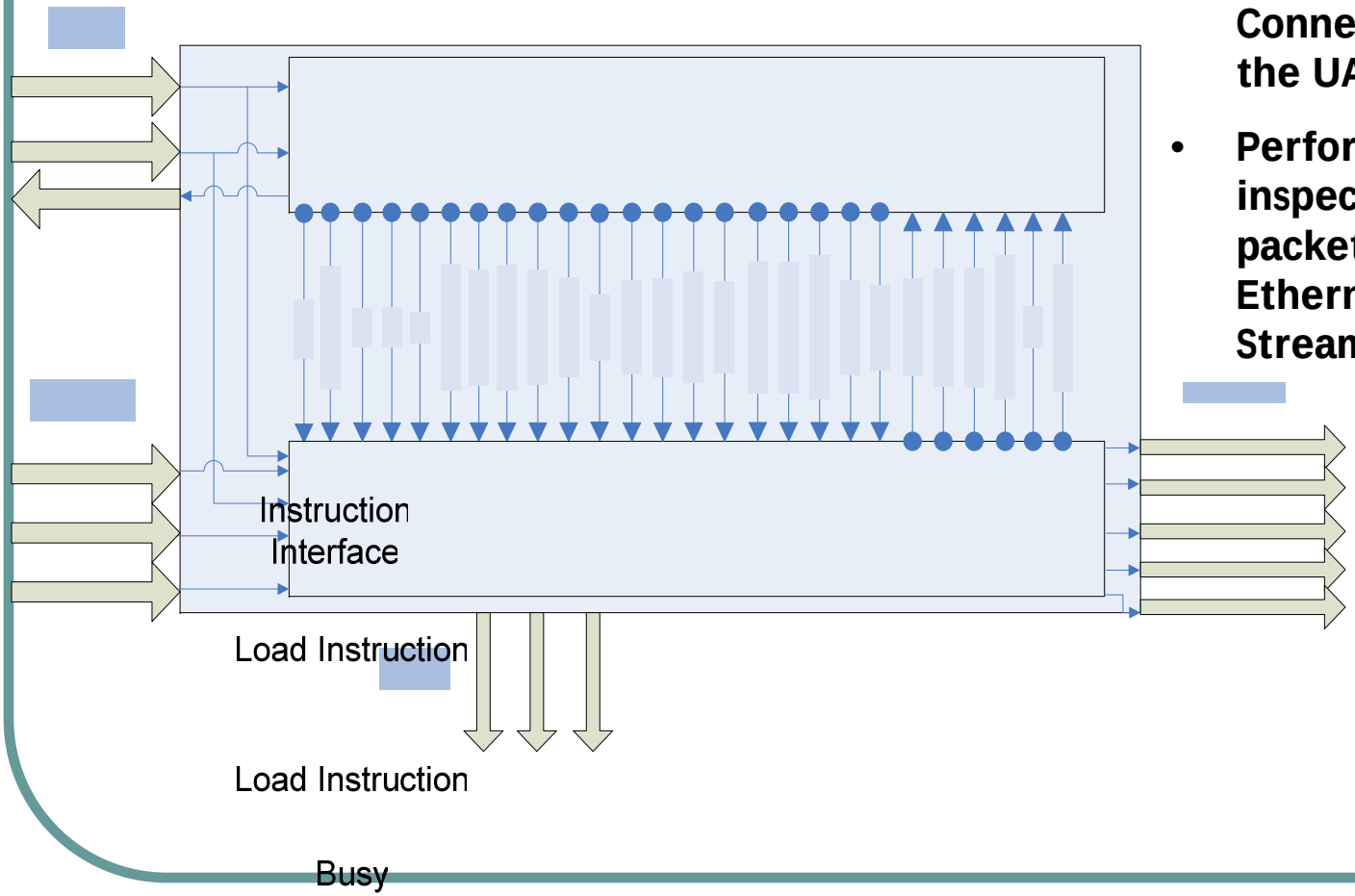
RX – Receive Commands

Packet Classifier



- Provides classified data to the pattern matcher for inspection
- Field_type indicates which portion of the packet is being provided
- Data_ready signals to Pattern Matcher that Field_data is valid
- Composed of an FSM that executes the Ethernet Protocol

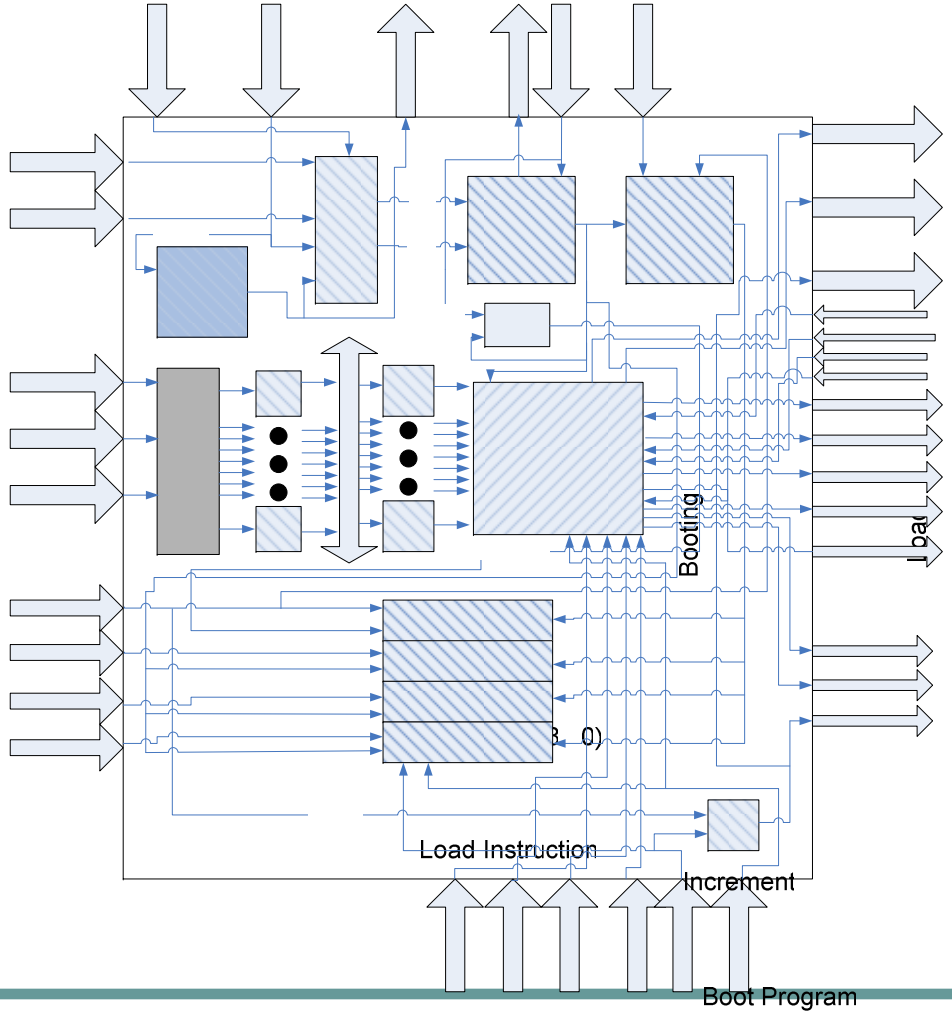
Pattern Matcher



- **Interactive Interface Connects to UI via the UART Driver**
- **Performs the actual inspection of the packets via the Ethernet Frame Stream**

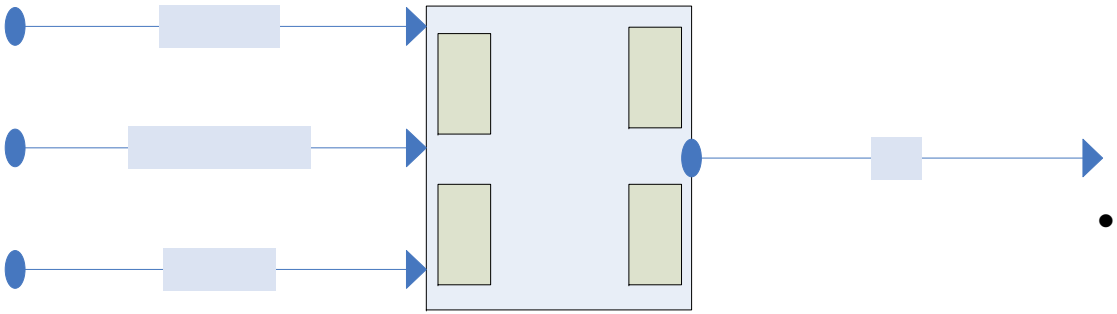
g uction bined nplex bined nplex nple All rget urce rand tion Done Contrib Contrib tion

Data Unit



- **Stack Oriented Processing**
- **Logic Units Perform Comparisons**
- **Alert Engine Enables more complex signatures**

Logic Unit – The Heart of Our Design



- Compares the incoming classified data to the target programmed
- Enables all relational operators (=, !=, <=, and >=) based on the operand
- Output “Match” triggers a counter to increment
- An intermediate place for classified packet data
- Outputs are fed to the Logic Unit for Comparison

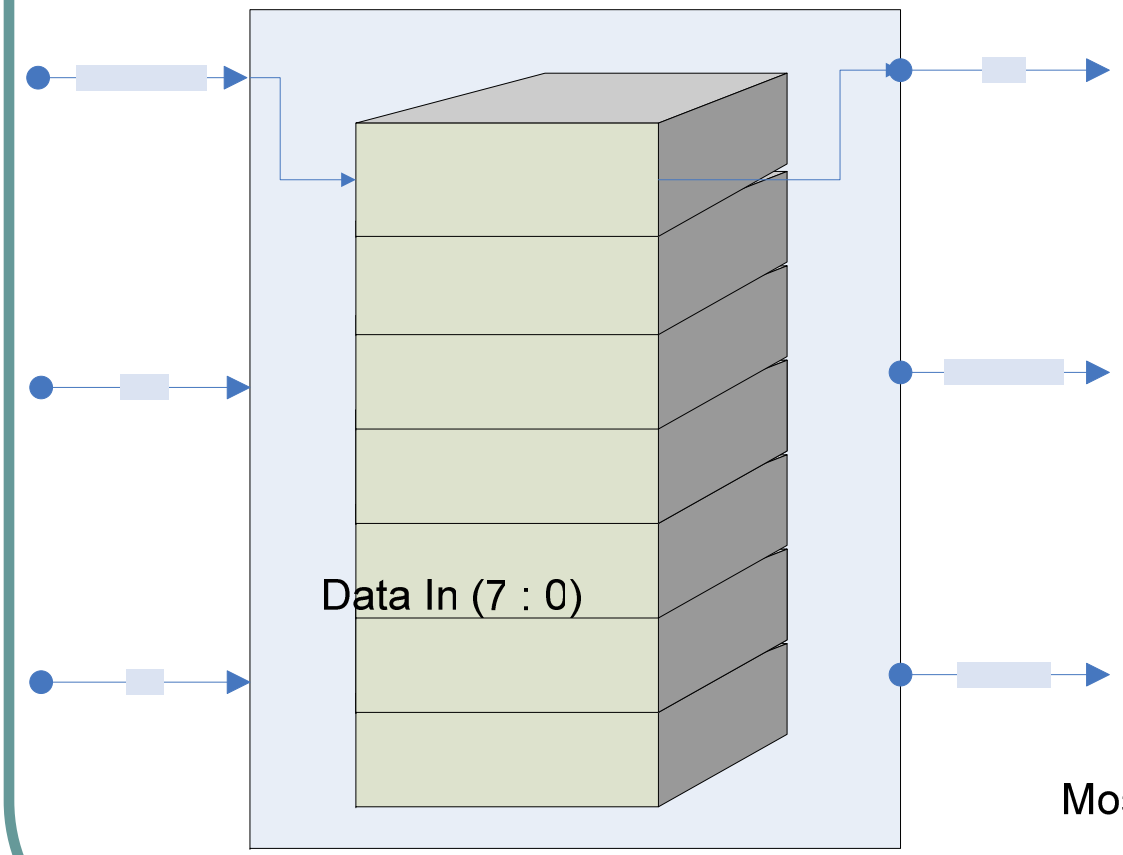
Operand (1 :0)

=

!=

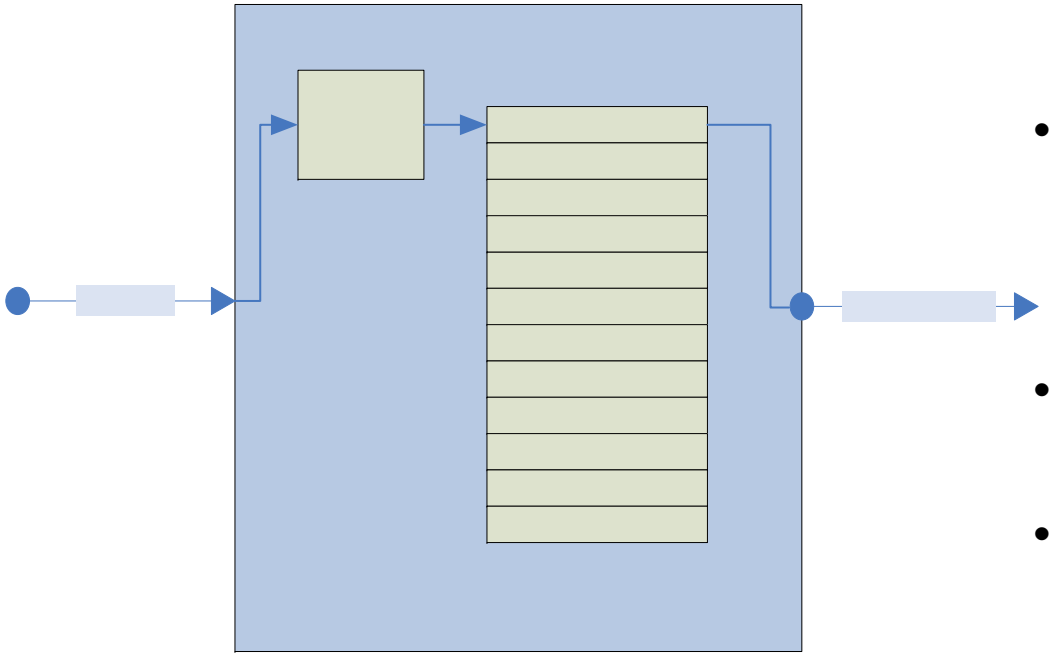
Frame Stream (21 : 0)

Data Stack (LIFO)



- **Stores data used to execute instructions**
- **Provides streamlined execution for Control Unit**
- **Serves as internal memory for execution of instructions**
- **State of Data Stack provides Control Unit with information for decision making**

Initialization Boot ROM



- **Provides an initial set of signatures upon power-up**
- **Control Unit initially loads instructions from Boot ROM, then from the UI**
- **Establishes a known state upon startup**
- **Outputs are fed to the Data Stack and Control Unit for execution**

Pointer “000000000”

…

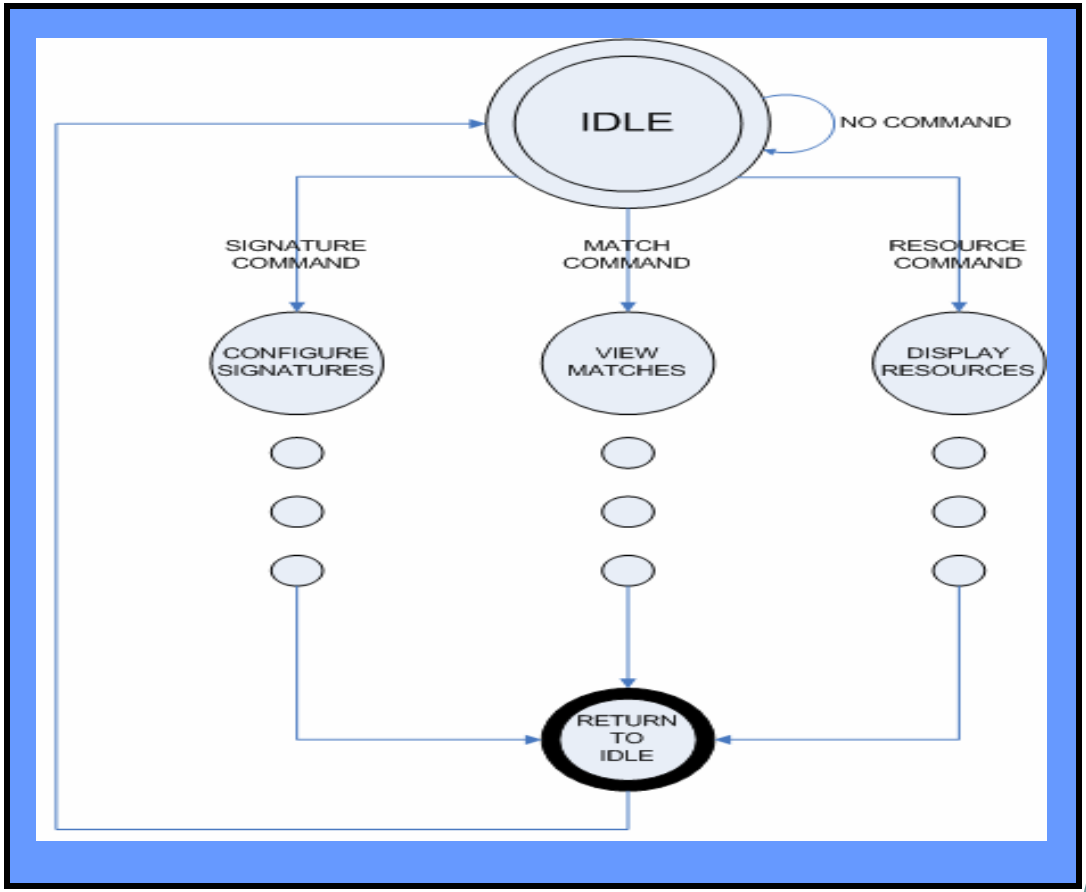
…

…

…

Control Unit Schematics

- **Driven by the Boot ROM or through the Interactive Interface by the UI**
- **Executes instructions and obeys user commands**
- **Connects directly to the Data Unit**
- **The “Brains” of the system, controlling all decision making**



Performance Evaluation

	NIBS	Wireshark (software-only approach)
Memory Space Used	**10.8MB**	**40MB**
Performance (Minimum Required Clock Speed)	**130MHz**	**1.3GHz Machine**

NIBS - is the real deal!!

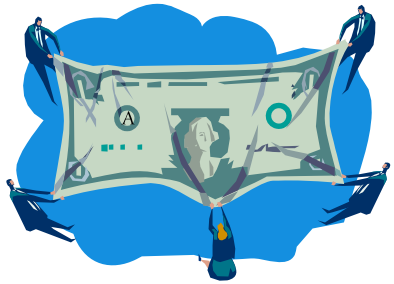
Cost Analysis

Project Design Budget

- FPGA board < $1,000
- Software < $100
- Other Expenses < $400
- TOTAL < $1,500

Projection for Commercial Use

- PCB † < $100
- Design tools - $0
- Total < $100



† Printed Circuit Board (PCB) is used to mechanically support and electrically component electrical components

Ethics and Standards

- Engineers are responsible for design integrity
- IEEE 802.3
- RS-232
- IEEE 1003 †

† IEEE 1003 is more often referred to as Portable Operating System Interface (POSIX)

Conclusion

- **Performance and Affordability**
- **We must prepare for future challenges of IPv6 †**
- **The design lays the foundation for offloading network intrusion detection from the CPU to a dedicated processor**

† Internet Protocol version 6 (IPv6) is the designated successor for IPv4, the current version of the internet protocol, defines much larger packet sizes and supports transmission speeds in excess of 40GB/s