

High Speed Hardware Based Ethernet Packet Analyzer

Mikroelektronik / Prof. Dr. Marcel Jacomet
Experte: Felix Kunz

In the modern communication society, the filtering of Internet data is an important subject. Nowadays there are a lot of software products on the market handling this issue. Most of these products suffer from the fact that the faster the web link is, the more cpu time is used for filtering. This missing cpu time is slowing down the computer performance. For this reason we developed an analyzer witch scans the bit stream directly on the high-speed hardware level. The extracted information concerning the transmission protocols can be used to reject attacks, for QoS (Quality of Service), and to detect virus infected packets.



Ocaña Cedric
1980
079 443 36 03
ocana@postmail.ch

Ethernet packet

The most common standard for communication over network is Ethernet. The data is sent in frames containing the essential data and header information. In the data section of the Ethernet frame, many protocols, like TCP/IP or ARP are encapsulated. Our analyzer does a qualification based on protocol types, transmission sources and the transmitted data. A complementary project with two computer engineering students is running in parallel and handles the Linux drivers and transmission protocol definitions (see p. 97).

Interface

Implemented in a computer, our device would be housed on the network card. The extracted information is directly accessible by the CPU and can be used for a simplified and fast handling on the operating system level. Our packet analyzer is configurable with rules defined by the operating system, enabling the analyzer to face actual and future security requirements.

Evaluation board and software

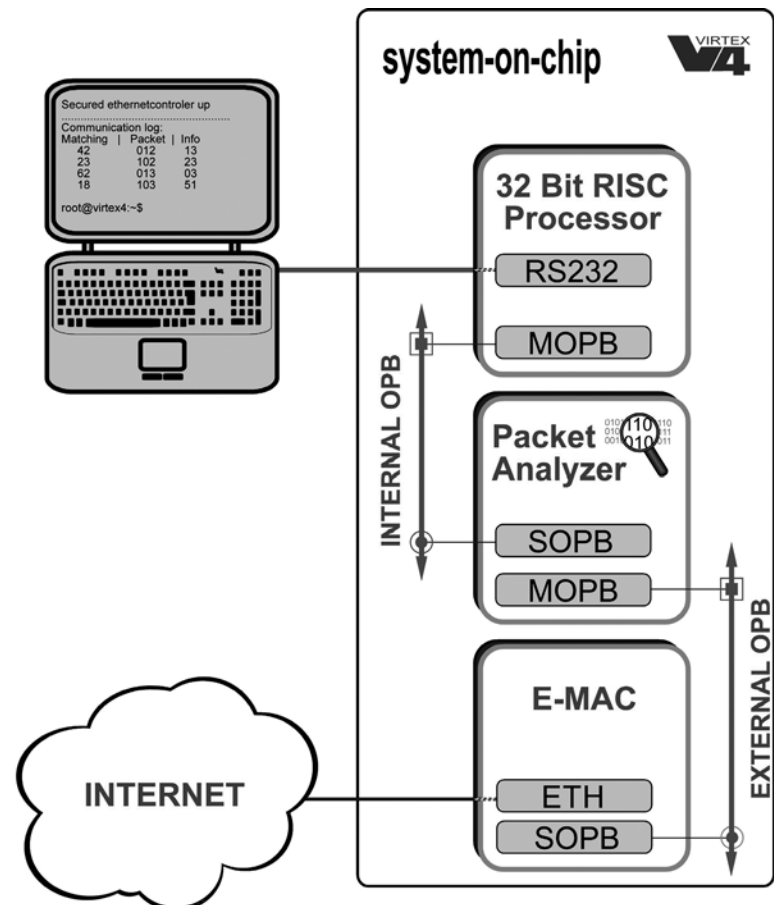
As development platform, we used the Xilinx development board ML401. Among other devices, it contains a virtex 4 FPGA and an Ethernet transceiver. The used development software was the Xilinx Platform Studio(XPS). This tool allows connecting IP cores (intellectual property hardware components)

by buses or signals on an abstract level. Integrated Software Environment (ISE) was used to include our VHDL code and to synthesize the overall design. Verification, simulation and testing have been done with the Modelsim tool.

System

An embedded system including a MicroBlaze CPU was generated to evaluate the performance of our

packet analyzer. This set-up made it possible to use uClinux as operating system with a standard serial connection (RS232) to communicate with the system. The internal connection over the on-chip peripheral bus (OPB) handles the communication between the MicroBlaze, the analyzer and the e-mac (Ethernet controller). As depicted in the block diagram, any Ethernet frame has to pass through the analyzer.



Block diagram of realized Ethernet packet analyzer



Zaugg Philipp
1983
079 504 09 87
ph.zaugg@gmx.ch