

Caracterización y Monitoreo de Redes Ethernet Mediante Plataformas de Hardware Reconfigurable

IPD438 - Seminario de Redes de Computadores

Alonso Rodríguez

Departamento de Electrónica

Universidad Técnica Federico Santa María, Valparaíso, Chile

Email: alonso.rodriguez.13@sansano.usm.cl

Resumen—La creciente expansión en el uso de redes Ethernet en diversos aspectos del ámbito industrial y científico requieren de herramientas de caracterización y medición de desempeño de alta precisión y capacidad de configuración. Soluciones por software, así como las soluciones comerciales por hardware dedicado, no han logrado satisfacer este nicho debido a insuficiencias en su precisión, bajo grado de configuración y precios privados. Ante este panorama emergen iniciativas de código abierto que buscan satisfacer estos requerimientos. Este trabajo se enfoca en la presentación de NetFPGA, la principal de estas plataformas, y como esta constituye un desarrollo base que ha sido extendido a fin de construir equipamiento de alta precisión y capacidad de configuración para la caracterización de redes Ethernet.

I. INTRODUCCIÓN

La caracterización y monitoreo de redes son cruciales para la correcta implementación de la transmisión de información entre los nodos que componen una red, otorgando garantías de confiabilidad y desempeño. En particular, las redes Ethernet han adquirido una popularidad creciente en los últimos tiempos, en que se busca que estas reemplacen protocolos pre-existentes en distintas áreas de la industria, en particular se destaca la aparición de redes Ethernet en aplicaciones de control industrial [1], así como la inserción de estas como protocolo unificador de los múltiples sistemas computacionales de los vehículos modernos [2]. La inserción de redes Ethernet en estos y otros entornos requiere de la caracterización de su desempeño para entregar garantías en su operación, así como el análisis científico de su utilidad.

II. DESARROLLOS ANTERIORES

II-A. Soluciones por Software

Existen herramientas de software ya desarrolladas por la comunidad científica para la caracterización de redes tales como Iperf[3], Netperf[4], Netmap[5], entre otras. Estos desarrollos incluyen una serie de bibliotecas y aplicaciones de usuario las cuales permiten su utilización como elementos de medición. Si bien existe utilidad en la utilización de estas herramientas, estas no son lo suficientemente precisas para la caracterización de tiempos de propagación en redes Ethernet, ya que funcionan sobre un sistema computacional tradicional en que se agrega un *overhead* de procesamiento por la pila de protocolos implementados tanto por el sistema operativo como por las aplicaciones de usuario e interfaces de red. Además, en forma general, estas herramientas operan sobre protocolos de capas

superiores, por lo que el tiempo de procesamiento de estos no representa exclusivamente el tiempo de transmisión Ethernet entre nodos. Surge entonces la necesidad de usar dispositivos basados en hardware para lograr una caracterización con la precisión deseada.

II-B. Soluciones Comerciales por Hardware

En el mercado se encuentran disponibles sistemas comerciales basados en hardware desarrollados por múltiples compañías y diseñados para la caracterización de redes Ethernet. Estos dispositivos están generalmente orientados a redes empresariales, por lo que presentan baja posibilidad de configuración y precios privados[6]. Ante este panorama surgen diversos proyectos de código abierto que buscan formar una comunidad de colaboradores que contribuyan a desarrollar herramientas para la construcción y monitoreo de redes Ethernet. Las secciones siguientes se enfocan en una de estas iniciativas, y en como estos desarrollos pueden ser empleados en conjunto con otros proyectos para la construcción de dispositivos de caracterización.

III. NETFPGA

NetFPGA es una iniciativa de software y hardware abierto diseñada por miembros de la academia para facilitar el acceso a la implementación de dispositivos de redes de alta precisión y capacidad de configuración[7]. El diseño original ha recibido múltiples iteraciones llegando a los cuatro diseños actuales para redes de diferentes tasas de transmisión y tecnologías de cableado.

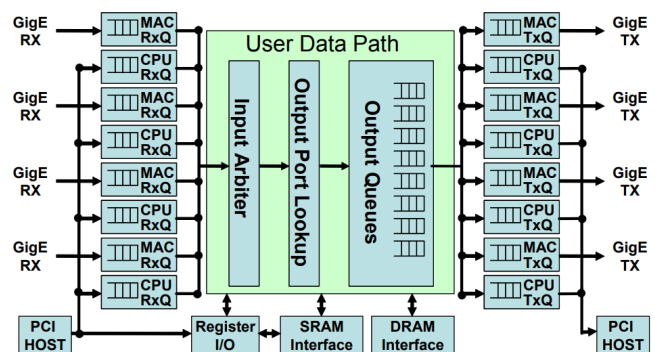


Figura 1. Pipeline de referencia NetFPGA[8]

La organización NetFPGA provee los planos para el diseño de múltiples tarjetas basadas en FPGA, la descripción *Register-Transfer Level* (RTL) de componentes estándar a implementar en el hardware reconfigurable, y un conjunto de bibliotecas y herramientas de software para facilitar el desarrollo. En nuestro caso utilizamos la plataforma NetFPGA-1G-CML, la cual dispone de 4 interfaces Gigabit Ethernet. Una de las principales contribuciones del proyecto NetFPGA es el establecimiento de un diseño de pipeline de referencia (figura 1), en que el usuario puede basar su desarrollo incluyendo sus propias funcionalidades diseñadas mediante el uso de un *Hardware Description Language* (HDL). Este sistema digital se puede dividir en las siguientes componentes:

- Interfaces AUI-MAC: Interfaces físicas de recepción/transmisión conectadas a cada uno de los cuatro puertos de la tarjeta y por las cuales transitan los paquetes. Incluyen colas de recepción/transmisión.
- *Input Arbiter*: Arbitrador Round Robin que determina la interfaz desde la cual se extrae el paquete a procesar.
- *Output Port Lockup*: Decide por cual interfaz de salida se emite un paquete. Es el punto principal a modificar para implementar lógica de usuario.
- Colas de salida: Agrupan los paquetes a ser transmitidos por cada interfaz a espera de que estas se liberen.
- Interfaces PCI: Interfaces mediante las cuales se puede transmitir información al sistema computacional anfitrión para su posterior procesamiento o análisis.

Este diseño de referencia facilita el desarrollo de nuevas funcionalidades, proporcionando un acceso directo y simple al contenido de los paquetes recibidos.

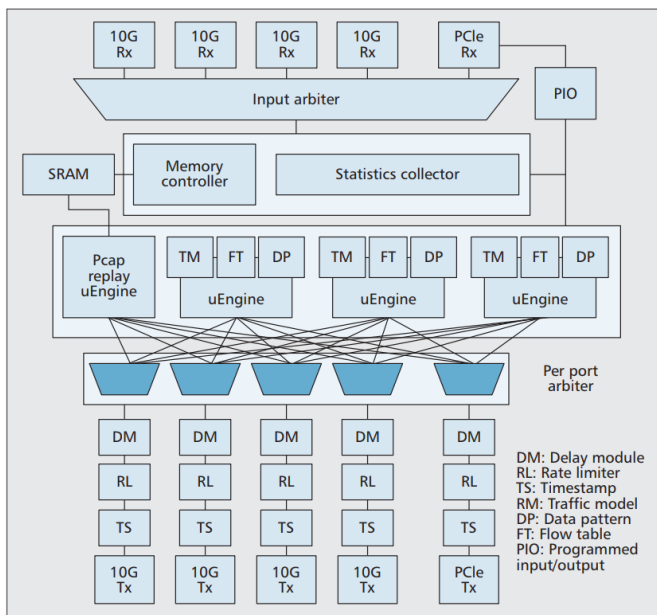


Figura 2. Diseño de referencia OSNT inyector de tráfico[6]

IV. CARACTERIZACIÓN Y MONITOREO DE REDES ETHERNET UTILIZANDO NETFPGA

Mediante la utilización de la plataforma NetFPGA se busca diseñar un sistema capaz de inyectar tráfico controlado y monitorear la transmisión de paquetes a fin de determinar la latencia de transmisión en la interacción de componentes de la red a analizar. Existen iniciativas que han implementado algunas de estas funcionalidades (Covington G. Adam et al., (2009) [8], Antichi G. et al., (2012) [9], Oeldemann A. et al., (2018) [10]). En particular, la implementación planteada en la descripción del *Open Source Network Tester* (OSNT)[6], presenta una serie de dispositivos para el monitoreo y caracterización de redes Ethernet que operan sobre la base de la NetFPGA. Son de particular interés dos diseños: un inyector de tráfico y un monitor de tráfico descritos en las figuras 2 y 3 respectivamente.

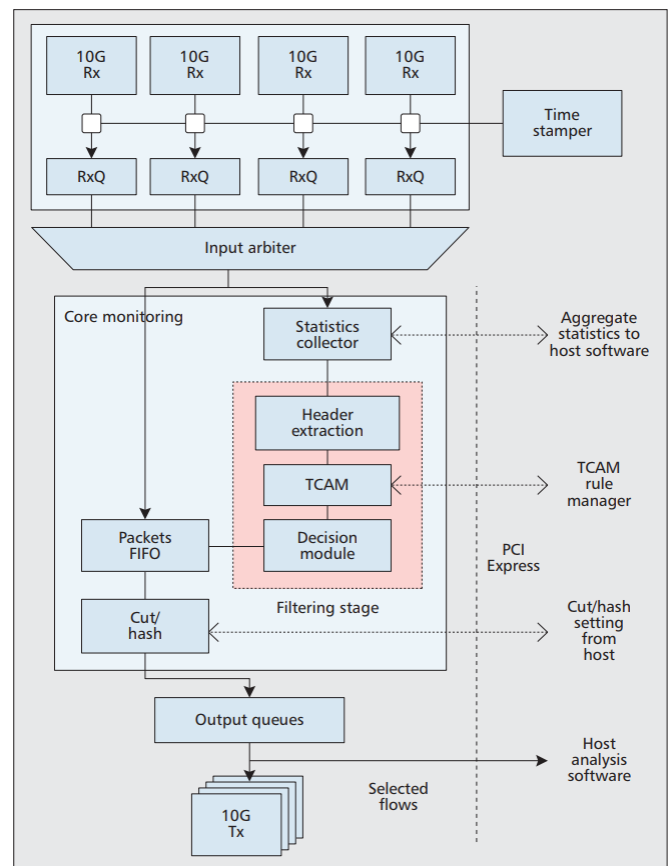


Figura 3. Diseño de referencia OSNT monitor de tráfico[6]

Se observa que estos diseños hacen uso del pipeline de referencia otorgado por la NetFPGA, evitando el rediseño de interfaces físicas y enfocándose en funcionalidades de alto nivel. Se busca entonces implementar en primera instancia una versión simplificada de estos diseños, lo cual se resume en la inyección de marcas de tiempo en los paquetes a monitorear así como el establecimiento de rutinas de envío

controlado de tráfico mediante las interfaces proporcionadas por la NetFPGA.

V. PRUEBAS REALIZADAS

Para verificar el funcionamiento de la NetFPGA se sintetizan y compilan las componentes necesarias para su interconexión con el computador anfitrión. Una vez configurada, se verifica su funcionamiento con la implementación de interfaces NIC dentro de la NetFPGA y la ejecución de una prueba de *loopback* entre interfaces enviando paquetes del máximo tamaño posible a una velocidad de transmisión máxima y constante para luego determinar en el otro extremo si los paquetes son recibidos correctamente analizando el largo esperado de estos.

```

root@moore: ~/Desktop/NetFPGA-1G-CML-live/tools/bin
NetFPGA environment:
  Root dir: /home/alonso/Desktop/NetFPGA-1G-CML-live
  Project name: reference_nic_nf1_cml
  Project dir: /tmp/root/test/reference_nic_nf1_cml
  Work dir: /tmp/root
  Root directory is /home/alonso/Desktop/NetFPGA-1G-CML-live
  Running global setup... PASS
  Running test both loopback_maxsize... /tmp/root/test/reference_nic_nf1_cml/both_loopback_maxsize/
  run.py --hw exited with value 1
  FAIL
  Output was:
  WARNING: No route found for IPv6 destination :: (no default route?)
  Loading the nf10_lib library..
  Running test using the following physical connections:
  nf3:nf0
  nf2:nf1
  nf1:nf2
  nf0:nf3
  -----
  Sending now:
  49
  Error: barrier timed out after 10 seconds
  Error: device nf0 missed 3 expected packets

  nf3 finishing up
  nf2 finishing up
  nf1 finishing up
  nf0 finishing up
  Error: 3 expected packets not seen
  -----
  HW Test results
  -----
  Test status : FAIL
  packet_missed errors : 4
  register_read errors : 0

  Running global teardown... PASS
root@moore:~/Desktop/NetFPGA-1G-CML-live/tools/bin#

```

Figura 4. Pruebas de *loopback* con cables cortos.

```

root@moore:~/Desktop/NetFPGA-1G-CML-live/tools/bin
Unexpected packet 42 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 43 : Packet lengths do not match, expecting 1514 but saw 82
Unexpected packet 44 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 45 : Packet lengths do not match, expecting 1514 but saw 82
Unexpected packet 46 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 47 : Packet lengths do not match, expecting 1514 but saw 82
Unexpected packet 48 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 49 : Packet lengths do not match, expecting 1514 but saw 82
Unexpected packet 50 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 51 : Packet lengths do not match, expecting 1514 but saw 82
Unexpected packet 52 : Packet lengths do not match, expecting 1514 but saw 102
Unexpected packet 53 : Packet lengths do not match, expecting 1514 but saw 70
Unexpected packet 54 : Packet lengths do not match, expecting 1514 but saw 70
-----
HW Test results
-----
Test status : FAIL
packet_missed errors : 223
register_read errors : 0

Running global teardown... PASS

```

Figura 5. Pruebas de *loopback* con cables largos.

En las figuras 4 y 5 se muestran las pruebas realizadas con un largo de cable de interconexión corto ($\sim 10[cm]$) y largo ($\sim 1,5[m]$) respectivamente. Se observa que en ambos casos el largo de algunos paquetes difiere del esperado y son por lo tanto marcados como errores. Queda por verificar en que parte de la cadena es que ocurre este error, si es en la captura interna

de la NetFPGA o en el procesamiento posterior realizado por el computador anfitrión. En cualquier caso, se verifica el funcionamiento de la plataforma junto con el desarrollo base del pipeline de referencia, el cual puede ser modificado a fin de ampliar sus funcionalidades. Queda como trabajo futuro la incorporación de elementos similares a los descritos por el Open Source Network Tester (OSNT) para expandir las capacidades de monitoreo y caracterización de redes Ethernet del sistema.

REFERENCIAS

- [1] D.M. Moyné, J.R.; Tilbury. The emergence of industrial control networks for manufacturing control, diagnostics, and safety data. *Proceedings of the IEEE*, 95, 2007.
- [2] Martin; Jones Edward; Trivedi Mohan; Kilmartin Liam Tuohy, Shane; Glavin. [ieec 2013 ieee intelligent vehicles symposium (iv) - gold coast city, australia (2013.06.23-2013.06.26)] 2013 ieee intelligent vehicles symposium (iv) - next generation wired intra-vehicle networks, a review. 2013.
- [3] iperf, TCP and UDP Bandwidth Performance Measurement Tool, <http://code.google.com/p/iperf>.
- [4] Netperf, <http://www.netperf.org>.
- [5] L. Rizzo. Netmap: A novel framework for fast packet i/o, usenix annual technical conf., 2012. 2013.
- [6] Muhammad; Geng Yilong; Zilberman Noa; Covington Adam; Bruyere Marc; Mckeown Nick; Feamster Nick; Felderman Bob; Blott Michaela; Moore Andrew; Owezarski Philippe Antichi, Gianni; Shahbaz. Osnt: open source network tester. *IEEE Network*, 28, 9 2014.
- [7] Nick; Watson Greg; Gibb Glen; Hartke Paul; Naous Jad; Raghuraman Ramanan; Luo Jianying Lockwood, John W.; Mckeown. [ieec 2007 ieee international conference on microelectronic systems education - san diego, ca, usa (2007.06.3-2007.06.4)] 2007 ieee international conference on microelectronic systems education (mse'07) - netfpga—an open platform for gigabit-rate network switching and routing. 2007.
- [8] Glenn; Lockwood John W.; Mckeown Nick Covington, G. Adam; Gibb. [ieec 2009 17th ieee symposium on field programmable custom computing machines - napa, ca, usa (2009.04.5-2009.04.7)] 2009 17th ieee symposium on field programmable custom computing machines - a packet generator on the netfpga platform. 2009.
- [9] S.; Miller D. J.; Moore A. W. Antichi, G.; Giordano. [ieec 2012 ieee/ifip network operations and management symposium (noms 2012) - maui, hi (2012.04.16-2012.04.20)] 2012 ieee network operations and management symposium - enabling open-source high speed network monitoring on netfpga. 2012.
- [10] X. Niu, n. changhai, H. K. N. Leung, Y. Lei, X. Wang, J. Xu, and Y. Wang. An interleaving approach to combinatorial testing and failure-inducing interaction identification. *IEEE Transactions on Software Engineering*, pages 1–1, 2018.