Infraestructura de red de nodos cifradores/descifradores AES basada en ApSoC

Jesús Rodríguez Heras

24 de septiembre de 2020

Índice

Índice

Objetivos

Los objetivos generales de este proyecto son los siguientes:

- Diseñar red de nodos basada en la tecnología ApSoC.
- Establecer comunicación entre nodos de la red.
- Cada nodo aportará información a un fichero común de forma secuencial.

Descripción

Nodos

Los nodos de la red serán tarjetas de desarrollo Zybo Zynq 7010.

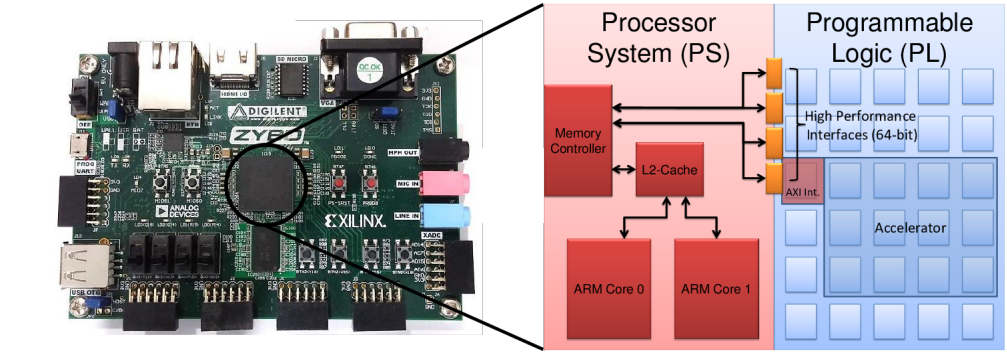


Imagen sustraída del artículo "Implementing high-performance, low-power FPGA-based optical flow accelerators in C.", escrito por: Joshua Scott Monson.

Alcance

Infraestructura de red

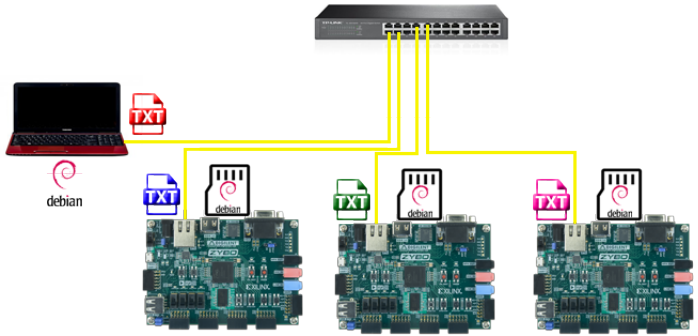
- Instalación de Linux sobre el núcleo ARM de las tarjetas.
- Interconexión física de los elementos de la red.
- Desarrollo de scripts para automatizar la comunicación y el agregado de información por parte de cada nodo.
- Creación y ejecición de pruebas.

Índice

Tecnologías a utilizar

Componentes

- Ordenador central (monitor).
- Tarjeta Zybo Zynq 7010.
- Switch.



Análisis del sistema

- Sistema operativo del ordenador central: Debian 9 Stretch.
- Sistema operativo de las tarjetas de desarrollo: Debian 8 Jessie (compilado para ARM en tarjeta micro SD).
- Uso de SSH en las comunicaciones.
- Uso de SCP para el envío de ficheros.
- Comprobación de directorios con el comando `stat`.

Análisis del sistema

Las tareas a realizar por cada nodo se realizan en los siguientes scripts:

`Recibiendo.sh` (Nodo)

Comprobar recepción del fichero de texto.

`Cristian.sh` (Nodo)

Comprobar el directorio de trabajo. Añade la información local.

`Enviando.sh` (Nodo)

Comprueba el directorio de envío. Envía el fichero mediante SCP.

Análisis del sistema

Contar aquí como conseguir que todo se automatice. Hemos usado la herramienta cron que lanza Lanzador.sh para no saturar el arranque del sistema con el demonio cron. Plasmarlo con algunas palabras para saber que hay que contarlo.

Análisis del sistema

Para evitar saturar el arranque del sistema, hacemos una planificación del arranque de cada tarjeta con los siguientes scripts:

`Lanzador.sh` (Nodo)

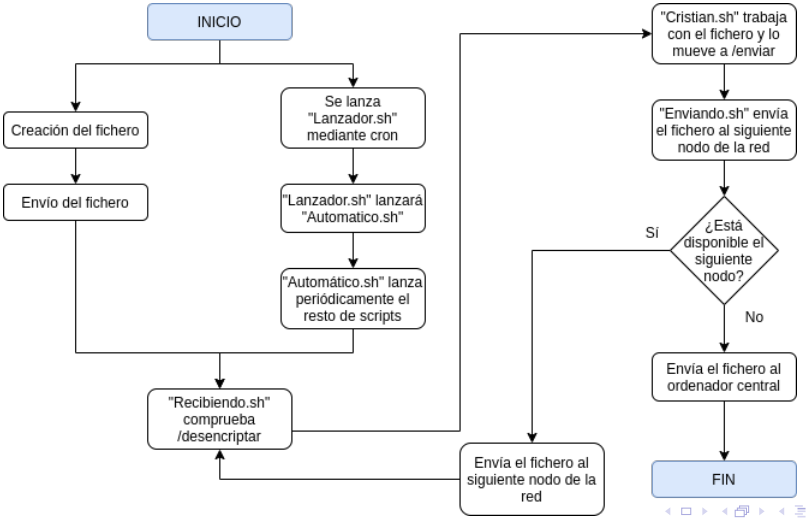
Es ejecutado por la herramienta cron del sistema operativo. Ejecuta el script `Automatico.sh`.

`Automatico.sh` (Nodo)

Periódicamente, ejecuta los scripts `Recibiendo.sh`, `Cristian.sh` y`Enviando.sh`. El parámetro de tiempo seleccionado es de un segundo.

Análisis del sistema

La secuencia de trabajo de estos scripts será la siguiente:



Diseño y desarrollo

- Todos los dispositivos de la red han de estar conectados al switch y tener una IP fija.
- El proceso de comunicación se inicia en el ordenador central (monitor).
- Los nodos reciben el fichero, añaden información y lo envían al siguiente nodo de la red.
- El proceso de comunicación finaliza cuando el fichero es recibido por el monitor.

Pruebas del sistema

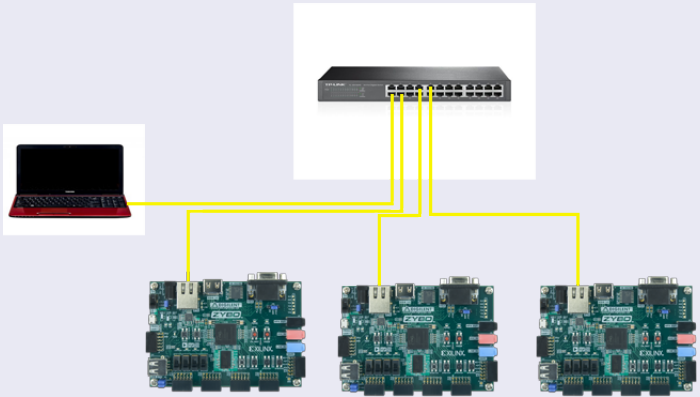
Enumerar las dos pruebas, la de conexión de red y la de comunicación completa. Como usuario del sistema lanzo Inicio.sh y se ejecuta la de red. Y la otra se verá en directo.

Índice

Conclusiones

Escenario de trabajo 1

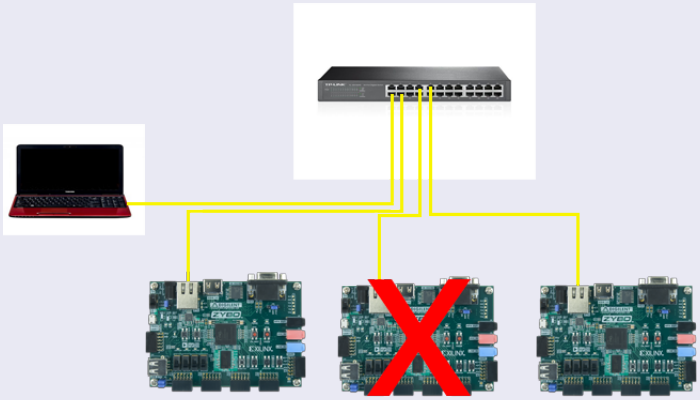
Todos los nodos están conectados correctamente a la red.



Conclusiones

Escenario de trabajo 2

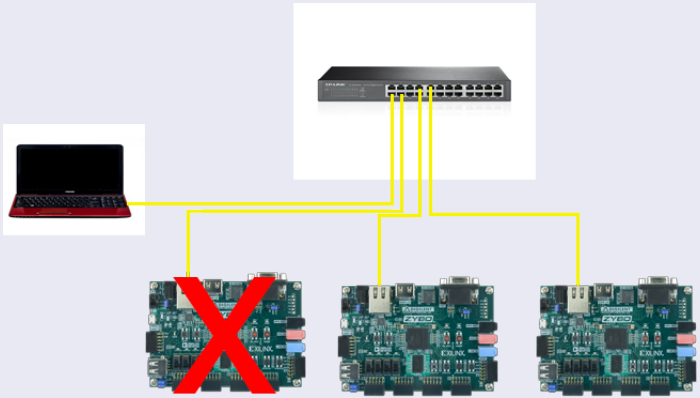
Un nodo intermedio se encuentra desconectado.



Conclusiones

Escenario de trabajo 3

El primer nodo está desconectado.



Trabajo futuro

- Cambiar cadena de conexiones a aleatorio.
- Completar el trabajo de cifrado/descifrado incluyendo el IP cifrador/descifrador AES de Cristian Ambrosio Costoya.
- Implementación de un módulo IEEE 802.11 para conexiones inalámbricas.