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

Jesús Rodríguez Heras

24 de septiembre de 2020

Índice

Índice

Objetivos

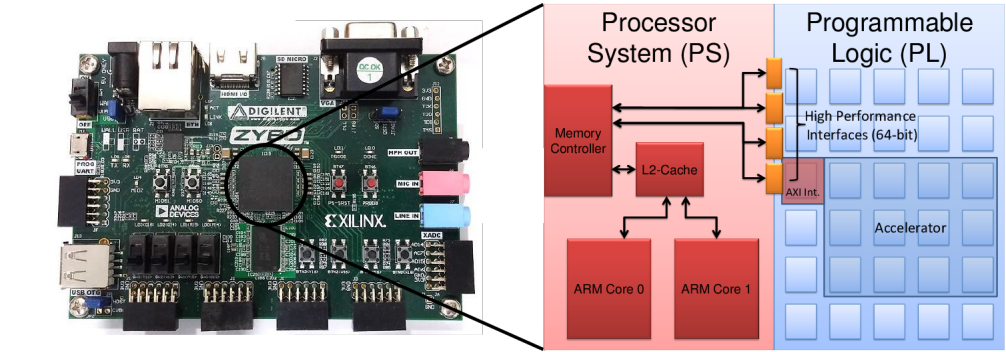
Los objetivos generales de este proyecto son los siguientes:

- 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.



Fuente: Artículo “Implementing high-performance, low-power FPGA-based optical flow accelerators in C.”, escrito por: Joshua Scott Monson.

Alcance

Infraestructura de red

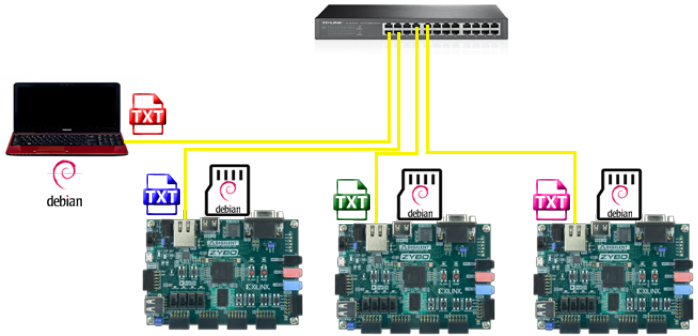
- Instalación de Linux sobre el núcleo ARM de las tarjetas.
- Interconexión física de los elementos de la red.
- Desarrollo de scripts para automatizar la comunicación y el agregado de información por parte de cada nodo.
- Creación y ejecución de pruebas.

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`.
  - Genera un HASH por cada cambio en el estado del directorio.

Análisis del sistema

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

`Recibiendo.sh` (Nodo)

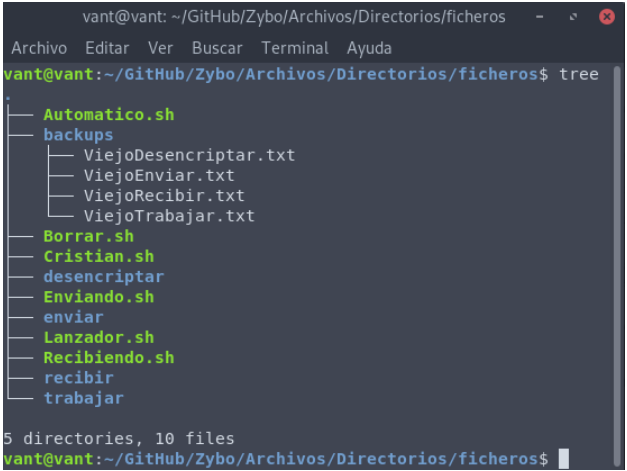
Comprobar (stat) recepción del fichero de texto.

`Cristian.sh` (Nodo)

Comprobar (stat) el directorio de trabajo. Añade la información local.

`Enviando.sh` (Nodo)

Comprobar (stat) el directorio de envío. Comprobar la conexión del siguiente nodo (ping). Envía el fichero mediante SCP.



Análisis del sistema

¿Cómo conseguir la automatización?

- Lanzamiento de scripts al inicio del Sistema Operativo con la herramienta `cron`.
- Evitar la saturación del arranque del Sistema Operativo.
- Periodicidad de las comprobaciones de los directorios de trabajo y lanzamiento de scripts.

Análisis del sistema

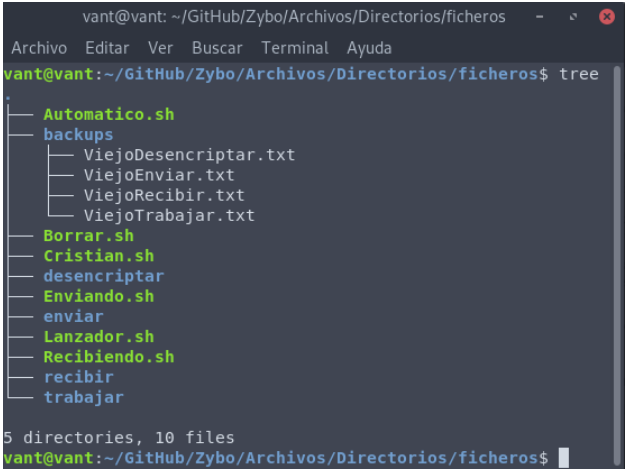
Para evitar saturar el arranque del sistema, hacemos una planificación del arranque de cada tarjeta con los siguientes scripts:

`Lanzador.sh` (Nodo)

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

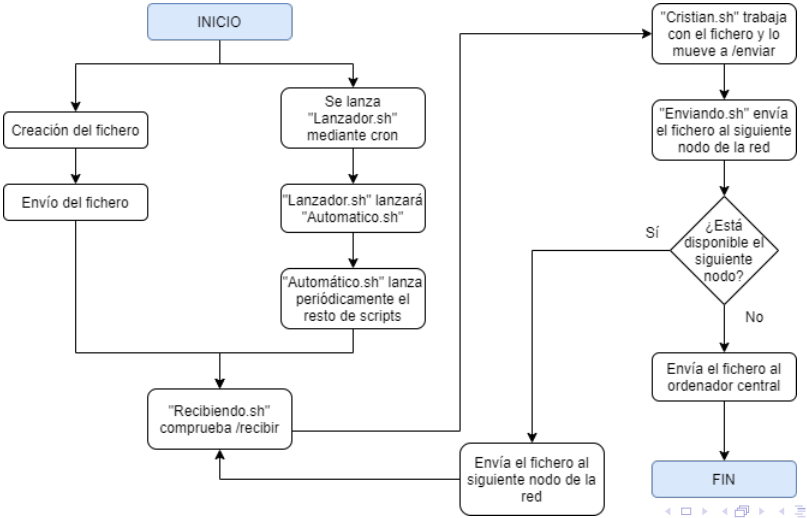
`Automatico.sh` (Nodo)

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

Tendremos dos pruebas principales:

- Prueba de conexión de red con el lanzamiento de `Inicio.sh` por parte del monitor.
- Prueba de comunicación del sistema completamente automatizado.

Índice

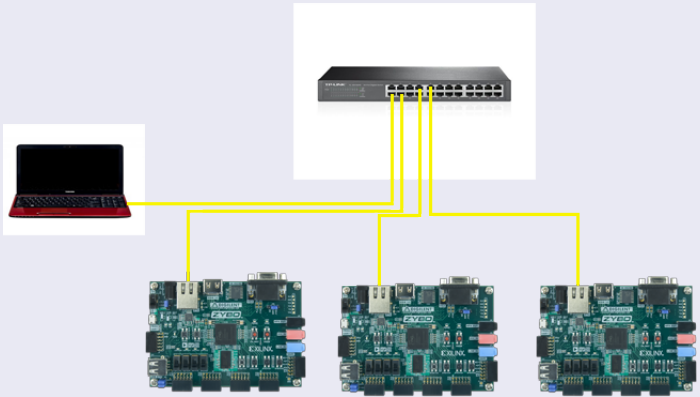
Conclusiones

- Aunque la red se pensó inicialmente para un cifrado/descifrado AES, realmente, puede usarse para cualquier tipo de módulo hardware implementado en la FPGA de la tarjeta de desarrollo Zybo Zynq 7010, como por ejemplo, el tratamiento de imágenes.
- El sistema está preparado para soportar tantos nodos de red como capacidad física tenga la red usada.

Conclusiones

Escenario de trabajo 1

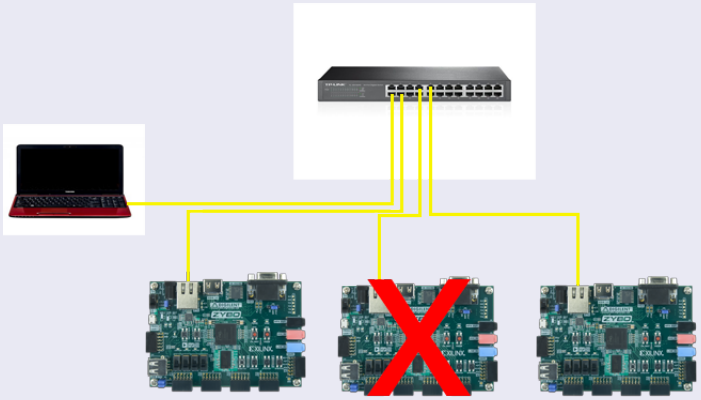
Todos los nodos están conectados correctamente a la red.



Conclusiones

Escenario de trabajo 2

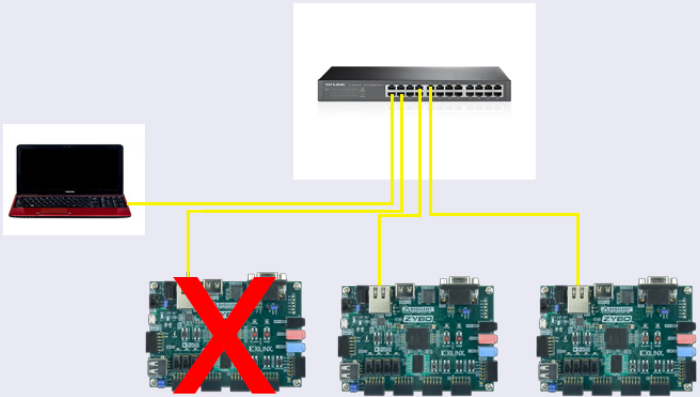
Un nodo intermedio se encuentra desconectado.



Conclusiones

Escenario de trabajo 3

El primer nodo está desconectado.



Aclaraciones

- Hay un cifrado en la comunicación ya que se usa el protocolo SSH y SCP para las comunicaciones y envío de ficheros.
- No hay cifrado local de la información del nodo aportado por el Trabajo de Fin de Grado de Cristian Ambrosio Costoya por incompatibilidad con el Trabajo de Fin de Grado de Gabriel Fernando Sánchez Reina, el cual debía proporcionar el driver Linux para comunicarse con este módulo cifrador.

Trabajo futuro

- Evitar que se rompa la cadena de envío debido a que un nodo no esté conectado.
- Cambiar cadena de conexiones a aleatorio.
- Completar el trabajo de cifrado/descifrado incluyendo el IP cifrador/descifrador AES de Cristian Ambrosio Costoya y el driver de Gabriel Fernando Sánchez Reina.
- Implementación de un módulo IEEE 802.11 para conexiones inalámbricas de todos los nodos de la red.