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:

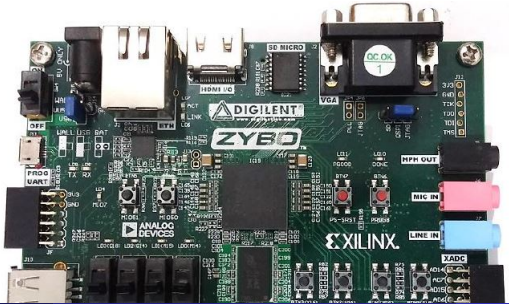
- Diseñar red de nodos basada en la tecnología ApSoC.
- Establecer comunicación entre nodos de la red.
- Cada nodo aportará información a un fichero común de forma secuencial.

Descripción

Añadir zoom en el chip del medio para que quede claro que ahí dentro está el ARM y la FPGA. Una vez comentado, hay que justificar que esa pareja es lo interesante de la red de nodos. Una flecha que salga del centro y lleve a otra imagen que describa lo que tiene dentro de forma básica. Poner la imagen roja y azul y poner de donde ha salido.

Nodos

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



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.

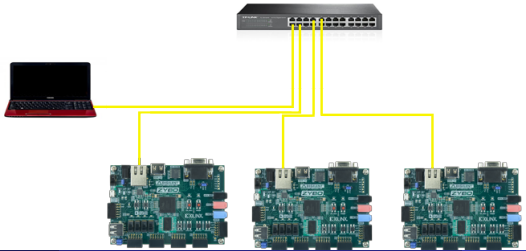
Índice

Tecnologías a utilizar

Componentes

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

Poner un simbolito de debian al lado de cada elemento. Poner un simbolito de un fichero de texto numerado al lado de cada elemento.



Análisis del sistema

Comentar que el sistema operativo del portátil es debian (x86). Y, el de las tarjetas puede ser Xiliunx o debian compilado para ARM, pero que hay que incluir el devicetree (fichero de linux que recopila los dispositivos). De momento, no incluye ningún driver. Como ya tenemos un sistema operativo Linux, nos permitirá la creación de scripts en bash y la comunicación mediante SSH.

Análisis del sistema

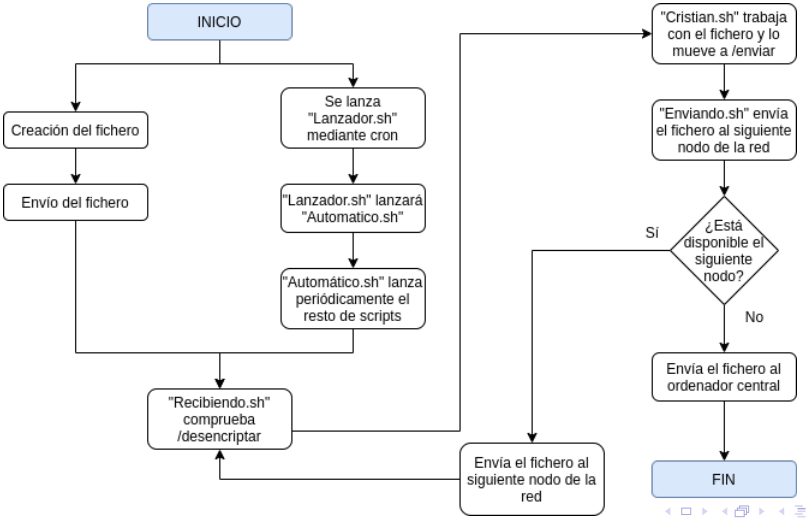
Para la transmisión del fichero de datos a través de la red, usaremos el protocolo SSH y una serie de scripts:

Scripts

- `Inicio.sh`
- `Lanzador.sh`
- `Automatico.sh`
- `Recibiendo.sh`
- `Cristian.sh`
- `Enviando.sh`
- `Borrar.sh`

Análisis del sistema

La secuencia de trabajo de estos scripts será la siguiente:



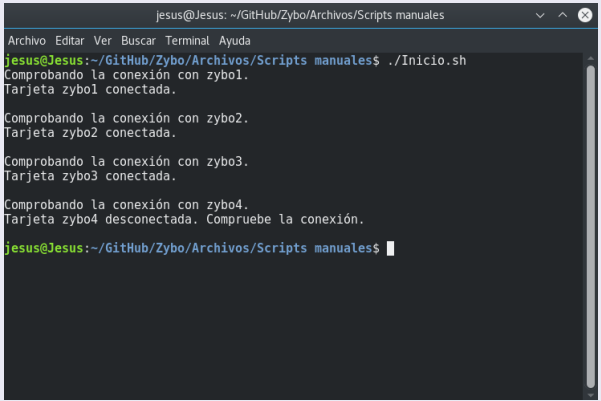
Diseño y desarrollo

- 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

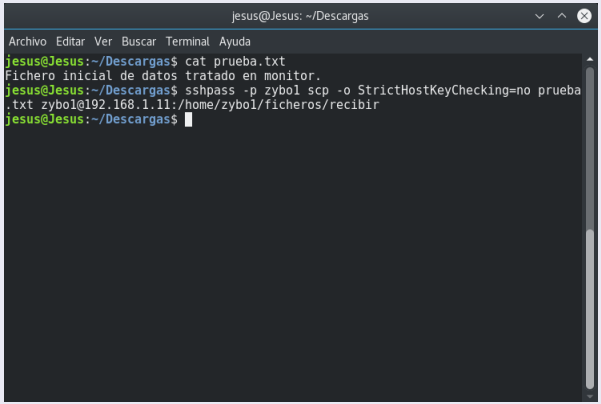
Prueba de conexión

Lanzamos el script `Inicio.sh` en el ordenador central.



Prueba de funcionamiento (I)

Creamos el fichero de pruebas y lo enviamos al primer nodo de la red.

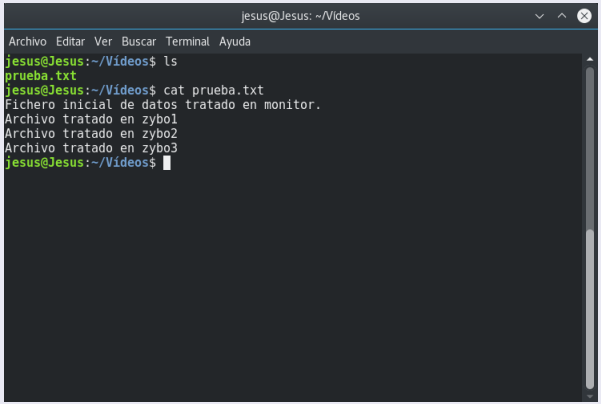


Prueba de funcionamiento (II)

Comprobamos el paso del fichero por la tarjeta Zybo.

Prueba de funcionamiento (III)

Una vez completada la cadena de nodos, comprobamos el fichero en el monitor.

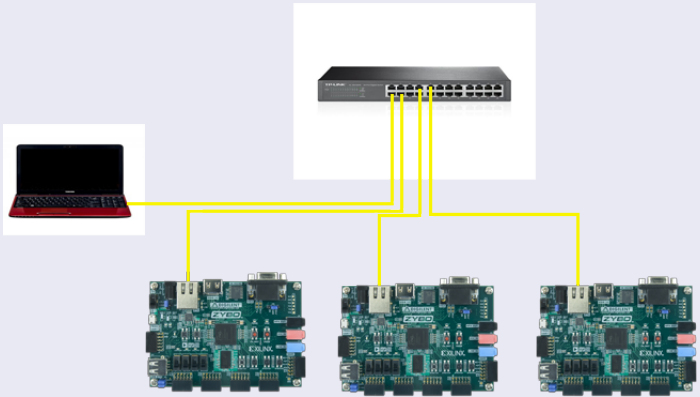


Índice

Conclusiones

Escenario de trabajo 1

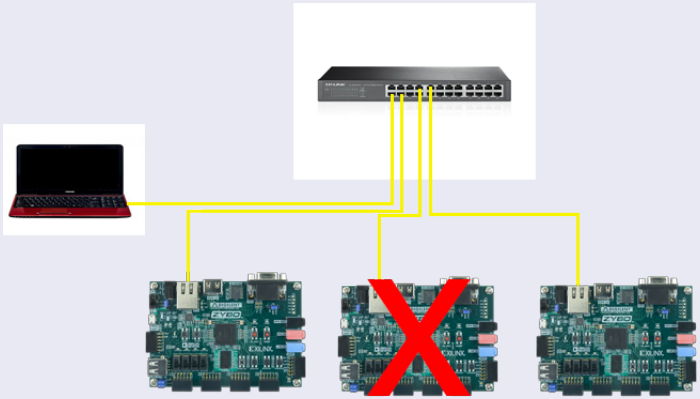
Todos los nodos están conectados correctamente a la red.



Conclusiones

Escenario de trabajo 2

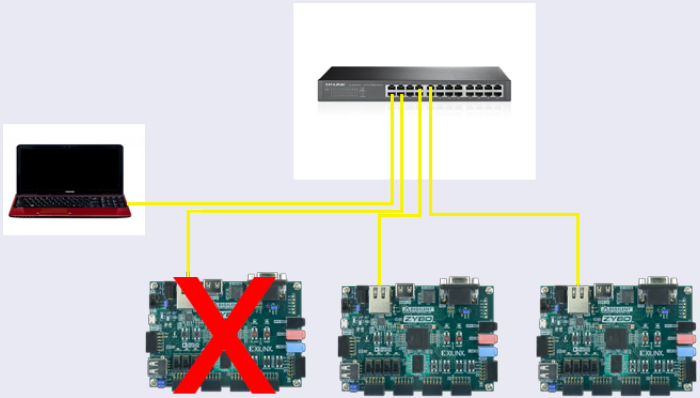
Un nodo intermedio se encuentra desconectado.



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.