

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

Jesús Rodríguez Heras

24 de septiembre de 2020

## 1 Introducción

- Objetivos
- Descripción
- Alcance

## 2 Metodología

- Tecnologías a utilizar
- Análisis del sistema
- Diseño y desarrollo
- Pruebas del sistema

## 3 Conclusiones y trabajo futuro

- Conclusiones
- Trabajo futuro

## 1 Introducción

- Objetivos
- Descripción
- Alcance

## 2 Metodología

- Tecnologías a utilizar
- Análisis del sistema
- Diseño y desarrollo
- Pruebas del sistema

## 3 Conclusiones y trabajo futuro

- Conclusiones
- Trabajo futuro

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.



## 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.

## 1 Introducción

- Objetivos
- Descripción
- Alcance

## 2 Metodología

- Tecnologías a utilizar
- Análisis del sistema
- Diseño y desarrollo
- Pruebas del sistema

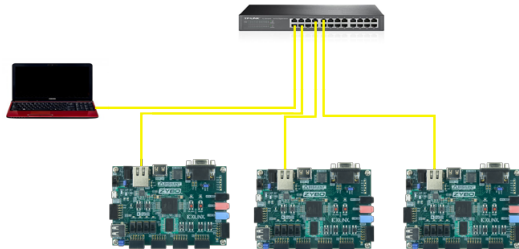
## 3 Conclusiones y trabajo futuro

- Conclusiones
- Trabajo futuro

## Componentes

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

Poner un simbolito de debian al lado de cada elemento dentro de una tarjeta SD. Poner un simbolito de un fichero de texto numerado al lado de cada elemento.





Comentar que el sistema operativo del portátil es debian (x86). Y, el de las tarjetas puede ser Xilliunx 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. SSH porque permite comunicación serie mediante consola a través de la red y de forma cifrada. De tal forma que la información que añade cada nodo al fichero, queda cifrada durante el proceso de comunicación. Gracias a SCP (utilidad de SSH) podemos enviar ficheros entre dispositivos que estarán cifrados durante el proceso de comunicación. Contar también que usamos 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.

Ver si se puede añadir una imagen pequeña de la tarjeta.

Contar aquí como conseguir que todo se automaticice. 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 ontarlo.

# 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)

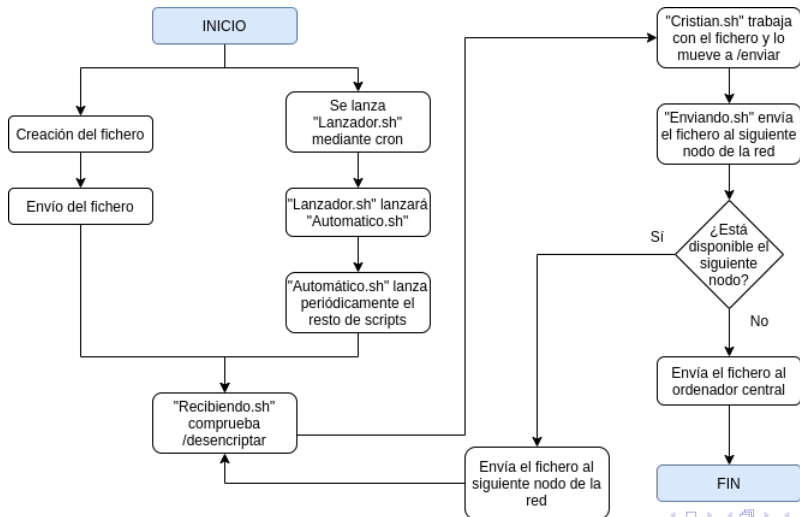
Es ejecutado por la herramienta cron del sistema operativo. Ejecuta el script Automatico.sh.

## 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:



- 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.

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.

## 1 Introducción

- Objetivos
- Descripción
- Alcance

## 2 Metodología

- Tecnologías a utilizar
- Análisis del sistema
- Diseño y desarrollo
- Pruebas del sistema

## 3 Conclusiones y trabajo futuro

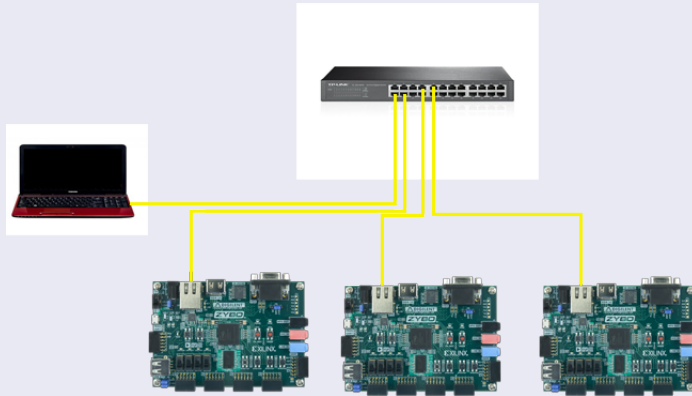
- Conclusiones
- Trabajo futuro



# Conclusiones

## Escenario de trabajo 1

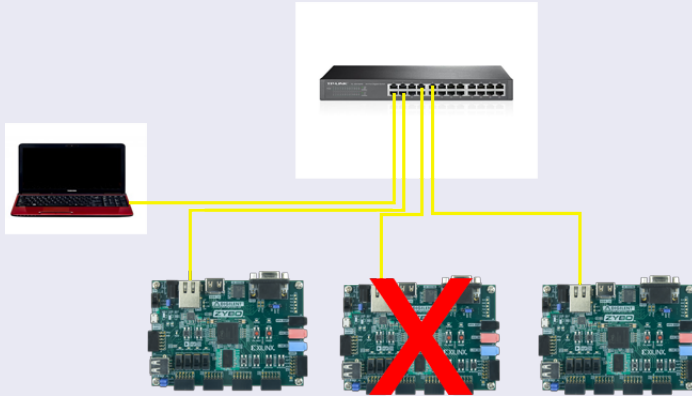
Todos los nodos están conectados correctamente a la red.



## Conclusiones

## Escenario de trabajo 2

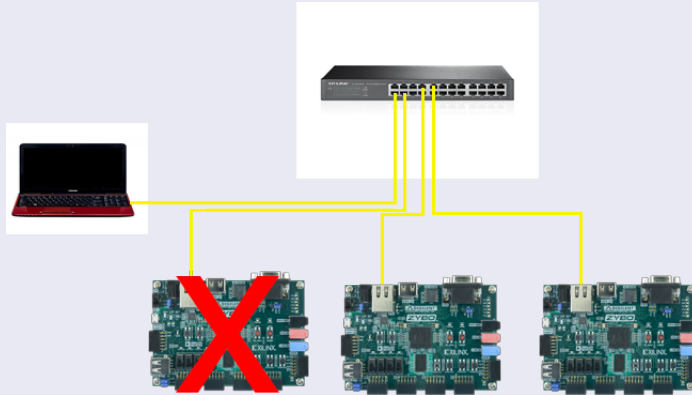
Un nodo intermedio se encuentra desconectado.



# Conclusiones

## Escenario de trabajo 3

El primer nodo está desconectado.



- 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.