Sistemas de monitorización de latencias en redes de visibilidad

J. Álvaro Garrido López

Universidad de Granada

Tutores: Javier Díaz y Miguel Jiménez

Trabajo de Fin de Grado

September 9, 2019

Índice

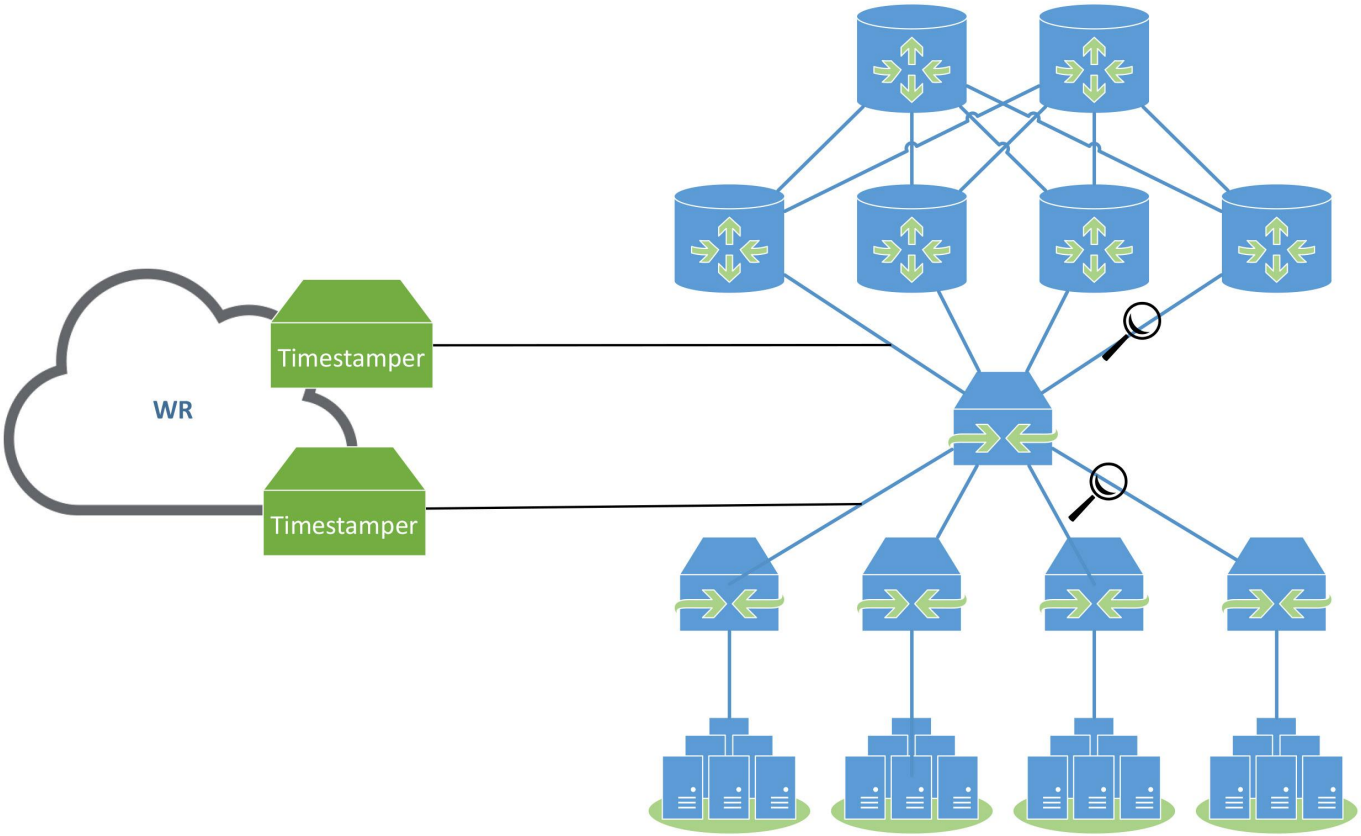
Introducción

Redes de visibilidad y aplicaciones

¿Qué son las redes de visibilidad?

Son la infraestructura en una red que permite la monitorización de la misma, con el fin de conocer el estado sobre su rendimiento y de detectar posibles fallos de seguridad.

Redes de visibilidad y aplicaciones



Motivación y contexto

Contexto

- Volúmenes ingentes de datos
- Preocupación por la seguridad
- Servicios de altas prestaciones (telecom y finance)
- Necesidad de controlar constante y eficientemente el tráfico
- Auge del *Big Data*

- Ingredientes perfectos para que se requiera de una recopilación, distribución y entrega de datos eficaz y escalable.
- De este punto parte la **visibilidad en redes**.

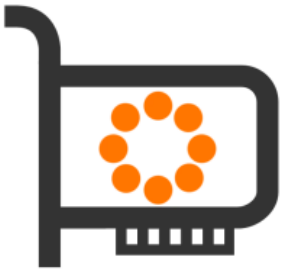
Objetivos (I)

- Estado de la técnica sobre captura eficiente
- Aplicaciones comerciales y libres para visibilidad
- Análisis sobre las características de las tecnologías encontradas
- Evaluación del funcionamiento lógico de tecnologías

Objetivos (II)

- Diseño y desarrollo del sistema. Favorecer escalabilidad y flexibilidad
- Integración de los componentes *hardware* y *software*
- Integración de un sistema de alerting

Material y métodos



Estado de la técnica

Métodos para implementar visibilidad (I)

- Mediante peticiones **SNMP**
- A través de **gestión directa** del tráfico (e.g. mediante **TAP**)
- Gestión del tráfico **por flujos** (e.g. **sflow**)

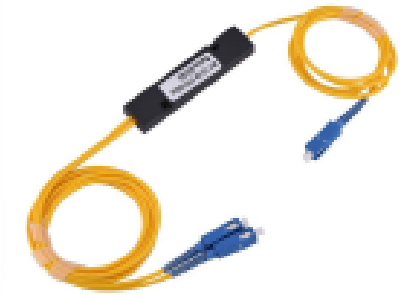
Métodos para implementar visibilidad (II)

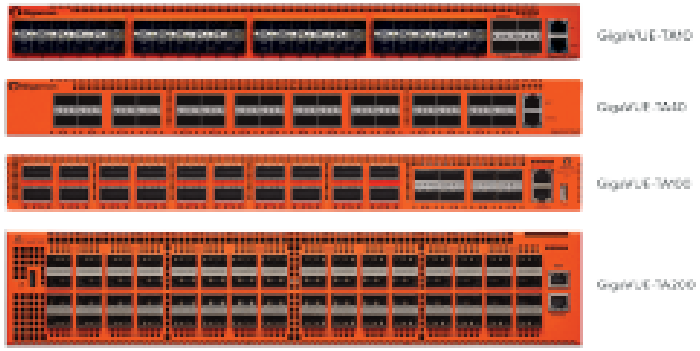
La figura que hablamos con snmp, flow o extracción directa de tráfico + dispositivos hw de captura/análisis 1 slide

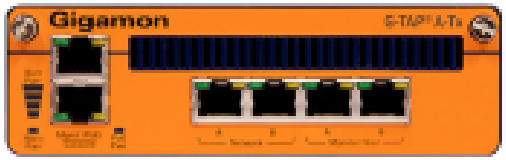
Hardware específico para visibilidad (I)

- Divisores ópticos
- SPAN
- TAP
- Agregadores

Hardware específico para visibilidad (II)







Implementación

Pruebas preliminares

Treatments	**Response 1**	**Response 2**
Treatment 1	0.0003262	0.562
Treatment 2	0.0015681	0.910
Treatment 3	0.0009271	0.296

Table: Table caption

Captura de paquetes

- **libpcap**
- **pf_ring ZC**. Búffer circular con **DMA**.
- **NetSniff**

- Captura de paquetes con .... 1 slide (para esta y las siguientes, discute las alternativas, indica las pruebas más relevantes y acaba con la solución final)

Filtrado

Almacenamiento

Visibilidad

Setup final

Resultados

Resultados

fitrados, visualizacioń de latencias, setups utilizados, etc..

Resultados

fitrados, visualizacioń de latencias, setups utilizados, etc..

Resultados

fitrados, visualizacioń de latencias, setups utilizados, etc..

Conclusiones

Conclusiones

fitrados, visualizacioń de latencias, setups utilizados, etc..

Trabajo futuro

fitrados, visualizacioń de latencias, setups utilizados, etc..

Referencias

John Smith (2012)

Title of the publication

Journal Name 12(3), 45 – 678.