Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del

Análisis de

problema

Reconstrucci caminos

Identificación y clasificación de

Decisiones generale

Tests y

Pruebas de códig Resultados con

Trabajo futuro

Reconstrucción de caminos y detección de dispositivos

David Moreno Maldonado

Tutor: Guillermo Julián Moreno Ponente: Javier Aracil Rico

Universidad Autónoma de Madrid Ingeniería Informática y Matemáticas

15 junio, 2020

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducció

arte

Análisis de problema

Reconstrucción caminos
Identificación y clasificación de dispositivos

Decisiones generale Estructura del programa

Tests y resultados Pruebas de código Resultados con trazas reales Introducción

Estado del arte

Análisis del problema

• Reconstrucción de caminos

• Identificación y clasificación de dispositivos

4 Desarrollo

Decisiones generales

Estructura del programa

Tests y resultados

• Pruebas de código

Resultados con trazas reales

Descripción general

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado arte

Análisis del

Reconstrucción caminos Identificación y clasificación de dispositivos

Decisiones generale Estructura del

Tests y resultados Pruebas de código Resultados con trazas reales

Situación:

- Existencia de redes de gran tamaño y complejidad.
- Varios puntos de captura de tráfico en estas redes.

Problemas:

- Pérdida de paquetes.
- Ralentización de red.
- Paquetes duplicados.



Necesidad de **detectar los puntos exactos** de la red donde se producen estos problemas.

Solución:

Reconstrucción de caminos IP

Detección y clasificación de dispositivos

Objetivos:

- Eficiencia en tiempo de ejecución y uso de memoria.
- Abstracción para su uso en diferentes entornos.

Reconstrucción de flujos IP

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del arte

Análisis de

problema Reconstrucción

ldentificación y clasificación de dispositivos

Decisiones generale

Estructura del programa

resultados
Pruebas de código
Resultados con
trazas reales

- Trazas pcap capturadas.
- Útiles como herramientas auxiliares.
- Análisis no específico en reconstrucción.
- Poca eficiencia con trazas de gran tamaño.







Detección de dispositivos

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del arte

Análisis del

Reconstrucción

Identificación y clasificación de

clasificación de dispositivos

Decisiones generale Estructura del

Tests y resultados

Pruebas de códig Resultados con trazas reales

- No existen métodos generalizados.
- Estudio de las características para inferir el dispositivo.
- Existencia de dispositivos compuestos.







Planteamiento del problema y caso inicial

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

arte Análisis de

Análisis del problema

Reconstrucción de caminos

Identificación y clasificación de dispositivos

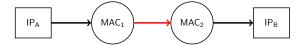
Decisiones ge

Estructura del programa

Tests y resultados

Pruebas de códig Resultados con trazas reales

- La información recibida es a nivel de paquete con IP origen y destino y MAC origen y destino.
- Almacenar los flujos IP en un grafo unidireccional.
- Aristas abiertas y cerradas dependiendo de si la conexión entre nodos se ha visto físicamente.



Inserción estándar

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducciór

arte

Análisis del problema

Reconstrucción de caminos

Identificación y clasificación de dispositivos

Desarrollo

Estructura del programa

Tests y resultados

Pruebas de código Resultados con trazas reales

Trabajo futur 7 / 23 Cuando vemos un paquete con MAC destino igual al primer nodo MAC del grafo:



Cuando vemos un paquete con MAC origen igual al último nodo MAC del grafo:



Bifurcación

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducció

arte

Análisis del problema

Reconstrucción de caminos

Identificación y clasificación de dispositivos

Decisiones general

Estructura del programa

Tests y resultados

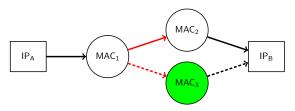
Pruebas de código Resultados con trazas reales

Trabajo futur 8 / 23

¿Por qué ocurren?

- Caída temporal de una parte de la red.
- Congestión de la red.
- Funcionamiento usual de la red.

Las detectamos cuando observamos un paquete con un nodo MAC en el grafo, pero no estamos en el caso de inserción estándar:



Camino huérfano

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducció

arte

Análisis del problema

Reconstrucción de caminos

clasificación de dispositivos

Decisiones generale

Estructura del programa

Tests y resultados

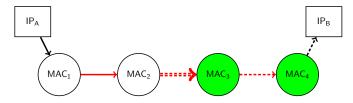
Pruebas de código Resultados con trazas reales

Trabajo futui

Analizamos un paquete cuyas MAC no están en el grafo.

Necesitamos utilizar información extra. TTL del paquete.

Se genera una arista virtual conectando los nodos.



Identificación de dispositivos

Reconstrucción y detección de tráfico

David Moren Maldonado

Introducció

Análisis de

Análisis de problema

caminos Identificación y

dispositivos

Desarrollo

Decisiones general Estructura del

Tests y resultados

Pruebas de códig Resultados con trazas reales

- Identificamos como dispositivos las aristas virtuales.
- 2 Agregamos la información de todos los flujos (MAC de entrada y de salida, bytes, *frames*, ...).
- Resolvemos las dependencias existentes entre dispositivos.

Clasificación de los dispositivos

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado de arte

Análisis del

problema

Reconstrucción
caminos

Identificación y clasificación de dispositivos

Desarrollo

Tests y resultados

resultados Pruebas de código Resultados con trazas reales

Trabajo futu 11 / 23 Diferenciamos entre *firewalls*, *routers* y balanceadores de carga a nivel MAC. Se siguen estas reglas:

- **1** Los dispositivos con $\Delta TTL = 0$ se clasifican como *firewalls*.
- Aquellos que conecten más de una MAC física y unicast se clasifican como balanceadores de carga a nivel MAC.
- 3 El resto se clasifica como router.

Planteamiento inicial del desarrollo

Reconstrucción y detección de tráfico

David Moren Maldonado

Introducció

arte

Análisis de problema

Reconstrucción caminos Identificación y

clasificación de dispositivos

Decisiones generales Estructura del

Tests y

Pruebas de código Resultados con trazas reales

Trabajo futuro

El programa se desarrollo para la empresa Naudit, dedicada al análisis y monitorización de redes.

Integración con fisher

Reconstrucción y detección de tráfico

David Moren Maldonado

Introducció

Análisis de

Análisis de problema

Reconstrucción de caminos Identificación y clasificación de dispositivos

Desarrollo

Decisiones generales Estructura del

Tests y
resultados
Pruebas de código
Resultados con
trazas reales

Trabajo futuro 13 / 23

- Aplicación dedicada a la lectura de trazas pcap.
- Se utilizaron y modificaron librerías internas (estructuras IP y MAC, diccionarios, listas, log, test).
- Uso de memoria estática. Se evita el uso continuo de malloc y free.

Estructura general del programa

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del

Análisis de

Reconstrucción

caminos Identificación y

Identificación y clasificación de dispositivos

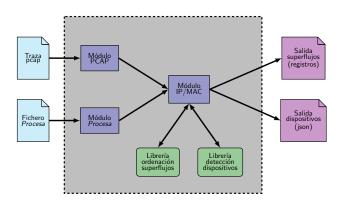
Desarrollo

Decisiones gener

Estructura del

resultados

Pruebas de códig Resultados con



Librería de ordenación de superflujos

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

arte

Análisis del

Reconstrucción caminos Identificación y

Identificación y clasificación de dispositivos

Decisiones gene
Estructura del
programa

Tests y
resultados
Pruebas de cód
Resultados con

trazas reales Trabajo futi Librería abstracta, capaz de manejar flujos multicapa de diferentes características. Estructuras de datos definidas:

- Grafo unidireccional.
- Información de cada capa.
- Nodos.
- Aristas.
- Camino: Enlace entre estructuras externas.

Es necesario indicar la memoria disponible para estos elementos.

Módulo IP/MAC

Reconstrucción y detección de tráfico

Estructura del

- Especifica la librería de ordenación de flujos para las capas IP y MAC
- Encargada de definir el número de estructuras de cada tipo requerido.

Estructura	Número de estructuras por superflujo
Superflujos Elementos IP Elementos MAC Nodos Aristas	$\begin{matrix}1\\2\\\alpha\\2+\alpha\\(nodos-1)+\lambda\end{matrix}$

Entrada al programa

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducció

arte

Análisis de problema

Reconstrucción caminos Identificación y clasificación de dispositivos

Desarrollo

Estructura del

resultados
Pruebas de cód
Resultados con

Trabajo futur 17 / 23

Ficheros pcap:

- Aprovecha totalmente la estructura interna de fisher.
- Formato estándar de captura de tráfico.

Ficheros Procesa:

- Fichero por registros de conexiones. Formato interno Naudit.
- Ficheros más compactos que los pcap.
- Necesidad de calcular menos datos internamente (RTT, número de frames, ...).

Salida del programa

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducció

Análisis de

Análisis de problema

Reconstrucción o caminos Identificación y clasificación de

Desarrollo

Estructura del

resultados Pruebas de códig Resultados con trazas reales

Trabajo futuro 18 / 23

Salida de los superflujos:

- Un registro por arista en el grafo
- Se indica información recopilada (número de frames, bytes, ...)

Salida de dispositivos:

- Formato JSON
- Información sobre interfaces MAC del dispositivo, flujo de paquetes y bytes o IPs que conecta.

Pruebas realizadas al programa

Reconstrucción y detección de tráfico

Pruebas de código

- Uso del módulo de test integrado en fisher.
- Test específicos para las librerías de ordenación y clasificación.
- Uso del CI (Continuous Integration) disponible en GitLab.
- Depuración de memoria usada con Valgrind.

Tiempo de ejecución

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del

Análisis de

problema

caminos

Identificación clasificación dispositivos

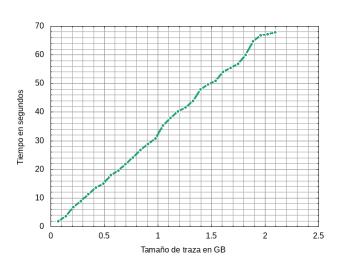
Desarrolle

Decisiones generale Estructura del

Tests y

resultados

Resultados con trazas reales



Uso de memoria

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estado del

Análisis de

problema

Reconstrucción

Identificación clasificación

esarrollo

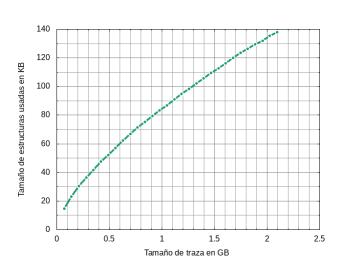
Decisiones ge

Estructura del programa

Tests y

Pruebas de có

Resultados con trazas reales



Trabajo futuro

Reconstrucción y detección de tráfico

David Moren Maldonado

Introducció

Análicie de

Análisis de problema

caminos Identificación y clasificación de dispositivos

Decisiones gener

Tests y

Pruebas de códig Resultados con

Trabajo futuro 22 / 23

- Aumento de la información recopilada en cada dispositivo, por ejemplo, subredes.
- Clasificación más detallada (balanceadores de carga a nivel IP, routers NAT, ...).

Reconstrucción y detección de tráfico

David Moreno Maldonado

Introducción

Estada dal

Análisis del

problema

Reconstruccio

Identificación y clasificación de

Desarrollo

Decisiones genera

Estructura del

Tests y

Pruebas de código Resultados con

Trabajo futuro 23 / 23

Muchas gracias.