

Escaneo de redes IEE 802.11: Análisis de datos

Prof. Laudin Alessandro Molina T.

Universidad de Los Andes, Venezuela

Octubre de 2014

Contenidos

1 Introducción

2 Caracterización de despliegues

Agenda

1 Introducción

2 Caracterización de despliegues

Motivación

Usuarios móviles Redes inalámbricas populares y en crecimiento

- En 2011, 175MM + de *laptops* en el mundo (Cisco, 2012)
- En 2011, 34MM + de *tablets* en el mundo (Cisco, 2012)
- Para 2016 los equipos Wi-Fi y móviles generaran 54 % del tráfico IP (Cisco, 2014)
- Tráfico móvil crecerá 11x entre 2013 y 2018 (15,9 *exabytes/mes*) (Cisco, 2014)
- ~53MM de hotspots para 2018 (Cisco, 2014)

Redes IEEE 802.11

Características

- Inalámbricas
- ISM – 2,4GHz / 11 canales
- CSMA/CA
- Variaciones en el medio
- Interferencia de otras redes



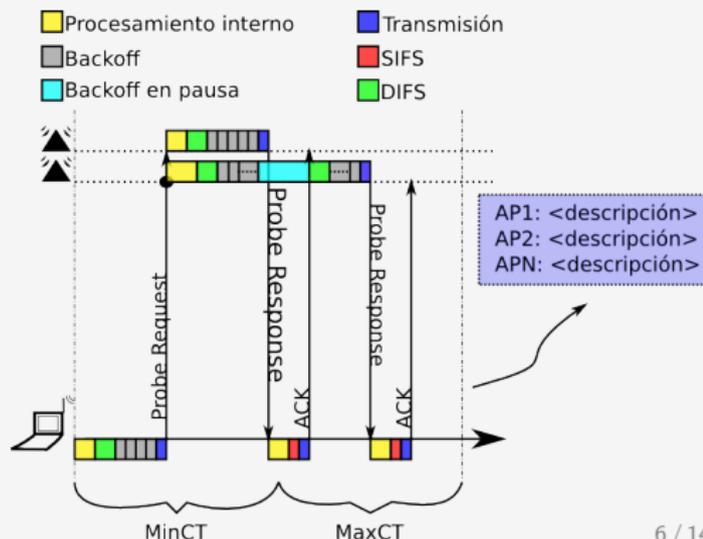
Despliegues
Densos y Espontáneos

Escaneo activo

Para cada canal i:

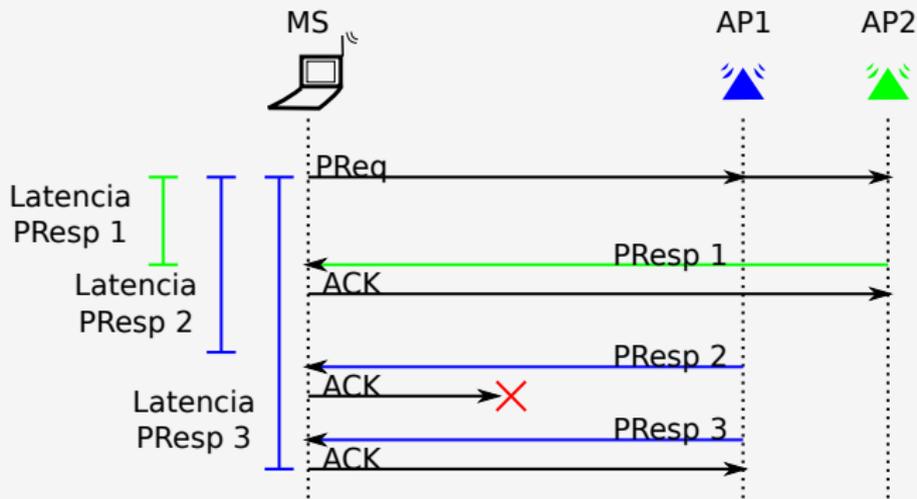
- 1 Broadcast *Probe Request* en canal i
- 2 Esperar *Probe Responses* durante *MinChannelTime*
- 3 Si se recibió al menos un *Probe Response* aumentar la espera hasta *MaxChannelTime*
- 4 Cambiar al siguiente canal

CSMA/CA ordena los P_{resp}



Latencia de las respuestas

- Tiempo entre P_{rq} y el P_{resp}
- Cada P_{resp} tiene asociada una latencia
- Múltiples P_{resp} por AP son posibles

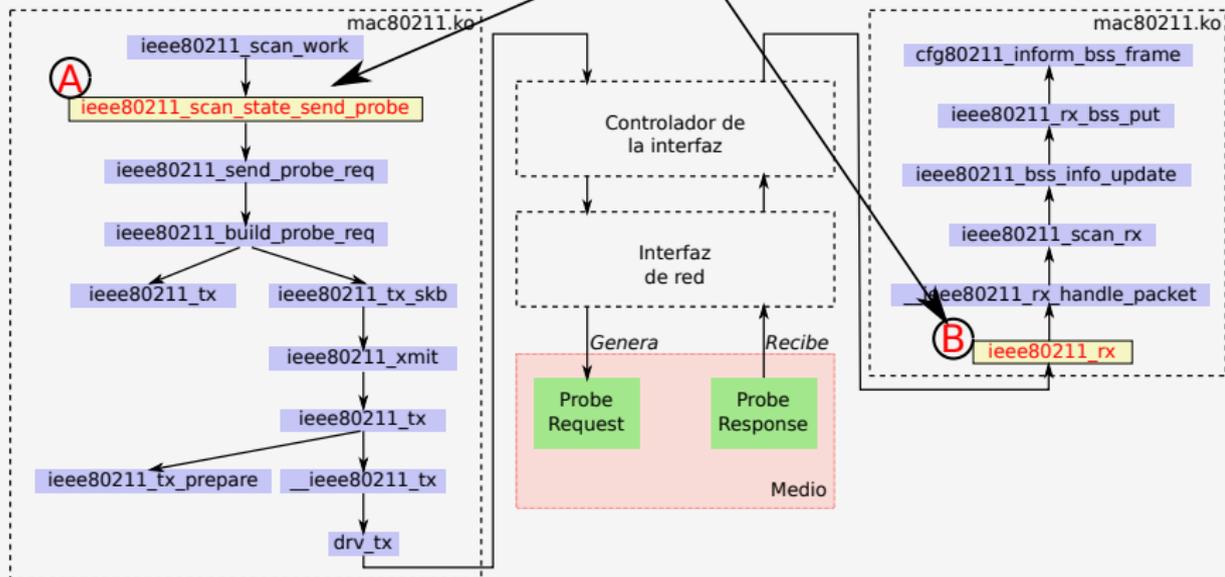


Escaneo en el kernel de Linux

$A = t(P_{rq})$ = tiempo en `ieee80211_scan_state_send_probe`

$B = t(P_{resp})$ = tiempo en `ieee80211_rx`

latencia = B - A



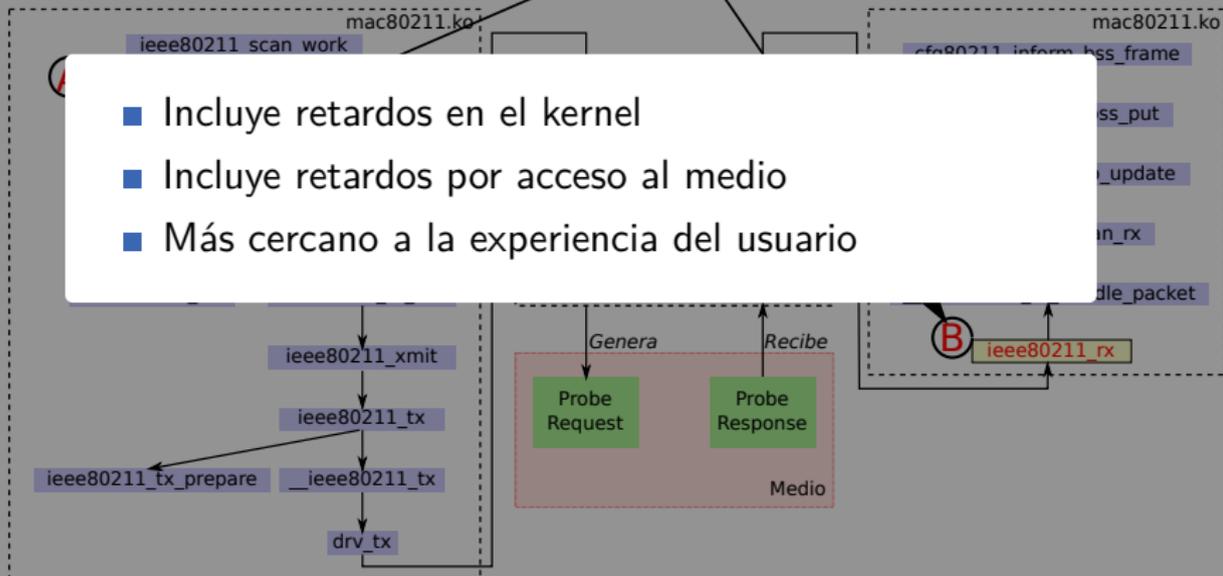
Escaneo en el kernel de Linux

$A = t(P_{rq})$ = tiempo en `ieee80211_scan_state_send_probe`

$B = t(P_{resp})$ = tiempo en `ieee80211_rx`

latencia = B - A

- Incluye retardos en el kernel
- Incluye retardos por acceso al medio
- Más cercano a la experiencia del usuario



Agenda

1 Introducción

2 Caracterización de despliegues

Experimentos controlados

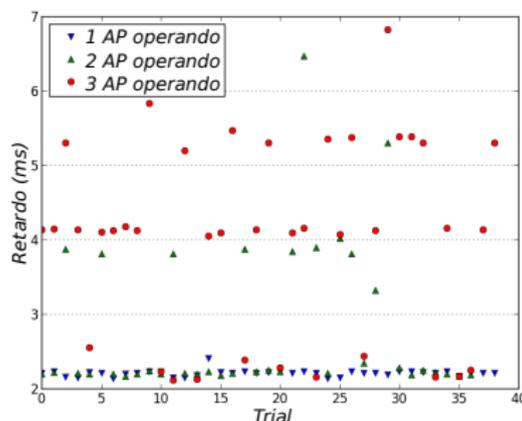
Latencia afectada por:

Modelo del AP

AP	\bar{x} (ms)	σ (ms)
R2	1,28	0,18
R3	1,93	0,06
R1	2,20	0,02
R4	2,66	0,50
R5	3,51	0,45

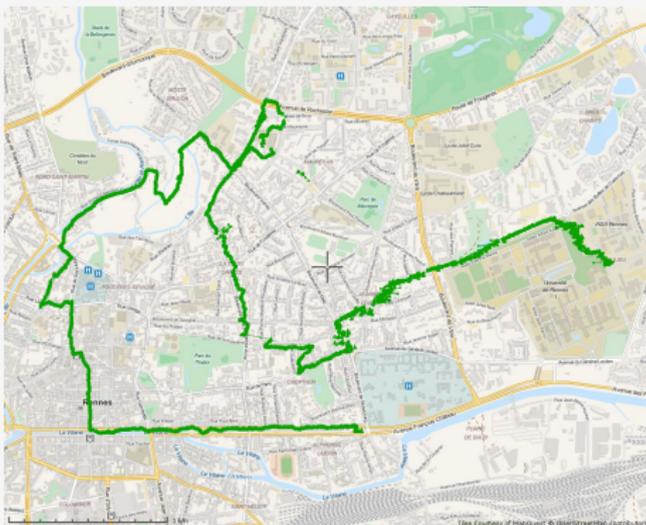
- Experimentos controlados
- No se detectaron otros dispositivos operando
- 5 AP de diferente modelo
- 1 AP a la vez

Ocupación del medio



- Igual modelo y configuración
- Mayor contención \Rightarrow mayor aleatoriedad

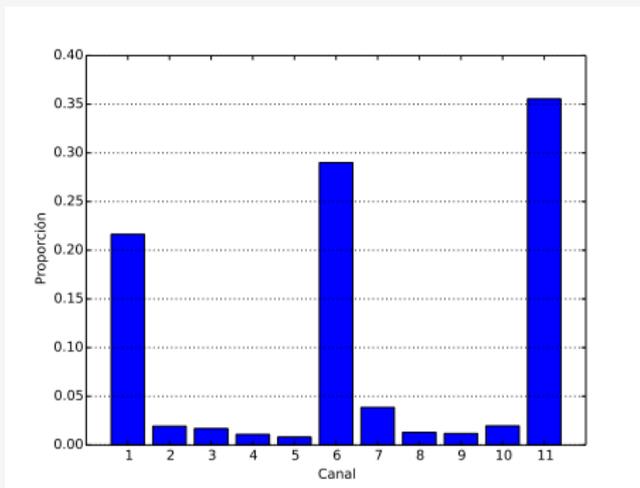
Despliegues espontáneos



- Rennes, Francia
- Recorrido de 11Km caminando
- Canales 1 a 11, secuencialmente
- Tiempo de espera 500ms/canal
- 11166 P_{rq} transmitidos
- 19165 P_{resp} registrados
- 3441 redes / 1937 AP
- Varias redes por AP

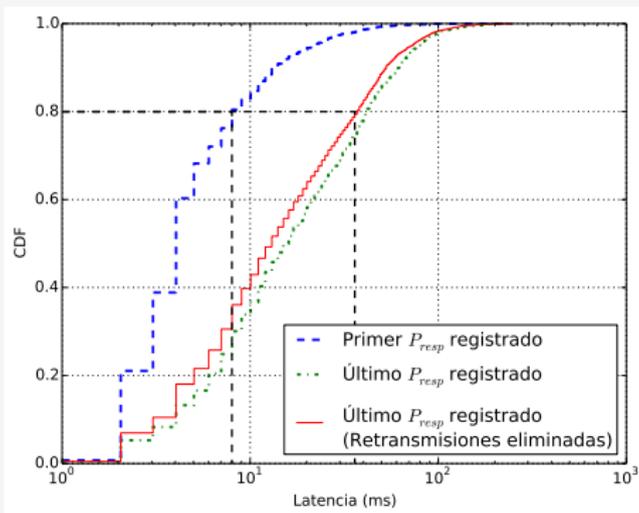
Caracterización del despliegue

Canales



- 86,18% de las redes en los canales 1, 6 y 11

Latencia de las respuestas



- Primera respuesta en menos de 8 ms el 80% de los escaneos
- Última respuesta en menos de 36 ms el 80% de los escaneos posiblemente por acceso secuencial

Realizar taller propuesto