Asiganción de direccionamiento IPv6 en la red de la Universitat de València

Jose Miguel Femenia Herrero
Servei d'Informàtica Universitat de València
jose.m.femenia@uv.es

XXXI Grupos de Trabajo RedIRIS
Barcelona, 1 y 2 de junio de 2011

Direccionamiento IPv6 @ UV

- Direccionamiento IPv6 asignado por RedIRIS:
  - 2001:720:1014::/48
- Asignado /64 a cada una de las subredes IPv4 existentes → 113 subredes IPv6
  - Exceptuando algunas conexiones punto a punto dónde se asigna un /126

Mecanismos de asignación analizados.

- Automáticos:
  - DHCPv6 (stateful).
    - ISC – DHCP 4.2
  - Stateless address autoconfiguration (SLAAC).
    - RA Cisco routers.
    - Router advertisement daemon (radvd).
- Manual

Mecanismos de asignación utilizados

- Equipos en subredes de usuarios (cable y WiFi)
  - SLAAC
  - Extensiones de privacidad
  - Combinado con DHCPv4
- Servidores
  - Manual
- Electrónicas de red
  - Manual

Subredes de usuario

- SLAAC
  - EUI-64 modificado.
    - 00:1A:B1:06:B7:14 → 00:1A:B1:FF:FE:06:B7:14
  - Extensiones de privacidad: RFC 4941
  - Seguridad: SeND, IPv6 RD Guard, IPv6 ND Inspection.
- DNS y otros parámetros por DHCPv4
  - ffc0:0:0:ffff::1 (obsoleto)

Extensiones de privacidad RFC 4941

- Evita asociar, en una configuración SLAAC, una dirección IPv6 a una MAC.
- Genera direcciones IPv6 temporales creando cadenas de bits aleatorias con un tiempo de vigencia corto (de horas a días) y las usa como dirección de cliente en las conexiones.
- Está activado por defecto en Windows Vista, 7 y Server 2008.
  - netsh interface ipv6 set global randomizeidentifiers=disabled

Seguridad con RFC 4941

- ¿Quién tenía la IP 2001:720:1014:160:484:a0f8:f8d6:c908 a las 12:25 horas del día 2011-05-20?
- Extracción periódica de la tabla de vecinos de IPv6 de los routers y registro en una base de datos.
  - Limpieza cada cierto tiempo de esa base de datos:
    - 7000 equipos con IPv6 activado → 26000 direcciónes IPv6 distintas al cabo de 5 dias.
- Netdisco1.1

Netdisco 1.1 IPv6

Search Results

MAC	Vendor	Match	Device or Node	First Seen	Last Seen
00:1a:80:a2:e0:68	Sony Corporation	MAC -> IP	2001:720:1014:160:6067:43f0:c3d3:3b5d ([No DNS])	May 25 09:35 2011	May 25 11:55 2011
		MAC -> IP	fe80::b8de:a476:e892:aa90 ([No DNS])	Apr 28 09:55 2011	May 25 11:55 2011
		MAC -> IP	(quifis)	Dec 9 09:37 2008	May 25 11:55 2011
		MAC -> IP	2001:720:1014:160:a59c:9852:e3ba:40dc ([No DNS])	May 23 10:35 2011	May 23 13:55 2011
		MAC -> IP	2001:720:1014:160:484:a0f8:f8d6:c908 ([No DNS])	May 20 09:35 2011	May 20 12:55 2011
		MAC -> IP	2001:720:1014:160:6105:db7d:4b73:bf7 ([No DNS])	May 19 09:55 2011	May 19 12:55 2011
		MAC -> IP	2001:720:1014:160:b457:6ccc:4aa1:8c9a ([No DNS])	May 18 09:35 2011	May 18 12:55 2011
		Switch Port	147.156.. [FastEthernet0/5] (.red)	Feb 3 14:04 2011	May 25 12:09 2011
		NetBIOS	\\CLARAGROUP\LABMACRO [No User]@147.156.	Mar 22 09:23 2011	Apr 6 09:21 2011

- No es exhaustivo, pero se pueden ajustar los tiempos para que no se pierda mucha información de una IPv6 activa.
- Funciona incluso con la red WiFi

IPv6 en servidores.

- Se desconfigura el envio de RA en los puertas de los routers de su subredes.
  - ipv6 nd ra suppress
- Por precaución, desactivación de la escucha de RA para SLAAC en los interfaces de los servidores.
- IPv6 manual ↔ Herramienta de gestión de IPv6 ↔ resolución DNS directa e inversa.

Debian: desactivar SLAAC

- Debian squeeze(estable)/wheezy(testing)
  - /etc/network/interfaces

```
iface eth0 inet static
        ...
        pre-up echo 0 > /proc/sys/net/ipv6/conf/eth0/autoconf
        pre-up echo 0 > /proc/sys/net/ipv6/conf/eth0/accept_ra
        pre-up echo 0 > /proc/sys/net/ipv6/conf/eth0/accept_ra_defrtr
        pre-up echo 0 > /proc/sys/net/ipv6/conf/eth0/accept_ra_pinfo
        pre-up echo 0 > /proc/sys/net/ipv6/conf/eth0/accept_ra_rtr_pref

iface eth0 inet6 static
        address 2001:720:1014:x::x
        netmask 64
        gateway 2001:720:1014:x::y
```

Debian: desactivar SLAAC

- Debian sid(inestable)
  - /etc/sysctl.d/ipv6.conf

```
net.ipv6.conf.default.autoconf = 0
net.ipv6.conf.default.accept_ra = 0
net.ipv6.conf.default.accept_ra_defrtr = 0
net.ipv6.conf.default.accept_ra_rtr_pref = 0
net.ipv6.conf.default.accept_ra_pinfo = 0
net.ipv6.conf.all.autoconf = 0
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.all.accept_ra_defrtr = 0
net.ipv6.conf.all.accept_ra_rtr_pref = 0
net.ipv6.conf.all.accept_ra_pinfo = 0
```

IPv6 en WiFi

- SLAAC como en la redes cableadas.
- Routing separado:
  - IPv4: 3750G-16TD
  - IPv6: 7206VXR (NPE-G1)
- Bastante carga de tráfico multicast con el IPv6 activado.
- Falta de recursos para IPv4+IPv6 en el 3750G

IPv6 WiFi y VLANs dinámicas.

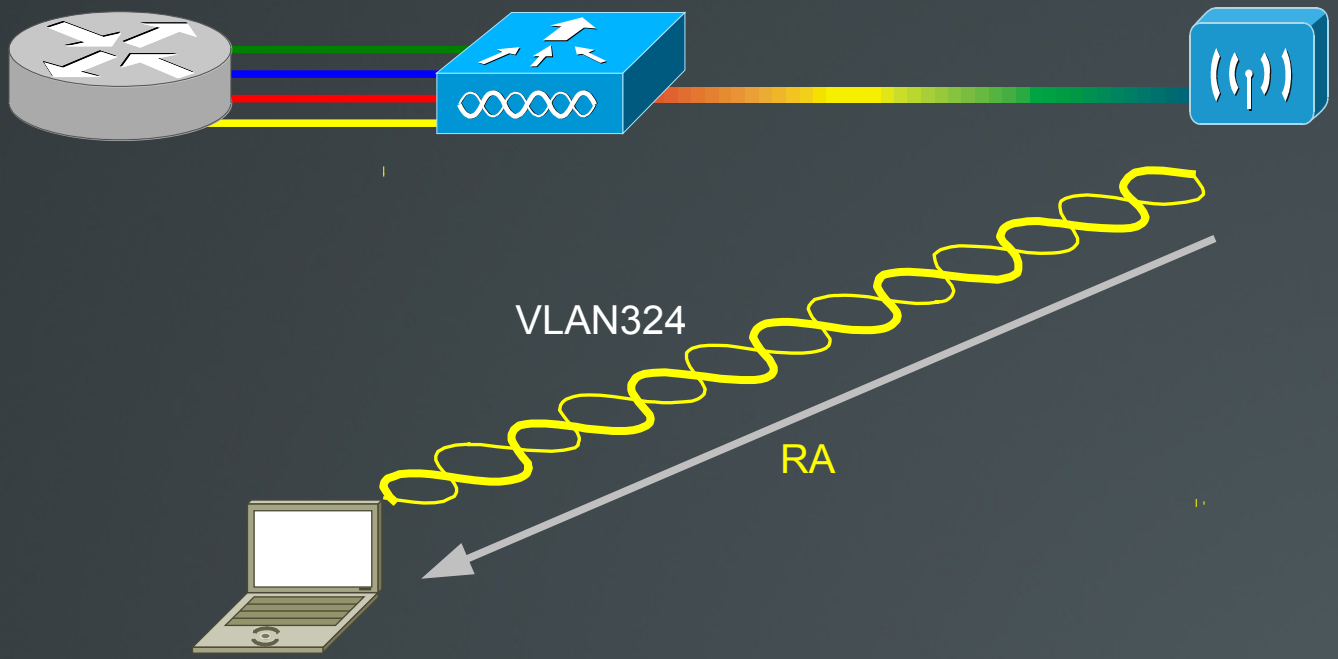
- Se crean pools de VLAN dinámicas son subredes /24 para ”controlar” el broadcast en la red inalámbrica y sus correspondientes /64 de IPv6. Sobre el mismo SSID (eduroam).
- Por ejemplo:

VLAN321	147.156.248.0/24	2001:720:1014:AAA1::/64
VLAN322	147.156.249.0/24	2001:720:1014:AAA2::/64
VLAN323	147.156.250.0/24	2001:720:1014:AAA3::/64
VLAN324	147.156.251.0/24	2001:720:1014:AAA4::/64

IPv6 WiFi y VLANs dinámicas.

- Un equipo se asocia al AP y se le asigna a la VLAN324, con lo que por DHCP recibe la IPv4 147.156.251.202 y demás parámetros. Por ende, recibe el primer RA del router IPv6 y se configura con una dirección 2001:720:1014:AAA4:0224:d7ff:fe08:c404/64 y su ruta por defecto adecuada a la dirección de link-local del interfaz en esa VLAN del router.
- Hasta aqui, todo correcto.

IPv6 WiFi y VLANs dinámicas.

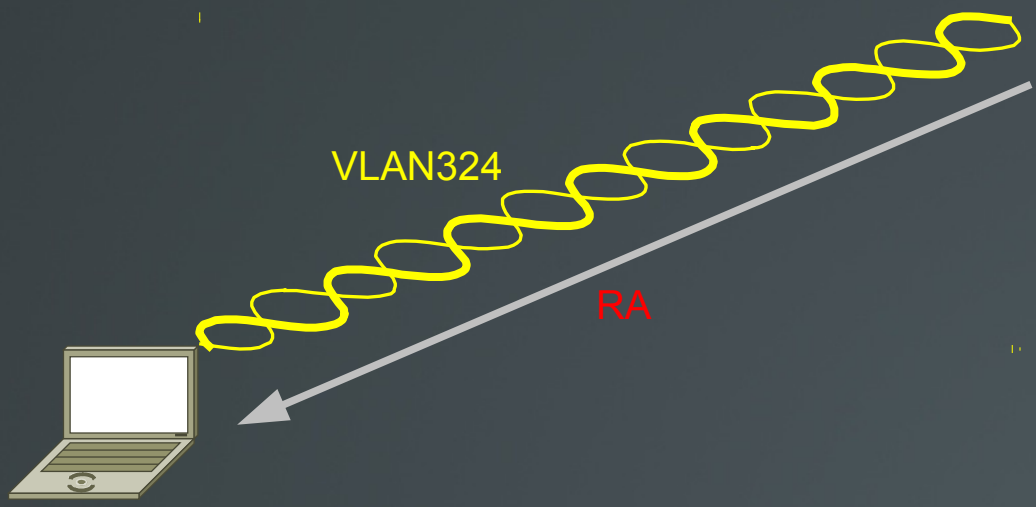


147.156.251.202
2001:720:1014:AAA4:0224:d7ff:fe08:c404/64
::0 → link-local anunciado por RA para VLAN324

IPv6 WiFi y VLANs dinámicas.

- Se asocia una segunda estación a ese mismo AP pero se le asigna (normalmente de forma rotativa) una VLAN distinta
- El nuevo cliente solicita la información para configuración por SLAAC y recibe el RA para su VLAN322 y la información de IPv4 por DHCP.
- ¡¡¡La estación en la otra VLAN también recibe el nuevo RA y se autoconfigura con los parámetros nuevos!!!

IPv6 WiFi y VLANs dinámicas.



147.156.251.202
2001:720:1014:AAA4:0224:d7ff:fe08:c404/64
::0 → link-local anunciado por RA para VLAN324
2001:720:1014:AAA2:0224:d7ff:fe08:c404/64
::0 → link-local anunciado por RA para VLAN322

147.156.249.229
2001:720:1014:AAA2:0224:d7ff:fe08:c404/64
::0 → link-local anunciado por RA para VLAN322

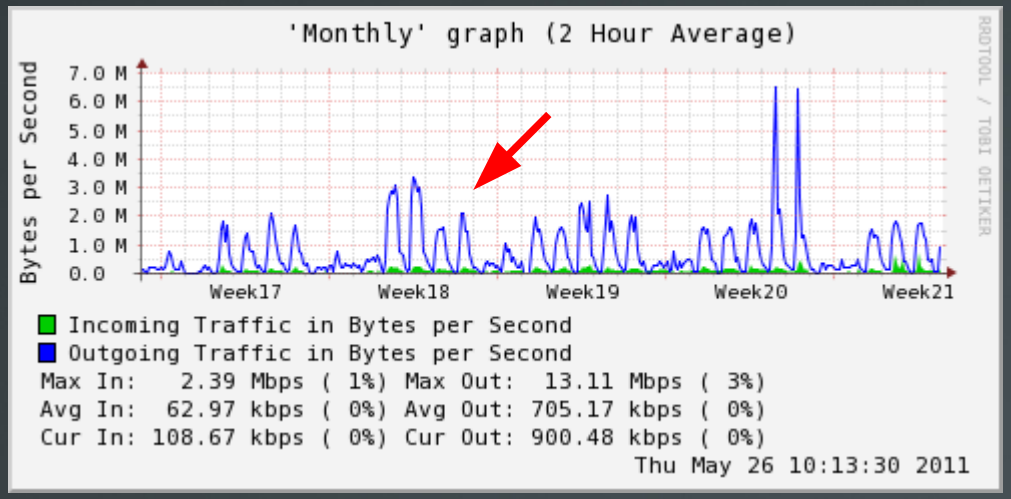
IPv6 WiFi y VLANs dinámicas.

- Los clientes pierden conectividad IPv6.
- Los Router Advertisements se emiten por multicast a todos los nodos.
- En 802.11 el tráfico por radio no va marcado con VLAN (el AP registra una tabla de MAC asociadas a cada VLAN).
- En WPA(x)-Enterprise, las claves son únicas para cada cliente unicast, pero son la misma para el tráfico broadcast y multicast de todas las estaciones en el mismo SSID en el mismo AP.

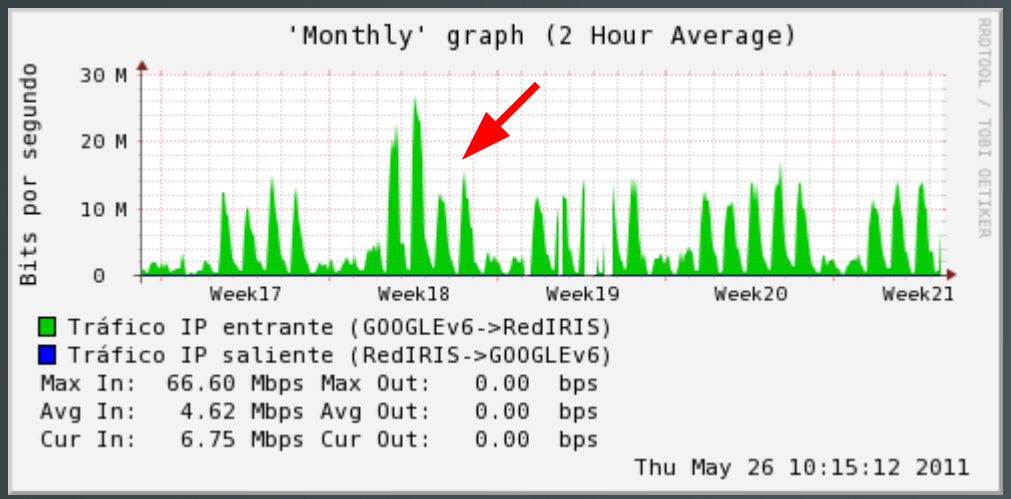
IPv6 WiFi y VLANs dinámicas.

- Todas las estaciones escuchan todo el tráfico broadcast/multicast.
  - Problema para la autoconfiguración de IPv6
  - "Hole 196" WPA2 Attack
- De momento, se ha desactivado la conectividad IPv6 de la red inalámbrica.
- Espera de soluciones ”propietarias”:
  - Conversión de los RA multicast en unicast antes de enviarlos.

Implicaciones en el tráfico IPv6



Tráfico UV-RedIRIS



Tráfico GOOGLEv6 - RedIRIS

DNS: resolución inversa.

- SLAAC → problema con la resolución inversa.
- DNS dinámico
- v6rev.pl (Kazunori Fujiwara)

$ host 2001:720:1014:AAA4:0224:d7ff:fe08:c404
4.0.4.c.8.0.e.f.f.f.7.d.4.2.2.0.4.a.a.a.4.1.0.1.0.2.7.0.1.0.0.2.ip6.arpa domain name pointer 200107201014aaa40224d7fffe08c404.ipv6.eduroam.uv.es.