IPv6 Community Wifi

Unique IPv6 Prefix per Host

IPv6 Enhanced Subscriber Access for WLAN Access
• Gunter Van de Velde
• 19-04-2016
IPv6 timeline
4 waves… as noticed by ALU IP Division

~2000
IPv6 INIT
- IPv6 native routing

~2005
IPv6 infrastructure
- Interconnecting IPv6 clouds (6PE/6VPE)

~2010
IPv6 for services
- Residential (BNG)
- Business VPN

~2015
IPv6 for Mobile access (3GPP)
- IPv6 for Carrier Wi-Fi
Carrier wi-fi
Who? What? How?

- Who?
- What?
  - Community Wi-Fi (residential Wi-Fi, like Fon/Wifree/…)
  - Hotspot aggregation (venues, stadiums, airports, …)
  - Mobile off-load (connect to mobile network over Wi-Fi)
- How?
  - Offering seamless (and secured) connectivity over Wi-Fi
  - Tunneling traffic from access points towards centralized gateway (*next slide*)
Wireless LAN gateway
Ecosystem

- Hotspot
- Small Cell
- Enterprise
- Mobile Wi-Fi Hotspot
- Homespot

Captive Portal & Analytics
AAA-server
POLICY & SUBSCRIBER MANAGEMENT
WIRELESS PACKET CORE
IP EDGE
WLAN GATEWAY
IPv6
IPv6
IPv6

Cellular
Carrier cloud
Internet

MDM
HLR/HSS
PCRF

© Nokia 2016
What are the IPv6 enablers for carrier Wi-Fi?

1. Dynamic behavior of sessions, consuming more IP-addresses
   - Each session, being redirect, active or passive will consume IP address
   - NAT44 only option for IPv4, with clear disadvantages (next slide)

2. Huge variety of IPv6 enabled, host-OS’s (IOS, Android, windows...)
   - Note that for Wi-Fi (in opposite to mobile) not only SIM-based devices are present. Regular PC’s/laptops/gaming consoles may connect as well.
Wlan gateway
IPv4 addressing challenges

1. IPv4 inefficient address usage
   - Open SSID: no detection mechanism when UE disappears
   - Closed SSID (PMK caching): UE will return in Wi-Fi range and will request/re-use the previous IPv4 address

2. IPv4 NAT44 characteristics
   - Only few hundred ports per UE required
   - Data retention and lawful intercept (NAT logging)
   - Focus on fragmentation/reassembly over tunnels
Wlan gateway
IPv6 only?

IPv6 only the best way forward for Wi-Fi?

- Long term... yes
- Today... technically yes

But today...

- Still NAT required: NAT64 (DNS64)
- Most Wi-Fi devices are dual stack (initial start with IPv4), and still some Wi-Fi devices are IPv4-only
- In contrast to mobile/cellular, where a UE (Smartphone) is a controlled device, this is not the case for Wi-Fi. IPv4 will remain for a while...
WLAN gateway
dual stack approach

Why dual stack?

- Most of the Wi-Fi devices support dual stack
- Even some “legacy” IPv4-only devices
- Hitless introduction

Three dual-stack IPv4/v6 models are envisaged:

- DHCPv4 + SLAAC/64
- DHCPv4 + SLAAC/64 with DHCPv4 linking
- DHCPv4 + DHCPv6/128 IA_NA

... most of the devices start with SLAAC and may enable DHCPv6
WLAN gateway
IP address assignment

Following network elements can assign the IPv4 and/or IPv6 address:
1. AAA/Radius server
2. WLANGW/WAG (local DHCP server)
3. remote DHCP-server (not common)
IETF DRAFT - Unique IPv6 Prefix Per Host
(draft-ietf-v6ops-unique-ipv6-prefix-per-host-00)

- Draft is currently mainly focused around Comcast community Wi-Fi deployment use-case, under leadership of John Brzozowski
- The current draft explains the high level architecture and provides some technological details regarding IPv6 address assignment related aspects for community Wi-Fi access
- The implementation provides each Subscriber with a unique /64 address, allowing flexibility per subscriber on addressing technology used to derive /128 IPv6 addresses
- The architecture allows IPv6 support for UE’s with minimal address management capabilities
- The draft provides insight in a real deployment considerations regarding address assignments (other aspects were explained
- The documented use-case deploys a captive portal for subscriber identification
Details

Generalized Community WIFI Topology

- UE: User Equipment.
- 802.11: Wireless Network
- AP: Access Point.
- Soft-GRE: Stateless GRE tunnel
- WLAN-GW: Wireless LAN Gateway
- CP: Control Plane component of the WLAN-GW (uses DHCP, ARP, DHCPv6, ICMPv6 (RS/RA/NS/NA), Radius, Diameter, etc.)
- AAA: Accounting, Authorization and Authentication
- HTTP Captive Portal: Captive portal used to redirect traffic towards during subscriber onboarding process
When UE connects it sends a RS to learn
- IPv6 Gateway, Prefix information, DNS, remaining info for global routing
- RS send from UE via the AP-bridge onto the Soft-GRE the WLAN-GW
- Due to split-horizon for BUM traffic the RS is not seen by other UE's connected to the same AP

First time UE connects it is not Authorized and WLAN-GW queries AAA server

AAA server checks policy DB and returns /64 together with http-redirect to Captive portal via Radius-acknowledge message
WLAN-GW uses received Radius info to compose the “RA” response to the UE originated “RS” message.

RA contains few important bits of information:
- A IPv6 /64 prefix
- Some flags

(1) IPv6 /64 prefix
- Locally managed pool on WLAN-GW
- Pool signaled through Radius

(2) Some flags
- Indicate to use SLAAC and/or DHCPv6
- Prefix is on/off-link
- Is there need to request ‘Other’ information (e.g. DNS)?
### Details

IPv6 Wi-Fi Subscriber Onboarding Procedures (3)

- **IPv6 RA flags for best common practice**
  - **M-flag = 0** (UE/subscriber address is not managed through DHCPv6), this flag may be set to 1 in the future if/when DHCPv6 prefix delegation support over Wi-Fi is desired)
  - **O-flag = 1** (DHCPv6 is used to request configuration information i.e. DNS, NTP information, not for IPv6 addressing)
  - **A-flag = 1** (The UE/subscriber can configure itself using SLAAC)
  - **L-flag = 0** (The UE/subscriber is off-link, which means that the UE/subscriber will send packets ALWAYS to his default gateway, even if the destination is within the range of the /64 prefix)

---

<table>
<thead>
<tr>
<th>UE</th>
<th>WLAN-GW</th>
<th>AAA</th>
<th>Captive-Portal DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--------</td>
<td>-----</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>RS</td>
<td>Access-Req</td>
<td>Access-Acc</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>←-RA-</td>
<td>/64; M,L=0; G,A=1</td>
<td>←-NS(DAD)</td>
<td>←-DHCPv6 (info Req)</td>
</tr>
</tbody>
</table>

---
Deploying a unique IPv6 per UE/subscriber
- Each UE belongs to unique /64 subnet, hence through natural network behavior all traffic will be directed to the default gateway (=WLAN-GW)
- Due to the flags set hosts can keep using privacy addresses within the /64 prefix
- Accounting per UE can be done per /64 instead of per /128 IPv6 address

UE Learning about DNS
- Most common Stateless DHCPv6 is used by UE/subscribers
- RA extensions for RNDSS RFC6106 can be used also, albeit less supported on UE devices
- Both technologies can be used simultaneous and are non-mutual exclusive (however the address must be identical)

Captive portal used to identify the subscriber (other means could potentially be used also)
### IPv6 Wi-Fi Subscriber Onboarding Procedures (5)

**IPv6 ND Timers**
- IPv6 Router Advertisement Interval = 300s
- IPv6 Router Lifetime = 3600s
- Reachable time = 30s
- IPv6 Valid Lifetime = 3600s
- IPv6 Preferred Lifetime = 1800s
- Retransmit timer = 0s

**Geo-localization for UE**
- When DHCPv6 is used AP can insert interface-id in DHCP solicit message
- When using SLAAC alternate information can be used. E.g. NSoGRE to harvest the AP MAC address
Wi-Fi specific features:
Value-added-services (IPv6 aware)

• Carrier Wi-Fi mandates VAS in order to monetize Wi-Fi as a service. Only offering connectivity (bit-pipe) is not a future-save business case.

• Few examples:
  – HTTP(s) redirects are influencing QoE heavily. Soft-redirect recommended (white listing), with success verification
  – Parental control based on ICAP (blacklist filtering)
  – Usage based billing
  – Inserting pop-ups in http session (in-browser notifications)

Value-added-services supported over IPv6!
Wi-Fi specific features:
Voice over wifi (apple wifi calling)

- Delivering Voice over Wi-Fi in a secured way, over an “untrusted” connection
- Encryption/authentication from Smartphone, with dedicated encrypted tunnel
- IPv4 or IPv6 IPsec tunnels towards ePDG
- Inside address IPv4/IPv6

(*) ePDG: evolved packet data gateway
SUMMARY
What does IPv6 bring to carrier Wi-Fi?

• More available IP addresses
• Avoiding NAT44 means:
  – less logging/processing/resources
  – No fragmentation/reassembly issues
• Easy integration
  – Offering IPv6 over IPv4 infrastructure is possible
  – Hitless introduction of IPv6 Wi-Fi devices (single or dual stack)
  – Wi-Fi specific features are operational in IPv6 environment