Evolving Source Address Selection Rules for Mobility Awareness

Sri Gundavelli (Cisco)

Contributors/Reviewers:

Jouni Korhonen, Julien Laganier, Basavaraj Patil, Hui Deng, Dan Wing

Motivation

- Applications are typically configured to use a specific APN. The APN identifies a PDN and which is accessed by using a PDN-GW. The IP address of the associated PDN connection, to what an Application socket would be bound. This in affect is a mechanism for binding the application to a source address anchored on a PDN gateway.

- This model of service access and source address selection works fine when the UE is only in 3GPP access domain. This static binding however in the presence of trusted WLAN access, or when attached to any trusted non-3GPP access network, does not map quite well.

- Additionally, this does not provide a simple mechanism for any IP services to select the source interface/IP address based on the properties of that connection.
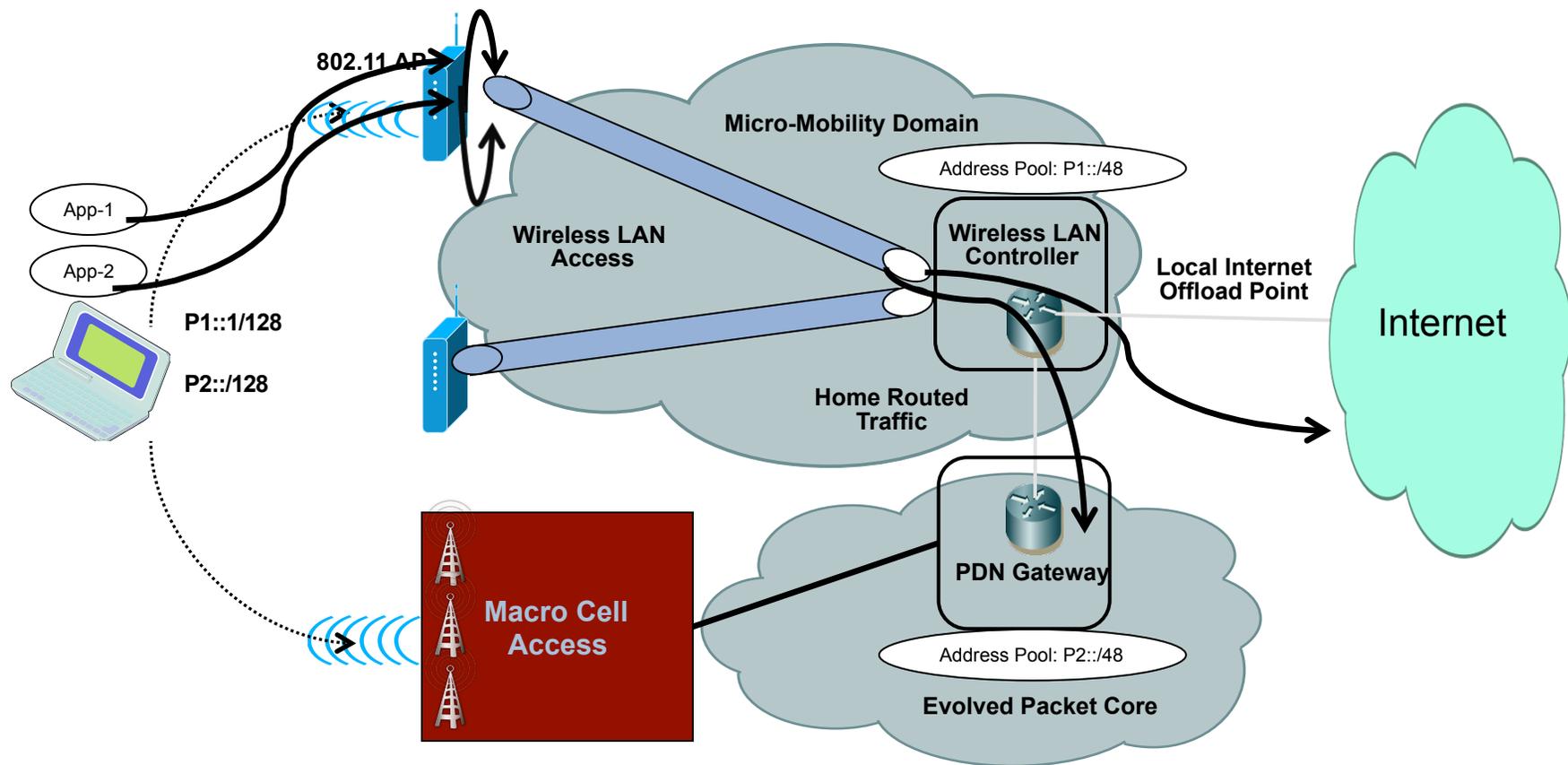
Roaming Scenarios

- When the UE is in a visitor network, it may be bound to both an APN in the Home network and in the visitor network. The application should have the ability to use the correct source address based on the application requirement. Example: Access local Google content.
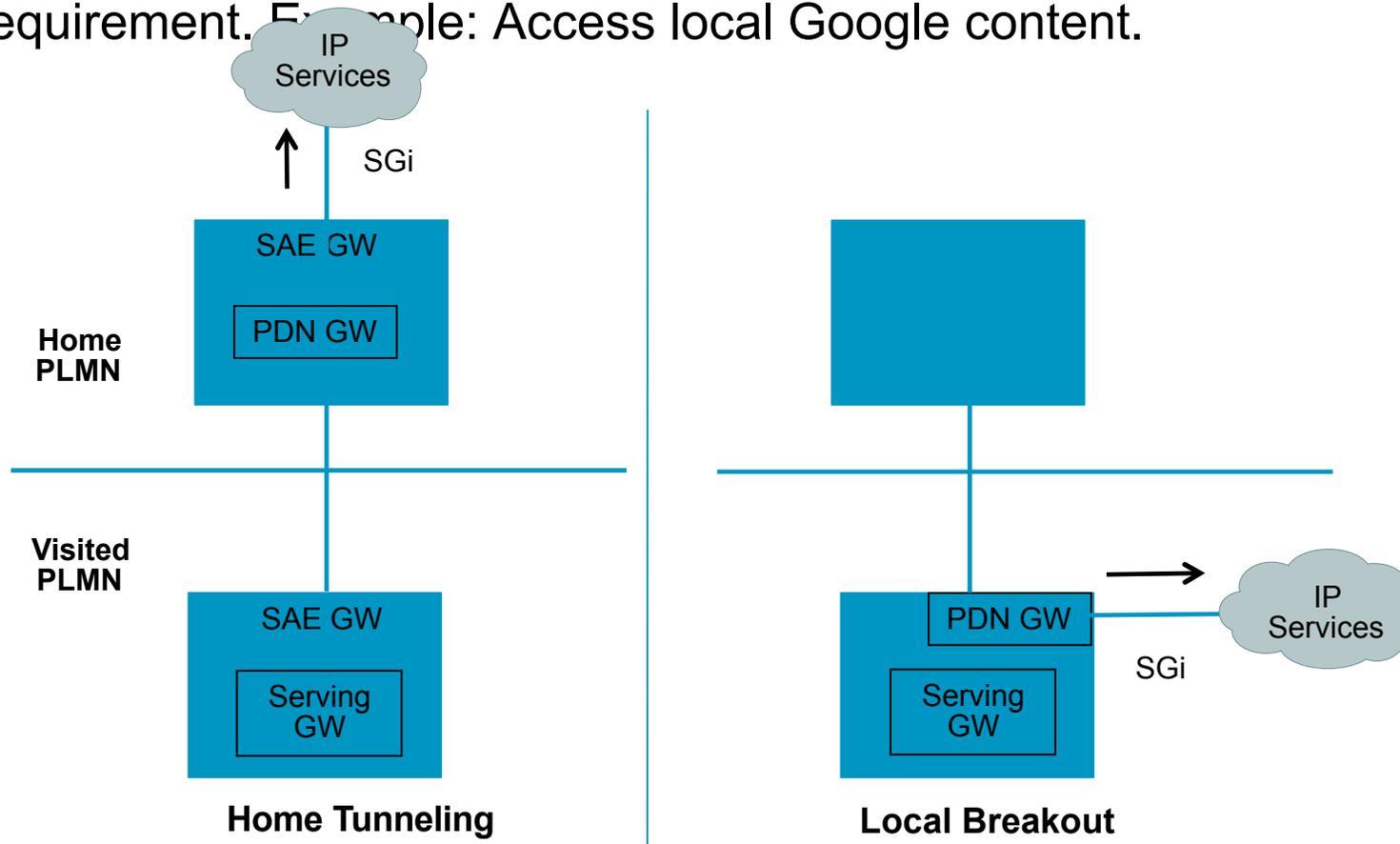
Home Tunneling

Local Breakout

Mobility Chaining (WLAN & EPC)

- For supporting offload function for certain traffic in chained mobility scenario, the UE needs to use the right source address for the right application flows, based on the offload requirements. The obtained address configuration can be from EPC or from the local domains.

Mobile IPv6 Scenarios

- A mobile node with Mobile IPv6 stack does have the ability to determine the home link from a visitor link. However, the inter-working scenarios mixing PMIPv6 and CMIPv6, modifies the properties of the address (hierarchical chaining scenarios). The home address may appear on the link, but may not be ideal for local-break out.
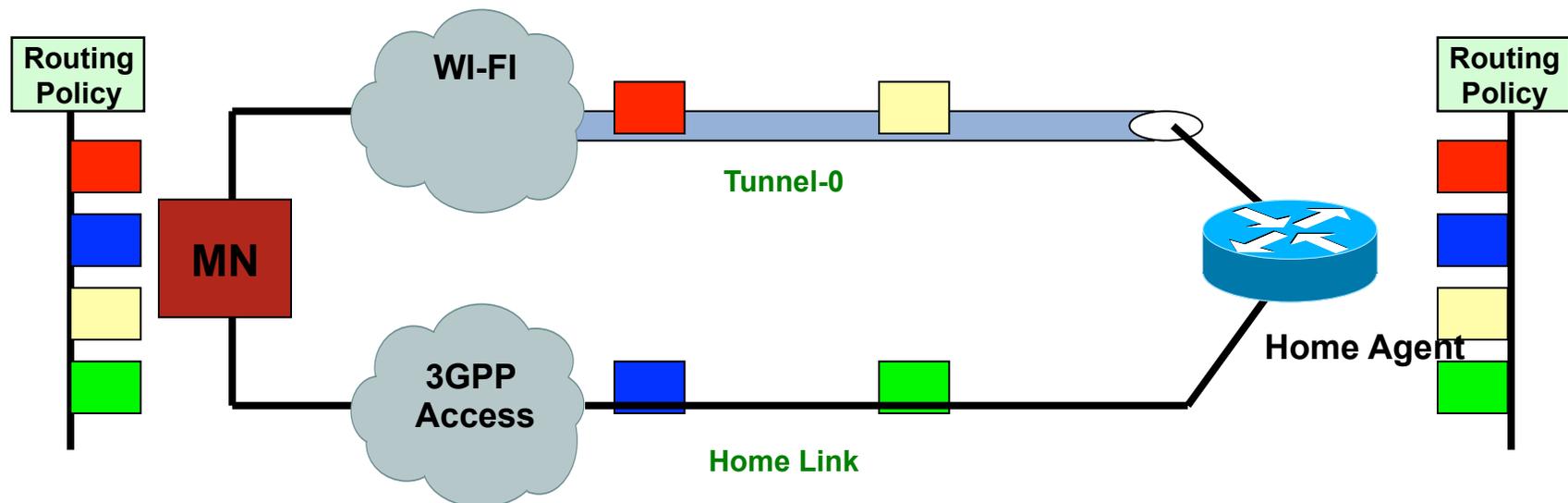
Goals

- Can we evolve the source address selection for mobility awareness ?

Prefix Coloring

Prefix Coloring

- Every network prefix that gets assigned to a mobile node can be marked with a specific attribute. Each of these attributes will have a standard definition on the usage scope and any other properties.

Attribute Type	Prefix Properties
Type-1	Home Routed
Type-2	Local Breakout

- The attributes identify the properties of a prefix. For example:

<Type-1 (Home Routed)>: A prefix has mobility support, its routed through the home network and is ideal for applications that require mobility.

<Type-2 (Local Routed)>: A prefix is from the local network, has no mobility properties, its ideal for applications such as Pandora box that requires no mobility.

* Should this be a complex object to additionally include a unique identifier of an APN

Application Configuration

- The applications on the host can be configured with the IP address property requirements.

Application	ATTRIBUTE REQ
VPN Session	Home Routed
Internet Browser	Local Breakout
SSH Session	Home Routed
Pandora Box	Local Breakout

- An UE in the visitor network having established PDN connections to both, an APN in visitor network (for LBO traffic) and an APN in the home network (for home-bound traffic), will allow an application such as internet browser to access local content, by setting the correct requirement tag.

Protocol Extensions

- The Default Address Selection for IPv6 [RFC-3484] currently does not specify how the host learns the mobility properties of an IPv6 address, its left out of scope (Refer to Sec 3.5).

- The protocols used for delivering the IPv6 address configuration to the mobile node can be extended to carry the mobility property tags along with the address configuration.

- The mobile node obtaining the address configuration for physical interfaces, virtual interfaces or PDN connections will have the attribute markings around the prefix. This allows the mobile node to add these attributes to the policy table.

Protocol	Extension
DHCPv6 (RFC-3315)	A new option in DHCPv6
IPv6 ND (RFC-4861)	A new option in IPv6 ND PIO option

Extending PIO Option (RA Message)

- The Prefix Information Option in the IPv6 RA message can be updated to use the reserved flags for including the Attribute-Type (to be managed under IANA name space).
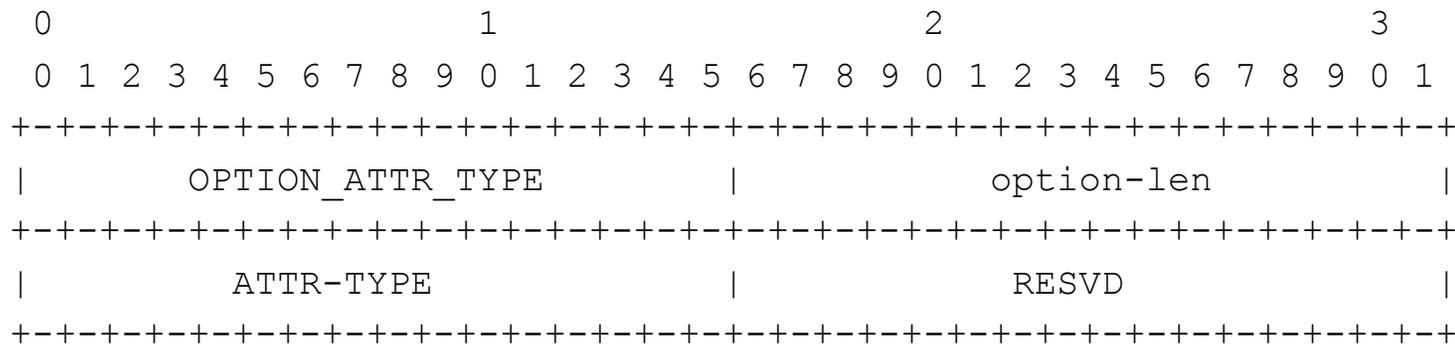
```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     | Prefix Length |L|A| Reserved1 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                         Valid Lifetime                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Preferred Lifetime                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Attr-Type  |                 Reserved2                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   |                            Prefix                             |
   |                                                               |
   .                                                               .
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
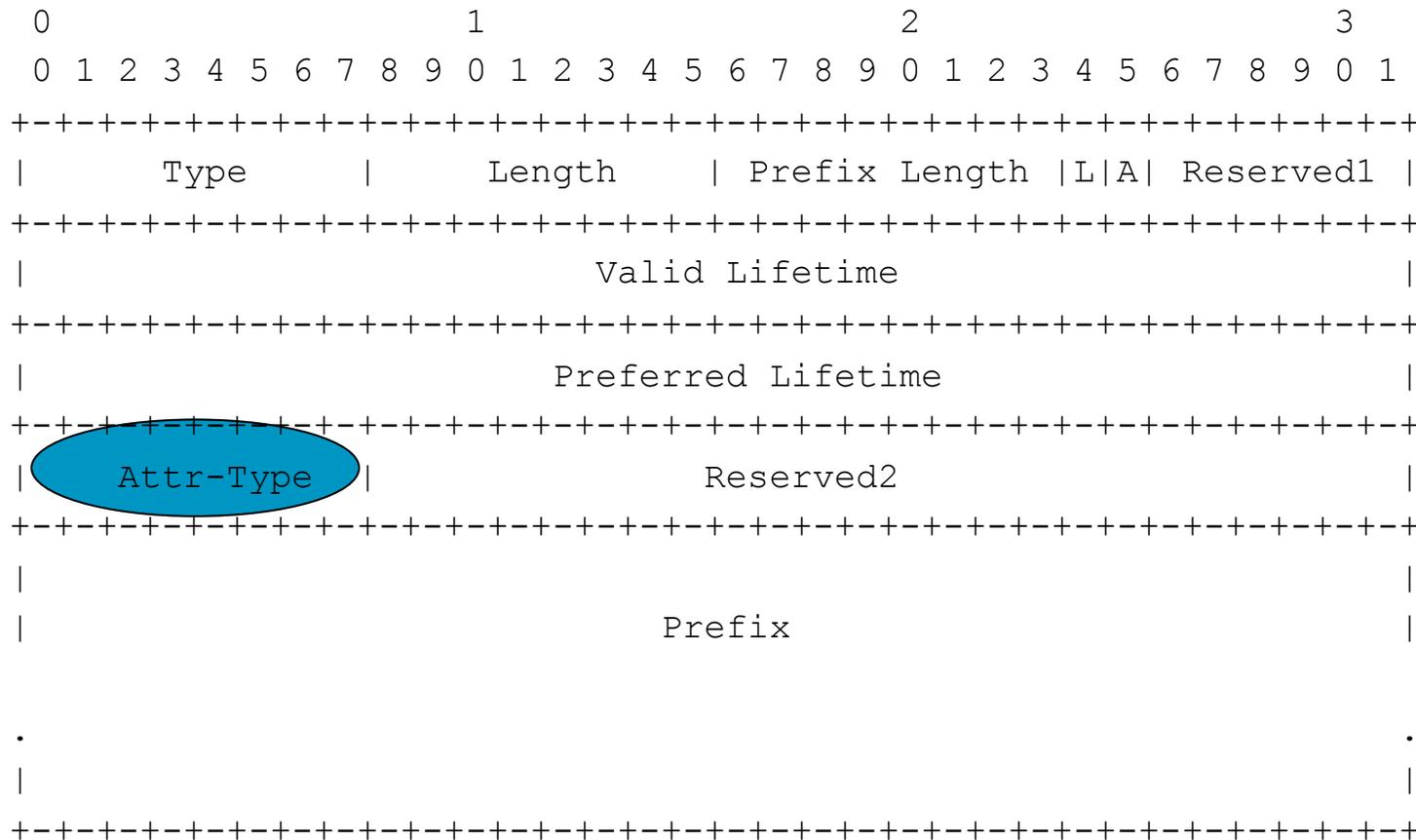
A new DHCPv6 Option

- A new DHCPv6 option specific to IA_NA binding, for carrying the address property can be defined.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         OPTION_ATTR_TYPE       |            option-len         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           ATTR-TYPE            |              RESVD            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

This option must only be present only in the specific IA_NA binding.
```
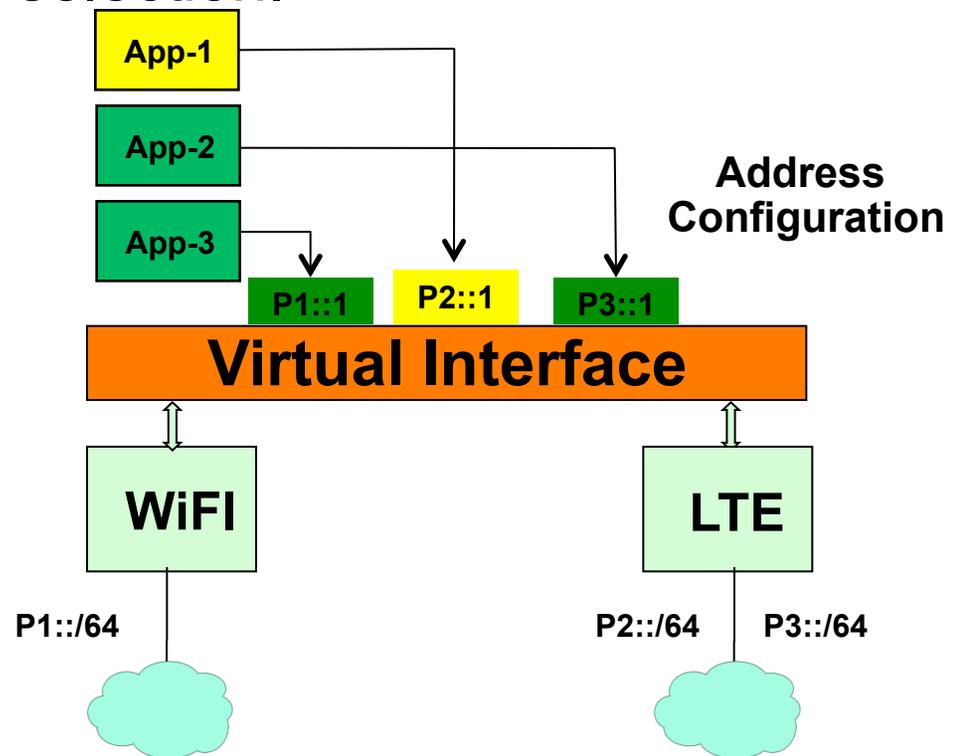
IPv6 Host Policy Table

- The Policy Table on the Host can include the property attributes that it obtained as part of the address configuration.

- Applications can use the RFC-3484 Source Address Selection rules for address selection.

Policy Table	
Prefix	**Attribute**
P1::/64	Attribute-1 (Home Bound)
P2::/64	Attribute-2 (Local Breakout)
P3:/64	Attribute-3 (Home Bound)

App-1

App-2

App-3

Address Configuration

P1::1   P2::1   P3::1

Virtual Interface

WiFI

LTE

P1::/64

P2::/64   P3::/64

Mobility Chaining (WLAN & EPC)

- For supporting offload function for certain traffic in chained mobility scenario, the UE needs to use the right source address for the right application flows, based on the offload requirements. The obtained address configuration can be from EPC or from the local domains.