Multiple APN Support for Trusted WLAN Access

(draft-gundavelli-netext-multiple-apn-pmipv6)

IETF 83 (Paris), March 2012

Sri Gundavelli (Cisco)
Mark Grayson (Cisco)
Yiu Lee (Comcast)
Hui Deng (China Mobile)
Hidetoshi Yokota (KDDI)

Problem Statement

- In SP WiFI architectures, with WLAN access network integrated to mobile packet core as trusted access network (3GPP S2a Interface), the MAG can establish PDN connection with a single APN at any point of time. There is a limitation with respect to simultaneous multiple APN access.
- This limitation is due to the lack of semantics for allowing multiple IPv4 address assignment to a given interface of a UE over DHCPv4. In WLAN networks, we can only assign a single IPv4 address to the WLAN interface of the UE. This forces us to keep a single APN access, specifically single PDN connection from a non-3GPP/WLAN access.
- Access to only a single APN from WLAN access is considered as a limitation. There are number of requests for allowing multiple APN access from WLAN access network. This support is required even for a mobile router with multi-tenancy support.

Problem Statement

- However, for IPv6 the MAG has the ability to project multiple prefixes in the RA messages and the UE can use Stateless Auto-configuration approaches for obtaining multiple IP address for the interface. This capability in conjunction with Prefix Coloring scheme, allows the host to use the source address based on the application type, and hence has a solution for multiple APN access.
- IPv6 Prefix Coloring Approach:

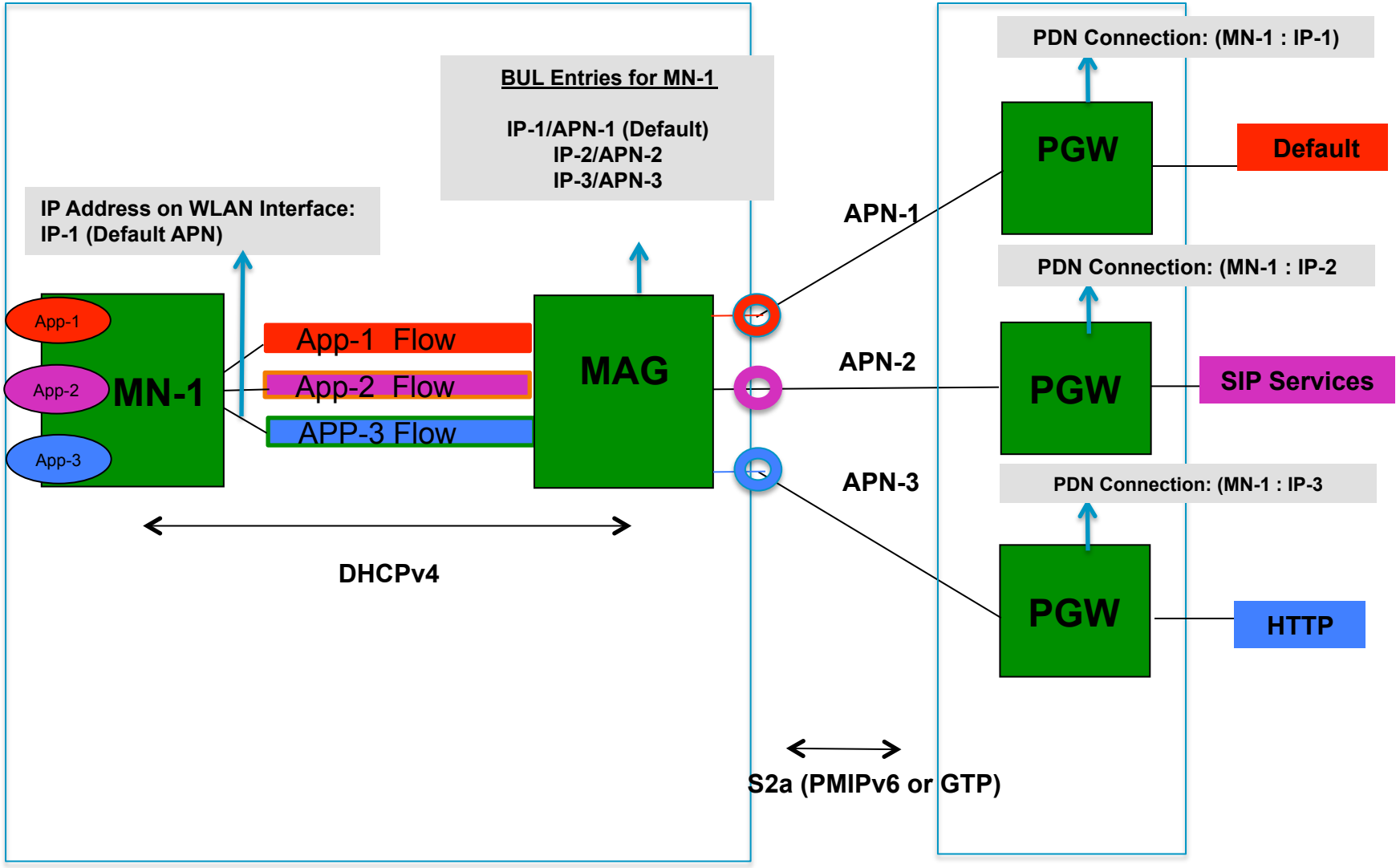
http://www.psg.com/~charliep/txt/ietf81/alt_mext/Evolving-The-SAS-Rules-for-Mobility-Awareness-2.pdf

- This document proposes an approach for extending MAG to support simultaneous multiple APN support.

Solution Overview

- MAG establishes a PDN connection for the default APN. The obtained IP address from this default APN is assigned to the WLAN interface of the UE over DHCP.
- MN launches different applications and starts sending IP packets with the source IP address from the default APN. Based on the application triggers, MAG establishes new PDN connections to the APN associated with that application type. The MAG may also choose to establish connections to all the APN's allowed for that UE in the initial phase.
- The MAG creates application specific translation entry for using the IP address associated with the APN bound to an application.
- IP packets from the UE and from the CN, now are translated to use the IP address assigned by the respective APN. The translated packets are forwarded through the right PDN.

Multi-APN Support for Trusted WLAN Access



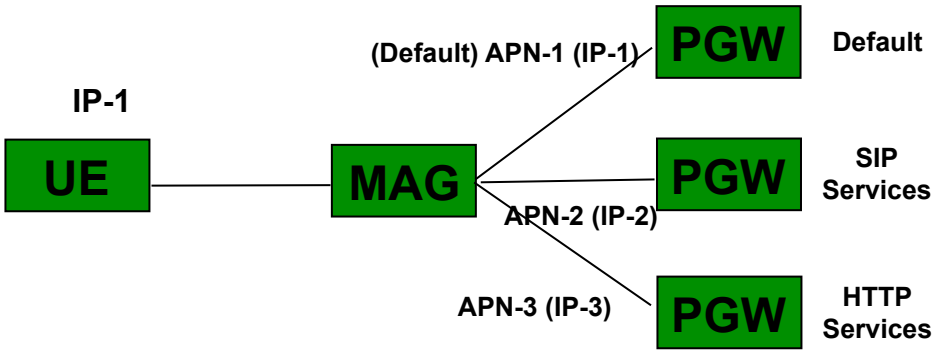
Flow-based Source Address Selection

- MAG creates Flow selector based NAT mappings and pushes the State to the NAT Mapping Table.
- The created state on the NAT will ensure the proper source address selection based on the Application Type. For example: A RTP/SIP packet from the UE with the source address of IP-1, will get translated to source address of IP-2 and will get tunneled to the respected packet gateway, while an HTTP packet gets the source address translated to IP-3.

Application (5-tuple ACL)	APN	WLAN Interface (Inner)	IP Address for the PDN Connection (Outer)
SIP	SIP Services	IP-1	IP-2
RTP	SIP Services	IP-1	IP-2
HTTP	Internet-Services	IP-1	IP-3
WAP	WAP Gateway	IP-1	IP-1

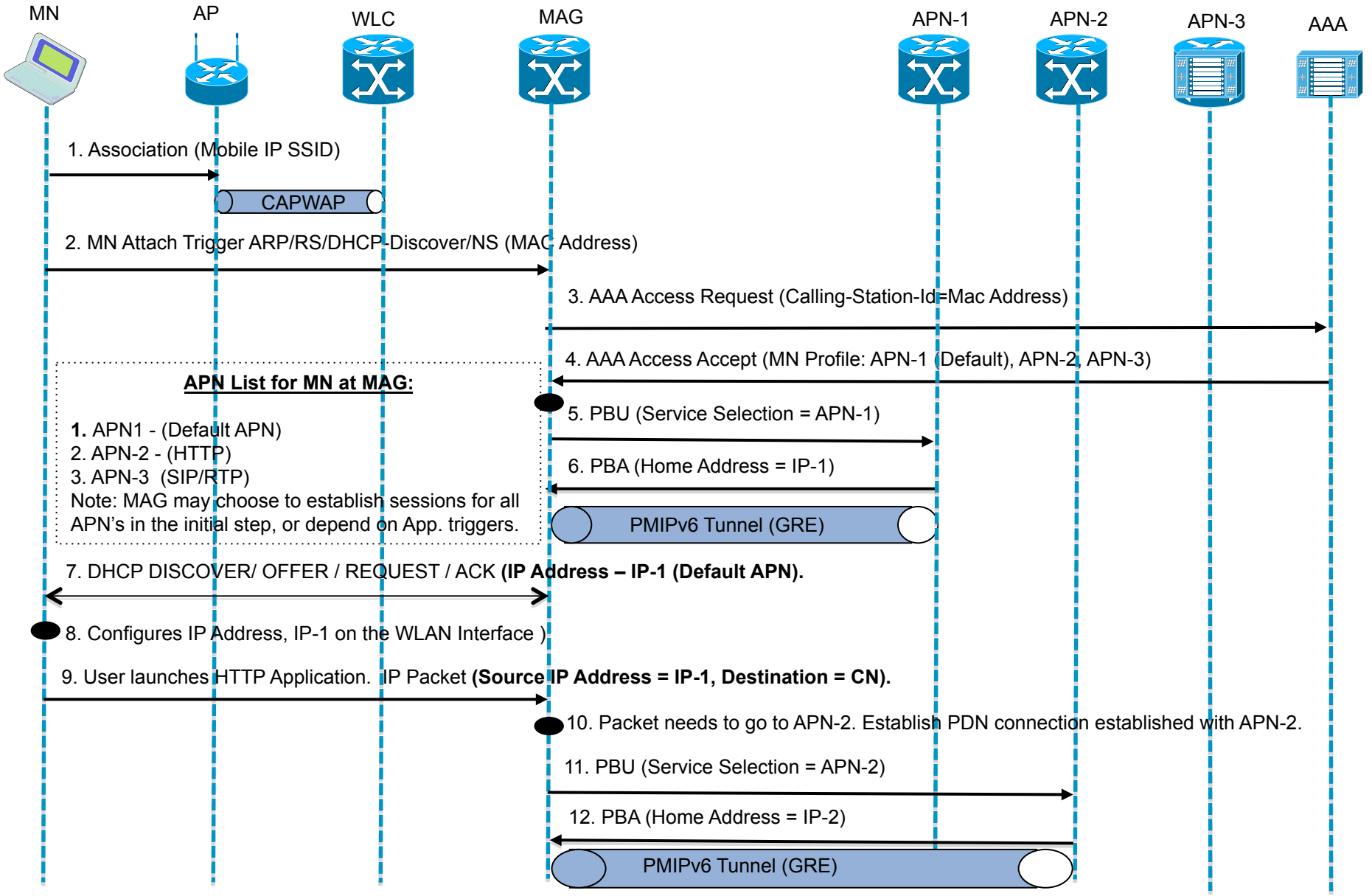
Data Path Considerations

- The following explains the packet match selectors in both paths and the translation and forwarding logic.

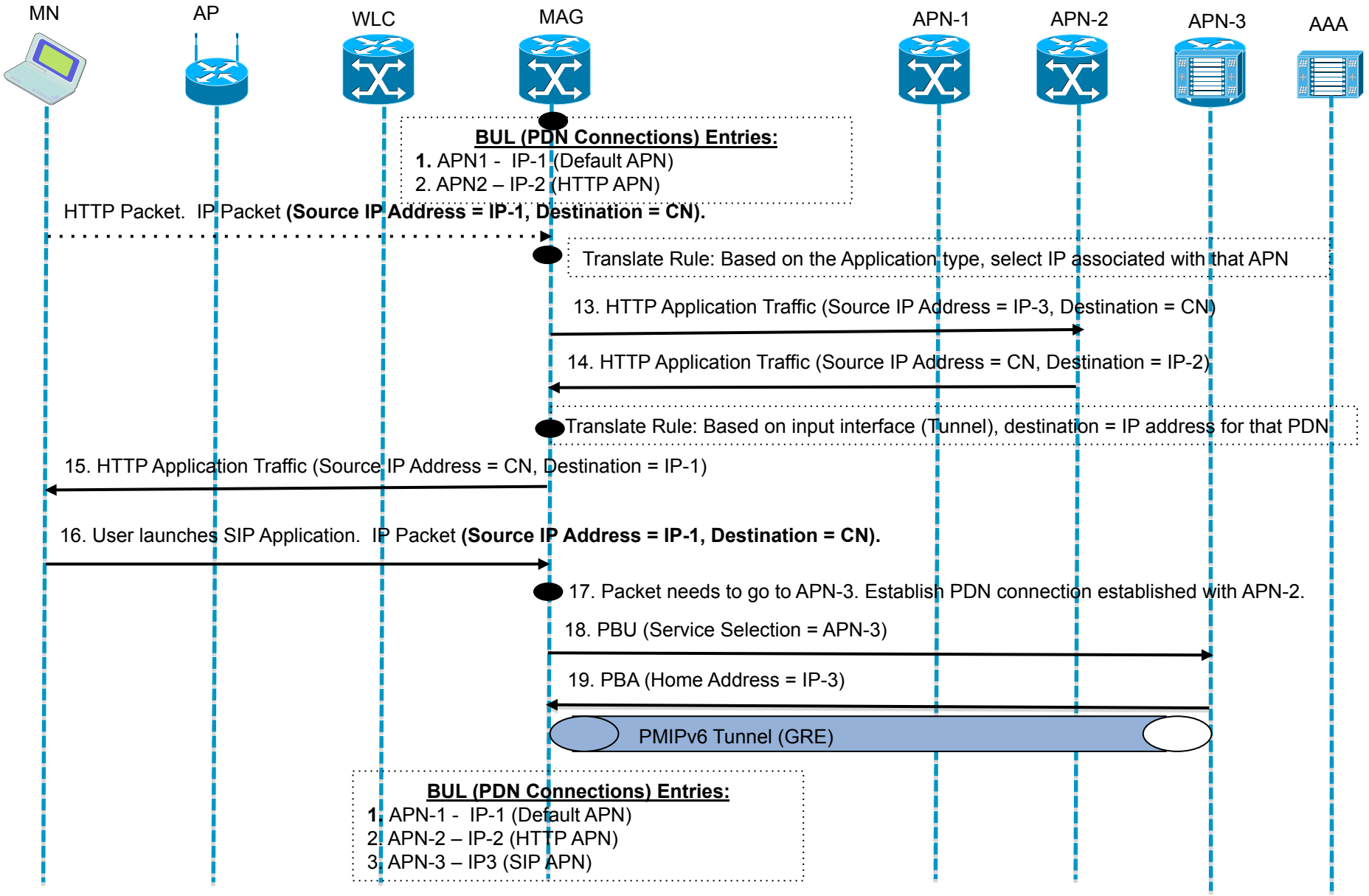


Flow Direction	Packet Selector	Translation	Outgoing Interface
Uplink (Source: IP-1 Destination: CN)	Application Type (SIP, RTP)	Source IP Address IP-1 → IP-2	PGW (Tunnel-0)
Downlink (Source: CN Destination: IP-2)	Destination IP Address (PDN Connection), or Incoming Tunnel Interface id	Destination IP Address IP-2 → IP-1	Access Link (UE-MAG Link)

Multiple APN Support – Call Flows



Multiple APN Support – Call Flows



Limitations

- This approach has two known limitations, but with the ability to enable the feature only when these requirements are met. There are some workarounds for these limitations.

1. If a given APN is hosting private DNS name space (not common in mobile deployments), the DNS resolutions from the mobile node will fail. The mobile node is assigned a DNS server from the default-APN and all resolutions will be routed to that server.
2. If the configured APN's are hosting same set of applications and if the MAG has no clear traffic selector for identifying the flows, this approach will have issues.

Next Steps

- Authors appreciate feedback from the WG, to be published this as a informational specification.