September 2020

MECHANISM TO ENABLE POLICY DRIVEN ROUTE SELECTION IN 5GC AND EPC

Dishant Parikh

Sanjeev Panem Jaya

MECHANISM TO ENABLE POLICY DRIVEN ROUTE SELECTION IN 5GC AND EPC

AUTHORS:
Dishant Parikh
Sanjeev Panem Jaya

ABSTRACT

In a Third Generation Partnership Project (3GPP) Fifth Generation (5G) core (5GC) network or in a Control and User Plane Separation (CUPS)-based Fourth Generation (4G) Evolved Packet Core (EPC) network, the control and data planes are separate. This allows for the user plane function to be deployed at the centralized datacenter (e.g., co-located with a Session Management Function (SMF) and/or a control plane System Architecture Evolution Gateway (SAEGW), at a remote datacenter (e.g., for a Mobile Edge Computing (MEC) implementation), or at customer premises (e.g., for an enterprise use-case). Such network implementations can increase network complexity as a network operator will need to provide efficient routing mechanisms to support the 5G use-cases, such as Enterprise 5G, Ultra-Reliable Low-Latency Communication (URLLC) flows, private 5G, low latency applications like gaming, etc. Techniques presented here provide for the ability to address these complexities by enabling dynamic selection of next-hop routes based on subscriber category/policy, user equipment (UE) location, the location/capabilities of User Plane Functions (UPFs), type of traffic/application, and/or UPF slice used.

DETAILED DESCRIPTION

In a 5GC network or a CUPS-based 4G EPC network, the control and data planes are separate. This allows for the user plane function to be deployed at the centralized datacenter (e.g., co-located with a SMF and/or control plane SAEGW (SAEGW-C)), at a remote datacenter (e.g., under a MEC implementation) or at the customer premises (e.g., under an enterprise use-case). This may increase network complexity as a network operator will need to provide efficient routing mechanisms, especially for use-cases such as, for example, URLLC, enterprises, and local breakout.

In order to address this complexity, a network operator may desire a mechanism to logically segregate their network using policy-based routing so that it can be dynamically varied depending upon, for example, the UE type (e.g., URLLC), subscriber categories (such as, for example, consumer vs. enterprise), traffic types (e.g., uplink classifiers, Voice over Long-Term Evolution (VoLTE) or data, applications requiring low latency like gaming, etc.), or application detection rules (such as, for example, an Application Detection and Control (ADC) service). In a 5G architecture, such policy-based packet forwarding may facilitate efficient routing for MEC scenarios, which may provide for the ability to classify and forward traffic to respective Internet Service Providers (ISPs) or Content Servers based on network deployments for such architectures.

Proposed herein is a solution to address problems noted above by leveraging next-hop Internet Protocol (IP) addresses (e.g., IP version 4 (IPv4) and/or IP version 6 (IPv6) and by offering multiple techniques in which next-hop IP addresses may be provided, such as:

1. Through Policy Control Function (PCF)/Policy and Charging Rules Function (PCRF) for enabling policy based forwarding at each Quality of Service (QoS) Flow ID (QFI) level/Rule level. This will aid in forwarding traffic to respective destinations at a flow level.

2. At the time of session setup to enable (a) enterprise session-level traffic forwarding to respective enterprise gateways and (b) slice-based forwarding addresses.

The proposed solution offers a mechanism through which the SMF (based on for example UE type, subscriber category, location, UPF selected, etc.) or a PCF/PCRF may specify the next-hop address that needs to be applied at the UPF for a specific subscriber/IP flow. This information may be sent by a SMF over an N4 interface to the UPF (or from a SAEGW-C to a user plane SAEGW (SAEGW-U) over an Sx interface in the case of a CUPS 4G EPC).

Aspects of the proposed solution may be illustrated and described through a series of exemplary use-cases, discussed below.

For a first exemplary use-case, Figure 1 below depicts elements of policy-based forwarding for subscribers belonging to different enterprises.

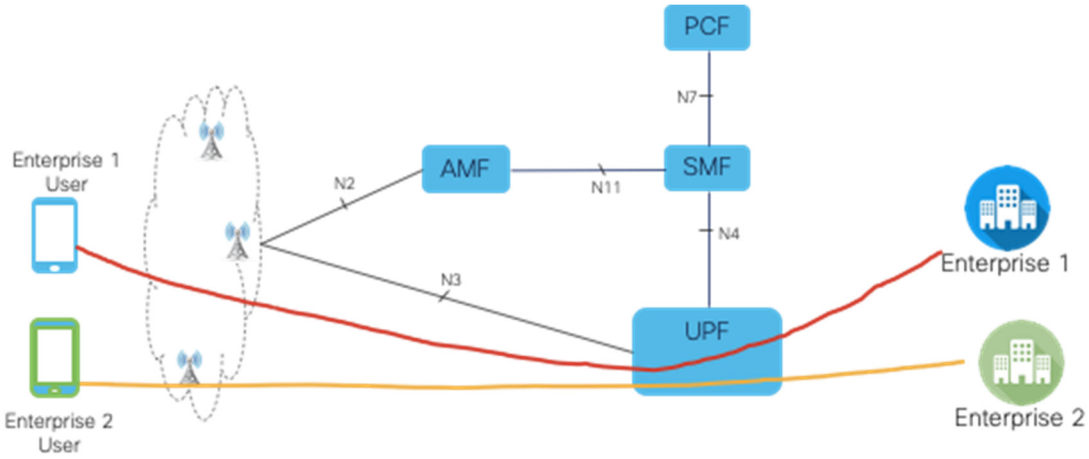

Figure 1

In this scenario, policy-based forwarding is applied at the subscriber level. The operator may provision a next-hop address at either a SMF/SAEGW-C or a PCF/PCRF based on the subscriber identity (such as for example International Mobile Subscriber Identity (IMSI), Mobile Station International Subscriber Directory Number (MSISDN), International Mobile Equipment Identity (IMEI), Access Point Name (APN), etc.). This information is sent to the UPF over an N4/Sx interface as part of an N4/Sx Session Establishment Request/Session Modification Request. All traffic belonging to these subscribers is then forwarded to the provisioned next-hop address.

For a second exemplary use-case, Figure 2 below depicts elements of a scenario where flow level policy-based forwarding is applied to the traffic belonging to a subscriber.

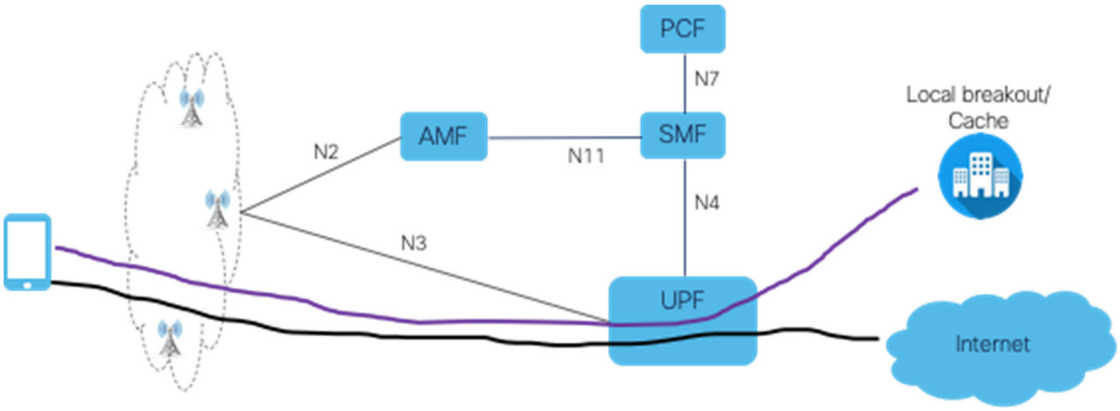

Figure 2

As illustrated above, the UPF receives different next-hop addresses for the same subscriber, either as part of rule installation or provisioned directly on the UPF (e.g., static/predefined rules). Based on the application or traffic type, the UPF classifies the flows and forwards the packets to the next-hop address that is associated with a rule. This can be used for use-cases like local breakout, traffic segregation based on applications being accessed, type of traffic (e.g., gaming, streaming from cache server, etc.), or segregation of worked related (e.g., enterprise) traffic from normal internet traffic for the same subscriber.

For a third exemplary use-case, Figure 3 below depicts elements of a UE mobility scenario where different next-hop address may be applicable for the same type of flows (e.g., matching the same Packet Data Rule (PDR)) on the two UPFs.

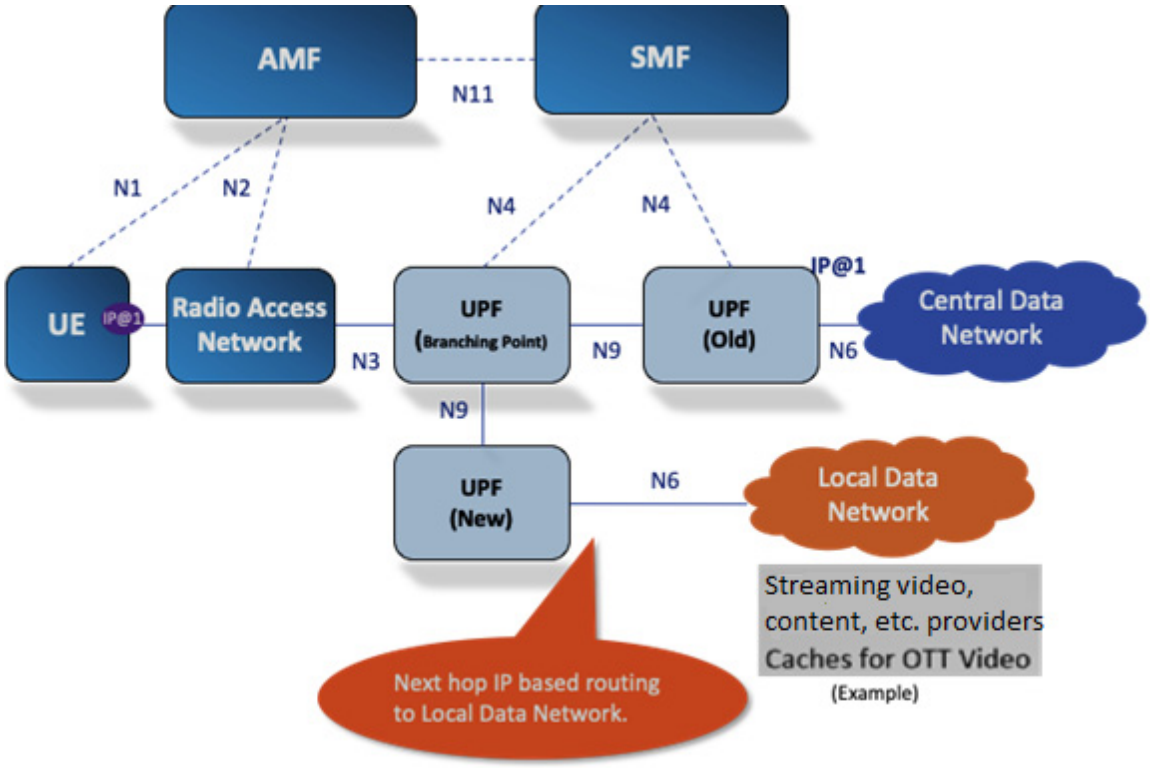

Figure 3

Under this scenario, the same rule (e.g., a PDR) may be installed on both the UPFs by a SMF but the forwarding action can be set to different next-hop addresses on the UPFs. This allows a SMF to use a routing policy in the PDRs while setting up the session on the new UPF which is different from those used on old UPF. This wouldn't be possible using a static configuration (e.g., either at APN or charging action level).

Various of the custom Information Elements (IEs) and call flows that are considered by the proposed solution are described below.

In the case of an N7 interface (e.g., between a SMF and a PCF) the following new fields, as shown in TABLE 1, below are added to Npcf_SMPolicyControl_Create and Npcf_SMPolicyControl_Update operations between a PCF and a SMF:

TABLE 1

Information Name	Description	Category	PCF Permitted to Modify for a Dynamic PCC Rule in the SMF?
Rule Identifier	Uniquely identifies the PCC rule within a PDU Session. Used between PCF and SMF for referencing PCC rules.	Mandatory	No
Dynamic Route Selection	This part defines the method for selecting route for packets belonging to a service data flow.		
Address Type	This parameter indicates the type of IP address sent by PCF (IPv4 or IPv6)	Optional	Yes
Next-hop IPv4 Address	This parameter provides the IPv4 Next-hop address to which traffic matching the PCC rule should be forwarded to	Conditional	Yes
Next-hop IPv6 Address	This parameter provides the IPv6 Next-hop address to which traffic matching the PCC rule should be forwarded to.	Conditional	Yes

Note: At least one IP address (IPv4 or IPv6) needs to be included if a "Dynamic Route Selection" parameter is included in the PCC rule information.

In the case of a 4G CUPS EPC, a similar parameter is added on to the Gx interface between a PCRF and a SAEGW-C (or PGW-C) as shown below:

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
{ Charging-Rule-Name }
[ Service-Identifier ]
.....
[ Callee-Information ]
[Dynamic-Route-Selection] - >New AVP
*[ AVP ]
Dynamic Route Selection is a grouped AVP containing the following
attributes:
Dynamic-Route-Selection ::= < AVP Header: xxxx >
[Address Type] => Enum value {0: IPv4, 1: IPv6}
```

```
[Next-hop IPv4 Address] => 4 bytes containing IPv4 address
[Next-hop IPv6 Address] => 16 bytes containing IPv6 address
[*AVP]
```

In the case of a Sx/N4 interface (e.g., between a SMF and a UPF) the next-hop IP address IE type shall be encoded as shown in Figure 4 (below) as a custom/private IE. This will be sent as a separate IE in a Sx Establishment Request and a Sx Modify Request. Next-Hop-ID (a unique-id per session) will be associated in respective Forwarding Action Rule (FAR) for referencing the next-hop IP address included at a message level. There can multiple next-hop IP address IEs included for load balancing aspects towards the end server.

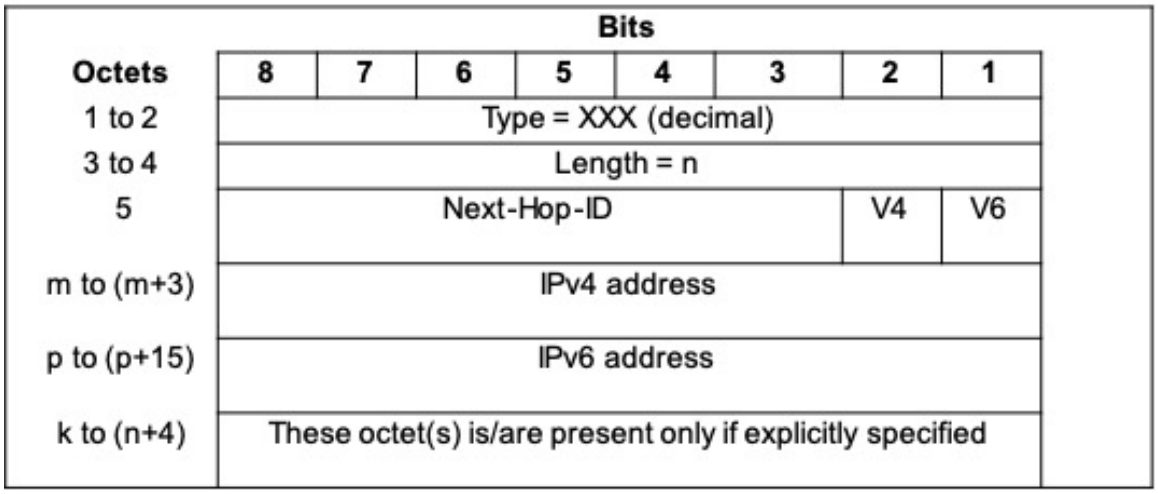

Figure 4

The following flags are coded within Octet 5:

- Bit 1 - V6: If this bit is set to "1", then the IPv6 address field shall be present, otherwise the IPv6 address field shall not be present.

- Bit 2 - V4: If this bit is set to "1", then the IPv4 address field shall be present, otherwise the IPv4 address field shall not be present.

- Bit 3 to 8 for unique Next-Hop-ID identifier

Octets "m to (m+3)", "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value. As one example, aspects of the above may encode the

value 24 for the IPv4 subnet 192.0.2.10/24. As another example, aspects of the above may encode the value 64 for the /64 IPv6 prefix.

Figure 5, below, depicts several illustrative flows:

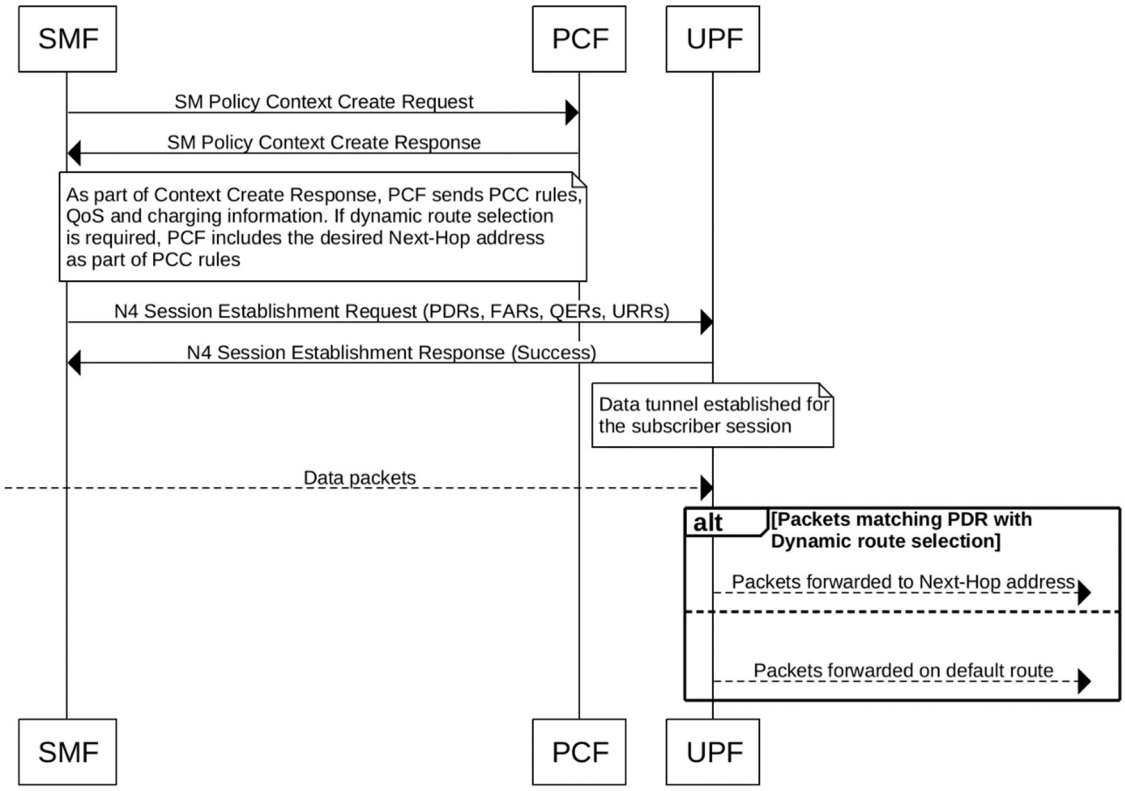

Figure 5

Various operations are portrayed in Figure 5, above, including:

Step 1. During Protocol Data Unit (PDU) establishment, a SMF sends a Session Management (SM) Policy Context Create Request to a PCF for policy, charging, and QoS information.

Step 2. A PCF sends a SM Policy Context Create Response with Policy and Charging Control (PCC) rules, QoS information, and charging information. Additionally, it provides a charging rule level next-hop IP address information using Attribute Value Pair (AVP) artifact (Dynamic-Route-Selection) as shown above.

Step 3. A SMF establishes an N4 connection using a PFCP Session Establishment Request message. It includes next-hop IP information as per Custom IE (Next-Hop IP Address IE) as shown in Figure 4. It includes a reference of this IE in a FAR.

Step 4. Uplink data packets are received from a UE side. During packet processing, the packets may match to a PDR. If the FAR associated to the matched PDR is configured with next-hop IP address, the packet is forwarded to the next-hop address..

In summary, in a 3GPP 5GC network or in a CUPS-based 4G EPC network the control and data planes are separate. This allows for the user plane function to be deployed at the centralized/remote datacenter or at customer premises. Such implementations can increase network complexity as a network operator will need to provide efficient routing mechanisms to support the 5G use-cases. The techniques presented above address these complexities by enabling dynamic selection of next-hop routes based on various criteria including for example subscriber category/policy, UE location, the location/capabilities of UPFs, type of traffic/application, UPF slice used, etc. Thus, the techniques presented herein may enable policy driven route selection, which is a basic functionality that may be utilized in 5GC and remote CUPS deployments and that hasn't been addressed by the 3GPP standard specifications.