August 2020

SMF ASSISTED FASTER AND EFFICIENT UPF REDUNDANCY MODEL

Filipe Rodrigues

Rajaneesh Shetty

Om Prakash Suthar

Raghavendra Suryanarayanarao

SMF ASSISTED FASTER AND EFFICIENT UPF REDUNDANCY MODEL

AUTHORS:
Filipe Rodrigues
Rajaneesh Shetty
Om Prakash Suthar
Raghavendra Suryanarayanarao

ABSTRACT

A solution is presented for a cost-effective way of providing redundancy for a user equipment (UE) session while utilizing resources of an active and a standby user plane function (UPF). UPFs are used efficiently by creating redundancy for each other with support from a session management function (SMF). The solution further enhances N:M redundancy. This model is fully applicable for edge UPF deployments where resources are limited. The solution can be used for providing ultra-reliable low latency communication services, enterprise services based applications supported using 5G core in which there is higher service level agreement (SLA) bearing and transport path diversity.

DETAILED DESCRIPTION

For virtualized environments, user plane functions (UPFs) are deployed using a management and orchestration (MANO) layer to achieve 100% resiliency for specific type nodes. MANO-based redundancy is achieved at virtual network function (VNF) level. For a VNF or application failure, a redundancy/resiliency solution at the IP session/flow layer is useful to achieve a faster convergence time becomes necessary.

The 3GPP specification quotes this statement/reference in TS 23.527 4.3.1: "When a UPF fails, all its Session contexts and N4/PFCP associations gets affected. PDU sessions in such case becomes invalid and may be deleted." This will cause a significant signaling storm in the network and loss of communication for the User Equipment (UE).

For a UPF hosting ultra-reliable low-latency communication (URLLC) applications, redundancy mechanisms with proactive measures, such as session replication on a standby UPF, are useful.

Currently there are two solutions for UPF redundancy for 5G deployments:

1:1 Resiliency model: In the 1:1 resiliency model, for every active user plane, there is a standby user plane that is working in a hot-standby mode so that when a failure is detected for the active user plane, the standby takes over and N4, GTP-U and N6 interfaces are established for it.

N:M resiliency model: There are N standby user planes for M active user planes and when there is a failure detected for any of the active user planes, these standby user planes assume the role of the active UPF.

Figure 1 below is a diagram depicting a planned switchover procedure for a N:M UP redundancy model.

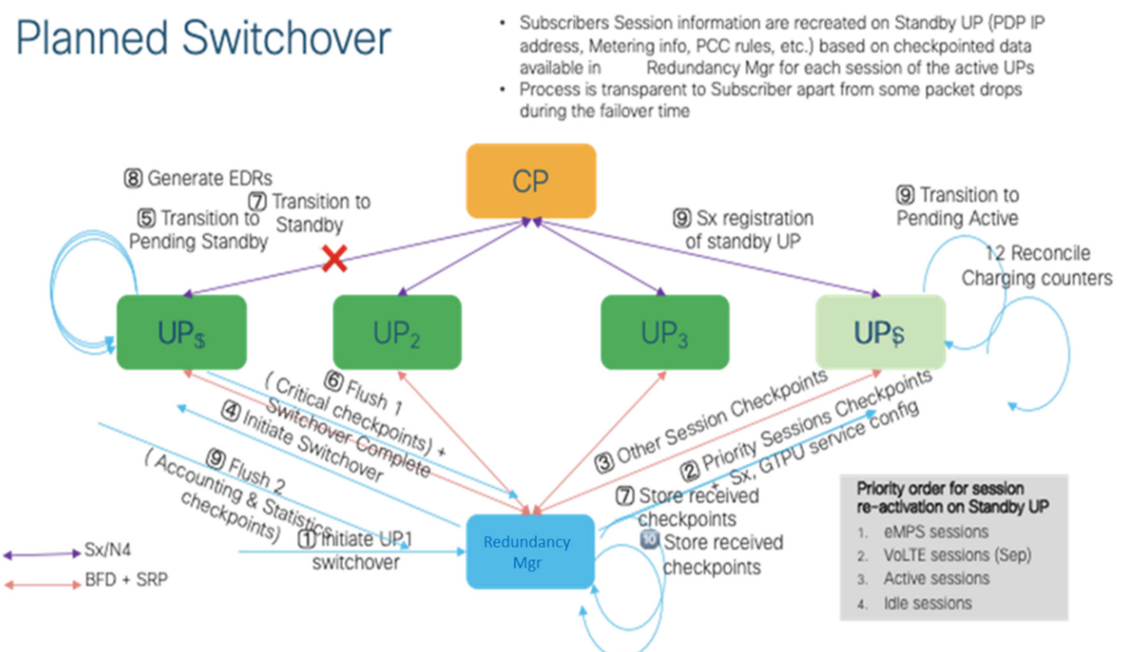

Figure 1

Figure 2 below is a diagram depicting an unplanned switchover procedure for an N:M UP redundancy model.

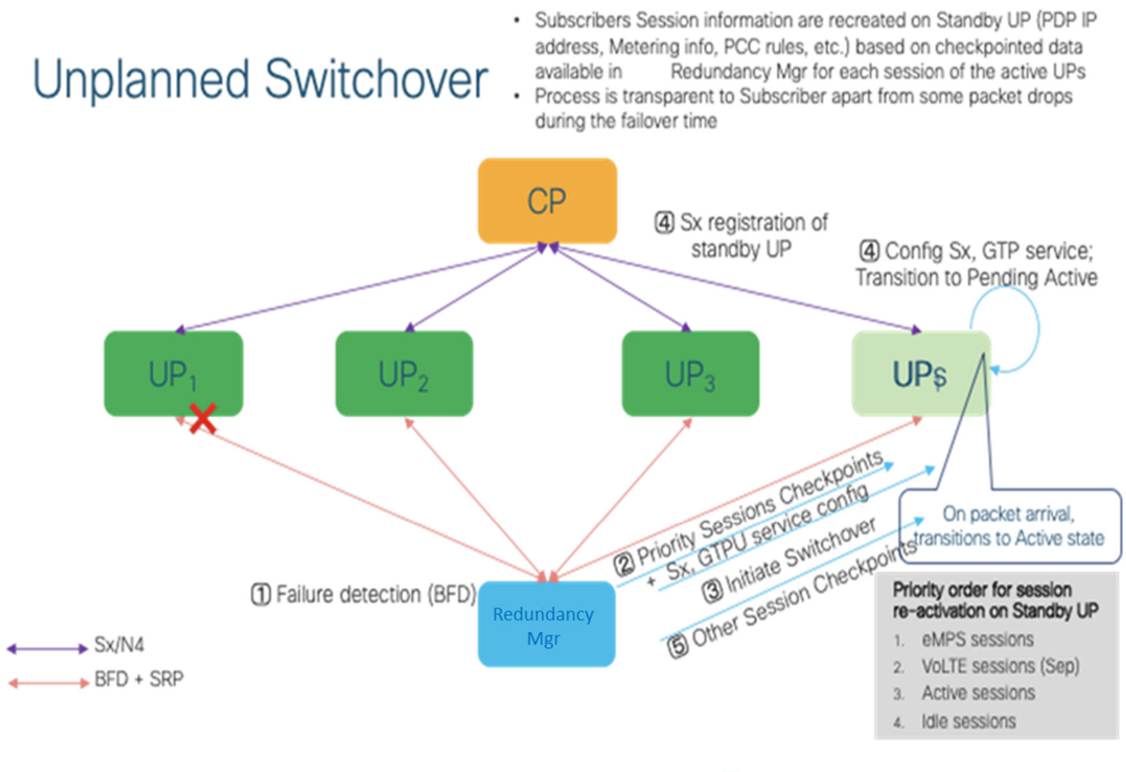

Figure 2

There are several problems associated with either the 1:1 or the N:M redundancy model. First, the connections for the standby UPFs are made only after the detection of the failure and there is a significant time gap for convergence or switching over to the standby UPF to resume the service operations. Second, UPF resources for the standby UPF are idle and not used until a failure occurs. This requires over-dimension of the network (and compute resources). Third, for URLLC applications with 5G 5QI's (stringent packet delay budget for delay-sensitive applications like voice and URLLC), N:M redundancy is not practical and having 1:1 redundancy for UPFs is a significant impact on the hardware cost. These redundancy models are not flow-aware and are purely triggered upon failure detection. Finally, as for the N:M redundancy model, there is a significant impact on the central processor unit (CPU) consumption as there is a frequent need to replicate or periodically checkpoint the session data for all the active nodes over the standby UPFs.

The proposal presented herein is designed to overcome these drawbacks and provide a standard UPF redundancy approach with an efficient resources utilization.

The proposed solution is described in the following steps.

Step-1: Installation of backup path by Session Management Function (SMF) for redundancy

The method uses the SMF function to provide redundant paths using following steps.

1. SMF will advertise the same Internet Protocol (IP) chunks to two different UPFs during the IP pool chunk allocation procedure as shown below. The SMF will send "same IP pool chunk" to active and standby UPFs using the N4 interface. The same PDN session is created on both active and standby UPF, but the flow is directed only to the active UPF. The diagram below provides message Sx flow sequences.

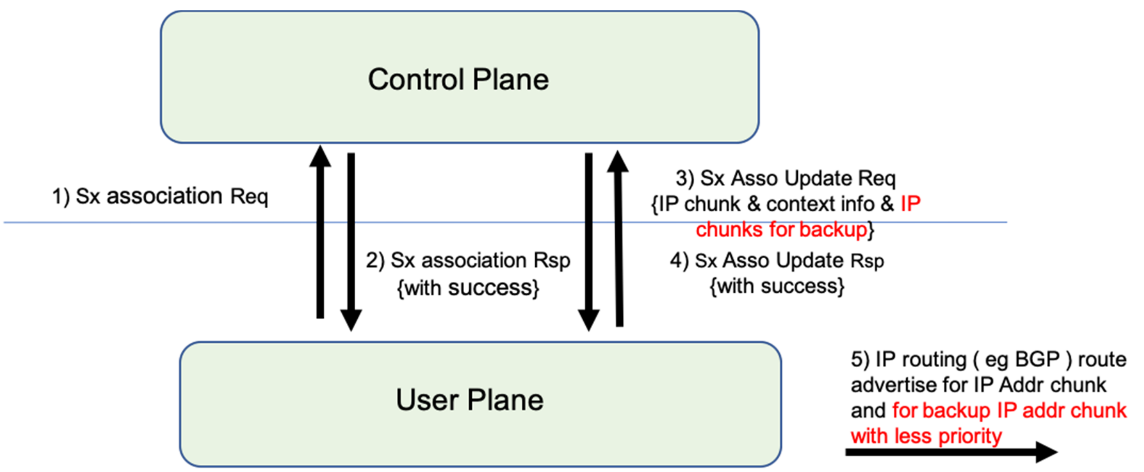

Figure 3

2. Both the primary as well as secondary UPFs will advertise on the N6 interface over a chosen routing protocol (example Border Gateway Protocol (BGP)). The IP pool chunks to the backup paths will be advertised with a lower priority so it is not selected until the primary path fails. For example, if BGP is the chosen protocol the standby path can be advertised with a bigger Autonomous System (AS) path with AS path prepending.

3. In the session creation response, the SMF allocates both primary and backup tunnel endpoint identifier (TEID) to the eNB with gtpu ip address of the UPF supporting backup path as shown in Figure 4 below.

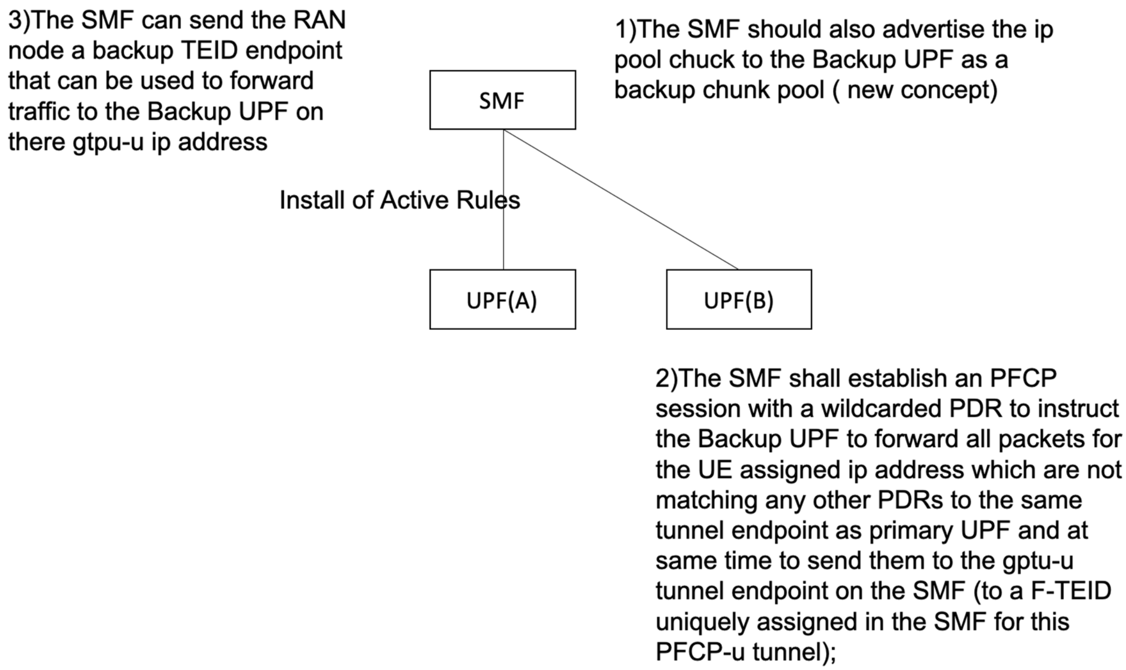

Figure 4

4. The SMF will install session information over N4 to the active path (as per 3GPP TS 23.502) and additionally, install a catch-all PDR and a FAR on the secondary UPF chosen to support the backup path. The catch-all PDR and FAR will ensure that the standby path will be ready to take forward packet decision and send the traffic to the gNB, effectively installing a backup path on the user plane function. Figure 5 below illustrates this.

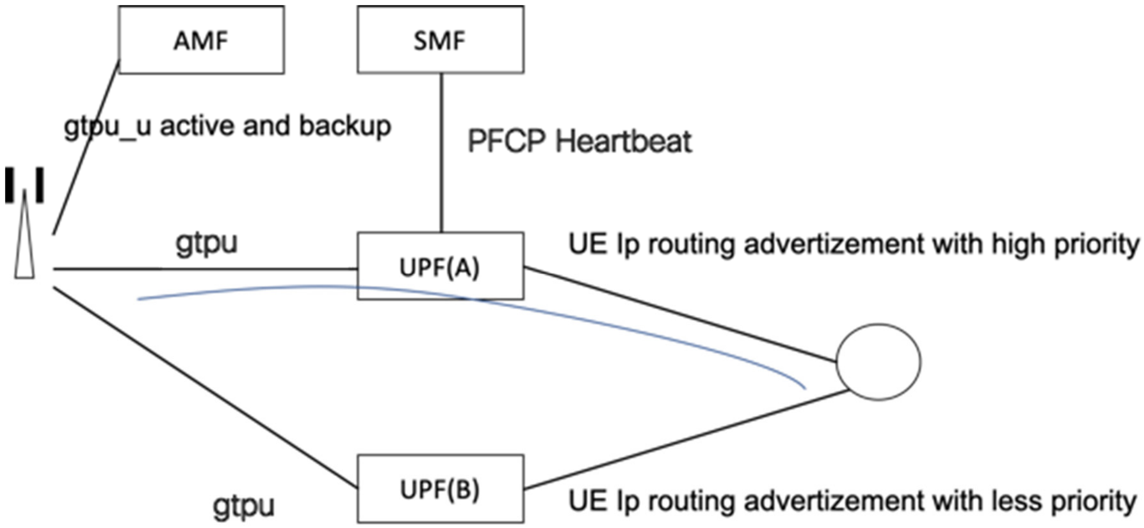

Figure 5

Step- 2: UPF Failure Detection and Recovery

Upon UPF failure, the normal routing protocol convergence mechanism will ensure routing the traffic to the secondary UPF. The SMF detects a PFCP protocol heartbeat failure to the active UPF. Upon receiving user-data traffic, the standby UPF will then inform the SMF function of the new traffic received and then the SMF will send all session information to the redundant UPF which would have taken up the active role. Ideally, a minor interruption on traffic will be noticed with the only contributor being the routing protocol convergence time. A different mechanism can be used to detect UPF failures and switchover using any of three mechanisms presented below.

1. Failure detection by gNB:

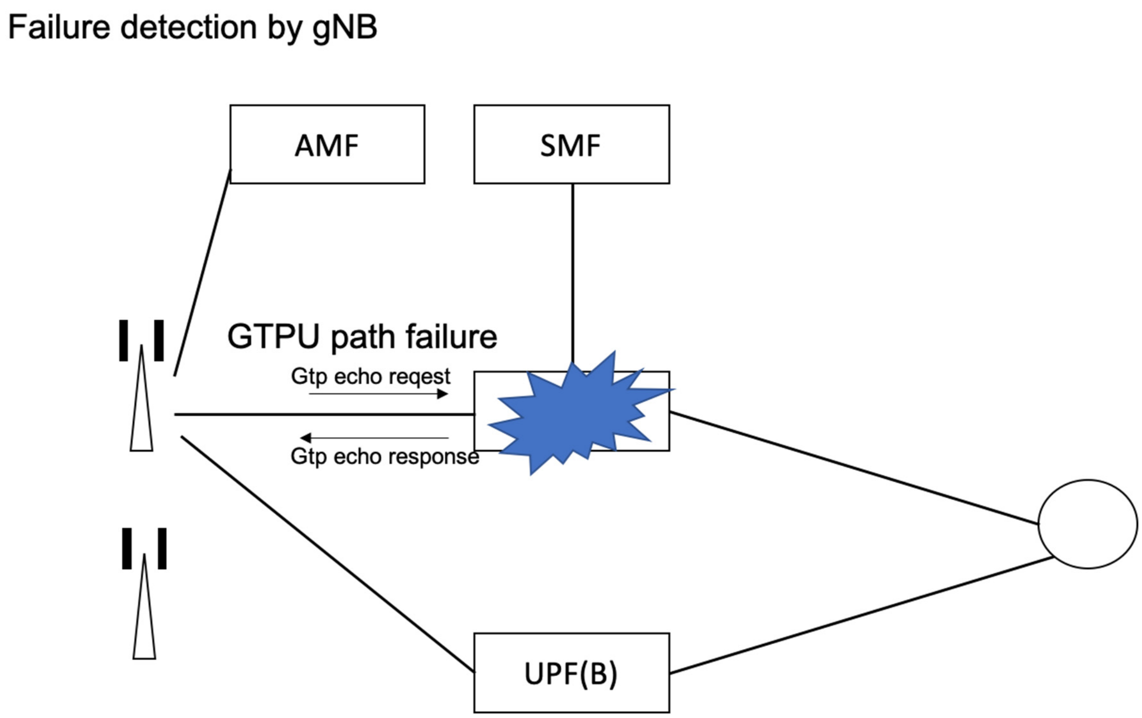

Figure 6

2. Failure detection by upstream N6 router

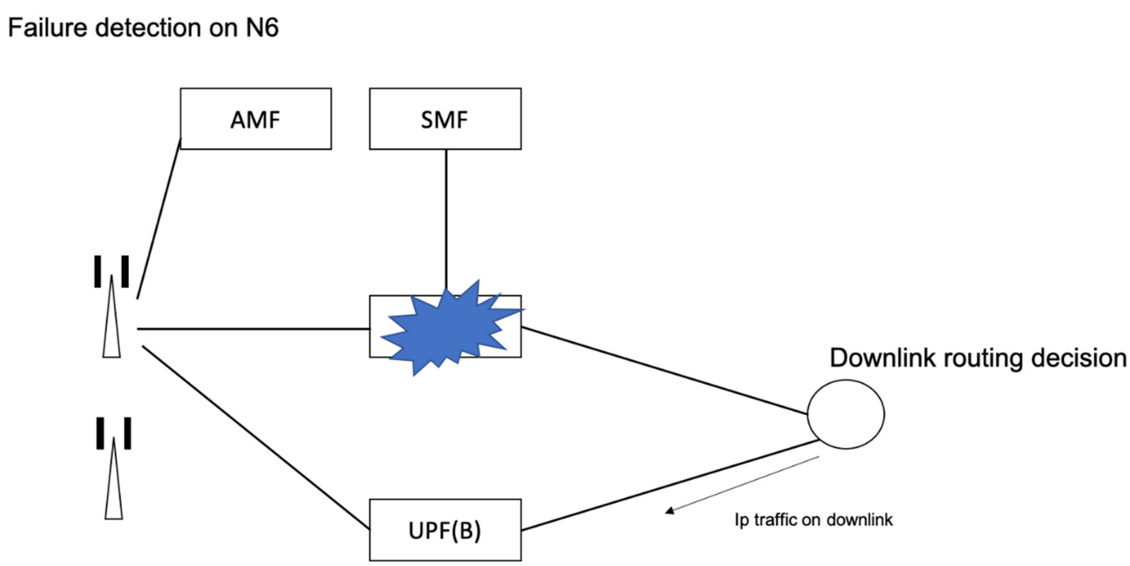

Figure 7

3. Failure detection by SMF and PDCP over N4

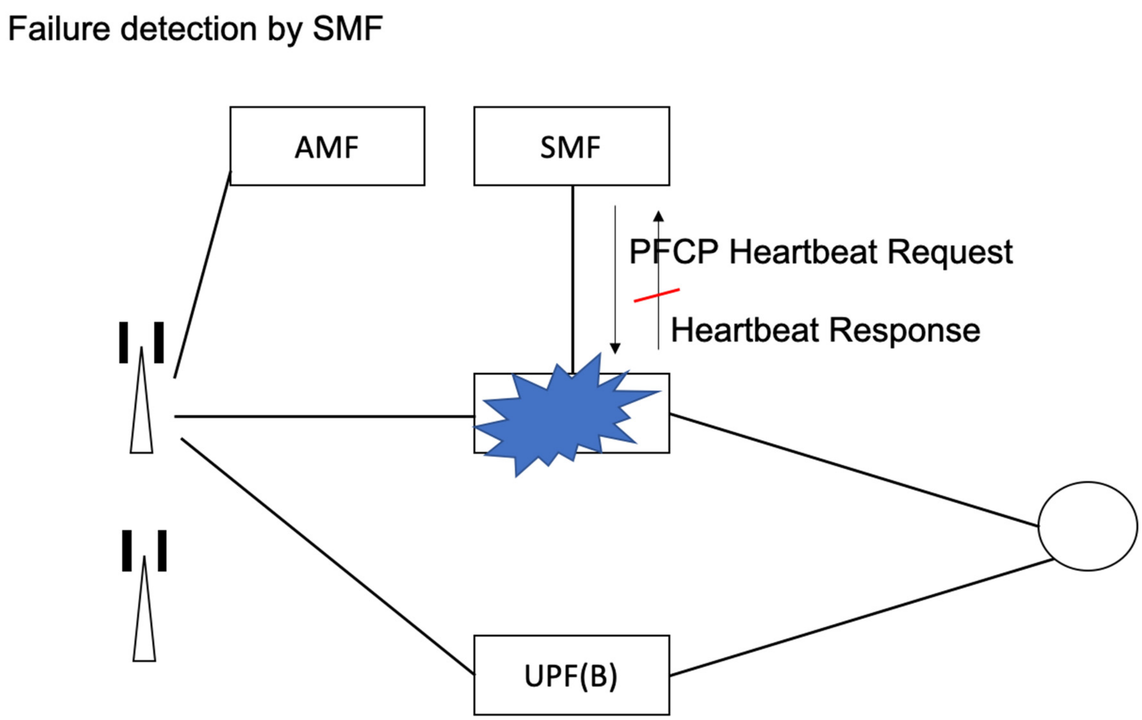

Figure 8

PFCP entity failure or restart is described in clause 19A of 3GPP TS 23.007. The same mechanism will be used by SMF to detect the failure of the active path of a session.

3GPP Specification Impact:

1. **3GPP TS 38.413 Next Generations Access Protocols (NGAP) - Section: 8.2.1.2 Successful Operation**

Include backup GTPU TEID of the redundant UPF for a particular PDU session as an additional indication that could be signaled, in advance, to the gNB by AMF during initial bearer setup (using N2 PDU Session Request/Response procedures) which would be considered later during Active UPF failure scenario.

2. 3GPP TS 23.502 Procedures for the 5G Systems (5GS) - Section: 4.3 Session Management Procedures

On Namf_Communication N1N2transfer message

Include backup TEID information of redundant UPF for a particular PDU session by SMF and signaled to AMF using the **Namf_Communication_N1N2MessageTransfer** procedure.

The call flow representation for PDU session Establishment and the improvements is depicted in Figure 8 below.

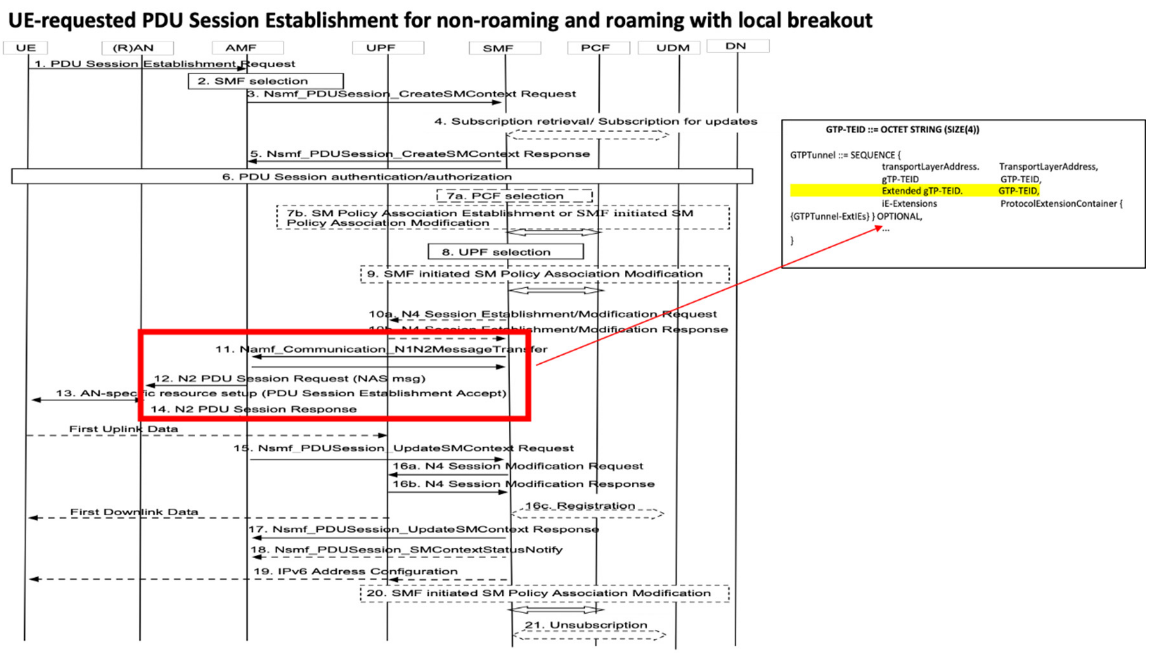

Figure 8

In summary, a method is provided to install a backup path and provide path diversity for mission critical applications to achieve fast switchover to a redundant UPF during disruption/outage in active UPF instance. A method is provided to optimize signaling for redundancy purposes. In the 1:1 UPF redundancy model or in the N:M UPF redundancy protocol, there is an additional interface/protocol stack which would be needed to periodically checkpoint the session information. A unique light-weight solution is provided which does not have any of this new redundancy interface/signaling protocol overhead and hence signaling optimization is achieved from a redundancy requirement perspective. In addition, a stateless redundancy mechanism is provided without relying on extra hardware resources. The solution optimizes resources required on N6 services functions.