May 2022

VXLAN EXTENSIONS FOR 5G USER EQUIPMENT SESSIONS

Mahesh Satyanarayana

VXLAN EXTENSIONS FOR 5G USER EQUIPMENT SESSIONS

AUTHOR:
Mahesh Satyanarayana

ABSTRACT

A Virtual Extensible Local Area Network (VXLAN) is typically used to create a Layer 2 (L2) fabric across datacenters and multi-cloud environments. A VXLAN is also useful in isolating traffic belonging to multiple tenants hosted in a cloud environment, or even to bridge applications spread across multi-cloud environments. Third Generation Partnership Project (3GPP) standards for Fifth Generation (5G) networks define an Ethernet Protocol Data Unit (PDU) type that provides L2 accesses to user equipment (UEs). Presented herein are techniques to enhance such Ethernet PDU capabilities in order to provide an L2 interconnect between 5G accesses and remote datacenters and/or cloud networks.

DETAILED DESCRIPTION

In Internet of Things (IoT) or Industrial IoT (IIoT) networks, such as Supervisory Control and Data Acquisition (SCADA) systems, the 3GPP standards-based Ethernet Protocol Data Unit (PDU) type that provides L2 access for UEs is especially useful because many IoT devices in such networks may be using proprietary or non-IP protocols over Ethernet layer connections that require L2 connectivity. With an Ethernet PDU, a User Plane Function (UPF) an a 5G mobile core network could forward raw Ethernet frames from UEs to data network(s) (DN(s)), and vice-versa.

However, IoT controllers and/or IoT application servers in such environments (e.g., an ‘IoT cloud’) could be located in a datacenter/cloud in a geographically different location from a 5G UPF handling data traffic for PDU sessions of IoT devices. For example, a UPF would typically be located on-premises or at the edge of a 5G access network such that it may not be feasible to provide a L2 circuit interconnecting the UPF to an IoT cloud to exchange Ethernet frames.

Presented herein are techniques to enhance Ethernet PDU capabilities as defined by 5G standards in order to provide an L2 interconnect between 5G accesses and remote

datacenters or clouds. These techniques include enhancing Session Management Function (SMF) and UPF functionality to support VXLAN termination on the UPF data plane. Such techniques can enhance the capabilities of Ethernet PDU Sessions, especially with 5G-as-a-Service (5GaaS) environments in which network operators could bridge their remote L2 networks (or enterprise networks) with a 5G access using a VXLAN.

Consider an example 5G network architecture, as illustrated in Figure 1, below, through which techniques of this proposal may be explained.

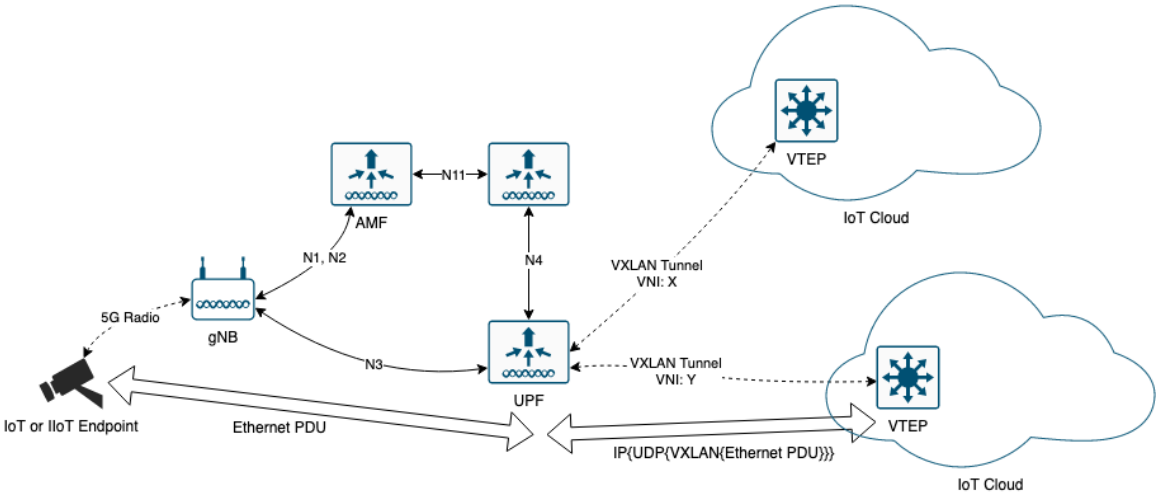

Figure 1: Example 5G Network Architecture

For the architecture of Figure 1, consider that VXLAN Network Identifier (VNI) and an associated VXLAN Tunnel Endpoint (VTEP) could be configured on the SMF per Data Network Name (DNN) or per network slice. Alternately, this information could be pushed from a Unified Data Management (UDM) entity or a Policy Control Function (PCF) at the time of PDU Session establishment for a UE (IoT device), or even from an Authentication Server Function (AUSF) at the time of UE registration at an Access and Mobility Management Function (AMF) in which the AMF could subsequently relay the information to the SMF that is to handle a PDU session for the UE.

When a UE establishes an Ethernet PDU Session, the SMF looks-up the VNI and VTEP information either from local configuration or from data pushed from the PCF/UDM/AMF, as discussed above. The SMF can send various information to UPF during N4 session establishment for the UE PDU session. The information could be carried

in custom Packet Forwarding Control Protocol (PFCP) information elements (IEs), which could be defined to carry:

1. The VNI and VTEP;
2. An uplink (UL) Forwarding Action Rule (FAR) that can be used to encapsulate UL Ethernet frames with a VXLAN header including the specified VNI; and
3. A downlink (DL) Packet Detection Rule (PDR) that can be used to decapsulate downlink traffic including the VXLAN header having the specified VNI.

During operation, the UPF could create a mapping between PDU session ID(s) and the VNI and could create a mapping between the VNI and the VTEP. When the UPF receives an UL Ethernet frame from a UE, the UPF could determine if a mapping exists between a PDU session ID for the UE and the VNI and, if a mapping does exist, could encapsulate the UL Ethernet frame with a VXLAN header including the mapped VNI and forward the VXLAN packet to the virtual network mapped to the VNI.

For downlink traffic that is to be communicated to a UE, when the UPF receives a DL packet from a VTEP, the UPF could determine whether a VNI contained in a VXLAN header of the DL packet is mapped to a corresponding VTEP. If the VNI is mapped to a corresponding VTEP, the UPF can decapsulate the VXLAN header to extract the inner Ethernet frame, can perform a look-up on the PDU session for the UE based on a destination Media Access Control (MAC) address contained in the inner Ethernet frame, and forward the Ethernet frame toward the UE.

Figure 2, below, is an example call flow illustrating control plane (e.g., SMF/UPF interactions) that may be involved in configuring VXLAN forwarding in accordance with the techniques proposed herein. Next, Figure 3, below, is an example call flow illustrating example UL/DL Ethernet frame processing that can be performed by a UPF in accordance with the techniques proposed herein.

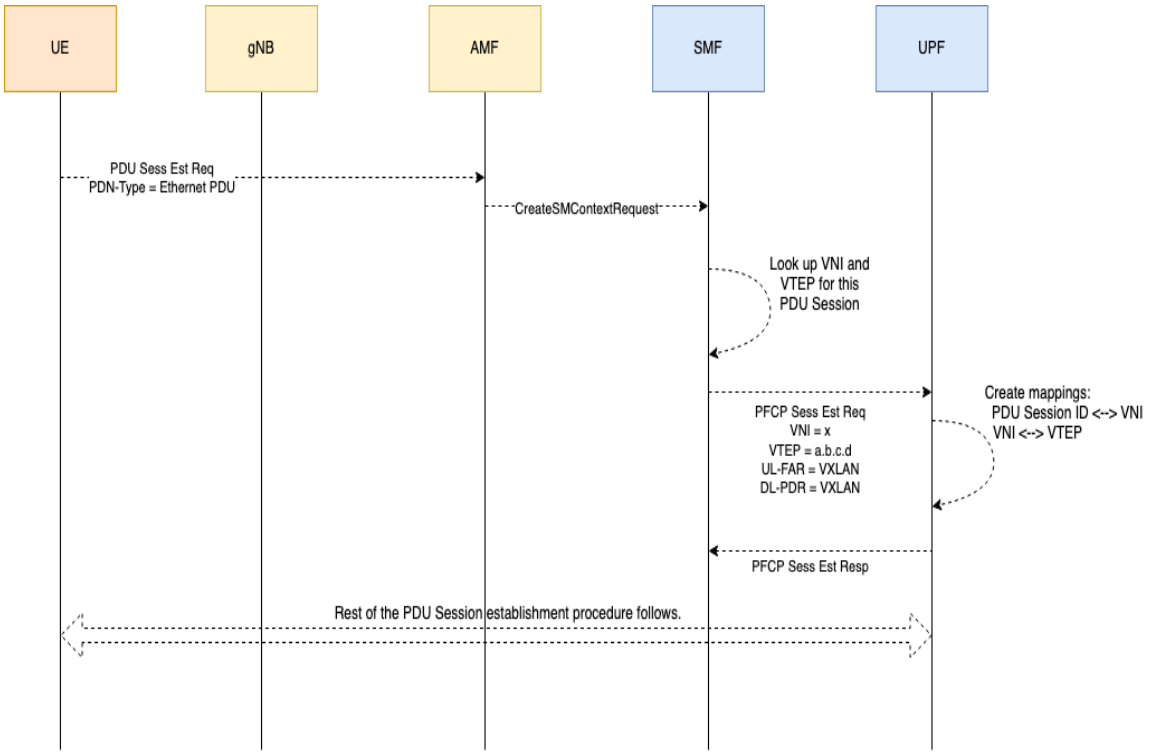

Figure 2: Example Control Plane Call Flow

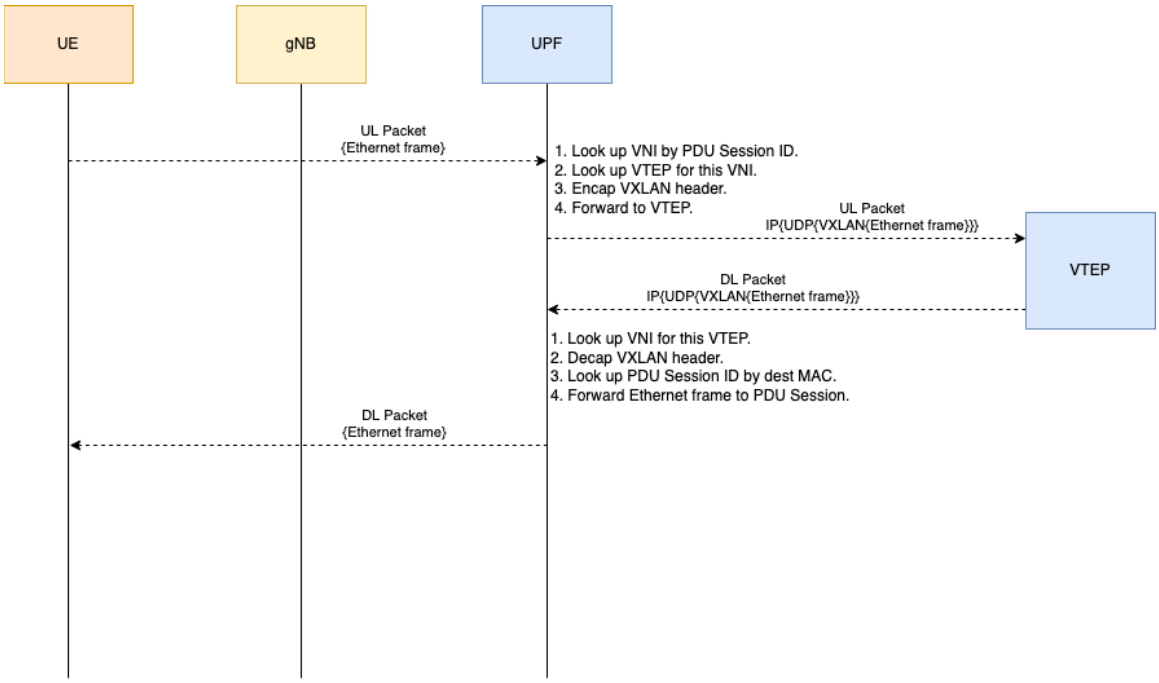

Figure 3: Example UPF UL/DL Frame Processing Call Flow

In summary, techniques herein may facilitate bridging remote L2 networks using VXLAN in a 5G network in order to provide an L2 interconnect between 5G accesses and remote datacenters or clouds. Such techniques can enhance the capabilities of Ethernet PDU Sessions, especially with 5GaaS environments in which network operators could bridge their remote L2 networks (or enterprise networks) with a 5G access using a VXLAN.