Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 28, 2019

X. de Foy
U. Olvera-Hernandez
InterDigital Communications

Jan 24, 2019

5G-Datacenter Interconnection Use Case
draft-defoy-nvo3-5g-datacenter-interconnection-00

Abstract

Interconnection between 5G networks and datacenter networks provide a new use case for NVO3 and for the 3rd Generation Partnership Project (3GPP) "5GLAN" feature. This document describes how layer-2 and layer-3 datacenter VPN technology can interoperate with anchor User Plane Functions (UPF) to interconnect 5G devices and datacenter servers over a virtual LAN.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 28, 2019.

Table of Contents

1. Introduction

1.1. About the 5GLAN Feature

In an ongoing work, 3GPP is seeking to enable LAN-like virtual networking between groups of end devices. Appendix A provides references and additional details relative to the 5GLAN work.

5GLAN requirements, defined in [_3GPP.22.261] can be shortly summarized as:

> A selected set of end devices can communicate with each other as if over a LAN, including over Ethernet or over IP, using a private addressing scheme.
>
> Unicast and multicast/broadcast communication is enabled between end devices, in some cases with a required latency (e.g. 180ms), or more generally a given consistent QoE.
>
> End device mobility is supported.

General concepts and use cases were described in [_3GPP.23.734].

> In home and enterprise deployments, a goal of 5GLAN is to facilitate interworking with, and sometimes replacing, existing infrastructure, composed of fixed and wireless LANs.

In enterprise deployments, 5GLAN will also provide a VPN-like service integrating mobile devices with enterprise networks.

In industrial automation deployments, 5GLAN can enable low-latency, reliable and deterministic LAN traffic in manufacturing, machine control, packaging and printing use cases.

1.2. Interaction between 5GLAN and Virtual Networks

5GLAN connectivity does not have to be confined entirely within a 5G network domain. The conclusion of the 5GLAN study [_3GPP.23.734] states that the standardized solution will include interconnection with (external) data networks. Data networks can be physical or virtual networks.

Within the context of edge computing, 5GLAN will make it possible to have 5G devices share a common IP address space with servers deployed in a mini/micro-datacenter. While a similar result could be achieved using an overlay solution terminated on the 5G device, using 5GLAN in this case makes it possible to benefit from 5G network features such as session continuity support, fine-grained QoS support, user and device authentication, and to make a more efficient use of the air interface.

1.3. Goals of this Document

The goals of this document are to describe:

New use cases for NVO3 and 5GLAN, related to interconnections between 5G networks and datacenters.

A more detailed discussion of the architecture and requirements of this interconnection.

Our primary scenario will be a virtual network domain located outside of the 5G domain (a "data network" in 3GPP terminology), that can be joined by 5G devices. It is NOT a goal of the present document to cover inter-UPF connectivity inside the 5G domain, which 3GPP intends to standardize in 2019.

2. New Use Case for NVO3 and 5GLAN: 5G/Datacenter Interconnection

In addition to already known base 5GLAN use cases (see Section 1.1), interconnection of 5GLAN with datacenters will enable new scenarios.

Support for Virtualization on 5G End Devices: 5G devices may be used as servers in a "mobile data center", or to extend a traditional/ fixed data center. This involves VM hosting on 5G devices, and VM

mobility between 5G devices, or between 5G devices and DC servers and enables, for example:

Transparent mobility of Fog RAN [I-D.bernardos-sfc-fog-ran] components between 5G devices and micro-datacenters,

Transparent offloading of application tasks towards the distant or edge cloud, or towards other 5G devices.

As discussed in Section 4, VM hosting on 5G devices under the control of a NVO3 network operator can bring new requirements on 5G networks interface with the datacenter data networks, including exposing a "tenant system interface" identity and state information, supporting adding/removing addresses, and supporting hot VM migration.

End-to-End Redundancy: 5G devices may connect to a 5GLAN virtual network over several paths, using active-active or active-passive configurations. For example, a 5G device running a critical application may use both WLAN and a cellular link to increase availability. Today, this type of connection are defined in 5G but are using a same anchor UPF for both links, which limits the scope of redundancy to the 5G network. Instead, path redundancy could be prolonged beyond the 5G network (e.g. using a different anchor for each path), into the datacenter.

3. Architecture Overview

A high level architecture view of the system is represented in Figure 1 (based on our interpretation of the conclusions of [_3GPP.23.734]).

In the data plane, the end device (user equipment) is connected point-to-point to an anchor gateway (UPF), through the radio access network and possibly through intermediate UPFs (not shown here). This point-to-point connection is called PDU session in 5G. In usual non-5GLAN communication use cases, IP or Ethernet packets are carried over a tunnel between the end device and the anchor UPF, decapsulated by the UPF and forwarded over a data network. In the 5GLAN case, the decapsulated packet should be tunneled/forwarded from the anchor UPF towards a remote virtualization edge, or another anchor UPF, which decapsulates and forwards the packet towards its destination end device. (Except in the simpler case where source and destination end devices are served by the same UPF.)

The section of network between anchor UPFs in the diagram is a datacenter VPN domain ("L2/L3 VPN domain"), with its own control and data plane. Anchor UPFs may be directly interconnected inside the 5G

network as well, for internal 5GLAN traffic (although it is not represented here).

In the control plane, 5G end device connectivity is today supported by the Access and Mobility Management Function (AMF) and Session Management Function (SMF). 5GLAN specific control plane support for a given 5GLAN network (e.g. to configure UPFs, and perform access control) will be implemented inside a single SMF.

There should be an interconnection between the 5G network and the L2/L3 VPN domain, in the control and/or management plane.

In the data plane, an edge function collocated or interconnected with the UPF is acting as a gateway between the 3GPP and L2/L3 VPN domain. This edge function corresponds to "provider edge" device in VPN terminology.

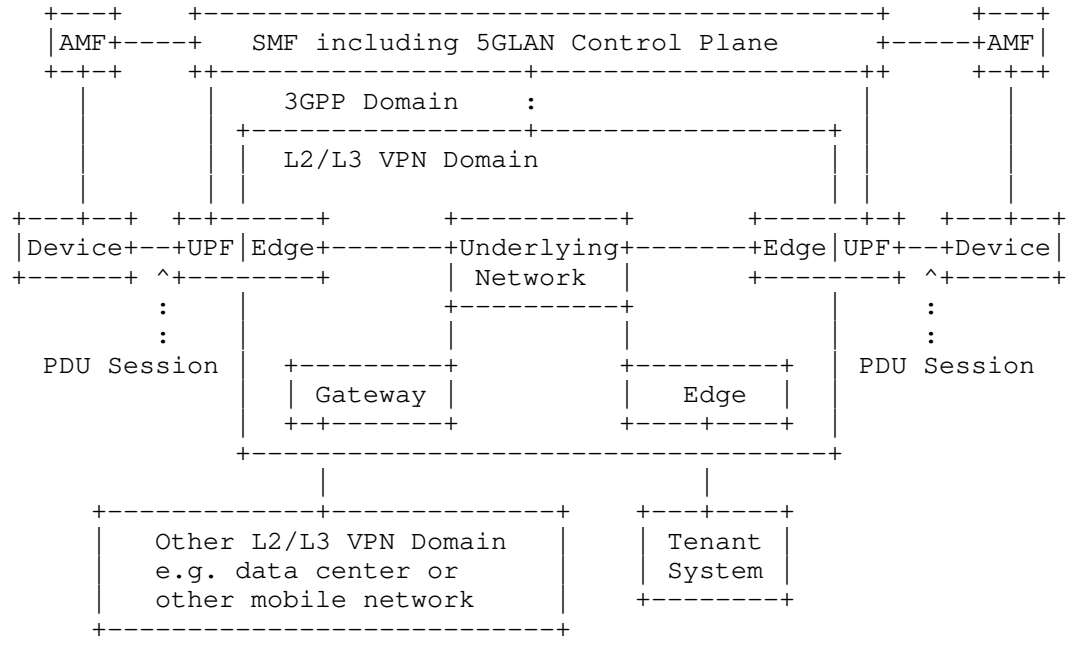

Figure 1: 5GLAN Network Interconnected with a L2/L3 VPN Domain

We will focus on NVO3 as the datacenter VPN technology. Nevertheless, applicability of other virtualization technologies to 5GLAN may be studied as well in future revisions of this document.

The 5GLAN architecture can be made to integrate with the NVO3 architecture [RFC8014], where:

A 5G end device corresponds to an end device in NVO3.

A 5G edge/UPF corresponds to an external NVE in NVO3 (the edge/UPF can encapsulate packets in network virtualization headers, as does the external NVE in NVO3, to avoid carrying those extra headers over the wireless link).

The PDU session in 5G corresponds to the VLAN connection between an end device and an external NVE (i.e. both are point-to-point connections).

An overview of the integration of NVO3 and the 5G network for 5GLAN is displayed in Figure 2

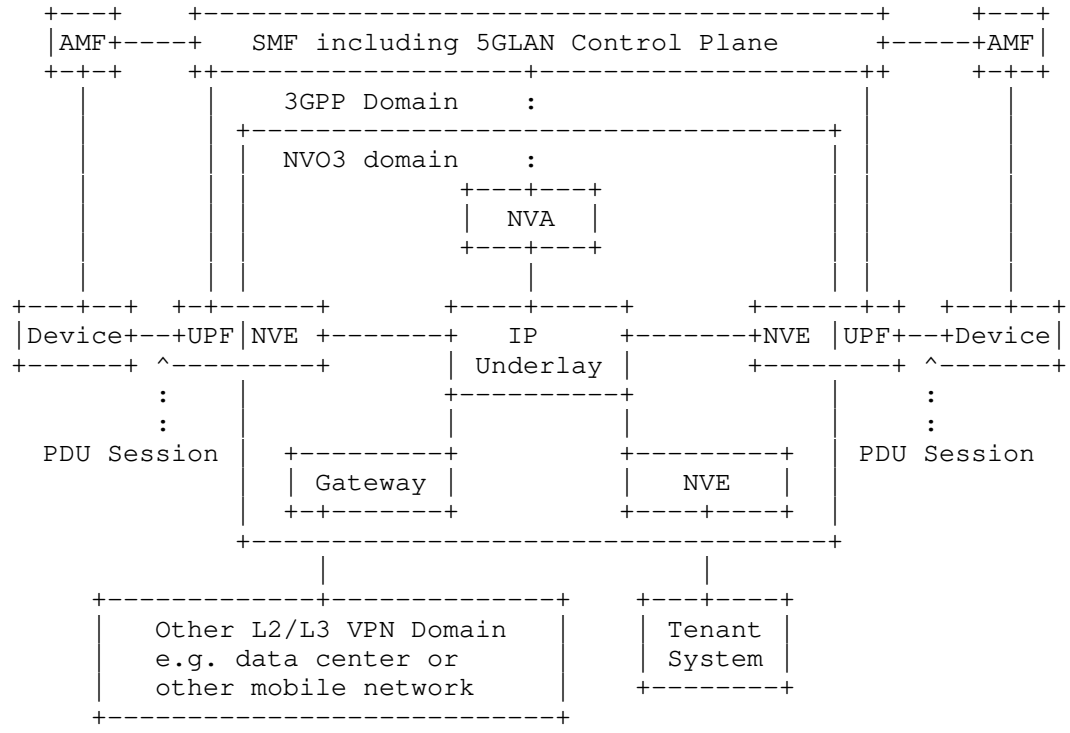

Figure 2: 5GLAN Network Interconnected with a NVO3 Domain

4. Major Features of a 5G/Datacenter Interconnection

The following discusses VPN-5G interconnection functionalities.

L2/L3 VPN: To support both IP-based and Ethernet-based 5GLANs, the L2/L3 VPN domain should provide L2 and L3 VPN services between

provider edges. NVO3 can support L2 and L3 VPNs over an IP overlay. For example, EVPN may be used in L2 case, as described in [I-D.ietf-nvo3-evpn-applicability].

VM Hosting and VM Mobility: The goal of this feature is to have the NVO3 network operator control connectivity for all VMs, including VMs hosted on 5G devices. Based on an analysis of End Device-to-NVE Control Protocol requirements [RFC8394] in the context of 5G LANs, here is a summary of potential requirements on 5G-NVO3 interfaces:

The concept of tenant system interface (TSI) identifies the connection to a single VM (e.g. it corresponds to a single VLAN tag on hypervisor-NVE connection in NVO3). This concept may also be useful to support VM migration. 5GLAN could for example restrict traffic to/from a single tenant system (e.g. a VM) to a single PDU session, and associate a TSI identifier to the connection, exposed to the L2/L3 VPN domain.

End Devices can communicate tenant system interface state information (associated and activated), which corresponds to different phases of a VM lifetime. Such information may therefore be carried over a PDU session to enable similar operations in 5GLAN.

A tenant system (e.g. VM) can add/remove IP/MAC addresses dynamically even after End Device-to-NVE connection is made for this tenant system.

The external NVE (i.e. edge/UPF in 5GLAN context) can dynamically initiate the deactivation or de-association of a MAC/IP address.

Hot and cold VM mobility may be supported. The 5G network should indicate when an event is caused by a hot VM migration event.

Active-active and active-passive redundant path to a 5G device (through multiple edge/UPFs) may be supported, to provide end-to-end path redundancy. To support this, the 5G network should expose reachability information towards a given IP or MAC address through multiple UPFs. Priority information may be exposed as well, to enable active-passive redundancy.

End Device Mobility and Session Continuity: End device mobility between anchor UPFs may be similar to hot VM migration events, although they occur more often and affect all hosted VMs on a device. They may also have more stringent requirements in term of packet loss and latency since, as opposed to the VM migration case, end device mobility requires no transfer of state.

Mobility requirements can vary: for example 5G devices using a fixed anchor ("session continuity mode (SSC) 1") will not expose any mobility event to the L2/L3 VPN domain. Nevertheless, in cases where mobility and low latency are required, break-before-make (in SSC mode 2) or make-before-break mobility (in SSC mode 3) events may be exposed to the L2/L3 VPN domain.

QoS: 5GLAN networks can be applied a wide range of QoS inside the 5G network, including ultra-low latency. Nevertheless, the level of QoS depends on the application, and therefore the level of QoS to apply to traffic to/from 5G devices in the L2/L3 VPN is not known at this time.

QoS mechanisms to be supported in the L2/L3 VPN domain can include best-effort, differentiated services, traffic engineered links, deterministic networking. Some form of coordination may be therefore needed between 5G and the L2/L3 VPN domain in control and/or management plane, e.g. to setup proper traffic engineering associated with NVO3 overlay networks (e.g. create/modify/release underlying TE paths when an end device changes its attachment point from one edge/UPF to another).

Privacy: Privacy is required for communication between end devices. The L2/L3 VPN, including the edge/UPF, should therefore support a secure protocol over the VPN domain (e.g. including encryption). Encryption of NVO3 traffic over the underlying network (e.g. using IPSec between NVEs) is mentioned in [RFC8014].

Access Control: Access control of end devices can be performed by the 3GPP domain (e.g. at network registration and later when creating the PDU session). Some form of cooperation between the 5G network and the L2/L3 VPN domain may be needed to authenticate the 5G subscription in the L2/L3 VPN domain (e.g. through the exposition of a subscription identifier).

Other Remarks: As already mentioned, UPFs can be directly interconnected with each other for internal 5GLAN communication. LAN communication between 5G devices may therefore entirely bypass the L2/L3 VPN.

Similarly, although device-to-device communication is currently not defined in 3GPP for 5GLAN, in the future it may also be leveraged to bypass the L2/L3 VPN for direct communication between devices.

A 5G device can become inactive, and may be paged/awaken when there is outstanding traffic for this device. This will be

handled entirely in the 3GPP system (traffic will be buffered at UPF and device will be paged).

5. IANA Considerations

This document requests no IANA actions.

6. Security Considerations

From the 5G operator perspective, traffic sent over the L2/L3 VPN domain should be secured against being misdelivered, being modified, or having its content exposed to an inappropriate third party. This requirement is also found in NVO3.

Additionally, 5G devices wishing to join a virtual network deployed in the L2/L3 VPN domain will need to be authenticated and authorized for joining. Mutual authentication and authorization between 5G devices and virtual networks may be needed and may be supported through coordination between the 5G network, which authenticated the 5G device, and the L2/L3 VPN domains.

7. Next Steps

We would like to propose this use case for further discussion and possibly adoption in a RTG working group such as NVO3 or RTGWG, as a new use case for datacenter networking.

At this time we do not expect a change in NVO3 protocols. On the other side, discussions at the IETF can provide valuable input to justify and drive any future enhancement to 5G networks, and align with IETF datacenter protocols (e.g. what information and operations should be made available to datacenter networks).

8. Informative References

[_3GPP.22.261]
3GPP, "Service requirements for next generation new services and markets", 3GPP TS 22.261, <http://www.3gpp.org/ftp/Specs/html-info/22261.htm>.

[_3GPP.22.821]
3GPP, "Feasibility Study on LAN Support in 5G", 3GPP TR 22.821, <http://www.3gpp.org/ftp/Specs/html-info/22821.htm>.

[_3GPP.23.501]
3GPP, "System Architecture for the 5G System", 3GPP TS 23.501, <http://www.3gpp.org/ftp/Specs/html-info/23501.htm>.

[_3GPP.23.734]
3GPP, "Study on enhancement of 5GS for Vertical and LAN Services", 3GPP TR 23.734, <http://www.3gpp.org/ftp/Specs/html-info/23734.htm>.

[_3GPP.33.819]
3GPP, "Study on security enhancements of 5GS for vertical and Local Area Network (LAN) services", 3GPP TR 33.819, <http://www.3gpp.org/ftp/Specs/html-info/33819.htm>.

[I-D.bernardos-sfc-fog-ran]
Bernardos, C., Rahman, A., and A. Mourad, "Service Function Chaining Use Cases in Fog RAN", draft-bernardos-sfc-fog-ran-04 (work in progress), September 2018.

[I-D.ietf-nvo3-evpn-applicability]
Rabadan, J., Bocci, M., Boutros, S., and A. Sajassi, "Applicability of EVPN to NVO3 Networks", draft-ietf-nvo3-evpn-applicability-01 (work in progress), October 2018.

[RFC8014] Black, D., Hudson, J., Kreeger, L., Lasserre, M., and T. Narten, "An Architecture for Data-Center Network Virtualization over Layer 3 (NVO3)", RFC 8014, DOI 10.17487/RFC8014, December 2016, <https://www.rfc-editor.org/info/rfc8014>.

[RFC8394] Li, Y., Eastlake 3rd, D., Kreeger, L., Narten, T., and D. Black, "Split Network Virtualization Edge (Split-NVE) Control-Plane Requirements", RFC 8394, DOI 10.17487/RFC8394, May 2018, <https://www.rfc-editor.org/info/rfc8394>.

Appendix A. 5GLAN Background Information

The 5G architecture is defined by 3GPP in [_3GPP.23.501], currently as part of release 15.

5GLAN is a new feature developed as part of release 16. Its requirements are currently being specified in [_3GPP.22.261] (based on results from an earlier study on requirements in [_3GPP.22.821]).

The architecture of 5GLAN has been studied in [_3GPP.23.734], along with other subjects. A specification phase for the 5GLAN

architecture will likely follow. Conclusions of the study included the following:

5GLAN traffic (IP or Ethernet traffic between a restricted set of "5GLAN group member" devices) will be transported between 5G devices and their anchor UPF. Anchor UPFs will forward this traffic, as applicable, to/from (1) a data network, (2) another anchor UPF, or (3) other devices using local forwarding through the anchor UPF, when devices are connected to the same anchor. In case (2), direct traffic between anchor UPFs will be encapsulated in per-5GLAN group tunnels.

In the control plane, a single SMF will handle connectivity of all devices connected to the same 5GLAN.

The user plane can be centralized (single anchor UPF involved in a single 5GLAN) or distributed (multiple anchor UPFs involved in a single 5GLAN).

Security aspects related to 5GLAN are currently studied in [_3GPP.33.819].

Authors' Addresses

Xavier de Foy
InterDigital Communications, LLC
1000 Sherbrooke West
Montreal H3A 3G4
Canada

Email: Xavier.Defoy@InterDigital.com

Ulises Olvera-Hernandez
InterDigital Communications, LLC
64 Great Eastern Street
London EC2A 3QR
England

Email: Ulises.Olvera-Hernandez@InterDigital.com