March 2023

ENHANCED VISIBILITY AND FORWARDING IN A TELCOMMUNICATION DATA CENTER FABRIC

Radha Krishnaiah Pusapati

Rajagopalan Janakiraman

Murukanandam Panchalingam

Javed Asghar

ENHANCED VISIBILITY AND FORWARDING IN A TELCOMMUNICATION DATA CENTER FABRIC

AUTHORS:
Radha Krishnaiah Pusapati
Rajagopalan Janakiraman
Murukanandam Panchalingam
Javed Asghar

ABSTRACT

In current telecommunication (telco) deployments, data center networks do not have visibility into subscriber traffic and cannot apply functions related to the subscriber traffic. Techniques presented herein provide for a methodology through which a General Packet Radio Service (GPRS) Tunneling Protocol (GTP) tunnel ID (TEID) in a packet GTP header can be used as endpoint security group classification criteria. Classifying packets into security groups may allow for aggregating subscriber mobile traffic and for facilitating the enforcement of granular policies.

DETAILED DESCRIPTION

In current telco 5G deployments, a User Plane Function (UPF) is hosted as a Virtual Network Function (VNF) in an edge/regional data center. A subscriber Protocol Data Unit (PDU) session transmitted between UPFs is encapsulated with a GTP tunnel header. In this case, the data center network operates as an underlay for the GTP encapsulated traffic and routes/steers the traffic in the data center fabrics (e.g., spine-leaf Clos topology) based on the GTP outer Internet Protocol (IP) address. The data center network may have limited visibility into the subscriber traffic and, therefore, cannot apply any functions related to the subscriber traffic.

Such a deployment may have several problems. First, if subscriber traffic is lost within the data center fabric or outside the fabric (e.g., in the case of distributed VNFs), it is not possible to debug or trace the packet/flow in the data center network(s) because the node does not have visibility inside the GTP header. Second, if some UPFs are busy with subscriber session traffic processing, the data center switching network continues to forward the traffic to the UPFs by applying regular Equal Cost Multi-Path (ECMP)

routing (e.g., based on outer IP headers). The data center network does not have visibility into the UPF load and cannot act on subscriber traffic.

A Simplified Telco Regional/Edge data center virtual Evolved Packet Core (vEPC)/Mobile Packet Core (MPC) for 5G deployments is illustrated in Figure 1, below.

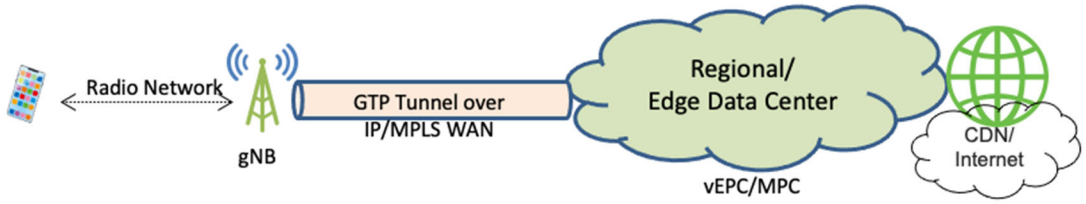

Figure 1: Example Diagram of 5G Network Deployment

Consider for the example network deployment shown in Figure 1 that the 5G control plane signaling sets up the GTP tunnels between the gNodeB's access network (AN) and the subscriber UPFs running in the Mobile Packet Core (MPC). Additionally, consider that the 5G subscriber data plane traffic uses GTP Tunnel identifiers (IDs) that have already been established.

Control plane signaling for the example network deployment of Figure 1 is depicted below in Figure 2, below, and a data path view for the network deployment is depicted in Figure 3, below.

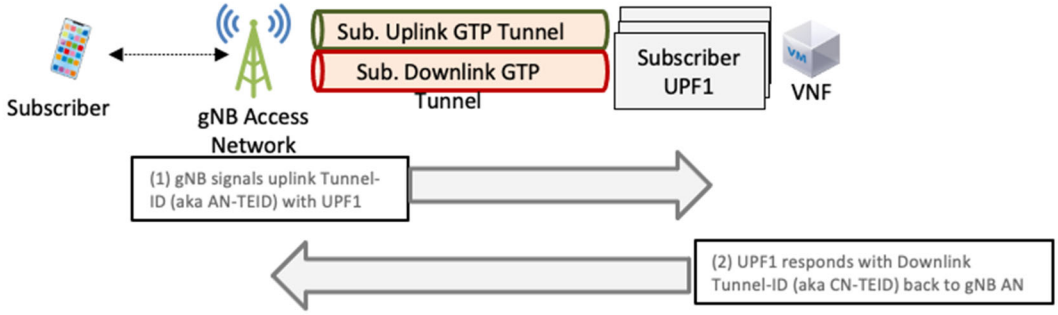

Figure 2: Example GTP Control Plane Signaling

Figure 3: Example GTP Data Plane

In the example illustrated in Figure 3, two tunnels are set up for the data path. The first tunnel is the uplink tunnel from the gNobeB AN toward the subscriber UPF (e.g., using the Tunnel ID: Core Network (CN)-TEID). The second tunnel is the downlink tunnel from the subscriber UPF toward the gNodeB AN (e.g., using the Tunnel ID: AN-TEID).

Figure 4, below, illustrates elements of a regional/edge data center acting as a vEPC/MPC.

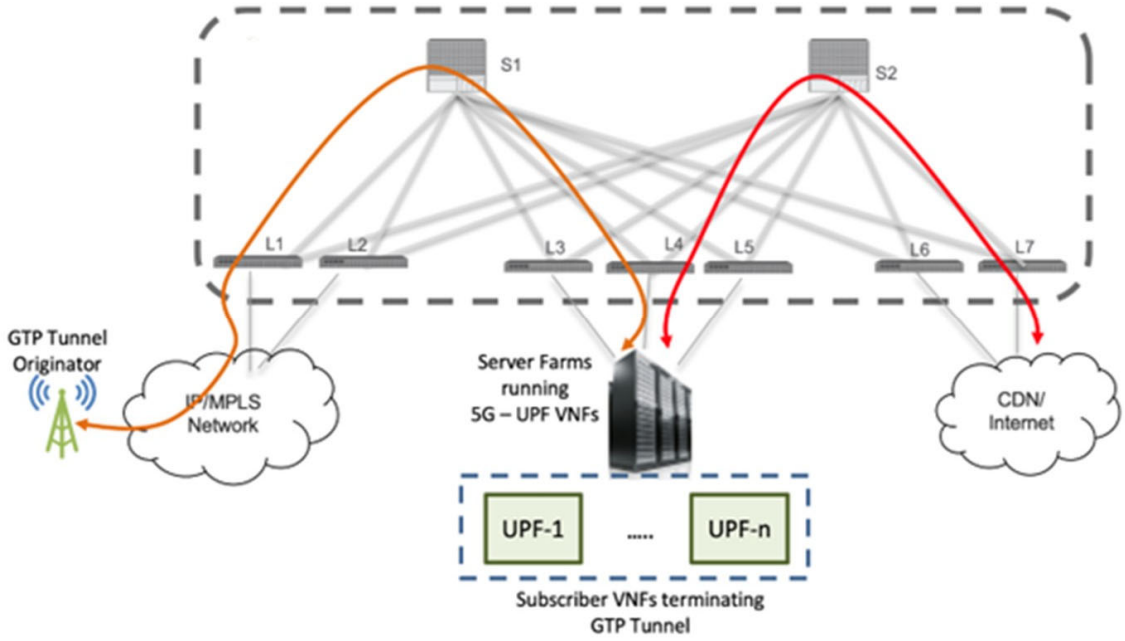

Figure 4: Example Data Center

Consider, in one example, that the data center is a standard Clos topology (e.g., with leaf nodes being L1 to L7 and spine nodes being S1 & S2) deployed with a Software-Defined Network (SDN) Controller. Further, consider that the leaf nodes are

grouped into three categories. In the first category, one or more leaf nodes (e.g., L1 & L2) connect toward the Midhaul/Backhaul networks (typically an IP/Multiprotocol Label Switching (MPLS) wide area network (WAN)). In the second category, one or more leaf nodes (e.g., L3, L4, L5) connect to server farms in the data center where the 5G UPF VNFs are run. In the third category, one or more leaf nodes (e.g., L6 & L7) connect towards the Content Delivery Network (CDN)/Internet (or other traditional Service Provider Gi-local area network (LAN) networks).

During operation of this example network deployment, subscriber traffic initiated by the 5G mobile customer/device/endpoint connects over a radio network with the gNodeB and the subscriber traffic is GTP tunneled to the subscriber UPFs running in the DC (depicted via the orange flow). Additionally, the regular IP traffic from the UPFs to the CDN/Internet is depicted via the red flow and both the orange and red flows are carried via another overlay tunnel inside the data center network, which could be a Virtual Extensible LAN (VXLAN), GENEVE, SRv6 or any IP-in-IP tunnelling protocol.

Now to bring visibility into this data center network, let's introduce the concept of "Endpoint Security Groups (ESGs)." An ESG is a collection of endpoints (virtual machines (VMs)/devices) and grouping the endpoints in this manner enables the network to provide robust micro-segmentation capabilities on which granular security, routing, and quality of service (QoS) policies can be enforced.

In the context of 5G vEPC deployments, for the orange GTP tunneled flows illustrated in Figure 4, the ESG for the subscriber traffic is carried in GTP tunnels, they are identified by the gNodeB and the UPF subscriber pool addresses and not by the actual subscriber's information since the subscriber PDUs are the payload of the GTP packets. Such identification utilizing subscriber pool addresses, as opposed to subscriber information, may represent a limitation of current deployments with respect to enforcement of granular classification of the mobile traffic inside the data center.

In order to address such potential issues, techniques presented herein provide for a methodology wherein the GTP tunnel ID (TEID) in the packet GTP header can be used as ESG classification criteria. Figure 5, below, illustrates ESG derivation in the MPC nodes.

Figure 5: Example Diagram of Endpoint Security Group Derivation

Figure 3 illustrates the concept of the CN-TEID being used in the uplink direction and the AN-TEID being used in the downlink direction. Figure 5 outlines how the TEIDs can be used as endpoint security group classification criteria.

In a first step, consider that, in the uplink direction, the CN-TEID in the GTP header along with destination IP address (which is the UPF's IP address), may be used to derive the destination endpoint security group. In a second step, consider that, in the downlink direction, the AN-TEID in the GTP header along with the destination IP address (which is the gNodeB AN's IP address), can be used to derive the destination endpoint security group. Therefore, for both directions, in a direction-agnostic manner, the nodes using the combination of {Dest.IP Addr+GTP TEID} can determine the destination endpoint security group for the flow (identified by the tag hereinafter known as the "dclass").

Figure 6, below, depicts the steps that occur in two stages inside the programmable application-specific integrated circuit (ASIC) pipeline.

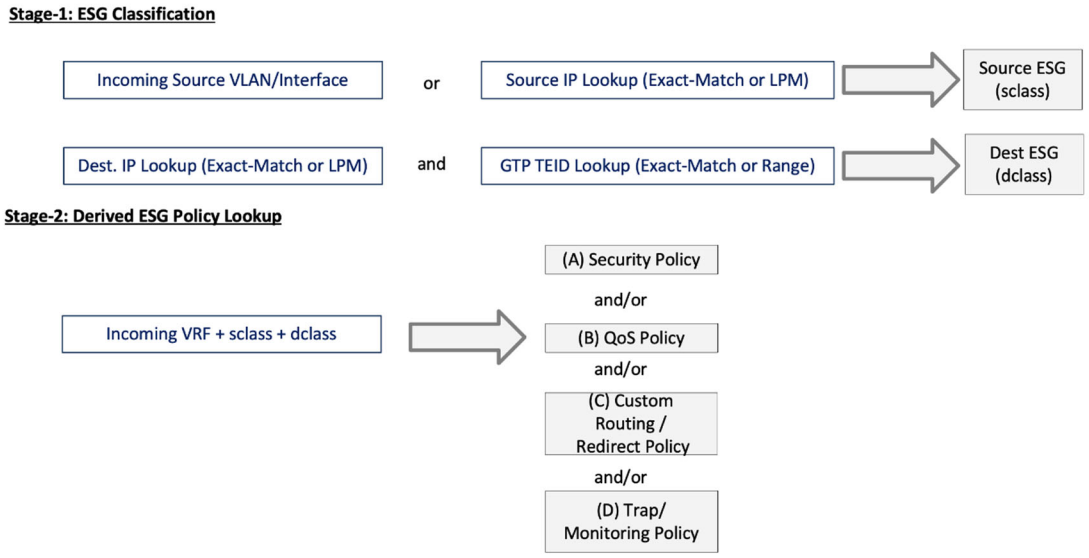

Figure 6: Example ASIC Pipeline

For the example ASIC pipeline as shown in Figure 6, the first stage may represent an endpoint security group classification. In a first step, the source VLAN/Interface and/or the source IP address in the GTP packet is used to derive the source endpoint security group (denoted by the tag hereinafter known as "sclass"). In a second step, the destination IP addresses along with the GTP TEID (which can be an exact match or range/mask-based match), is used to derive the destination endpoint security group (dclass).

Consider that the second stage determines an endpoint security group granular policy. Since the TEID is set up for the data path session per-subscriber, the TEID uniquely identifies the end 5G mobile subscriber/endpoint. Therefore, the derived sclass and dclass can be used in a security group lookup and the result can be a security policy, a QoS policy, a routing policy, or a trap/monitoring policy.

The security policy may define whether the flow is allowed or denied. The QoS policy allows for overwriting of the outgoing IP Differentiated Services Code Point (DSCP) or MPLS experimental bits (EXP), based on a TEID match (which may be useful if there is congestion, which results in reclassification of the QoS for the subscriber flow). The routing policy may overwrite the original intended destination user plane function

(UPF) cluster and redirect to another UPF cluster (which may be useful if there is congestion on the server side). The trap/monitoring policy may give much-needed visibility into the flows within the fabric and optionally implement debug-ability features (e.g., atomic counters or latency statistics). Consider that all these additional policies can be enforced only because the node was able to use the TEID in accordance with techniques presented herein.

As outlined in Figure 6, the configuration for the GTP TEID lookup in the first stage can be programmed in the ASIC as either exact match 32-bit TEID entries or TEID range programmed as a Longest Prefix Matching (LPM) or a masked lookup. Since the hardware lookup table is limited in size, the default mode may be using range-based lookups. However, using range-based lookups puts additional requirements on the TEID allocation in the UPFs (which may or may not be feasible in all deployments).

The next best option with TEID lookups is to have some form of horizontal sharding/scale out using the topology in Figure 3. The data center network is already capable of ECMP hash selection using GTP TEID. Consider that, armed with this capability, the subscriber traffic landing in the nodes L1 or L2 in the uplink direction may be redirected to one of N nodes (N=3 in Figure 1, i.e., L3, L4, L5) where the server farms hosting UPF clusters are connected.

For an example in which the traffic is transmitted from gNodeB AN1 to UPF1 for a TEID: X, assume the traffic hashes to the node L3 out of the 3 nodes. Since this hash selection can be predetermined, it is sufficient to have the endpoint security group match for the TEID: X and the corresponding policies for this endpoint security group apply only in the node L3 (and not the other two nodes L4 & L5). Some other flows may hash to the other two nodes in this manner. Therefore, in this mode, without replicating the same endpoint security group to match on TEID: X on all the 3 nodes, techniques described herein provide for using sharding/horizontal scale out of the GTP endpoint security group policies to maximize the hardware resource usage without replication. Once the relevant GTP-endpoint security group policies are applied, the subscriber flow is routed to its intended destination.

Techniques described herein include a GTP-TEID on-demand match capability. An operator may configure a range-based GTP-TEID match for coarse endpoint security

group policies. However, it is paramount the network provide an option for the operator to program a more-specific GTP-TEID for a 32-bit exact match. To achieve this on-demand programming capability, the role of the SDN controller should be explored.

At a high-level view, the SDN controller performs several functions. For example, the SDN controller allows the operator to pre-define the endpoint security groups for the TEID match based on labels. For example, consider the labels Red, Yellow, Blue, Green. The operator may pre-define that endpoint security group-A matches only label-Red, endpoint security group-B matches label-Yellow, and endpoint security group-C matches both these labels: Label-Blue and Label-Green.

For the NFVs implementing the 5G session setup and other control plane functions, the SDN controller may additionally provide the data of TEIDs to their label mapping. For example: {IP1, TEID: X} => Label-Blue, {IP2, TEID: Y} => Label-Blue,Label-Green. Finally, the SDN controller should be capable of sourcing this data, interpreting these labels, and associating the corresponding TEIDs to the pre-defined endpoint security groups (this functionality should be automated without operator's intervention).

As discussed in the above example, consider that the SDN controller automates endpoint security group-C to match {IP2, TEID: Y}. The automating of endpoint security group-C to match {IP2, TEID: Y} is now pushed by the controller to the node L3 and programmed in the hardware as a most-specific match (i.e., 32-bit exact match). Existing range/mask-based GTP TEID match entries in the node L3 do not have to change because exact match entries will always match before the range/mask based entries. GTP tunneled traffic destined to IP2 with a TEID is redirected to node L3 and endpoint security group-C's policies are applied.

Several steps may be performed to determine which subscriber (and, therefore, which group) is associated with a GTP-U tunnel ID. In a first step, a subscriber-to-label matching is created by the 5G system operator. A label represents a flexible group of subscribers. In a second step, the 5G control plane maintains the subscriber-to-TEID mapping. The session management context is extended to map a TEID to a corresponding label. The mapping is performed dynamically and without operator intervention. In a third step, a data center SDN controller identifies the label/TEID

mappings via polling/streaming from a 5G system. In a fourth step, the data center SDN controller operator maps one or more subscriber labels to an endpoint security group and defines endpoint security group-to-endpoint security group security/QoS/redirect/monitoring policies. The endpoint security group-based group policy implementation in ACI may be extended to map the TEID to the endpoint security group in the data plane.

To summarize, techniques presented herein provide the ability to use packets' GTP TEIDs to classify the packets into security groups, thereby aggregating subscriber mobile traffic and providing enforcement of granular policies. Techniques provided herein further provide the ability to scale out the GTP TEID matching via horizontal scale-out/sharding by taking an additional hop to the involved nodes. Techniques provided herein additionally provide for SDN controller integration with the 5G control plane to allow for the capability to add on-demand label-based TEID matching.

Given that the GTP TEID today is used only for calculation of hash entropy inside the fabric, techniques discussed herein extend the ability of the node in the packet core to also understand and derive meaningful classifications for the TEID and apply new policies, which was previously not feasible in any shipping solutions. The additional embodiments with horizontal sharding/scale-out and on-demand programming of TEID exact matches provide useful enhancements to network operators.