November 2023

END-TO-END ENCRYPTION AND DECRYPTION WITHIN A HIERARCHICAL SD-WAN WITH AN IPV6 TRANSPORT

Lianxiang Wang

Yunpeng Zhang

Avinash Shah

Alan Xiao-rong Wang

Pan Wu

END-TO-END ENCRYPTION AND DECRYPTION WITHIN A HIERARCHICAL SD-WAN WITH AN IPV6 TRANSPORT

AUTHORS:
Lianxiang Wang
Yunpeng Zhang
Avinash Shah
Alan Xiao-rong Wang
Pan Wu

ABSTRACT

Techniques are presented herein that address a singular pain point in a hierarchical software-defined wide area network (SD-WAN) deployment comprising an Internet Protocol (IP) version 6 (IPv6) transport – end-to-end encryption and decryption. Aspects of the presented techniques leverage the IPv6 address schema to support a new concept that may be referred to herein as a micro-Transport Locator (TLOC) or uTLOC. Under the presented techniques, when an Overlay Management Protocol (OMP) virtual private network (VPN) route is published a next hop may be set to the combination of all of the uTLOCs along a path. Within such a context, each router (along the path) may program a customized action (such as, for example, the shifting of a destination, an insertion into a source, etc.) into a routing table for a uTLOC prefix and then forward a packet to a destination edge without the need for decryption and re-encryption operations in an intermediate border router.

DETAILED DESCRIPTION

In a hierarchical software-defined wide area network (SD-WAN) deployment, the virtual private network (VPN) route within a remote region is redistributed, hop-by-hop, through a border router. Consequently, the traffic that is transiting from a source region's edge router to destination region's edge router must undergo, at each hop, encapsulation along with encryption and then decapsulation along with decryption. As a result, along such a path the traffic must undergo encryption and decryption operations multiple times, thus introducing overhead and causing latency. It is important to note that a border router in such a hierarchical SD-WAN environment is a transient router and at such a device decryption and re-encryption is not necessary.

Techniques are presented herein that support an end-to-end encryption and decryption approach that eliminates the above-described intermediate, repeated encryption-decryption operations. In support of achieving end-to-end encryption and decryption, aspects of the presented techniques introduce a new concept, which may be referred to herein as a micro-Transport Locator (TLOC) or uTLOC.

A uTLOC is a TLOC that employs an Internet Protocol (IP) version 6 (IPv6) transport and whose IPv6 address comprises two parts – block bits (which may range in length from one (1) bit to 80 bits depending upon a given address allocation and scale) and host bits (which are always 16 bits long and which are appended following the block bits). Exemplary uTLOC IPv6 addresses include A:B:1::, A:B:2::, etc. A uTLOC's block bits may be based on allocated prefix bits from the Internet Assigned Numbers Authority (IANA) such as, for example, 000A:000B/32. A uTLOC's host bits determine the TLOC number and, since 16 bits are employed for the host part, such an approach allows for at most 65,535 TLOCs within a given block, with their addresses ranging from 000A:000B:0001::/48 to 000A:000B:ffff::/48.

When a uTLOC is configured, two routing entries, which may conform to the following pattern:

```
block:host::/block+host length -> left shift destination address by
  16 bits, re-lookup and forward, insert egress host bits to source
  address
block:host::/128 -> for-us
```

may be added to a routing table.

Figure 1, below, presents elements of an exemplary network environment that is reflective of the above discussion.

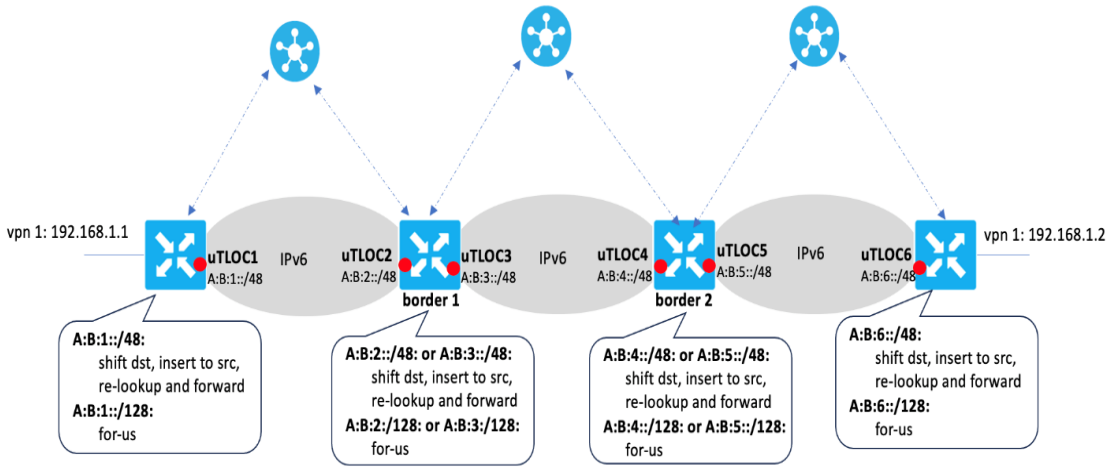

Figure 1: Exemplary Network Environment

As shown in Figure 1, above, the border router border 1 is associated with two uTLOCs (i.e., uTLOC2 and uTLOC3) and, respectively, the IPv6 addresses A:B:2::/48 and A:B:3::/48. Accordingly, four routing entries would be found in border 1's routing table (as depicted in the above figure):

```
A:B:2::/48 -> left shift destination address by 16 bits, re-lookup
  and forward, insert egress host bits to source address.
A:B:3::/48 -> left shift destination address by 16 bits, re-lookup
  and forward, insert egress host bits to source address.
A:B:2::/128 -> for-us
A:B:3::/128 -> for-us
```

According to the presented techniques, when a VPN route is published from a remote region's edge it may carry its uTLOC as the next hop entity and when a border router re-distributes that VPN route it may insert its uTLOC in the original next hop as the new next hop entity.

Further, a source region's edge may receive such a VPN route with the next hop containing a combination of an intermediate border router's uTLOC and a destination edge router's uTLOC. For example, as shown in Figure 2, below, when a source edge receives the route 192.168.1.2 at vpn 1 its next hop is identified as A:B:2:4:6.

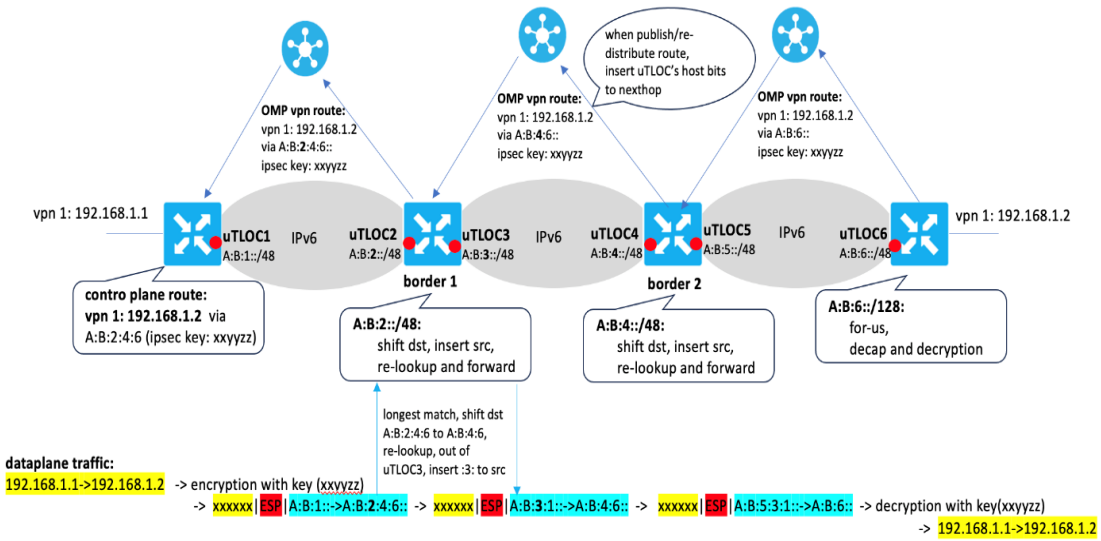

Figure 2: Exemplary Network Environment

Additionally, as shown in Figure 2, above, an Internet Protocol Security (IPsec) key (such as xxyyzz in the instant example) may also be published with a VPN route.

Figure 2, above, also demonstrates how data plane traffic may be forwarded from a source edge to a destination edge in a remote region. A source edge may encrypt a packet from vpn 1's traffic using the IPsec key xxyyzz, with an encapsulated outer header's source address as the local egress uTLOC A:B:1:: and the outer header's destination address as vpn 1's next hop of A:B:2:4:6::. Because border router border 1 has published its uTLOC prefix A:B:2::/48 to the transport network, such a packet will reach border 1. On border 1, the destination A:B:2:4:6:: will hit A:B:2::/48 according to a longest match, resulting in a left shift of the destination address by 16 bits (from A:B:2:4:6:: to A:B:4:6::) followed by a re-lookup operation and then a forwarding to border router border 2 because border 2 has published its uTLOC as A:B:4::/48. Additionally, since the egress uTLOC is A:B:3::/48, the value 3: is inserted into the source address A:B:1::. Finally, the packet that is forwarded by border 1 has the source address A:B:3:1:: and the destination address A:B:4:6:: and, accordingly, it will reach border router border 2.

On border router border 2, the above-described process may be completed for the received packet resulting in the packet reaching the remote region's edge router. When the packet reaches the last edge router, the source address is set to A:B:5:3:1:: and the

destination address is set to A:B:6:: which results in a hit against A:B:6::/128, whose action is for-us. Consequently, the last edge router will decapsulate the outer header and decrypt the packet using the IPsec key xxyyzz based on the Security Parameter Index (SPI) in the Encapsulating Security Payload (ESP) header. Finally, the payload packet may be forwarded over vpn 1.

If the above-described packet is dropped during a forward operation (e.g., border router border 2 dropped the packet) an Internet Control Message Protocol (ICMP) version 6 (ICMPv6) packet may be to the source edge. Under the presented techniques, such an ICMPv6 packet will successfully reach the source edge. As shown in Figure 3, below, the ICMPv6 packet's destination address is A:B:3:1:: (i.e., the original packet's source address). According to the packet forwarding process, that ICMP packet will be forwarded to the source edge and then locally consumed.

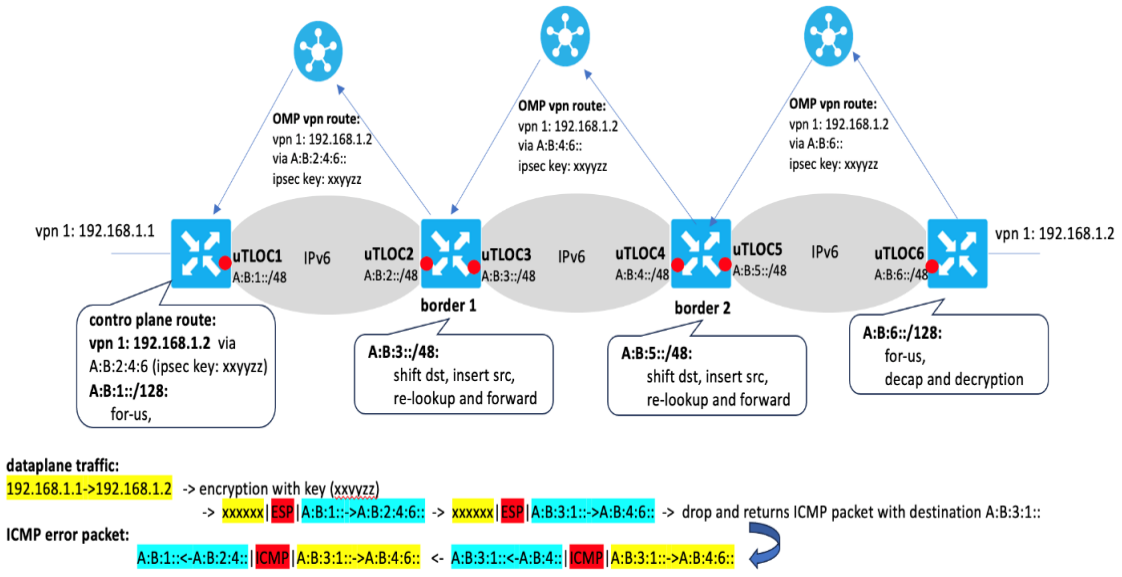

Figure 3: Exemplary ICMPv6 Packet

Currently, a SD-WAN may support an IPsec pairwise key feature. If such a feature is enabled, the presented techniques may employ an Overlay Management Protocol (OMP) security route to exchange IPsec keys among uTLOCs in different regions. Such a distribution process (over an OMP security route) is similar to an OMP VPN route, as shown in Figure 4, below.

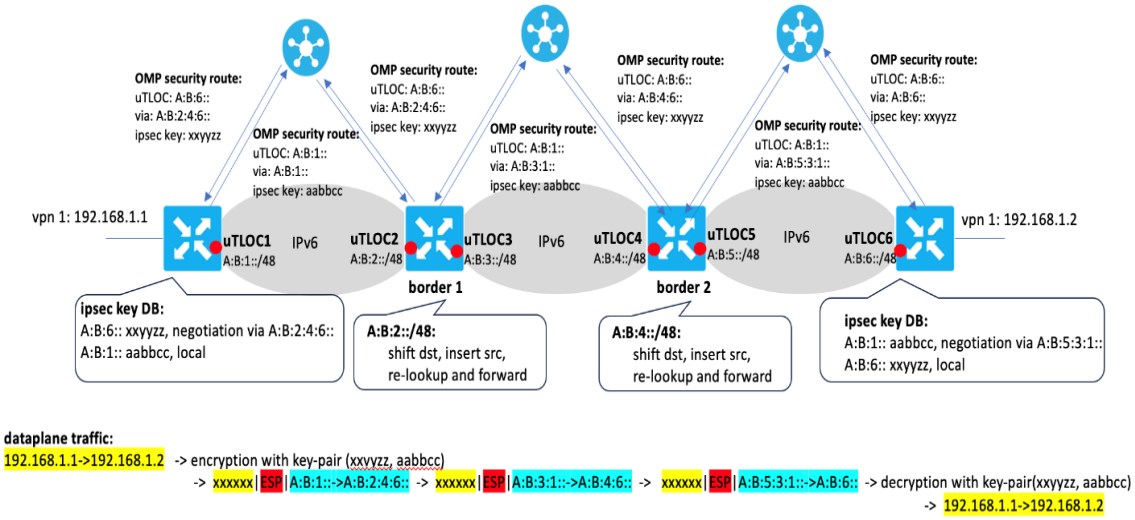

Figure 4: Exemplary OMP Security Route

After the necessary IPsec keys have been exchanged and negotiated, a source edge can encrypt a packet using an established key pair and a destination edge can, ultimately, decrypt a received packet using the same key pair.

It is important to note that an IPsec pairwise key feature, as described above, may not be enabled by default within an SD-WAN. Additionally, if scaling is a concern in a large network such a feature may be disabled in that network. Further, a route control policy may be configured on a central intelligence hub of the SD-WAN fabric within a region. For example, if a network administrator knows that there is no IPsec traffic between a first region and a second region, a control policy may be configured on a core region's central intelligence hub to prevent the security routes from redistributing to each other.

It is also important to note that within a SD-WAN an IPsec key exists for each TLOC. When each VPN route is published, a TLOC is its attribute, meaning that the VPN route is reachable through that TLOC. Under the presented techniques, an originating edge may insert that TLOC's IPsec key along with a uTLOC as the VPN route's attribute that is to be distributed. If the originating edge has multiple uTLOCs then it will have multiple IPsec keys. If each VPN route update carries multiple uTLOCs in its attribute, it also will carry multiple IPsec keys. This behavior is similar to how a VPN label is carried. Meanwhile, with the SD-WAN there is a configuration setting that determines how many

TLOCs will be carried in a VPN route and such a value may be used to control the scale of an environment.

Beyond the illustrative examples that were discussed above, aspects of the presented techniques address various of the challenges that may arise from the presence of different domains and the issues of scale.

For example, under the presented techniques some portion of the block bits of a uTLOC's address may be employed to define different domains. Under such an approach, only the uTLOCs in the same domain would receive and redistribute OMP routes. As shown in Figure 5, below, such an approach can control the scaling challenge that may arise if there are many uTLOCs.

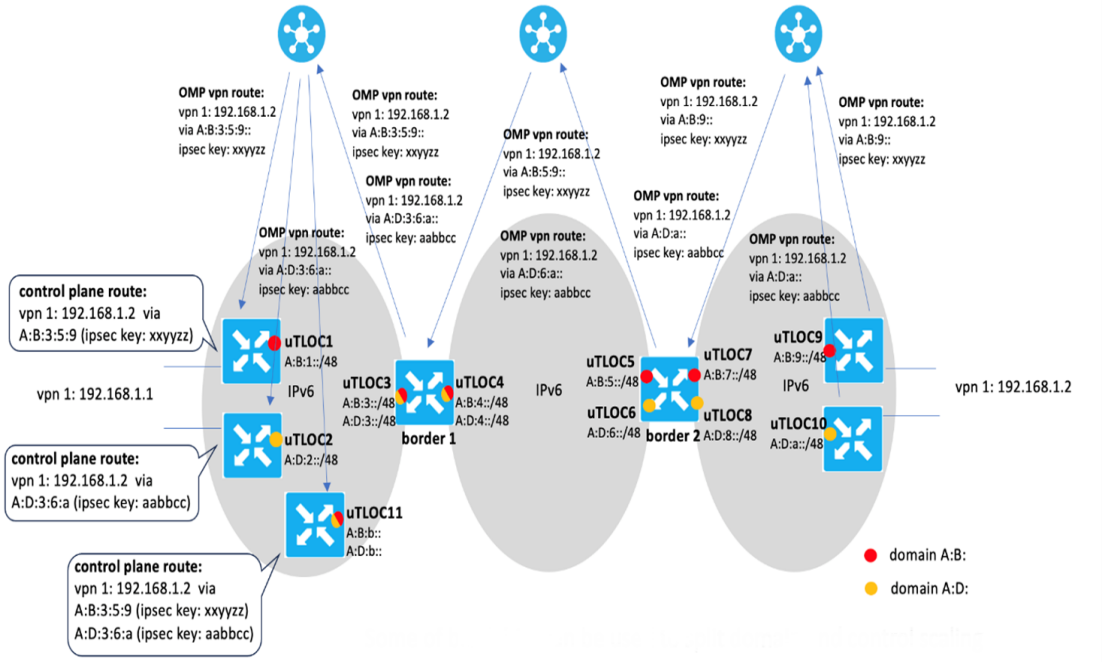

Figure 5: Illustrative Multiple Domains

The presence of different domain (as described previously and as illustrated in Figure 5, above) may arise when a customer is unable to obtain, from different providers in different regions, the same A:B prefixed addresses (as described and illustrated in the preceding examples) for all of their uTLOCs. Under such a circumstance, different uTLOCs may employ different prefixes, as will be further described below.

If all of the regions within an environment have common block bits (as was the case in the preceding examples), the block bits may be merged and just the host bits combined or shifted. In contrast, if the regions do not have a common prefix then all of the block bits and all of the host bits must be combined or shifted. In support of such an approach, the presented techniques may employ the below-described addressing schema.

All of the border routers within one region may share the same 32-bit long block and employ 8 bits as host bits, for a total allocation of 40 bits. Additionally, all of the edge routers within one region may share the same 32-bit long block and use 16 bits as host bits, for a total of 48 bits. For a packet to traverse from a local edge to a local border router to a remote border router to a remote edge, it may combine the address of the local border router TLOC (40 bits), the remote border router TLOC (40 bits), and the remote edge TLOC (48 bits) for a total of 128 bits that may be saved at the destination. Such an approach is illustrated in Figure 6, below.

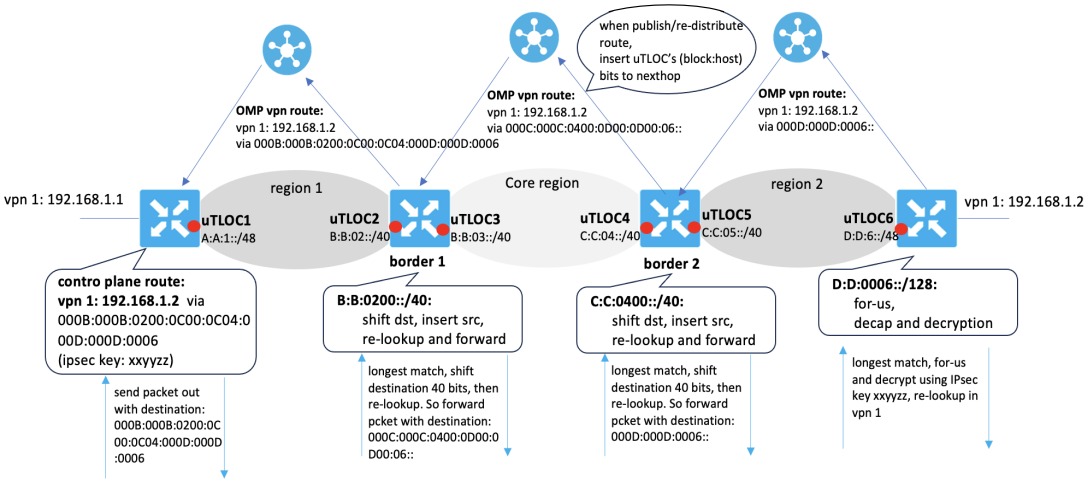

Figure 6: Alternative Addressing Scheme

As shown in Figure 6, above, the above-described addressing schema may scale to at most 256 border TLOCs within one region and at most 65,535 edge TLOCs within one region. It is important to note that the above-described bit allocation paradigm is illustrative only and a particular allocation may be shifted as needed (if, for example, the indicated bit length-driven limits are exceeded in a large network). For example, in a large network a

particular region may have more than 256 border router uTLOCs, in which case that region may employ different prefixes for different border routers.

The presented techniques may be further understood through another exemplary network, this network comprising (to illustrate an incrementally greater level of complexity) additional regions.

The flow of traffic in a typical hierarchical SD-WAN comprises a traversal from a source region, then to a core region, and finally to target region. Consequently, the total number of TLOCs that are transmitted consists of the local border TLOC, the remote border TLOC, and the target region TLOC (as described previously). Under certain conditions, traffic may need to traverse multiple regions to reach a target region, as shown in Figure 7, below.

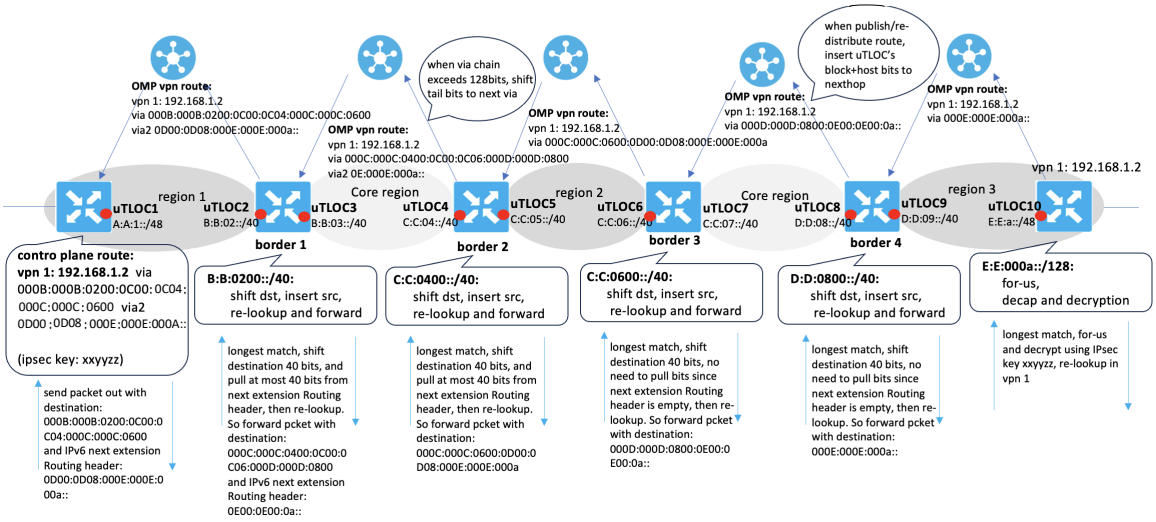

Figure 7: Exemplary Network Environment

As shown in Figure 7, above, a packet may flow from region 1's edge router, to region 1's border router, to region 2's local border router, to region 2's remote border router, to region 3's border router, and then finally to region 3's edge router. Under such an arrangement, the combination of the transmitted TLOC address bits may exceed 128 bits. Consequently, the first 128 of those bits may be placed in a packet's destination and then an IPv6 next extension routing header may be used to store the remaining bits. Then, at an intermediate TLOC when the destination bits are shifted, a check may be made for an IPv6 next extension header from which the appropriate bits may be retrieved (a field in the

extension header indicates if additional bits remain) and then appended to the tail of the instant operation.

It is important to note that the addressing paradigm of the presented techniques (as described and illustrated above) encompasses both publicly routable addresses and, if employed in a particular environment, addresses that have undergone a network address translation (NAT) process (where, for example, an edge's address may comprise 48 bits and a border's address may comprise 40 bits).

In summary, techniques have been presented herein that address a singular pain point in a hierarchical SD-WAN deployment comprising an IPv6 transport – end-to-end encryption and decryption. Aspects of the presented techniques leverage the IPv6 address schema to support a new concept that may be referred to herein as a uTLOC. Under the presented techniques, when an OMP VPN route is published a next hop may be set to the combination of all of the uTLOCs along a path. Within such a context, each router (along the path) may program a customized action (such as, for example, the shifting of a destination, an insertion into a source, etc.) into a routing table for a uTLOC prefix and then forward a packet to a destination edge without the need for decryption and re-encryption operations in an intermediate border router.