April 2023

SYSTEMS AND METHODS FOR SECURELY CONNECTING HETEROGENEOUS L3 NETWORK WITH SDWAN

Satyajit Das

Laxmikantha Reddy Ponnuru

Arul Murugan Manickam

Surya Mohapatra

SYSTEMS AND METHODS FOR SECURELY CONNECTING HETEROGENEOUS L3 NETWORK WITH SDWAN

AUTHORS:
Satyajit Das
Laxmikantha Reddy Ponnuru
Arul Murugan Manickam
Surya Mohapatra

ABSTRACT

At present, there are different methods and systems for connecting L3 heterogenous data networks. Current software-defined wide area network (SDWAN) solutions provide a secure way of interconnecting branches or data centers with various deployment models. However, existing solutions do not allow for connecting Internet Protocol version 6 (IPv6)-only networks to Internet Protocol version 4 (IPv4)-only networks. Presented herein are techniques for providing an efficient and secure way of connecting IPv4-only branches with IPv6-only branches and vice versa. In one instance, techniques presented herein provide for connecting an IPv4-only branch with an IPv6-only branch when the controller is located in the IPv6-only network. In another instance, techniques presented herein provide for connecting an IPv4-only branch with an IPv6-only branch when the controller is located in the IPv4-only network.

DETAILED DESCRIPTION

A recent SDWAN adoption requires connecting IPv6-only branches to Internet Protocol version 4 IPv4-only branches without making any changes to existing infrastructure. For example, assume an enterprise branch in Japan needs to be connected with a branch in the United States. If the Japanese region has an IPv6-only network and the American region has an IPv4-only network, connecting the two branches is not possible with the existing solutions. Additionally, SDWAN vendors currently do not provide a secure solution for connecting IPv6-only branches with IPv4-only branches, which is a critical requirement for some customers.

To explain the current problem, Figure 1, below, illustrates an example in which a router in an IPv4-only network attempts to connect with routers connected with an IPv6-only network.

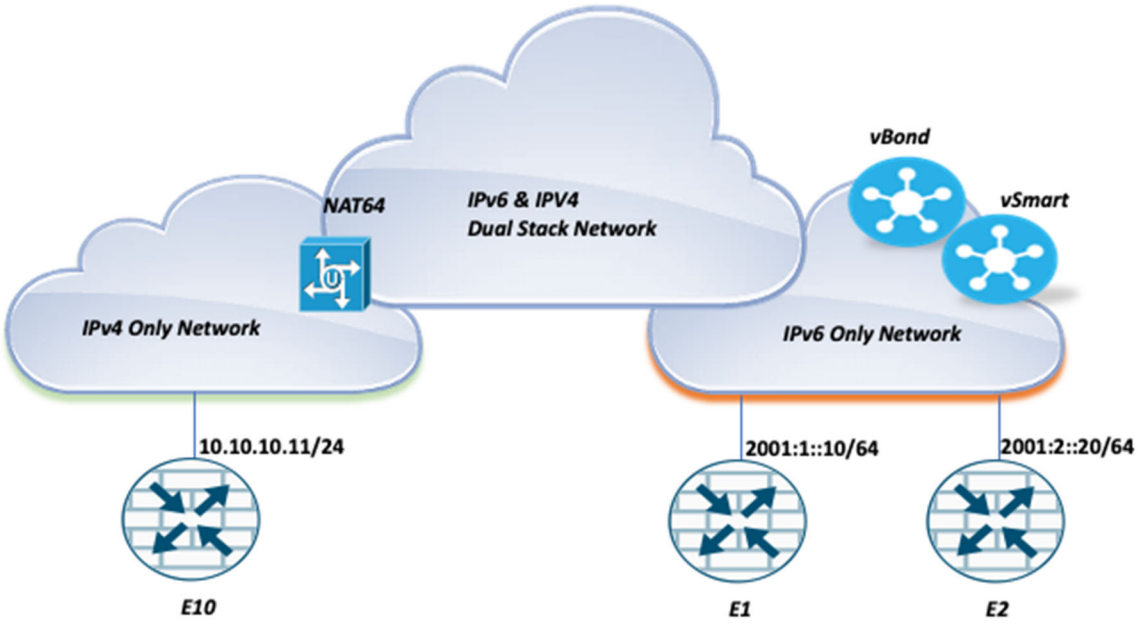

Figure 1: Example Network Diagram

For the example diagram illustrated in Figure 1, consider that branch router E10 is connected with an IPv4-only network and branch routers E1 and E2 are connected with an IPv6-only network. In addition, consider that the provider's network is a dual stack network that supports both IPv4 and IPv6 and the controllers are located in the IPv6-only network. In this example, routers E1 and E2 are already part of an SDWAN cloud and are securely connected. Consider that a customer adds router E10 with an IPv4-only network.

When router E10 attempts to connect, a number of steps occur as part of the bootstrapping process. As a first step, consider that a Plug and Play (PnP) agent bootstraps the E10 router and identifies the host name of an onboarding agent. As a second step, consider that the E10 router performs a Domain Name System (DNS) procedure to obtain the address of the onboarding agent. In a third step, consider that the router E10 obtains an IPv4 translated address for the onboarding agent with the aid of translation mechanisms NAT64 and DNS64. In a fourth step, consider that router E10 registers itself with the onboarding agent.

Next, as a fifth step, consider that the controller updates router E1 and router E2 with a transport locator address of router E10. In this step, the remote transport locator address is mapped to the IPv6 address (*::FFFF:10:10:10:11*). As a sixth step, the controller similarly updates router E10 with the transport locator addresses of router E1 and router E2. In this step, router E10 is updated with the IPv6 addresses of router E1 and router E2.

Consider that, on receiving the remote transport locator addresses, router E1 and router E10 will create a session entry, as shown in Figure 2, below, for the router E1.

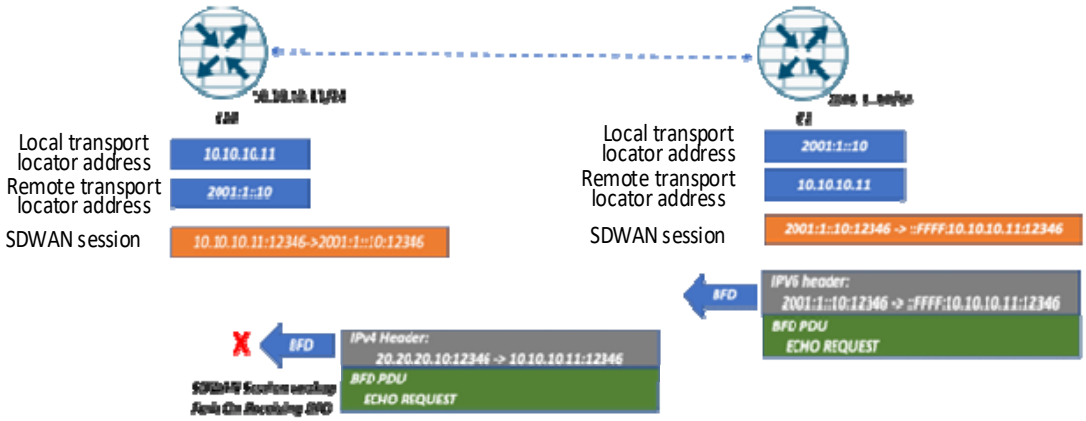

Figure 2: Example Connection Failure

As illustrated in Figure 2, a Bidirectional Forwarding Detection (BFD) packet generated by router E1 will be dropped at router E10 on session lookup as the source 2001:1::10. The NAT64 modifies the source 2001:1::10 to the IPv6 address 10.10.10.11. Consider that, with the above setup and topology, the BFD and SDWAN cannot become up.

Consider that the router E10 cannot generate a BFD packet because the source is an IPv4-only network and the destination is an IPv6-only destination. Router E10 is able to receive remote transport locator packets, but cannot connect directly because the equivalent IPv4 address of router E1 is unavailable to router E10. The NAT64 will translate the packet to ::FFFF:10:10:10:11:12346. However, because the E10 router is expecting a packet with the address 2001:1:1::10:12346, but received a packet with the IPv6 address of ::FFFF:10:10:10:11:12346 in the header, the packet will be dropped.

Presented herein are techniques for securely connecting IPv4-only branches with IPv6-only branches by introducing a Type Length Value (TLV) in the BFD protocol data unit (PDU) that contains details about the original session. Consider that, in the above example described with respect to Figures 1 and 2, the first session lookup by the SDWAN forwarding has failed. However, as illustrated in Figure 3, below, consider that a second lookup will pass because the TLV of the BDF PDU contains a valid IPv6 address of the E1 router. In this example, the BFD packet is accepted and the connection is successful.

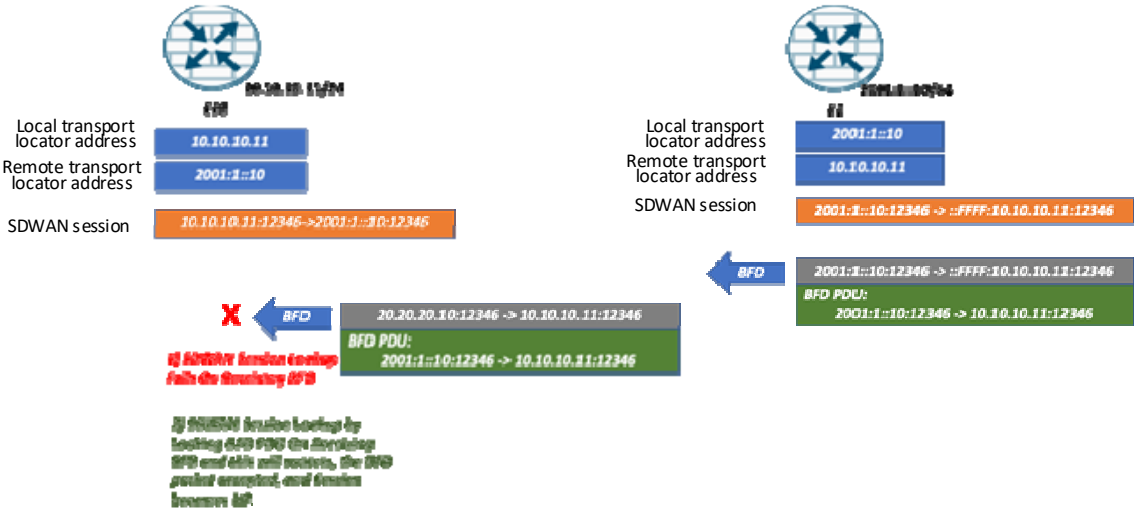

Figure 3: Example Successful Connection

In a similar manner, the solution may be extended to a situation in which the controllers have an IPv4 address and a branch router has an IPv6 address. In this situation, consider that the TLV in the BFD PDU contains the session information about the IPv4 address of the remote branch router. The session information facilitates establishing the BFD session.

In summary, as provided by the techniques described herein, the original session information can be securely carried in order to establish a BFD connection between a heterogeneous network belonging to two different address families. In this way, an SDWAN vendor can provide a method for connecting an IPv6 edge device to an IPv4 WAN edge device.