**Comparison: VXLAN vs NVGRE vs STT vs LISP - Overlay Network Technologies**

[3:16:00 AM](https://www.routexp.com/2020/03/comparison-vxlan-vs-nvgre-vs-stt-vs.html)  [Datacenter](https://www.routexp.com/search/label/Datacenter)

Today I am going to talk about the new protocol which i am damn sure most of you people are not aware of it. Now a days the concept of network overlays is used and in network overlays people have gained interest in the past few years because of their potential to address some of the requirements which are beneficial for the enterprise networks.  
  
With the time, there are lot of new encapsulation frame formats purpose-built for the data center, including Virtual Extensible LAN (VXLAN), Network Virtualization Using Generic Routing Encapsulation (NVGRE), Transparent Interconnection of Lots of Links (TRILL), and Location/Identifier Separation Protocol (LISP). So as we go through this article you will came to know some of the overlay transport protocols and they are 

* VXLAN: Virtual Extensible LAN
* OTV: Overlay Transport Virtualization
* LISP: Locator/Identifier Separation Protocol
* NVGRE: Network Virtualization Using Generic Routing Encapsulation
* STT: Stateless Transport Tunneling

Apart from the underlay network(IP network), Network overlays are virtual networks of interconnected nodes that share an underlying physical network, allowing deployment of applications that require specific network topologies without the need to modify the underlying network.  
  
With the help of Network overlay, you can optimise the device functions and also reduces the complexity of the network devices. In the case of server-based overlays, this function is implemented on the server. In the case of network-based overlays, this function is implemented on the first switch (at the top of the rack). With the help of Ovelay networks you can achieve and provide scalable Layer II networks for a multitenant cloud that extends beyond 4000 VLANs. This capability is very important for private and public cloud hosted environments.

You can also maintain the fabric scalability and flexibility, because the overlay virtual network no longer needs to be constrained to a single physical location. The overlay encapsulation also allows the underlying infrastructure address space to be administered separately from the tenant address space.

In this article I am going to talk about the NVGRE and STT protocol as an overlay protocol. NVGRE stands for Network Virtualization Using Generic Routing Encapsulation. So now question is what this NVGRE is all about ? How it is different from the other overlay protocols and why and where we are using this protocol

**NVGRE-Network Virtualization Using Generic Routing Encapsulation**

Well, NVGRE allows the creation of virtual Layer 2 topologies on top of a physical Layer 3 network. With the help of NVGRE you can achieve by tunneling Ethernet frames inside an IP packet over a physical network. NVGRE supports a 24-bit segment ID or virtual subnet identifier (VSID) similar to VXLAN, providing up to 16 million virtual segments that can uniquely identify a given segment.

The difference between VXLAN and NVGRE is that NVGRE header includes an optional flow ID field. In multi-pathing deployments, network routers and switches that can parse this header can use this field together with the VSID to add flow-based entropy, although this feature requires additional hardware capabilities.

|  |
| --- |
|  |
| Fig 1.1- NVGRE Header format |

**NVGRE, header has outer MAC of 18 bytes; outer IP of 20 bytes when using IPv4 and GRE with VSID of 16 bytes.**

As with VXLAN, the NVGRE draft standard does not specify a method for discovering endpoint reachability. Rather, it suggests that this information can be provisioned through a management plane or obtained through a combination of control-plane distribution or data-plane learning approaches.

**Note: Microsoft is one of the major vendor who uses NVGRE concept and still a lot of vendors are doing their efforts to develop NVGRE like Cisco, VMware and Juniper.**

**STT Protocol- Stateless transport tunnelling**

Well, now you understand basics of NVGRE protocol, similar to NVGRE we have another protocol named as STT and is an overlay encapsulation scheme over Layer 3 networks that use a TCP-like header within the IP header. The use of TCP fields has been proposed to provide backward compatibility with existing implementations of NICs to enable offload logic, and hence STT is specifically useful for deployments that are target end systems for example a virtual switches on physical servers.

|  |
| --- |
|  |
| Fig 1.2- STT tunneling |

STT is designed for a specific reason and is specifically addresses the issue of size mismatch between Ethernet frames and the maximum transmission unit (MTU) supported by the underlying physical network. Most of the end host operating systems set the value of the MTU at a small size so that the entire frame plus any additional (overlay) encapsulations can be transported over the physical network.

This setting may result in a potential performance degradation and additional overhead compared to frames that can be transmitted with their desired maximum segment size (MSS). STT seeks to exploit the TCP segmentation offload (TSO) capabilities built into many NICs today to allow frame fragmentation with appropriate TCP, IP and MAC address headers, and also the reassembly of these segments on the receive side.

Lets compare these protocols with VXLAN and LISP protocol to understand more where and what to use when we have the requirement of the overlay networks.

|  |
| --- |
|  |
| Fig 1.3- Comparison: VXLAN, NVGRE, STT and LISP |