
NVO3 Framework and Data Plane Requirement Addition

draft-yong-nvo3-frwk-dpreq-addition-00

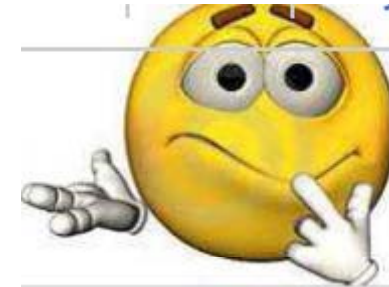
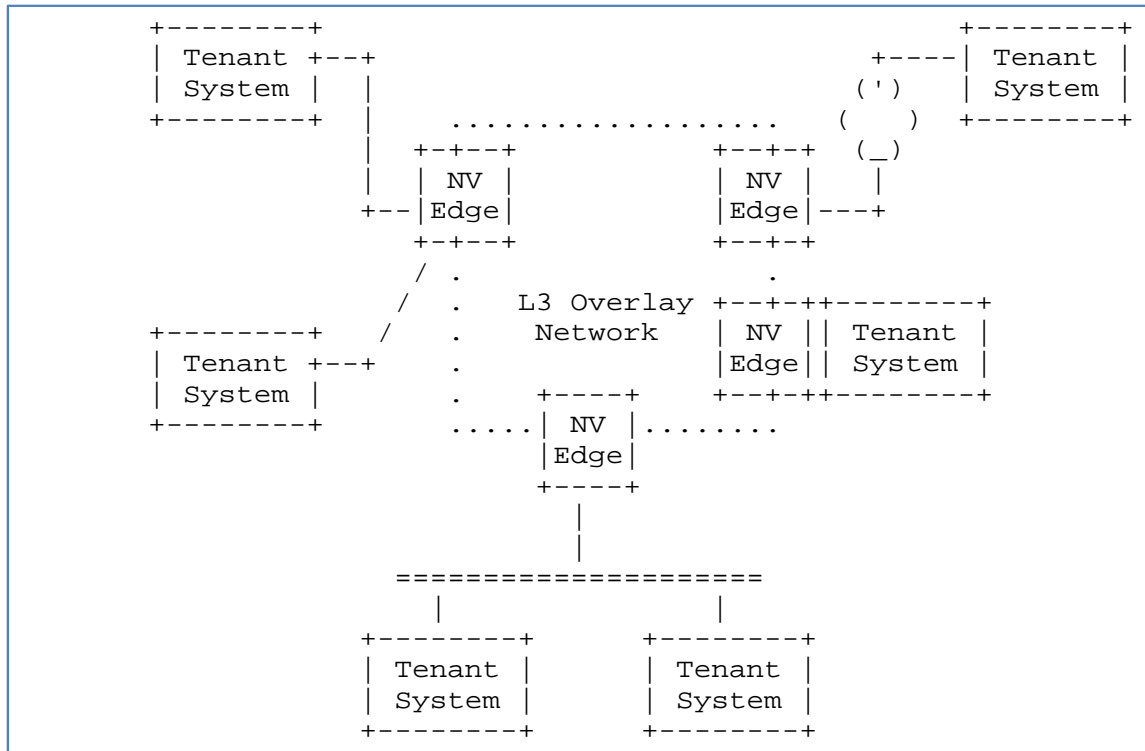
Lucy Yong Linda Dunbar

March 2013 Orlando FL

Abundant Inter-subnet communications in a Data Center!

- Communications between subnets belonging to one tenant
 - There could be still rules, or ACLs, to govern the communication between subnets belonging to one tenant
- Communications between subnets belonging to different tenants
 - The rules, or FW, to govern the communications between subnets belonging to different tenants are more stringent.
- Some end stations have default GW explicitly specified

But the framework only covers the intra-subnet communications



Doesn't it remind you of L2VPN or TRILL?

- The model applies to either an L2 NVO or L3 NVO
- For L2NVO, NVE uses L2 NVE Service Type
- For L3NVO, NVE uses L3 NVE Service Type

Common Network Practice today

- Tenant System, i.e. host, behavior:
 - For intra, insert remote TS MAC/IP as DMAC/Dest. IP on the packet
`DMAC = TS MAC | ... | Dest. IP = TS IP`
 - For inter, insert the router/gateway MAC as DMAC and remote TS IP as Dest. IP on the packet
`DMAC = GW MAC | ... | Dest. IP = TS IP`
 - ARP/ND for hosts to find TS/GW's MAC
- Rules, or ACLs, for Inter-subnet communication are enforced by GW router
 - Either among subnets belonging to one tenant or multiple ones.

What is the problem?

- It is suggested that L3 NVO should be used when it contains more than one subnet
- But...
 - The L3 NVE may not be the default GW specified by the hosts,
 - the data frame received by ingress NVE is destined to GW (as a layer 2 frame), even though the NVE is capable of supporting L3
 - The L3 NVE may not have the rules, or ACLs, specified between any two subnets (or virtual network instances)
- What if NVE acts as a proxy for default GW?
 - It is not L2 NVE, it is not L3 NVE either.
 - What should we call it?

L3 NVO Extension for Inter-Subnet

- Allow NVE to Proxy for “Default GW”
 - Option 1: tenant inter subnet policy MUST be placed at the NVEs
 - NVE performs inter-subnet proxy gateway function
 - Option 2: all NVEs of tenant NVO are aware of a default GW or proxy default GW, and can tunnel the overlay packets to the GW where inter subnet policy/firewall is placed
 - the default gateway performs inter-subnet gateway function
 - VRF table on an NVE only maintains intra subnet TS entries

These NVE functions are not yet described in the framework

Next Step

- Should Inter-subnet communication behavior, and Proxy GW NVE service type be added into the framework?
- or have a separated framework document to address inter-subnet communication in data centers?
 - This draft provides the needed description for either way