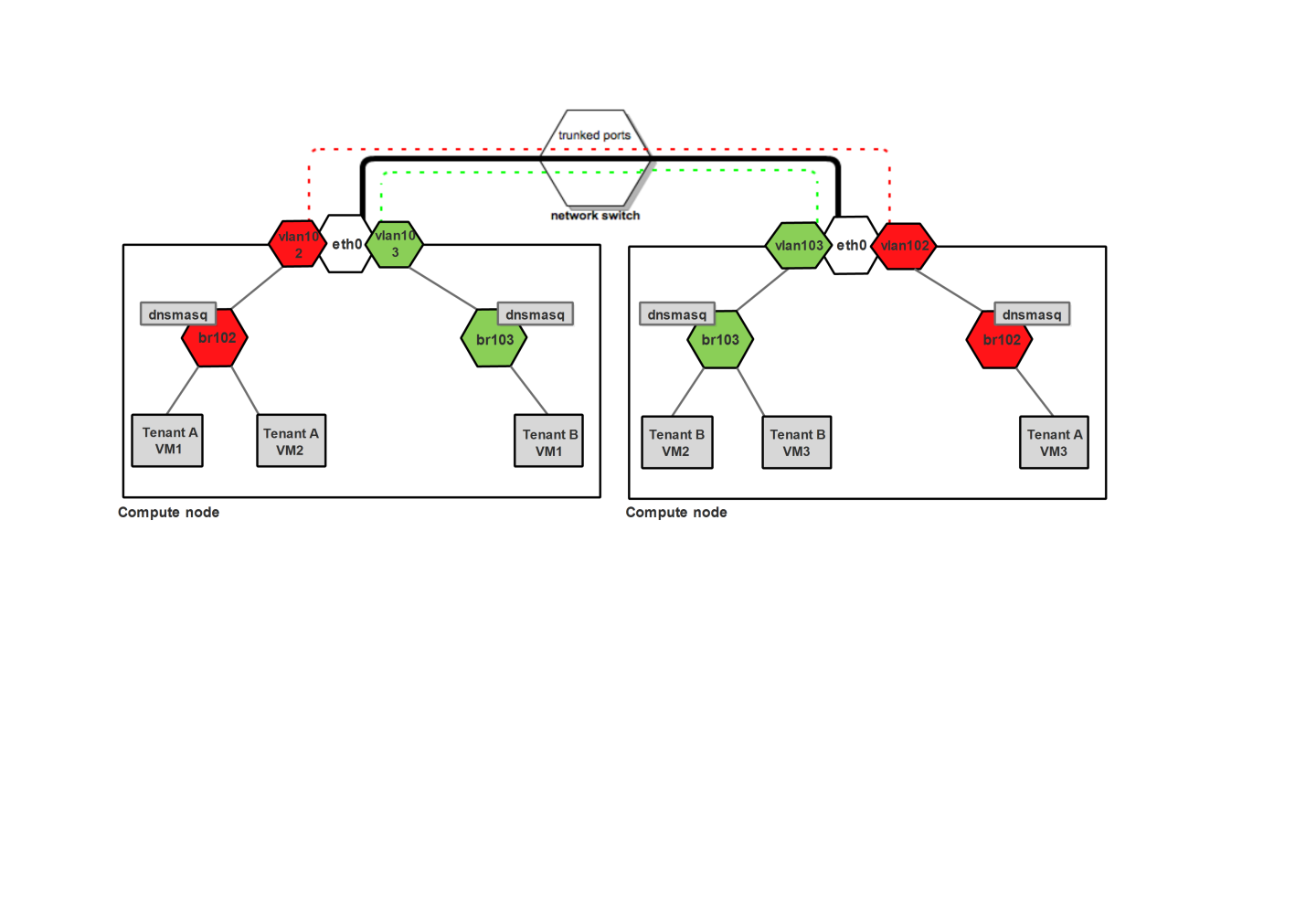
**Network slicing Overview**

Traffic for tenant “Tenant A” leaves the compute node via “vlan102”. Vlan102 is a virtual interface connected to eth0. Its sole purpose is to tag frames with a vlan number “102”, using the 802.1q protocol.

Traffic for tenant “Tenant B” leaves the compute node via “vlan103”, which is tagged with vlan tag 103. By bearing different vlan tags, “Tenant A’s” traffic will in no way interfere with “Tenant B’s” traffic.

They are unaware of each other, even though they both use the same physical interface eth0 and, afterwards, the switch ports and backplane.

Next, we need to tell the switch to pass tagged traffic over its ports. This is done by putting a given switch port into “trunk” mode (as opposed to “access” mode, which is the default). In simple words, trunk allows a switch to pass VLAN-tagged frames.



The thick black line from compute nodes to the switch is a physical link (cable). On top of the same cable, vlan traffic tagged by both 102 and 103 is carried (red and green dashed lines). There is no interference in traffic (the two lines never cross).

So how does the traffic look when tenant “Tenant A” wants to send a ping from VM1 to VM3?

* The packet goes from VM1 to the bridge br102 and way up to vlan102, where it has the tag 102 applied.
* It goes past the switch which handles vlan tags. Once it reaches the second compute node, its vlan tag is examined.
* Based on the examination, a decision is taken by compute node to put it onto vlan102 interface.
* Vlan102 strips the Vlan ID field off the packet so that it can reach instances (instances don’t have tagged interfaces).
* Then it goes down the way through br102 to finally reach VM3 of Tenant A.