Use case for Private Network inside HP Virtual Connect

I have always seen this as a GRAY area and not much light has been thrown, even from the HP perspective. Also there is a misconception happen just by looking at the technical term. I believe the below given explanation will clear the doubt.

A Private network is one where the systems can only talk out the uplink, not to each other (within the enclosure, as it's not enforced outside a single Virtual Connect domain). Suppose you had an out of band management VLAN for monitoring the servers at the OS level and you wanted to be sure that systems could not talk to each other on this VLAN. If you were using switches with the capability, you could use Access Control Lists (ACLs) to restrict which machines could communicate, but Virtual Connect doesn't support ACLs.

Private networks are not the same as isolated networks. They will not pass broadcast and multicast packets to servers in the VC Domain. These packets can be "routed" back inside but would have to leave the VC Domain, pass through a router (or switch / firewall) and come back through the Domain to a server.

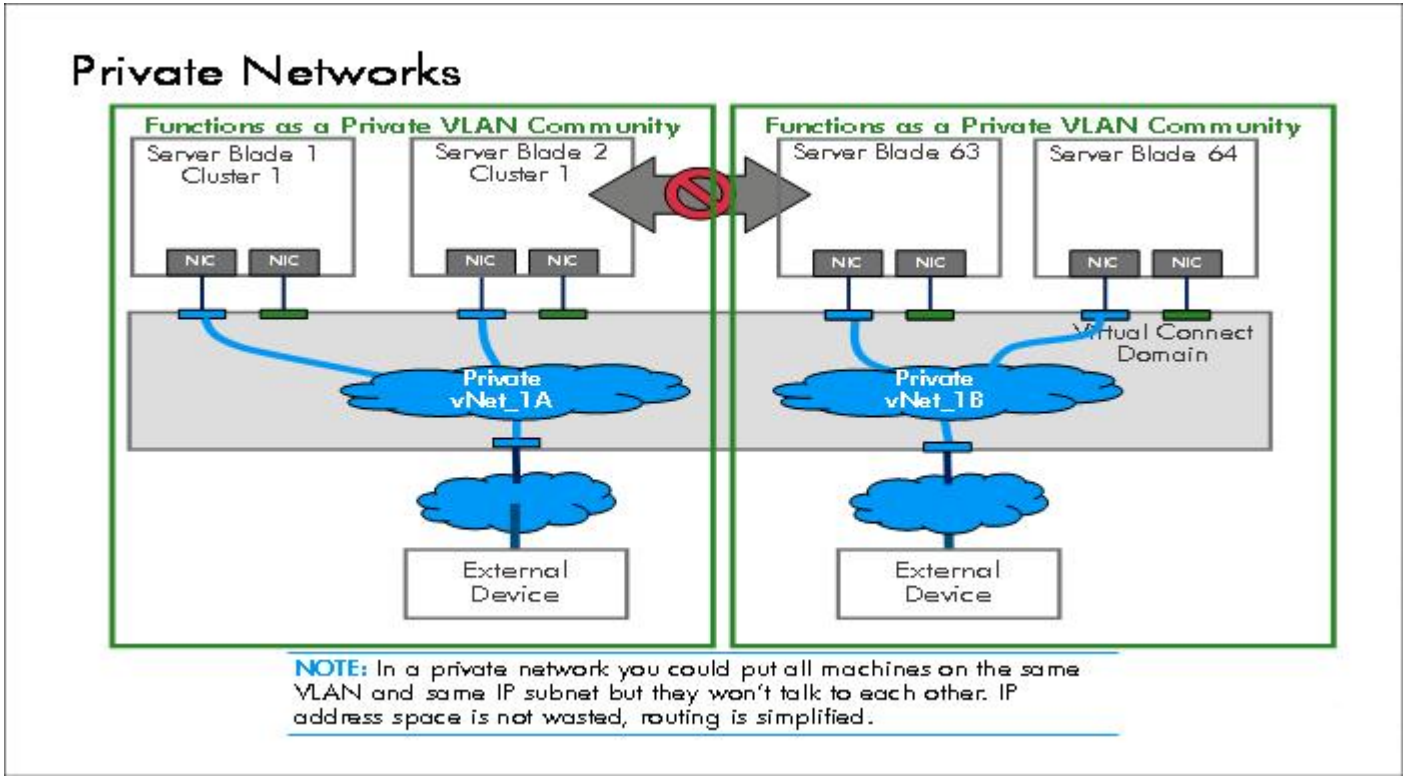
- Eliminates potential denial of service attacks
- Enables management and deployment servers

Note: If the packet hit the upstream switch, and the switch sent it back down the same path, that would be "hairpin mode," which is illegal for any self-respecting L2 device — at least until VEPA.

While Private Networks are similar (isolation of Layer 2) to Cisco's proprietary Private VLAN feature, it is not exactly the same. If you were using Cisco gear you could use their proprietary private networking capability (which is pretty flexible) – but that's Cisco only and works best when you have an end-to-end Cisco environment. VC never routes. It just forwards a packet.

This feature provides a type of firewall function from a Virtual Connect perspective. It merely prevents any switched communications through Virtual Connect between any ethernet ports that are members of the same VC 'private' network. Traffic will be forwarded through the 'private network' uplink ports only. It is the responsibility of the customer network management to configure access control lists or private networks to properly forward or switch the traffic once it leaves VC.

For example:


Private Networks
Functions as a Private VLAN Community
Server Blade 1
Cluster 1
Server Blade 2
Cluster 1
NIC
NIC
NIC
NIC
Private
vNet_1A
External
Device
Functions as a Private VLAN Community
Server Blade 63
Server Blade 64
NIC
NIC
NIC
NIC
Virtual Connect
Domain
Private
vNet_1B
External
Device
NOTE: In a private network you could put all machines on the same VLAN and same IP subnet but they won't talk to each other. IP address space is not wasted, routing is simplified.