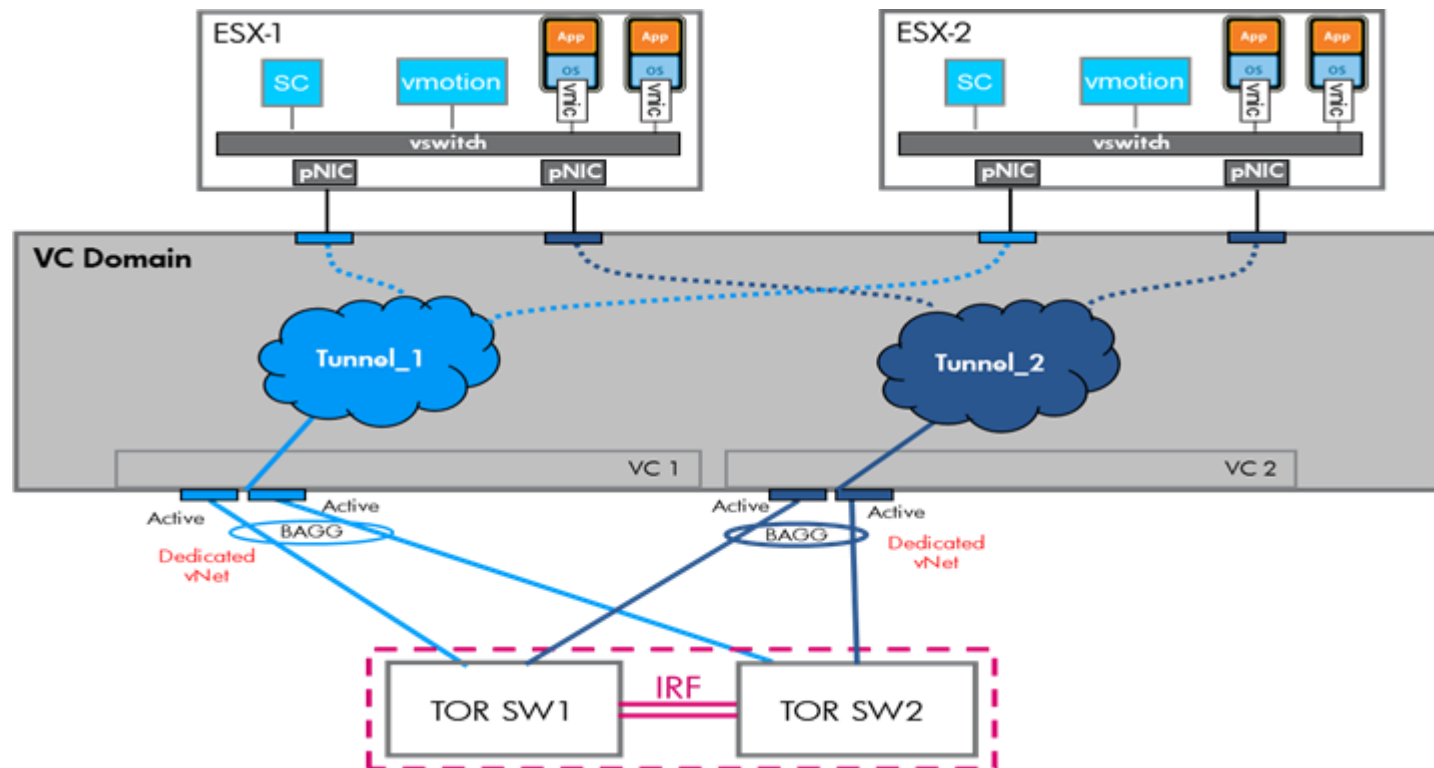


# Best Practice: Mixed Mode VLAN Tag in HP Virtual Connect FlexFabric

After I wrote the previous article to articulate the facts to keep in mind while choosing the Map VLAN Tag and Tunnel VLAN Tag, I thought it would make more sense if I make every one visualize the facts and then help them to choose the best model.

We know that today we are mostly running with VC 3.30/3.51 and there were many advances in both the mode, including maximize the number of VLAN support, Map Mode and Tunnel Mode co-existence. So, based on these facts let us explore the mode individually and then walk through the best model.

VC 3.30 VLAN Tunnelling:



Bridge-aggregation (BAGG) H3C term for Ethernet link aggregation, another name for LACP

In a Cisco Nexus environment it would be vPC in place of IRF (vPC = Virtual Port Channel)

Crossed uplinks shown in these diagrams are optional, and only make sense if IRF, vPC, or similar technology are available. These technologies deployed in this manner increase redundancy, and reduce failover times. Without these technologies, Virtual Connect will be responsible to recover for any network failures. VC failover times are in the neighborhood of 3-5 seconds. This would cause the loss of several pings, many connection oriented network application could fail. vPC/IRF failover times are sub-second. Chances are you wouldn't see any ping loss, and most connection oriented applications will stay connected.

#### Key Advantages:

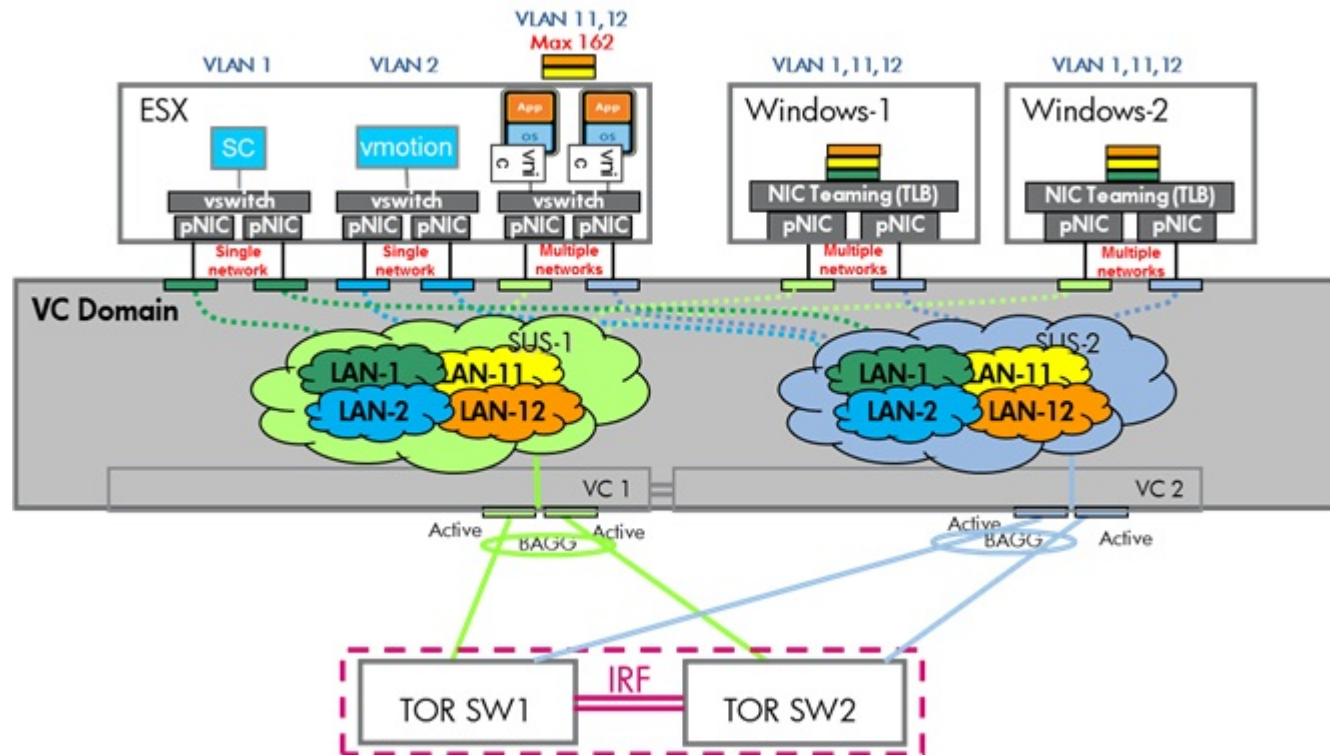
- Support 4094 VLANs
- No need to modify VC config when a VLAN is added
- Just update NetIOC to enable new VLAN on the entire ESX Cluster

#### Disadvantages:

- Misconfigure NetIOC, loses management to entire ESX cluster
- Security limitations: vulnerability to VLAN hopping
- Share the same broadcast domain: all hosts see all broadcast traffic

VLAN hopping (virtual local area network hopping) is a computer security exploit, a method of attacking networked resources on a VLAN. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.

#### VC 3.30 VLAN Mapping mode:



This is the traditional ESX network Configuration we've been using since 2.x

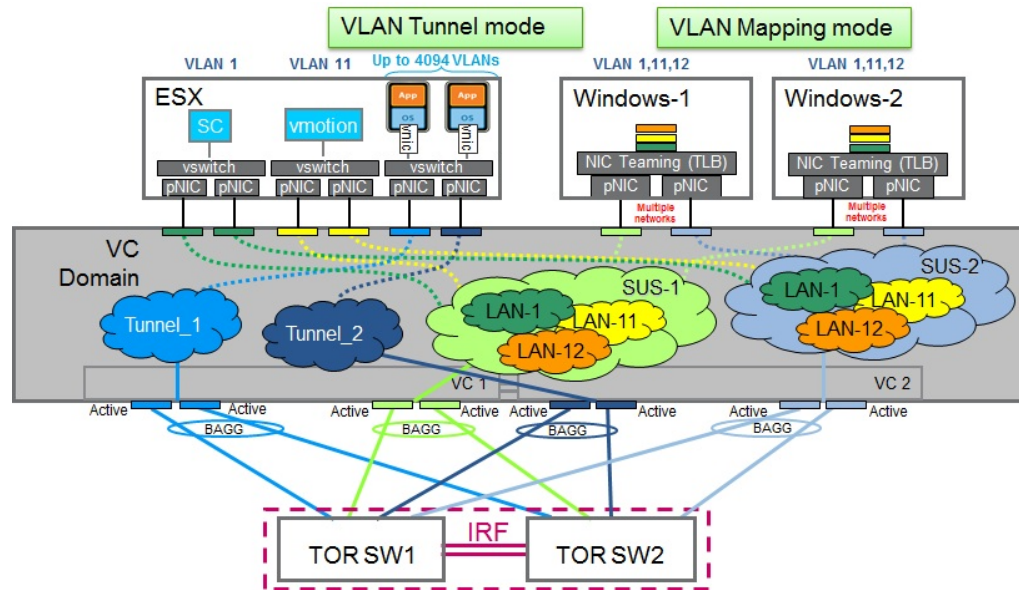
Limitations:

- 162 VLANs per Server NIC
- total 1000 VLANs for all uplinks

More Complex to configure. Adding a VLAN Requires 3 changes

Switch  
VC  
vSwitch

VC 3.30 VLAN Tunnelling & Mapping mode:



#### New Features since 3.30, mixing Mapped and Tunnel modes

- Ease of management due to VLAN Tunnel for VM traffic
- More robust due to dedicated Service Console connection
- Prefer to include vMotion in the VLAN Tunnel
- Only downside is increased number of uplinks from VC

#### Advantages of Mixed Mode VLANs – V3.30

- Simultaneous support for both Mapped and Tunnel VLANs
  - Any dedicated vNet can be configured as Tunnel
  - Tunnel and Mapped vNets cannot share the same uplink port(s)
  - Multiple Tunnel vNets cannot share the same uplink port(s)
  - Tunnel vNets cannot be part of the Shared Uplink Set
- Tunnel and Mapped vNet connections may coexist in the same server profile
  - Even on the same physical port, but different FlexNICs
  - “Multiple Networks” feature in server profiles only works with Mapped vNets

I would like to acknowledge Ken Henault (@bladeguy) for helping me to put forward this.

