Lunch and learn
VCP Networking

Presented by : Joseph Griffiths

@Gortees

contact@jgriffiths.org

Let’s get down to the brass of tacks

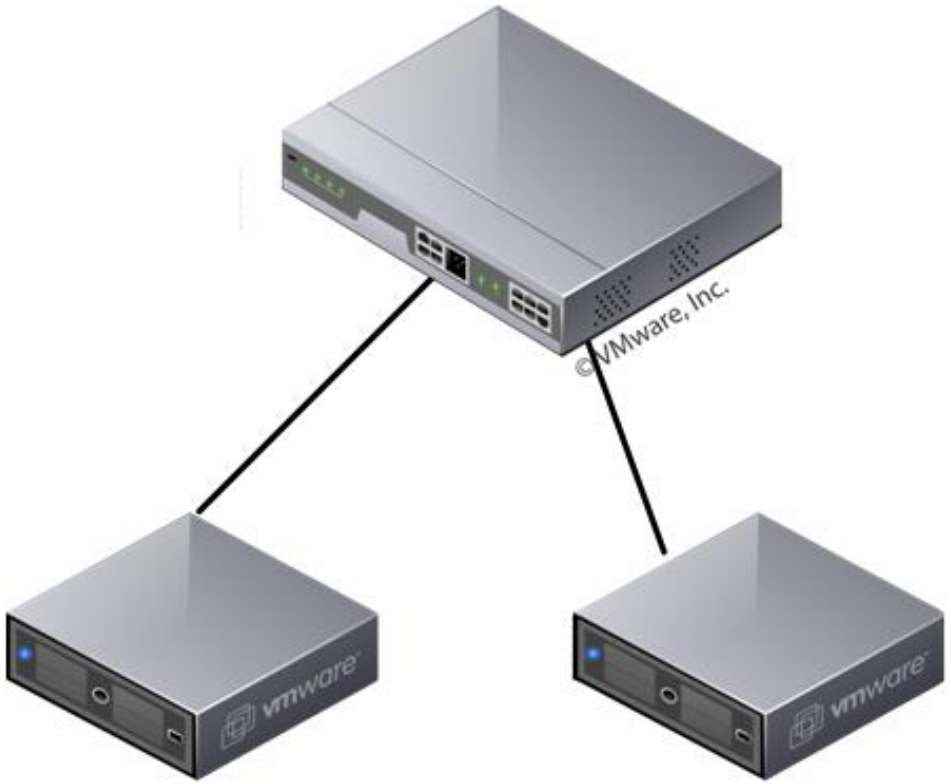
Image from: http://img2.wikia.nocookie.net/__cb20140418040056/despicableme/images/9/9b/000771.jpg

MAC Addresses

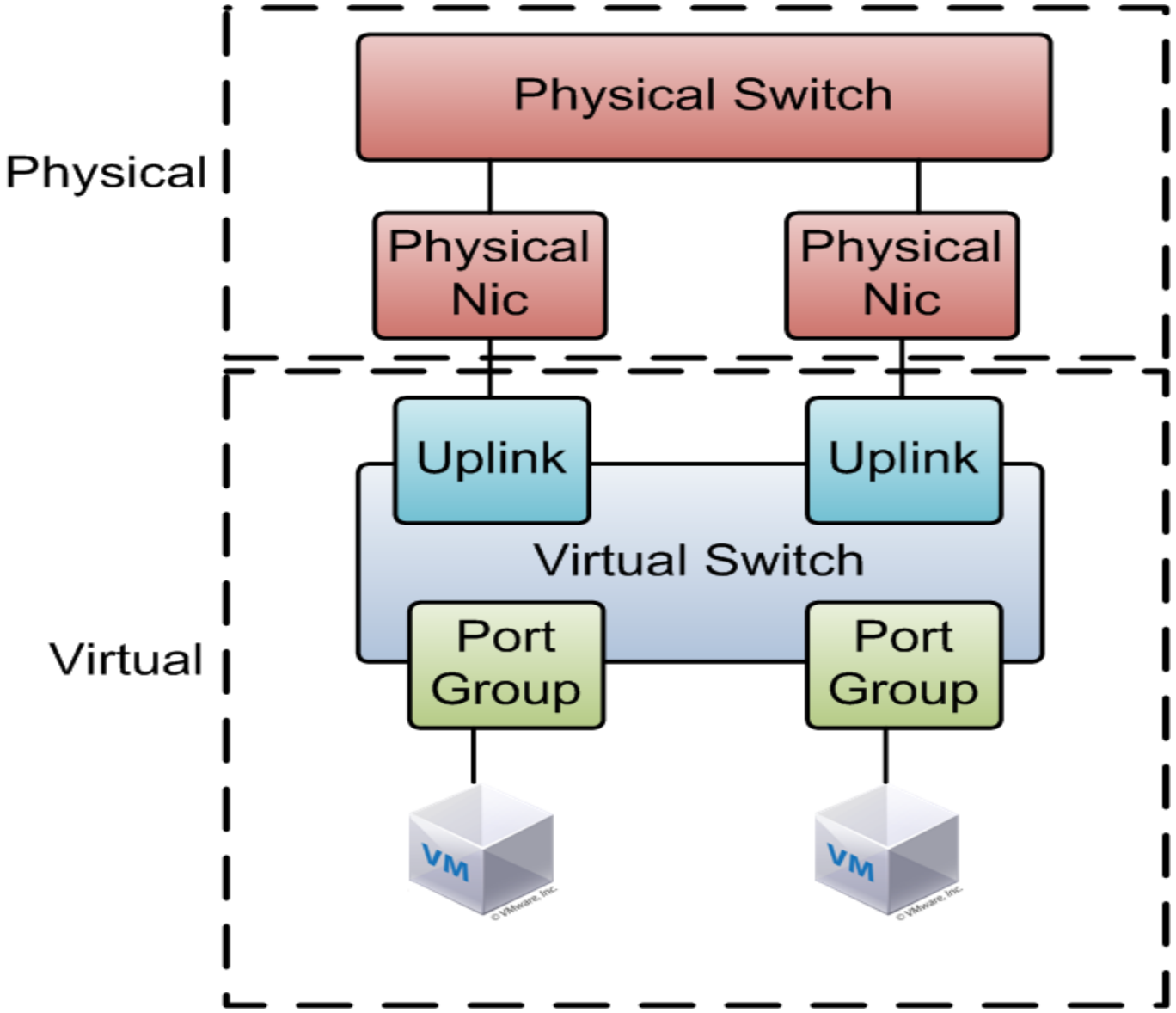
- How does a physical switch learn mac addresses?
- How does a virtual switch learn mac addresses?

What is a virtual switch?

- Layer 2 traffic handler
- Provides VLAN segmentation
- 801.1 Q tagging (VLAN Trunking)
- Network Adapter teaming
- Outbound Traffic shaping



Virtual switch architecture

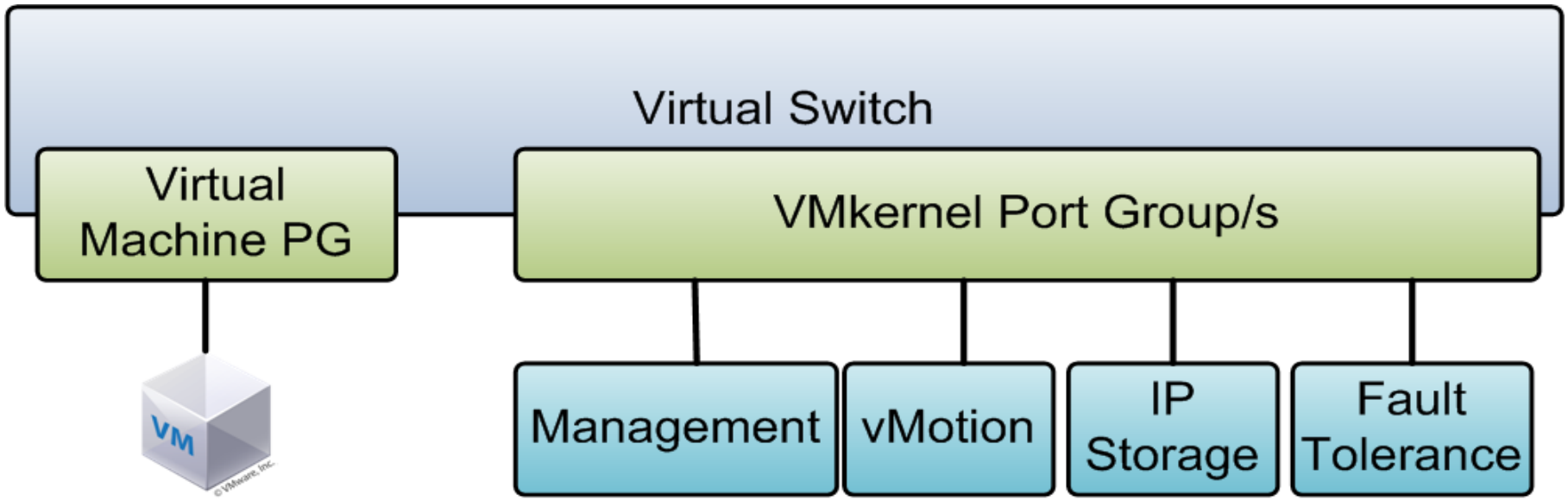


What are virtual ports

- They are just like physical ports on a switch, they can be dynamically allocated.
- Port Types in dVSwitch
  - Static – Port is assigned when machine is connected to port – Network stats persist
  - Dynamic – Allocated when a virtual machine is powered on and nic connected – Network stats lost when powered off or HA
  - Ephemeral – Can be allocated when powered on and nic connected – Network stats lost with any action

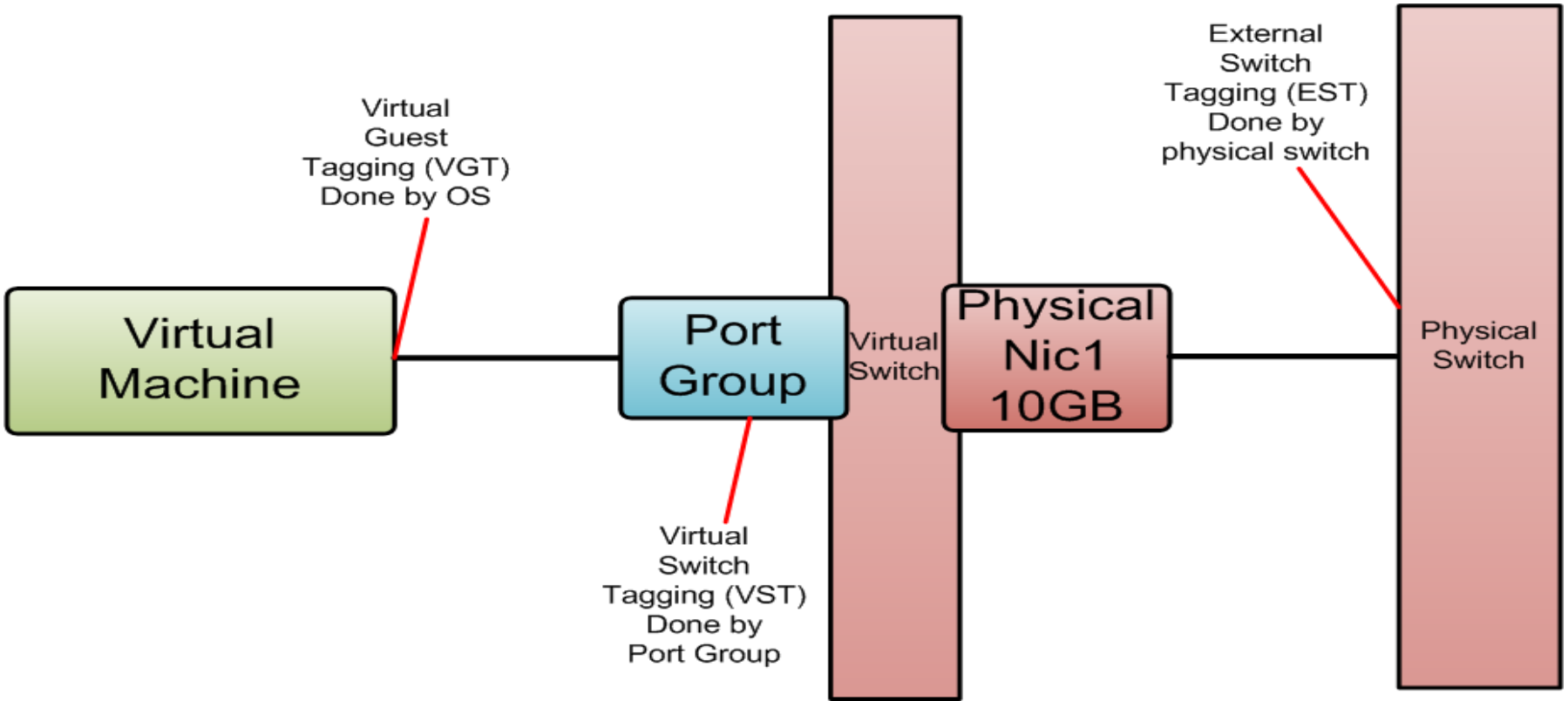
What are port groups?

- They are a virtual set of ports on a switch
- Each of the group of ports can be configured as a single entity
- Port groups provide security settings, traffic shaping, nic teaming and vlan segmentation



VLAN tagging in VMware

- External Switch Tagging (EST)
- Virtual Switch Tagging (VST) – Port group
- Virtual Guest Tagging (VGT)



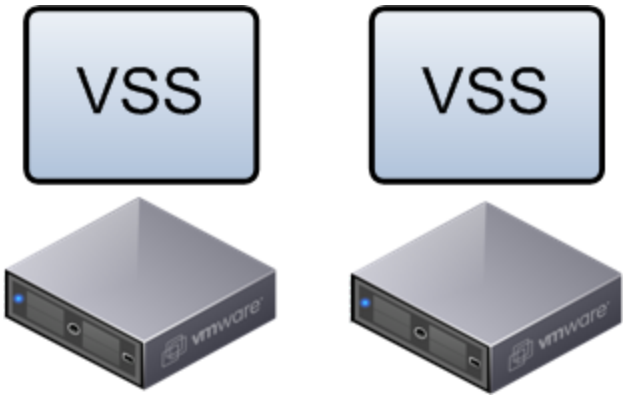
Virtual Switch Security

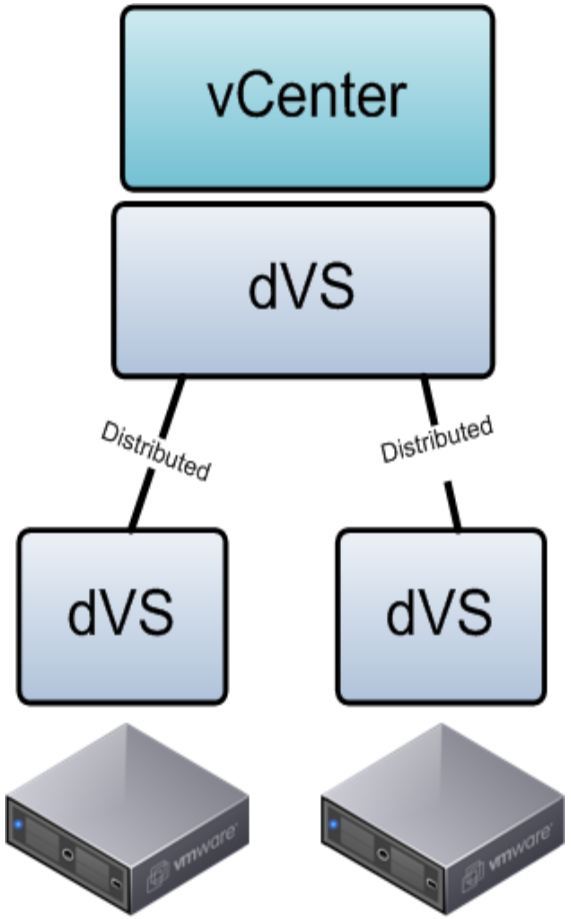
- Promiscuous Mode – Allows a guest OS to sniff all traffic on guests same port group
- MAC address change – Allows you to change the mac address of guest from inside the OS and it works
- Forged Transmits – Allows non-initial OS mac addresses to transmit

- Software iSCSI requires Accept on MAC Address changes
- Microsoft LB unicast requires Forged Transmits and Mac address to be enabled

Types of virtual switch

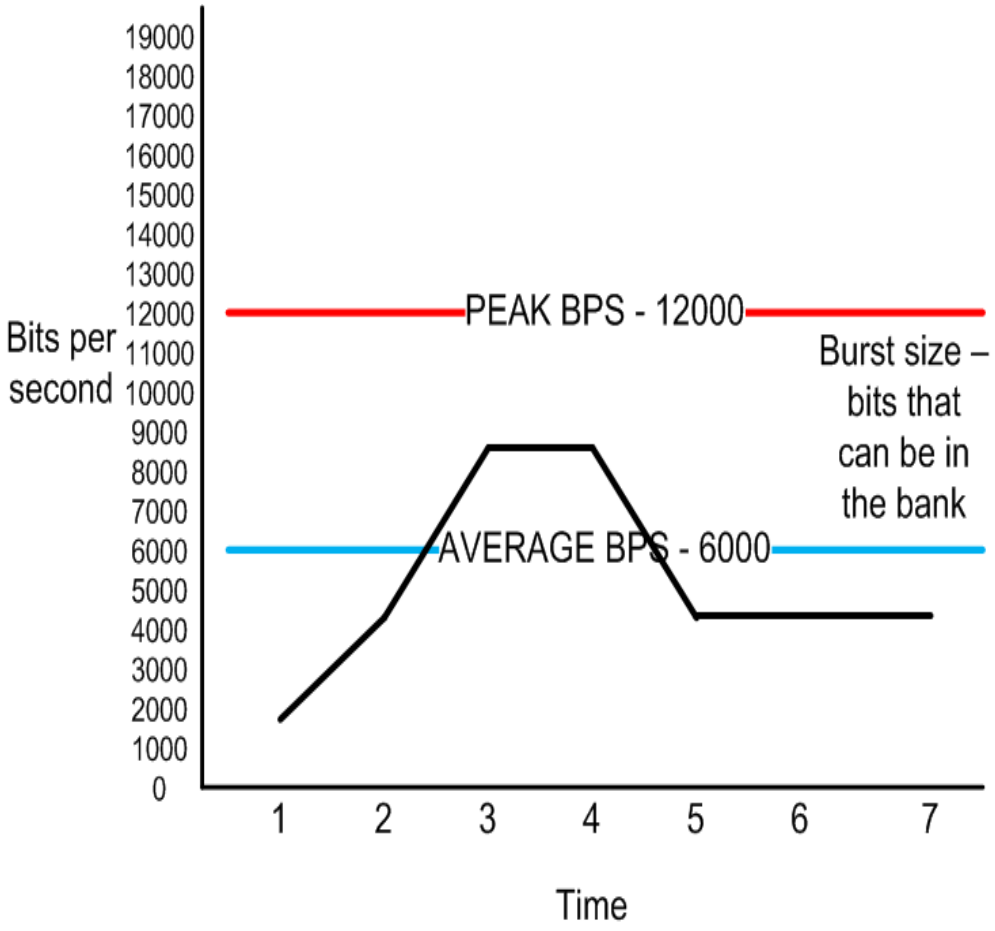
- Virtual Standard Switch (VSS)
  - Original switch works on ESXi without vCenter
  - Individually configured on each host
- Distributed Virtual Switch (dVS)
  - Managed by vCenter
  - Distributed by vCenter to each ESXi Host
  - Requires enterprise plus licensing





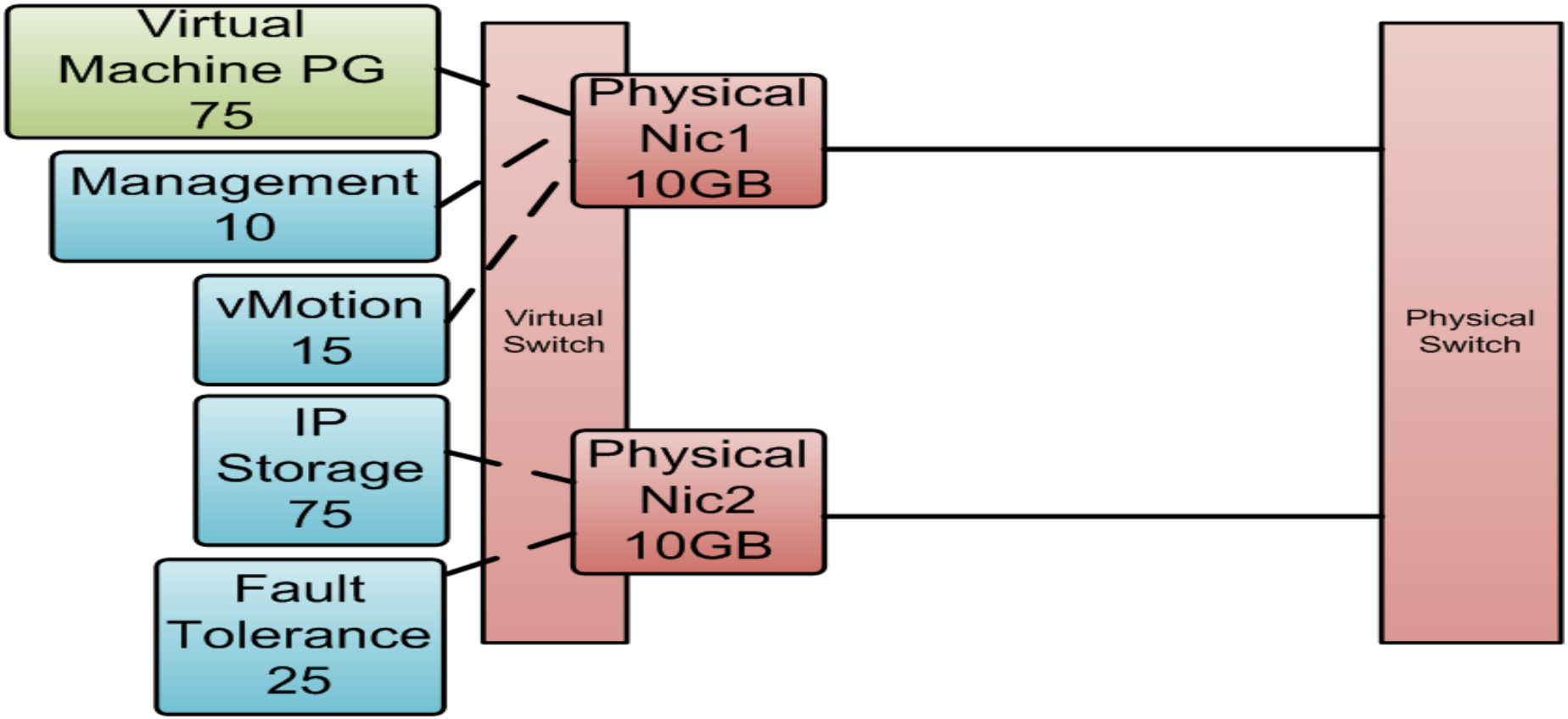
Traffic Shaping with Limits

- Limits can be applied upon port group, dV port group or dV port
- Limits can be applied on outbound traffic on VSS
- Limits can be applied on inbound and outbound traffic on vDS



Traffic Shaping with NIOC

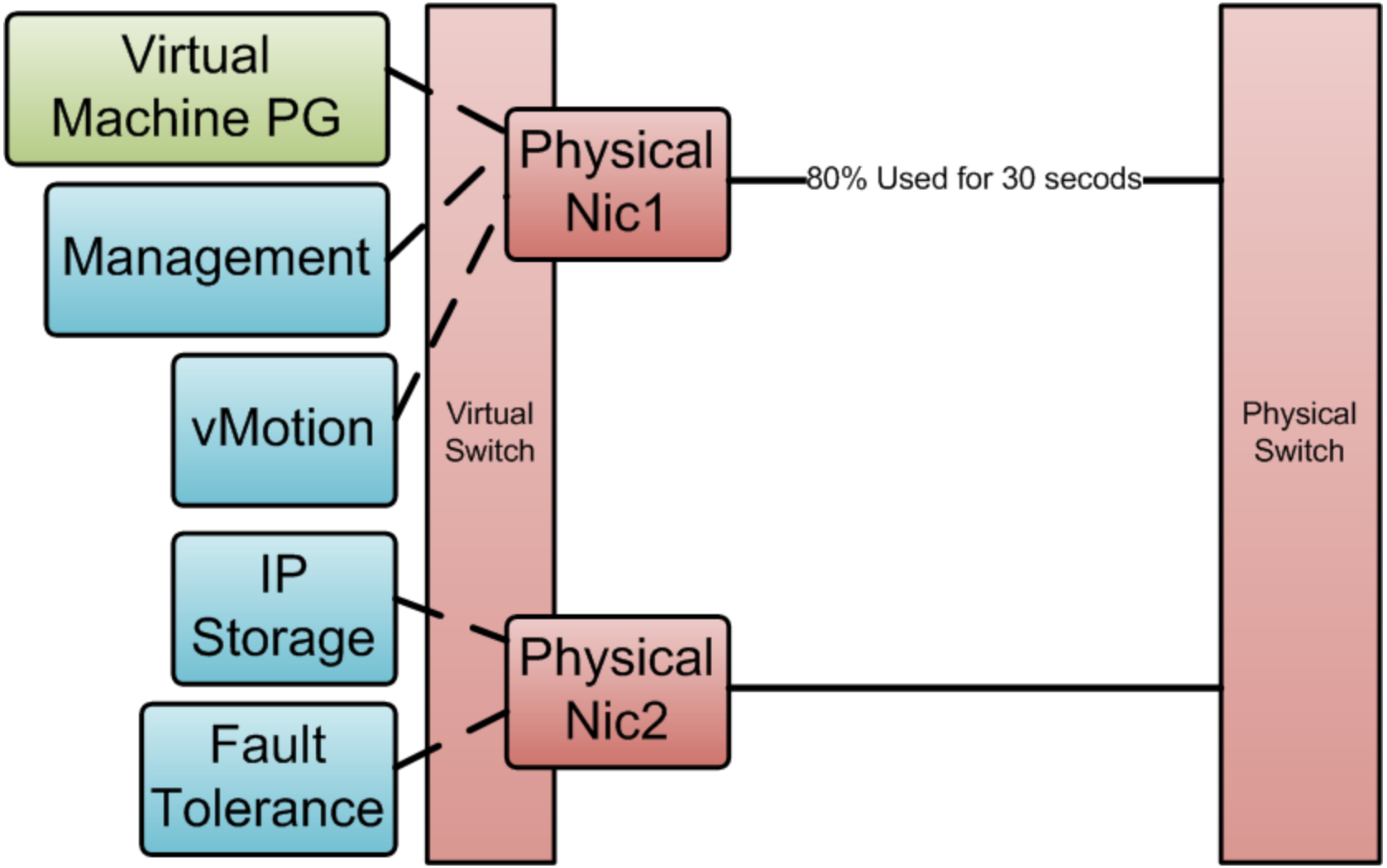
- NIOC – Network IO Control available only on dVS



Load Balancing

- All based upon choosing which physical nic to use for outbound traffic
  - Route based on originating virtual port ID
  - Route based on source mac hash
  - Use explicit failover order
  - Route based on IP hash – requires link aggregation on physical switch
- Which is best to use?

Load Based Teaming dVS only



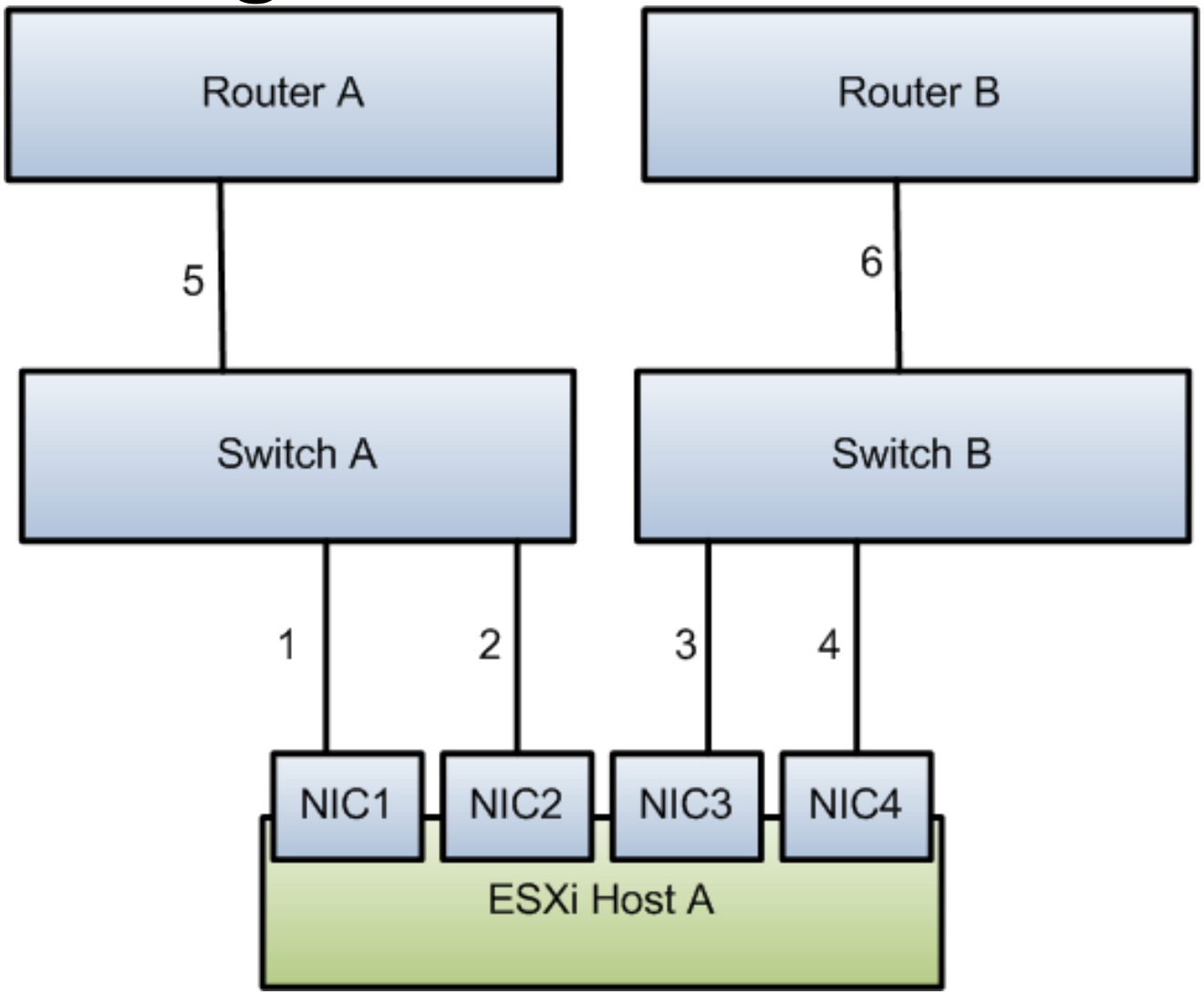
Detecting Link Failures

Methods:

- Link Failure
- Beacon Probing

Options:

- Switch Notification
- Failback



Virtual Standard Switch

- Port groups must be manually configured (case sensitive and spelling sensitive)
- Does not scale well
- Will always work

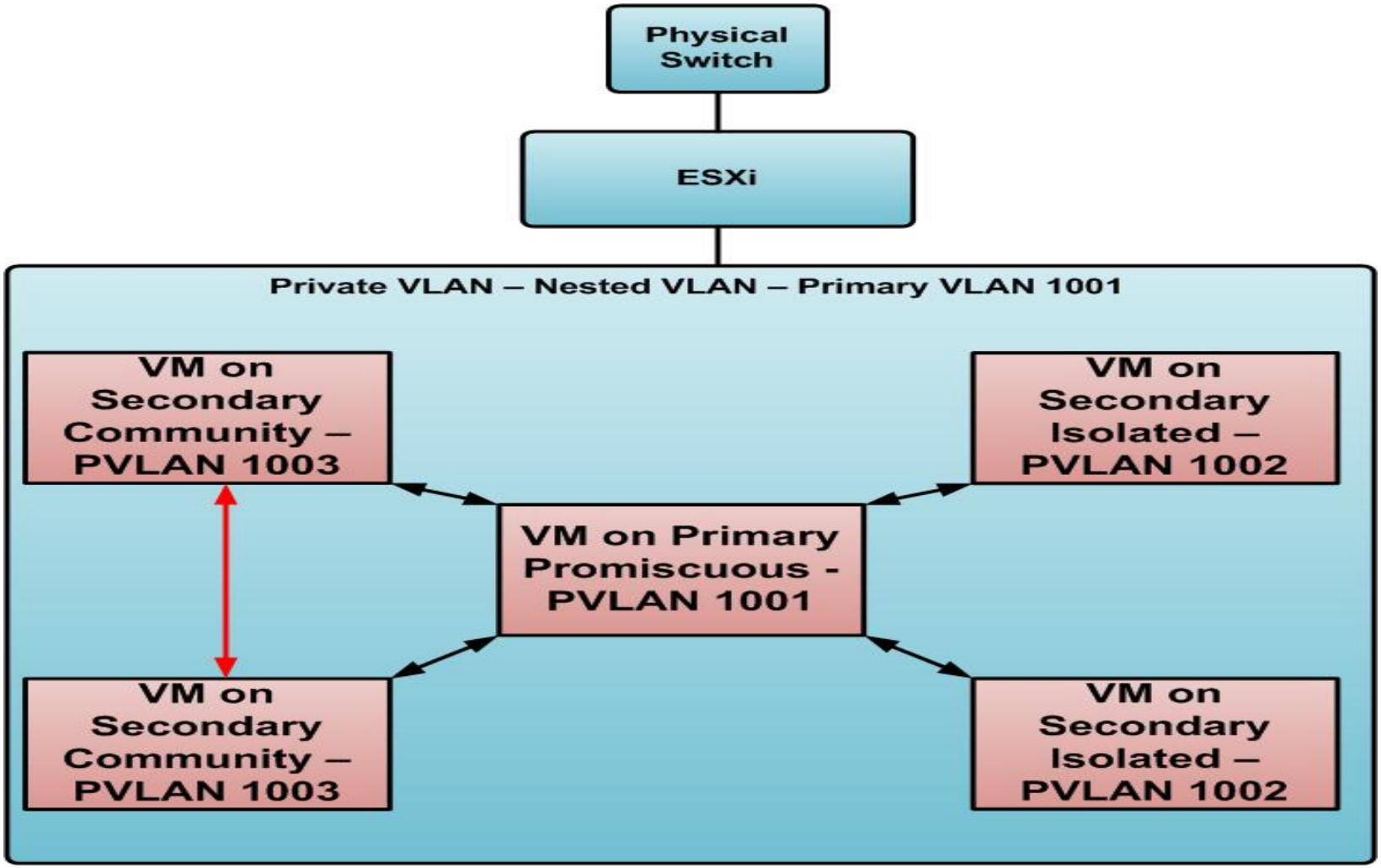
Advice for using VSS

- Use scripts to deploy switches and all port groups
- Always try vMotions after adding or removing a port group
- Don’t go complex on your design (300 VLAN’s don’t use VSS)

Distributed Virtual Switch (dVS)

- Inbound traffic shaping
- VM network port block
- Network vMotion
- Per port policy
- Link Layer Discovery Protocol
- NetFlow
- Port Mirroring

Private VLAN's



Questions?

Twitter: @Gortees

Email: contact@jgriffiths.org