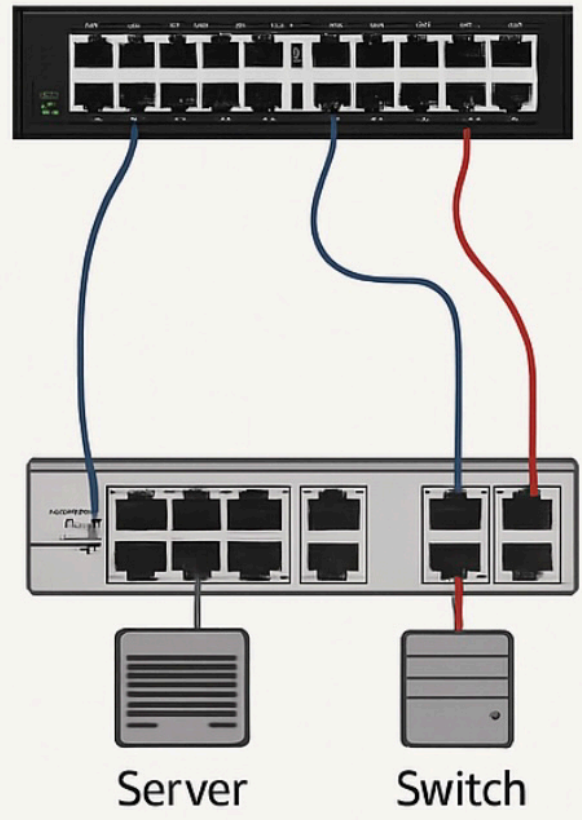


VMware Network

Physical Uplink

- Connecting your Server to Switch
- Connecting two uplink port switch



Two Types of Port

- Access
  - Assign to Single VLAN
- Trunk
  - Carry traffic of Multiple VLANs
  - Connected to another switch

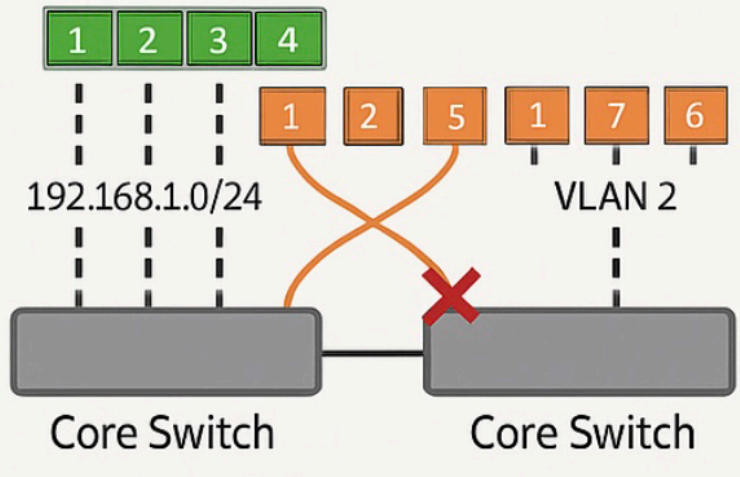
Link Aggregation

Link Aggregation (LAG)

- Bundle multiple network connections
- High availability and higher transmission
- All Ports need to be in the same speed

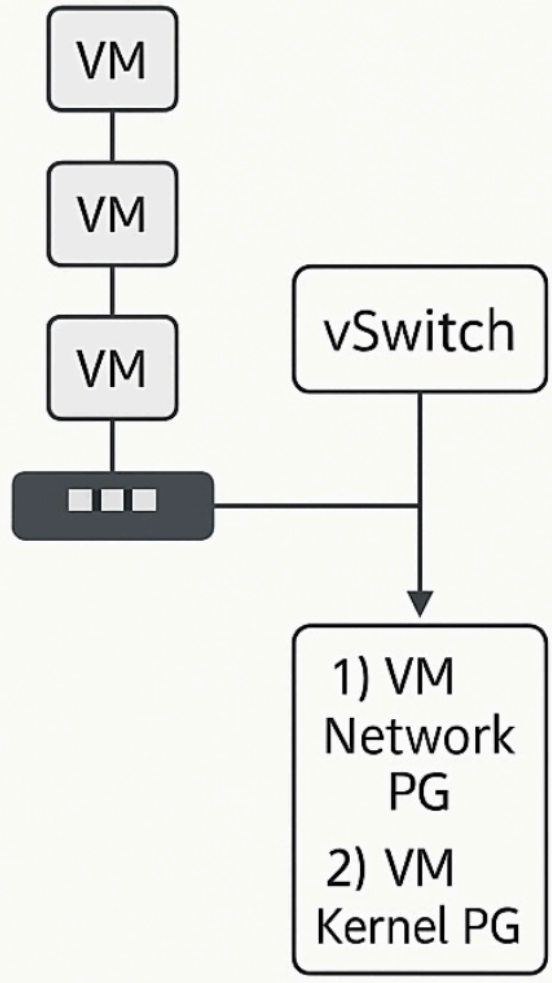
Two Types of LAG

- Static
  - Misconfiguration
- Dynamic (LACP)
  - Automatically remove faulty link



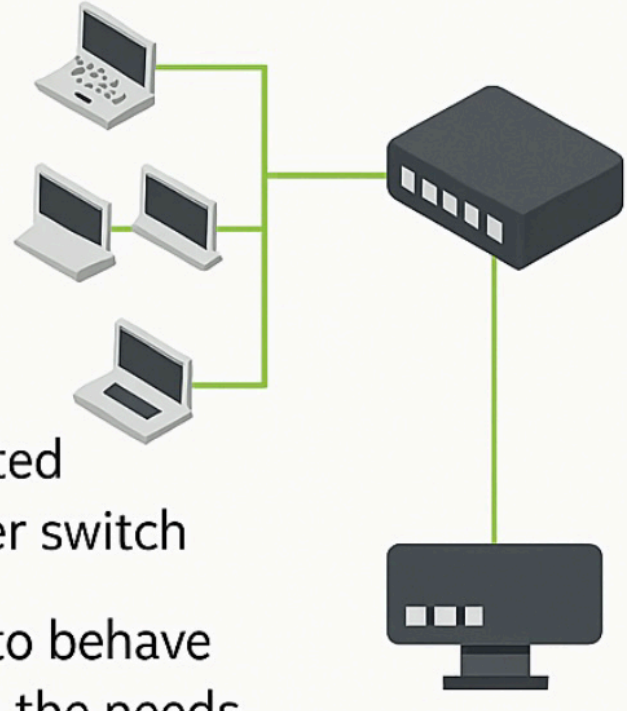
It works much like a physical switch

- vSwitch create a link between physical NIC and virtual NICs
- Virtual switches provide the connectivity between virtual machines on the same host or on different hosts
- Even if virtual switches do not have some of the advanced functionality of a physical swich
  1) A vSwitch can not connect directly to another vSwitch



Physical Switch

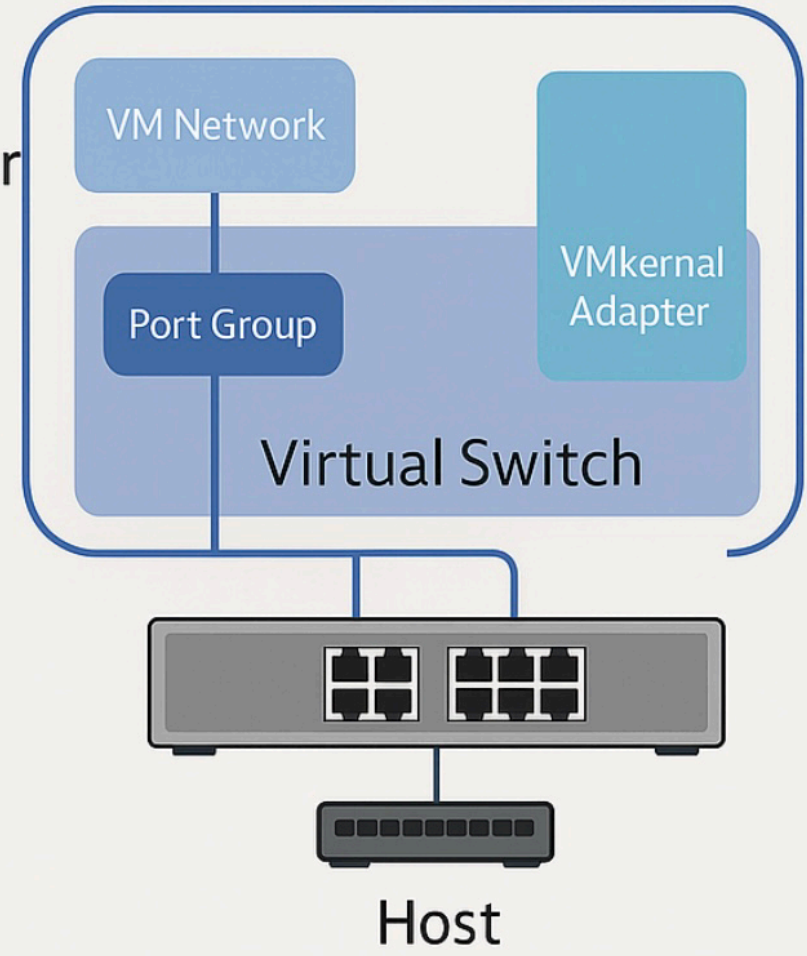
- A physical ethernet switch manages network traffic between machines on the physical network
- A switch has multiple ports, each of which can be oonnected to a single machine or another switch
- Each port can be configured to behave in certain ways depending on the needs of the machine connected to it



Physical Swich

Virtual Switch

- Port group
- VMKernal Adapter
- Uplink Ports



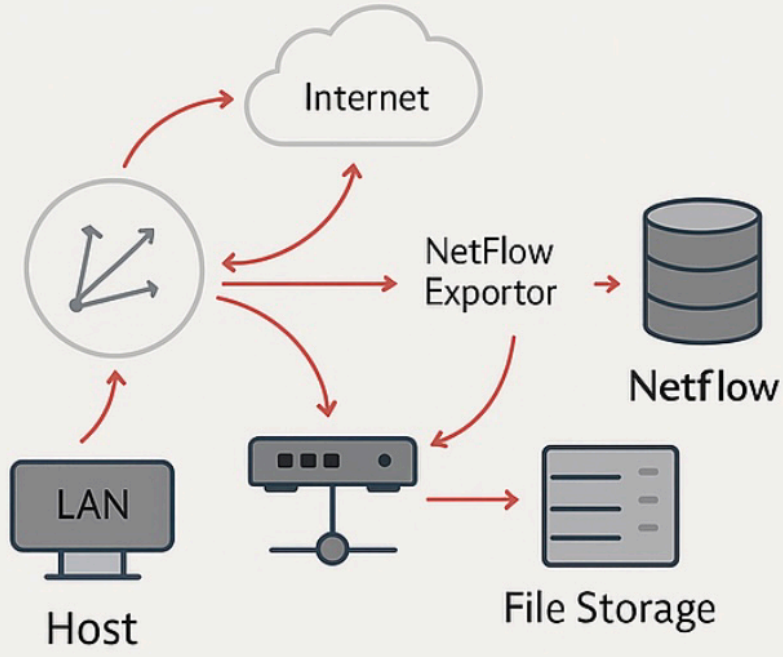


VM

Host

NetFlow

- Provide visibility about traffic flow
- Each flow contains many data points
  - IP Sourction
  - IB Destination
  - Source Port
  - Database
  - Service



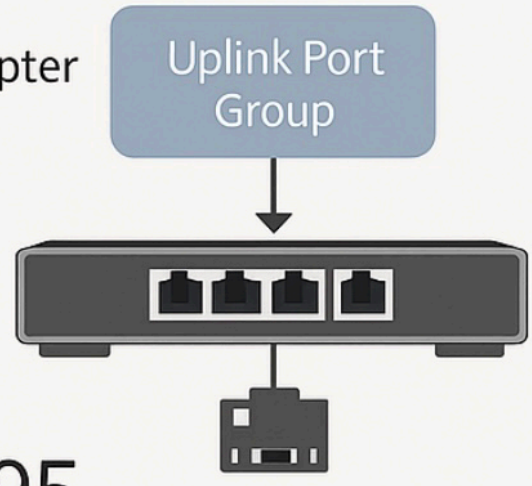
VMKernal Interface

VMKernal Interface

- A type of port used for vSphere services, such Management, viotion, Storage, FT, and replication
- Each Host can have multiple VMKernel Ports assigned and managet via vSS or vDS
- Each host can have a VLAN tag option enabled for all VMKernel ports on a host

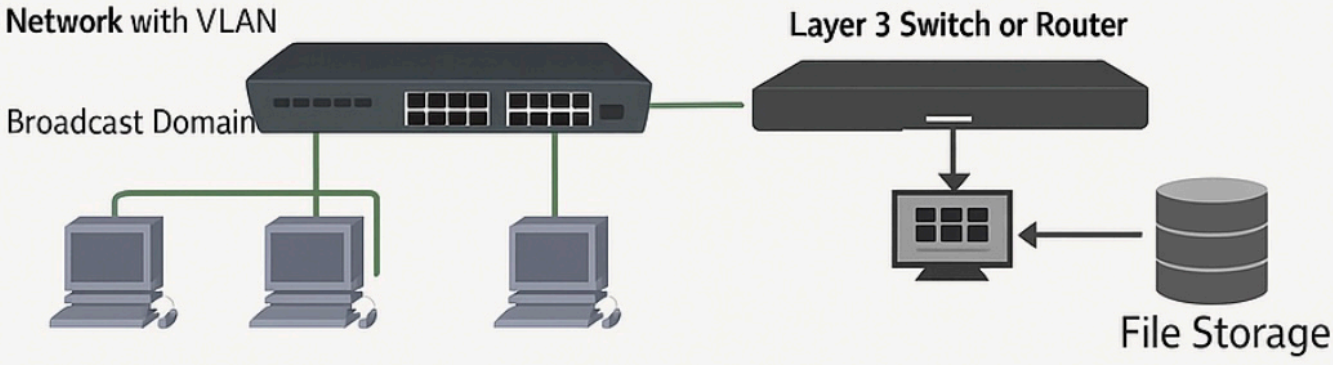
Uplink PortGroup

- Used to connect physical Network adapter from multiple hosts to a single vDS



VLAN Number 0–4095

- VLAN 0 is reserved
- VLAN 1 is usually typécal: ɕault but recommended for use
- Maximum number of VLANs
- Layer 3 routing is usually reqïiow communication between VLANs



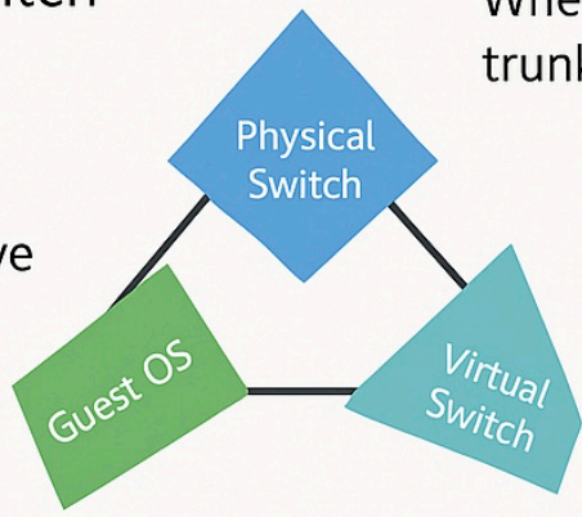
NIC Teaming

- NIC Teaming is a way to **group several physical network adapters** to behave as a single Logical NIC, It enables us to **increase network capacity** of virtual switch by including 2 or more physical adapters in a team.
- The main advantage of configuring NIC Teaming feature is, it **increases network bandwidth** for **virtual switch, load balancing algorithm** on be used to determine how **network traffic** can be distributed among physical NICs in a team.
- It provides **network redundancy** in event of **Adapter** failure or **network outage**.
- **Failover policies** determine how traffic can be forwarded in case of **Adapter failure** or network outage.

Three places where a VLAN can tagged

- Physical Switch
- Guest OS

When you don't have trunk port configured

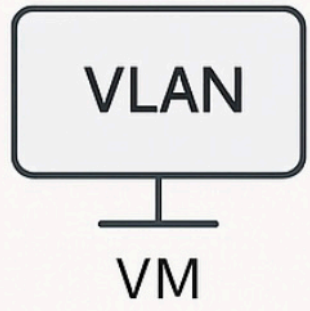


When you have trunk port configured at ESXI Host

When you have trunk port configured at ESXI

Promiscuous mode

- Security policy defined at the virtual switch or port group level
- Mode ON: VM receive all frames passed on virtual switch



Mac Address Changes and Forged Transmits

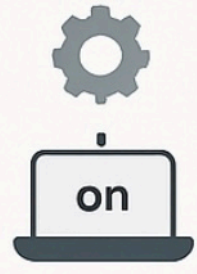
- Reject incoming traffic
- Forged Transmit – Reject outgoing traffic



Initial MAC Address (generated initially)



Effective MAC Address (used to replace initial MAC for communication



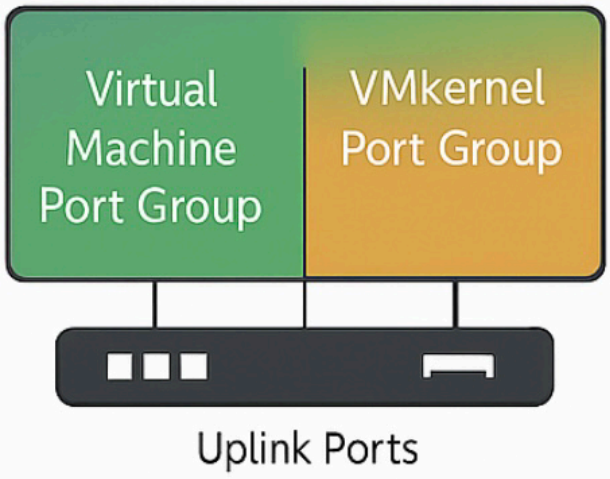
By default as on

What is VMkernel?

VMkernel is a Networking interface between ESXI and Virtual Machine. Provides Layer 2 and Layer 3 services to the ESXI Host. It is responssible for providing physical resources such as CPU, Memory, Storage to virtual ESXI is installed one default VMkarnel is created for management.

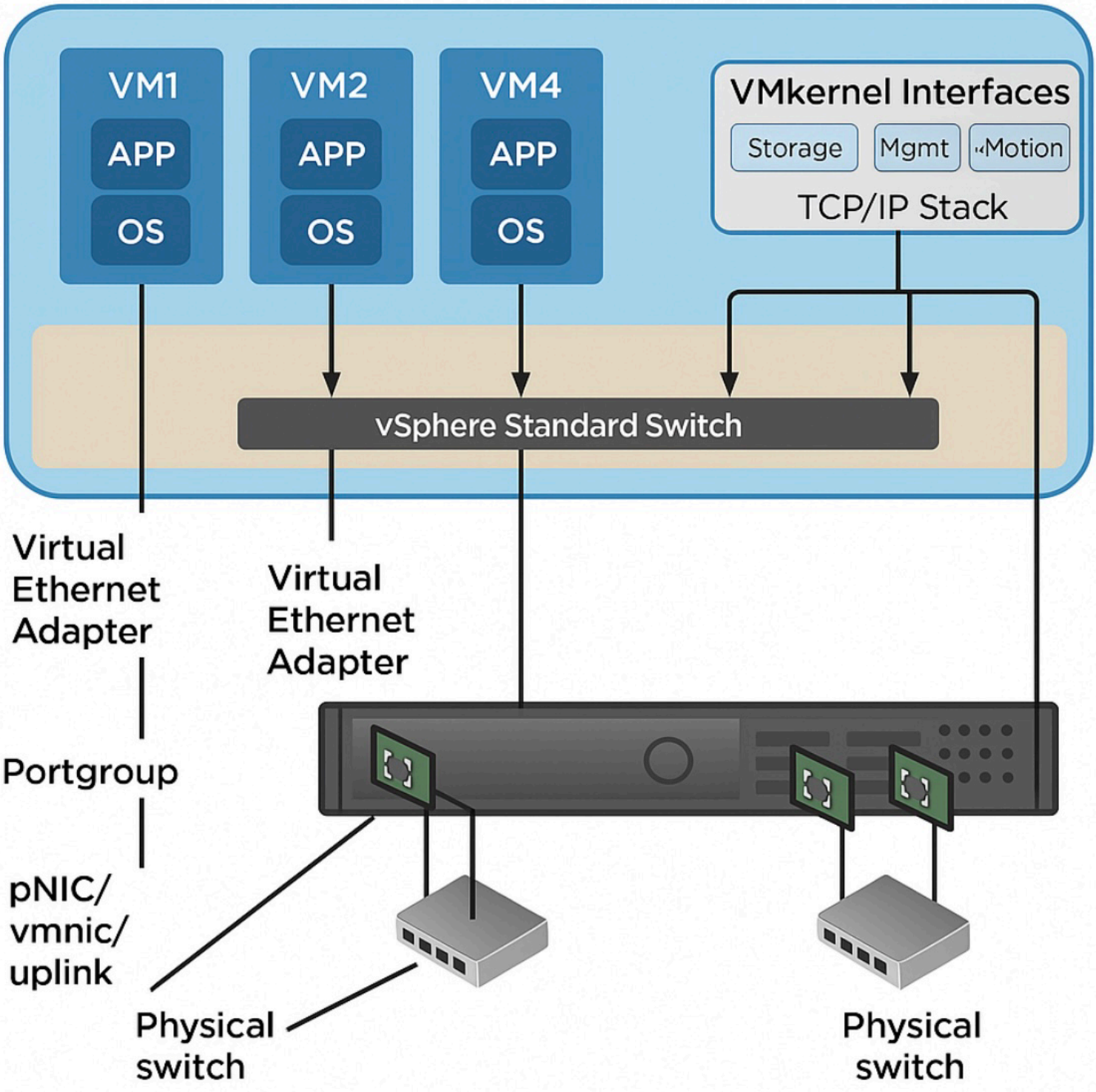
1. Management Traffic
2. vMotion Traffic
3. Fault Tolerance Logging
4. vSphere Replication Traffic
5. vSphere Replication NFC traffic
6. Provisioning Traffic
7. vSAN

- Virtual Machine Port Group:
  To manage virtual machines network
- VMkernel Port Group:
  To manage storage, vSphere Motion, Fault Tolerance, or management traffic



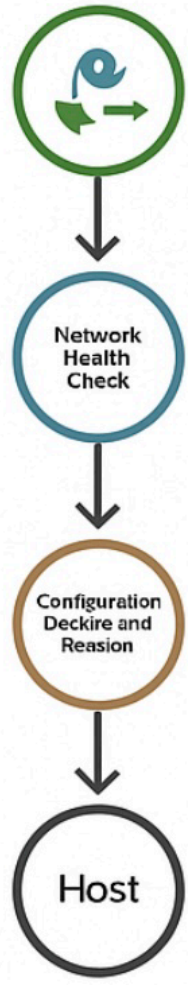
ESXi host Networking Maximums

ESXi Networking	Configuration Maximums
Virtual Network switch creation ports per standard vSwitch	**4096**
Total Virtual Network switch ports per host/ESXI	**4096**
Port groups per vSphere standard switch (vSS)	**512**
Physical NICs 10 Gbps/25 Gbps per host	**16**


VM1
APP
OS
VM2
APP
OS
VM4
APP
OS
VMkernel Interfaces
Storage
Mgmt
Motion
TCP/IP Stack
vSphere Standard Switch
Virtual Ethernet Adapter
Virtual Ethernet Adapter
Portgroup
pNIC/ vmnic/ uplink
Physical switch
Physical switch

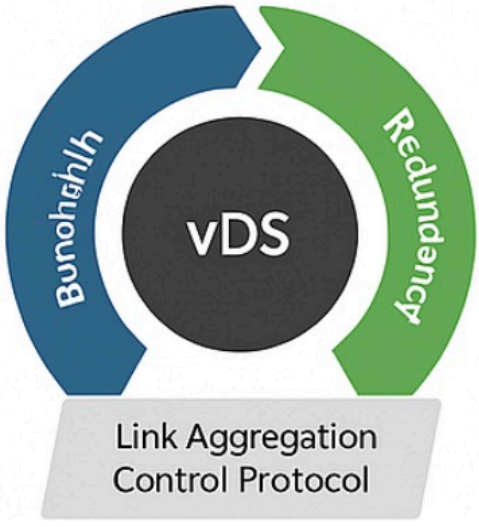
vSphere Distributed Switch (vDS) – Overview

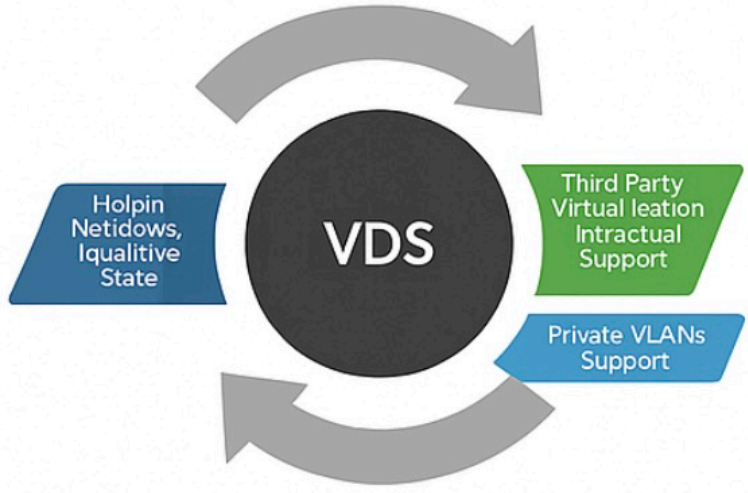
- vDS is the Enhanced version of virtual switch that can be configured and centrally managed from Center.
- VMware vCenter Server maintains the configuration of the vDS.
- The configuration is consistent across all the hosts that use it.
- We can configure VM Port Groups and VMkernel Port Groups
- A vDS enhances the use of NICs with a speed of 10 Gbps or faster.
- The behavior of vDS is consistent with standard switches
- It also enables software-defined network (SDN-y) configurations, reducing operational efforts



vSphere Distributed Switch (vDS)

- Simplify data center administration
- Provide support for advanced features, such as private VLANs, NetFlow, and port mirroring
- Enable networking statistics and policies to migrate with virtual machines during a migration with vMotion
- Provide for customization and third-party development





- It is used to provide VLAN isolation within single VLANs
- To use private VLANs between a host and the rest of the network, the physical switch must be VLAN-capable and configured with VLAN IDs for the private VLAN
- For physical switches with dynamic MAC+ VLAN ID based learning, all corresponding private VLAN IDs must be first entered into the switch's VLAN database
- Eventually, Private VLAN allows the isolation of traffic within a single VLAN

	Primary VLAN ID	Type	Name
	10	Promiscuous	Promiscuous VLAN 10
	101	Isolated	Isolated VLAN 101

Use Cases of Private VLANs

- Use default there are 4096 VLANs available for large erívore enoug wheng more than 4096 VLANs, tW PVLAN them solution.
- Ulse Case 2 for security purposes awe all. It mean in security purposes, wl. DMZ serve need to be aware of both external and internal network. But rarely communicawith other servers in the DMZ
- If you have a limited amount of uplins availal- le in your ESXI host, you can use use multiple VLAN traffic, PVLAN the solution
- Eventually, Private VLAN allows the location of traffic alow a singe VLAN

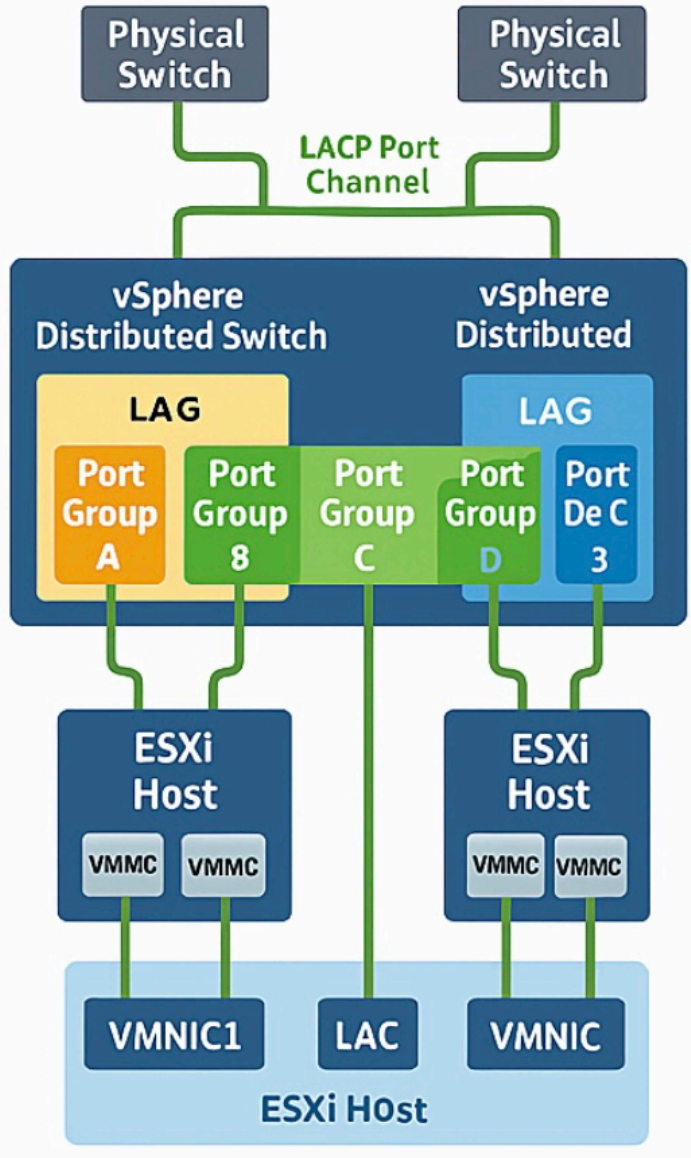
LACP Support on a vSphere Distributed Switch (vDS)

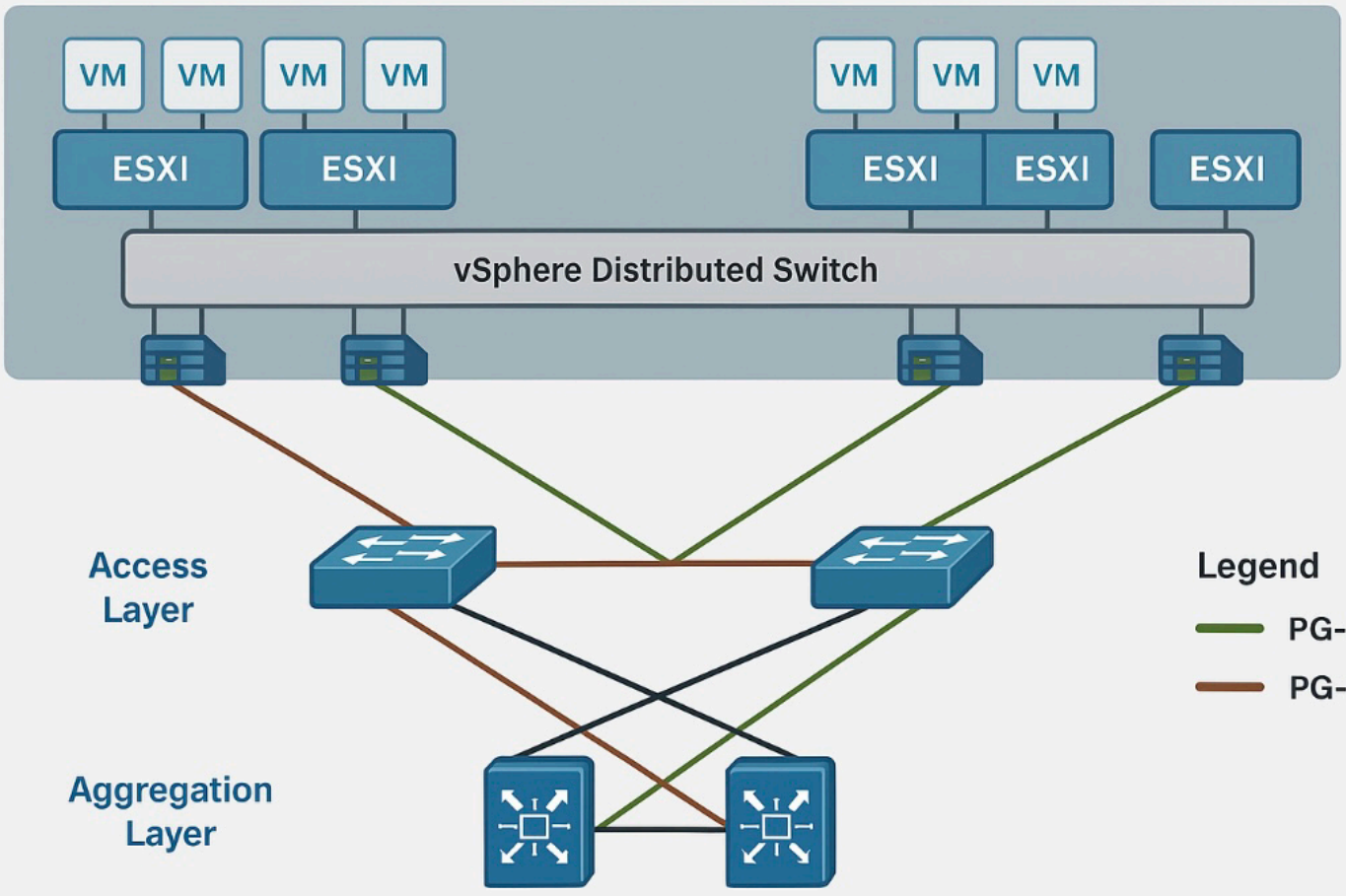
With **Enhanced Link Aggregation Control Protocol (LACP)** support on a vDS, we can connect ESXi hosts to physical switches by using dynamic link aggregation.

Create Multiple Link Aggregation Groups (LAGS) On a distributed switch, we-can aggregate the bandwidth of physical. NICs on ESXi hosts that are connected to **LACP port channels.**

We configure a **LAG with two or more ports**

- LACP allows us to aggregate (combined) both VMNICs together, into one logical link
- Network i/O Control (NIOC)
- Network Health Check
- Port Mirroring



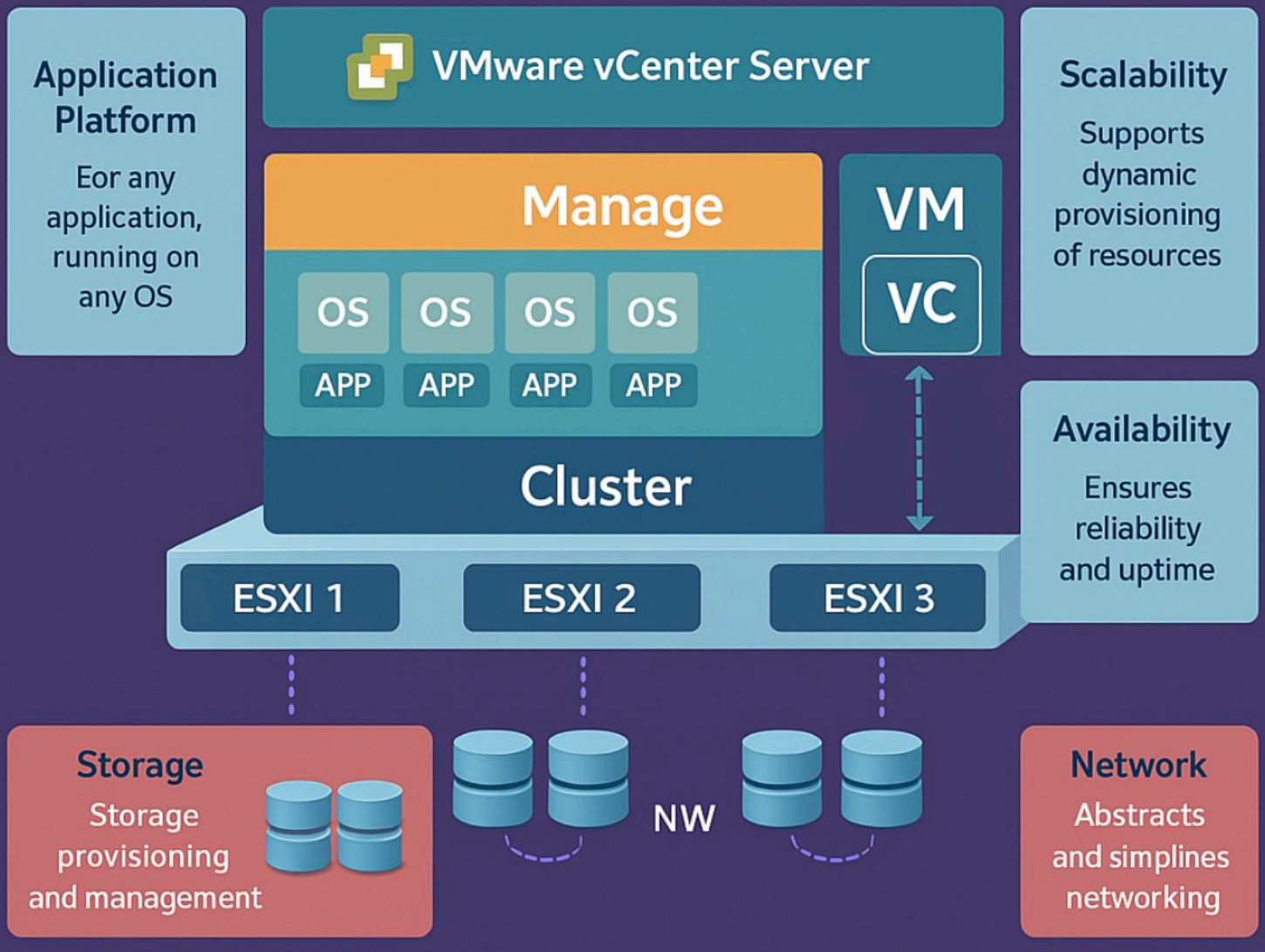

VM
VM
VM
VM
VM
VM
VM
ESXI
ESXI
ESXI
ESXI
ESXI
vSphere Distributed Switch
Access Layer
Aggregation Layer
Legend
PG-A
PG-B

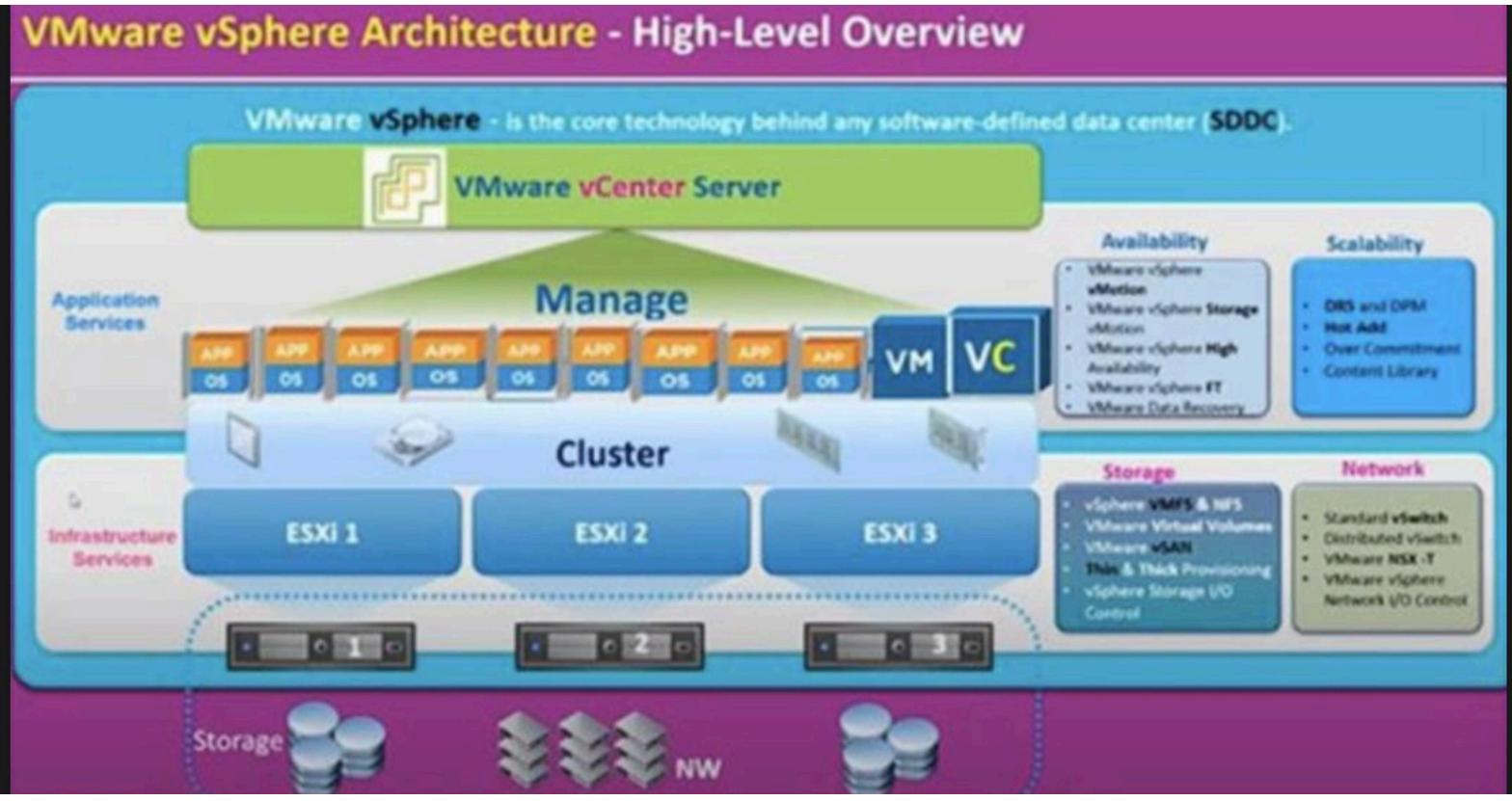
Sr No	Features	vSS	vDS
1	Layer 2 Forwarding	Available	Available
2	VLAN Segmentation	Available	Available
3	Private VLAN	Available	Available
4	Outbound Traffic Shaping	Available	Available
5	NIC Teaming	Available	Available
6	NIC Teaming	Not Available	Available
7	Load Based Teaming	Not Available	Available
8	NIF Teaming	Not Available	Available
9	Net Flow	Not Available	Available
10	Net Flantk	Not Available	Available
11	Network VMcion Settings	Not Available	Available
12	Third Party Switch API	Not Available	Available
13	Third Party Switch Support	Not Available	Available
14	Link Laver Discovery Protocol	Not Available	Available
15	User Based Network I/O Control	Available	Available
16	Backup & Restore Network Configuration	Available	Available

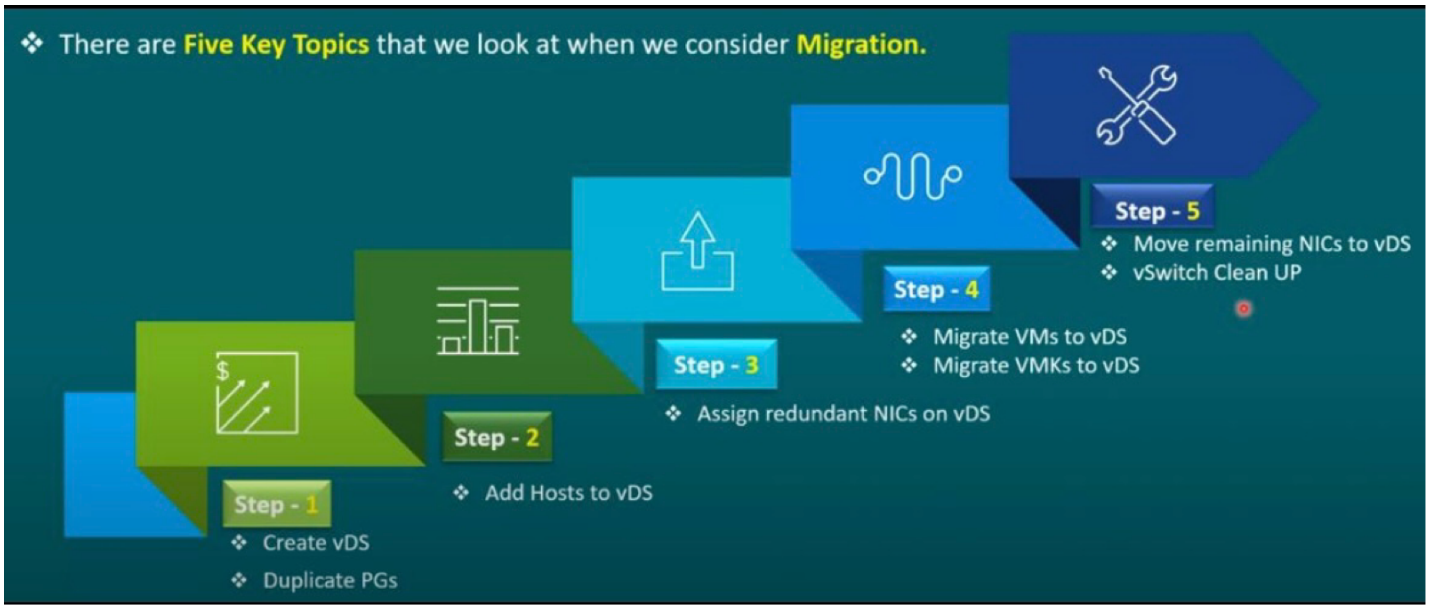
Scenario	ESXI Hosts Count	Virtual Network – Configuration	Time Consumption per Host	Overall Configura-tion Time	Observation
vSwitch	300	Standard Virtual Switch Creation • vSwtch Port group for VMotion • vSwtch Port group for vsan • vSwtch for Production VMs	15 Min.	=15×300 =4500/60 =75 Hours	
DvSwitch	300	Distributed Virtual Switch Creation • DvSwitch Port group for VMotion • DvSwitch Port group for vsan • DvSwitch Port group for Test/Dev VMs	15 Min.	75 Hours	DvSwitch saves time and presents a more efficient management construct by eliminating per host configuration

VMware vSphere Architecture – High-Level Overview

VMware vSphere - is the core technology behind any software-defined data center (SDDC)




VMware vSphere Architecture - High-Level Overview
VMware vSphere - is the core technology behind any software-defined data center (SDDC).
VMware vCenter Server
Manage
Application Services
APP
OS
VM
VC
Availability
VMware vSphere vMotion
VMware vSphere Storage vMotion
VMware vSphere High Availability
VMware vSphere FT
VMware Data Recovery
Scalability
DRS and DPM
Hot Add
Over Commitment
Content Library
Cluster
Infrastructure Services
ESXi 1
ESXi 2
ESXi 3
Storage
vSphere VMFS & NFS
VMware Virtual Volumes
VMware vSAN
Thin & Thick Provisioning
vSphere Storage I/O Control
Network
Standard vSwitch
Distributed vSwitch
VMware NSX -T
VMware vSphere Network I/O Control
Storage
NW


There are Five Key Topics that we look at when we consider Migration.
Step - 1
Create vDS
Duplicate PGs
Step - 2
Add Hosts to vDS
Step - 3
Assign redundant NICs on vDS
Step - 4
Migrate VMs to vDS
Migrate VMKs to vDS
Step - 5
Move remaining NICs to vDS
vSwitch Clean UP