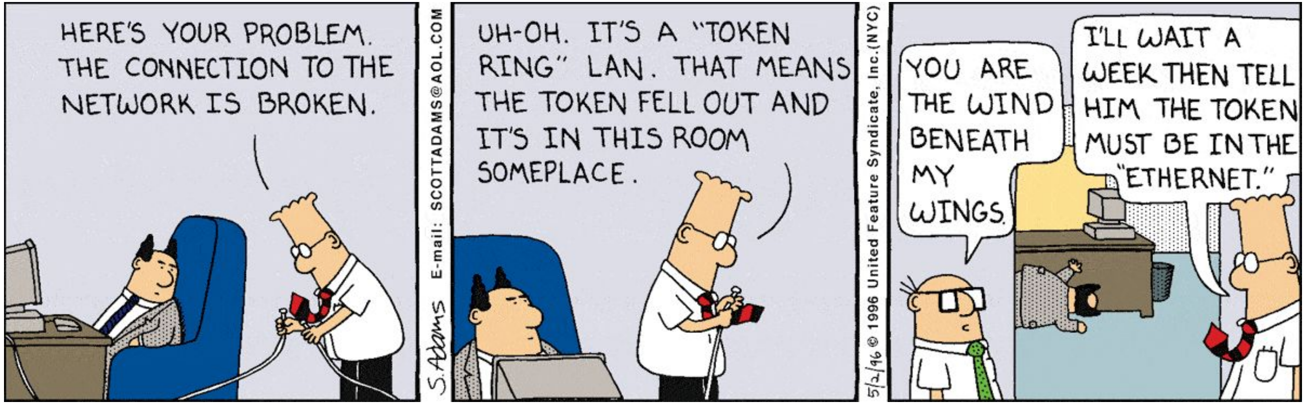
CA.COM/CLOUD-MONITORING
ALL I KNOW IS THE BOSS SAID WE HAD TO MONITOR THE CLOUD.
© D.Fletcher for CloudTweaks.com


HERE'S YOUR PROBLEM. THE CONNECTION TO THE NETWORK IS BROKEN.
UH-OH. IT'S A "TOKEN RING" LAN. THAT MEANS THE TOKEN FELL OUT AND IT'S IN THIS ROOM SOMEPLACE.
YOU ARE THE WIND BENEATH MY WINGS.
I'LL WAIT A WEEK THEN TELL HIM THE TOKEN MUST BE IN THE "ETHERNET."
E-mail: SCOTTADAMS@AOL.COM
S. Adams
5/2/96 © 1996 United Feature Syndicate, Inc.(NYC)

Waiting ROOM fun - Class will start in next 2 minutes

Virtual Networking

Let's more explore in detail in easy way !!

Till Now ..

We Understand fundamentals of network virtualization !!

Overview of Networking Device : Hub, Switches ..

Concept of LAN and VLAN (Network segmentation - Virtually)

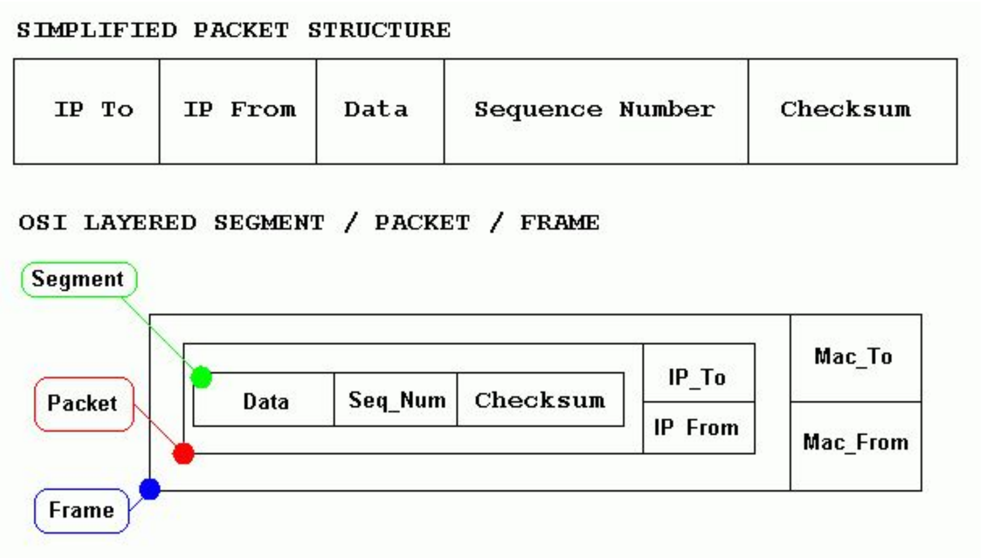
Little bit initiate the configuration demonstration of virtual networking in ESXI VM ..

Now, we will understand the concept and practically overview in little detail for network virtualization from scratch.

Basic remembrance

Networking Device Switch handles frames and

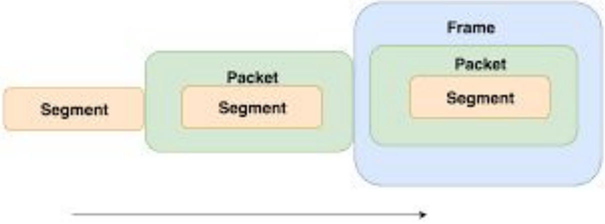
Router handles packets

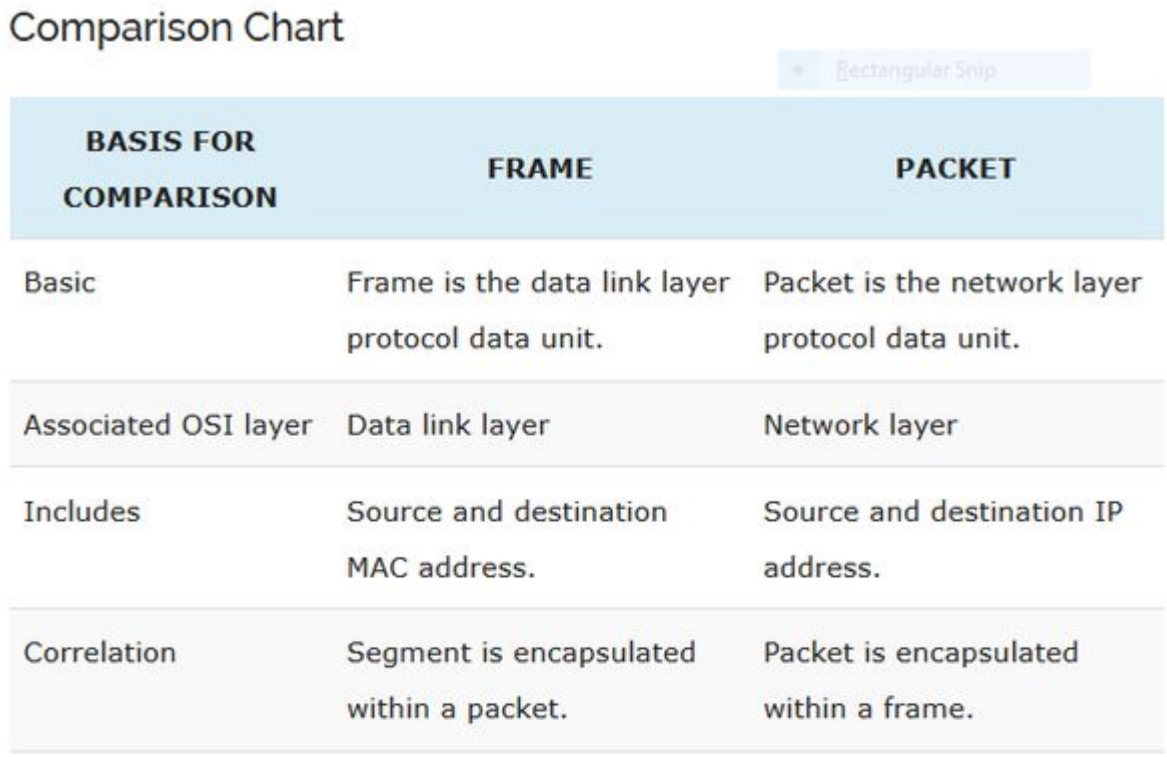


SIMPLIFIED PACKET STRUCTURE

IP To	IP From	Data	Sequence Number	Checksum

OSI LAYERED SEGMENT / PACKET / FRAME





Rectangular Snip

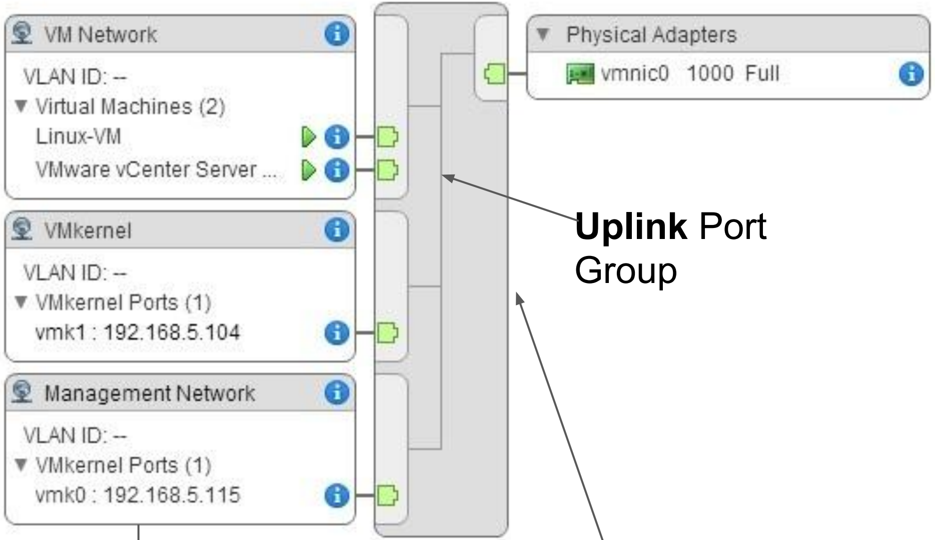
Comparison Chart

BASIS FOR COMPARISON	FRAME	PACKET
Basic	Frame is the data link layer protocol data unit.	Packet is the network layer protocol data unit.
Associated OSI layer	Data link layer	Network layer
Includes	Source and destination MAC address.	Source and destination IP address.
Correlation	Segment is encapsulated within a packet.	Packet is encapsulated within a frame.

Virtual Networking !!

Jon Carter
cartertoons
WITH THE COMPANY'S MOVE TO VIRTUALIZATION, THE NETWORK HARDWARE BECAME OBSOLETE. THEY LET US KEEP IT FOR THE BREAK ROOM AND THEY SOLD THE FURNITURE ONLINE.

Graphical representation of a standard switch in vSphere Web Client:



VM Network

VLAN ID: --

▼ Virtual Machines (2)

Linux-VM

VMware vCenter Server ...

VMkernel

VLAN ID: --

▼ VMkernel Ports (1)

vmk1 : 192.168.5.104

Management Network

VLAN ID: --

▼ VMkernel Ports (1)

vmk0 : 192.168.5.115

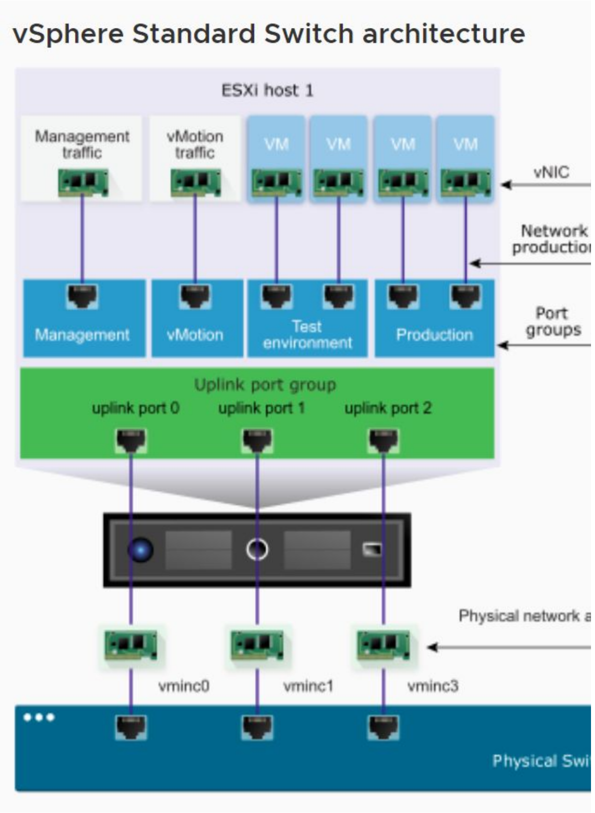
▼ Physical Adapters

vmnic0 1000 Full

Uplink Port Group

- **vNetwork standard switches** – managed at each individual host level.

Port groups - VM Network, VMkernel, Management Network


vSphere Standard Switch architecture

Standard Switch

A **standard switch** (sometimes called **vSwitch**) is created by default when ESXi is installed.

Like its **physical Ethernet** counterpart, a standard switch works at **layer 2**, forwards frames to other switch ports based on the MAC address, and supports features such as VLANs and port channels.

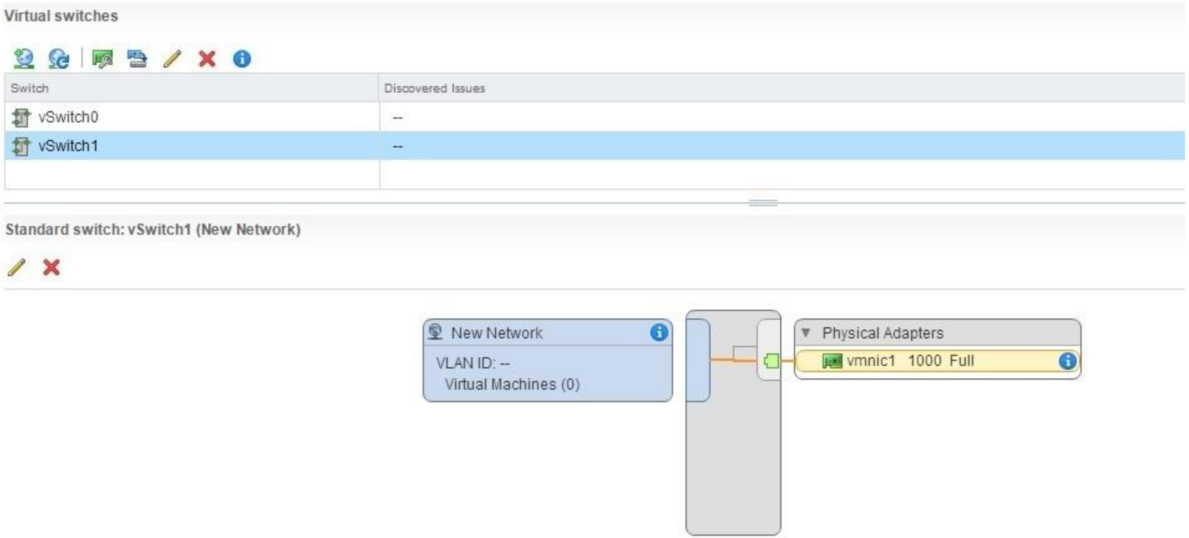
Standard switches have to be connected to the ESXi host’s **physical NICs as uplinks** to communicate with the rest of the network.

Standard switches provide the network connectivity:

- Between virtual machines within the same ESXi host.
- Between virtual machines on different ESXi hosts.
- Between virtual and physical machines on the network.
- For VMkernel access to networks for vMotion, iSCSI, NFS, or Fault Tolerance logging (and management on ESXi).

FACTS : You can have a total of 4096 standard switch ports per host, a maximum of 1016 active ports per host, and 512 port groups per switch.

Create a Virtual Switch



Virtual switches

Switch	Discovered Issues
vSwitch0	--
vSwitch1	--

Standard switch: vSwitch1 (New Network)

New Network

VLAN ID: --

Virtual Machines (0)

Physical Adapters

vmnic1 1000 Full

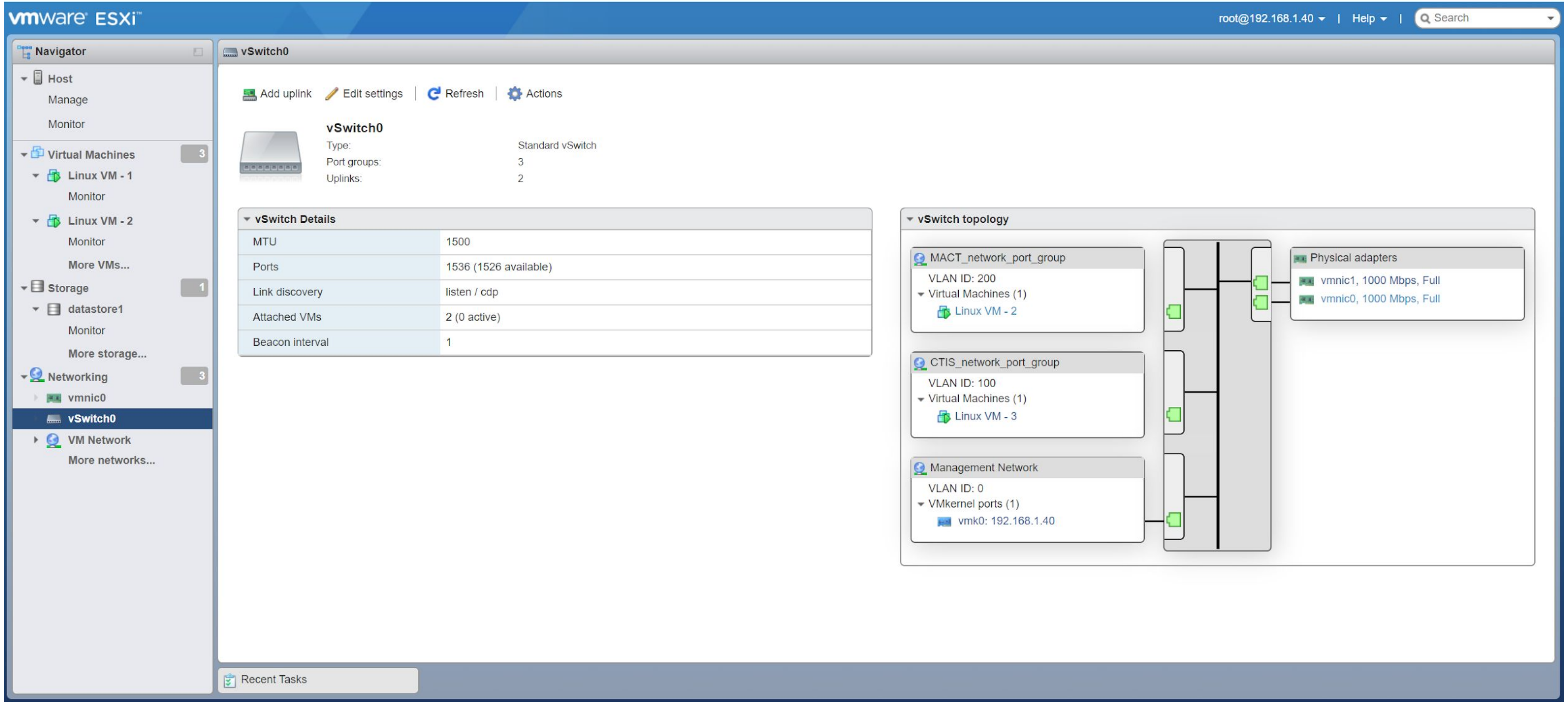
VLANS

VLANs (Virtual LANs) are **logical groupings of devices** in the **same broadcast domain**. They are usually configured on switches by placing some ports into one broadcast domain and other ports into another. VLANs can spread across multiple switches, enabling communications as if all virtual machines or ports in a VLAN are on the same physical LAN segment.

VLANs offer many advantages, including:

- broadcast traffic will be received and processed only by devices inside the same VLAN, which can improve network performance.
- users can be grouped by a department and not by the physical location.
- sensitive traffic can be isolated in a separate VLAN for the purpose of security.

Configuring port groups / VLANS



vSwitch0

Type: Standard vSwitch
Port groups: 3
Uplinks: 2

vSwitch Details

MTU	1500
Ports	1536 (1526 available)
Link discovery	listen / cdp
Attached VMs	2 (0 active)
Beacon interval	1

vSwitch topology

MACT_network_port_group
VLAN ID: 200
Virtual Machines (1)
Linux VM - 2

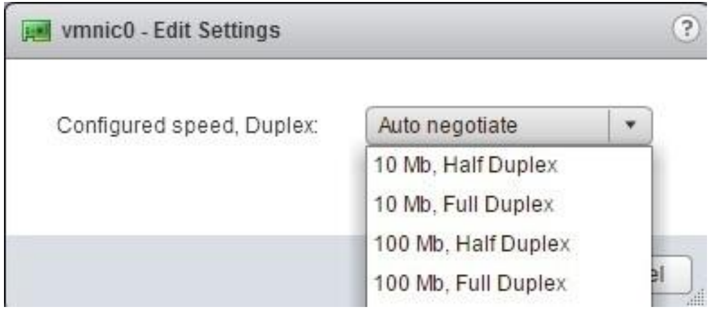
CTIS_network_port_group
VLAN ID: 100
Virtual Machines (1)
Linux VM - 3

Management Network
VLAN ID: 0
VMkernel ports (1)
vmk0: 192.168.1.40

Physical adapters
vmnic1, 1000 Mbps, Full
vmnic0, 1000 Mbps, Full

Configure speed and duplex

You can configure the speed and duplex of the ESXi host physical network adapter using vSphere Web Client. Here is how you can do that:



vmnic0 - Edit Settings

Configured speed, Duplex: Auto negotiate

Switch network security policies

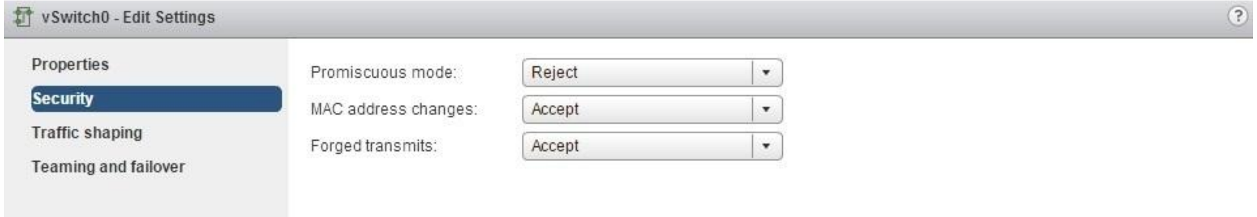
There are network security policies for virtual switches that enable you to protect virtual machines from impersonation or interception attacks. These policies are:

1. Promiscuous Mode – set to **Reject** by default to prevent guest operating systems from observing all traffic passing through a virtual switch. Set this mode to **Accept** only if you use a packet sniffer or intrusion detection system in the guest operating system.

2. MAC Address Changes – when set to **Reject** and the guest operating systems attempts to change the MAC address assigned to the virtual NIC, the virtual machine will stop receiving traffic. Set to **Accept** by default.

3. Forget Transmits – affects traffic that is transmitted from a virtual machine. When set to **Reject**, the virtual NIC drops frames that the guest operating system sends if the source MAC address is different than the one assigned to the virtual NIC. Set to **Accept** by default.

To set the security policies using the vSphere Web Client, go to the host's **Manage > Networking** tab. Choose the virtual switch you would like to modify and select the Edit settings icon:



vSwitch0 - Edit Settings

Promiscuous mode: Reject

MAC address changes: Accept

Forged transmits: Accept

Vswitch provides more functionality to manage Esxi Host

For Example -

Traffic shaping policies

Switch Load balancing policies

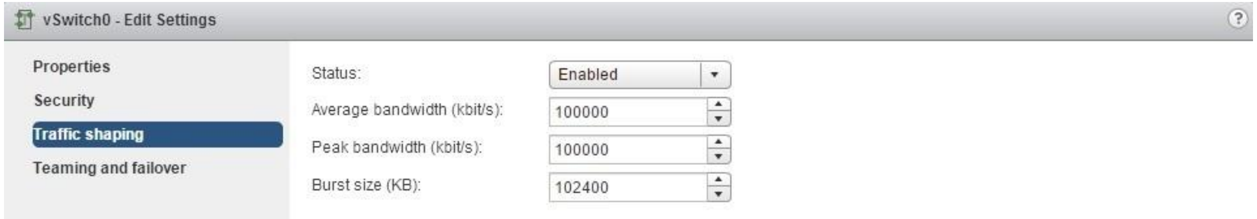
Network Failover detections

Switch traffic shaping policies

By default, all virtual network adapters connected to a virtual switch have access to the full amount of bandwidth on the physical network adapter with which the virtual switch is associated. You can use the network traffic shaping policies to control a virtual machine’s network bandwidth.

Traffic shaping is disabled by default. To establish a traffic shaping policy, you can configure these three parameters:

- **Average Bandwidth** – the number of kilobits per second allowed across a port. This number is measured over a period of time and represents the allowed average load.
- **Peak Bandwidth** – the maximum number of kilobits per second allowed across a port when it is sending a burst of traffic. This number is used to limit the bandwidth during a burst and cannot be smaller than the average bandwidth number.
- **Burst Size** – the maximum number of kilobytes allowed in a burst. This option can allow a port that needs more bandwidth than is specified in the average bandwidth value to gain a burst of higher-speed traffic if a burst bonus is available.



Status: Enabled

Average bandwidth (kbit/s): 100000

Peak bandwidth (kbit/s): 100000

Burst size (KB): 102400

Switch load balancing policies

The load-balancing policy determines how ESXi hosts will use their uplink adapters. Four load-balancing methods are available when using a standard virtual switch:

1. **Originating virtual port ID** – a VM’s outbound traffic is mapped to a specific physical NIC. The NIC is determined by the ID of the virtual port to which the VM is connected. This is the default.

2. **Source MAC hash** – a VM’s outbound traffic is mapped to a specific physical NIC that is based on the virtual NIC’s MAC address.

3. **IP hash** – a NIC for each outbound packet is selected based on its source and destination IP address. This method requires the use of **EtherChannel** on the physical switch.

4. **Explicit failover order** – an adapter that is listed highest in the order of active adapters and passes failover detection criteria will be used.

Network failover detection

Network failover detection is a mechanism used to detect a network failure. Two network failover detection methods are available in vSphere when using a standard virtual switch:

1. Link status only – relies on the link status provided by the network adapter. This method can detect failures like cable pulls and physical switch power failures, but can not detect configuration errors (e.g. wrong VLAN configuration of a physical switch port) or cable pulls on the other side of a physical switch. This is the default.

2. Beacon probing – probes are sent out and listened for on all NICs in the team. This method can determine link status and failures that the Link status only method can not, such as configuration errors and cable pulls on the other side of a physical switch.