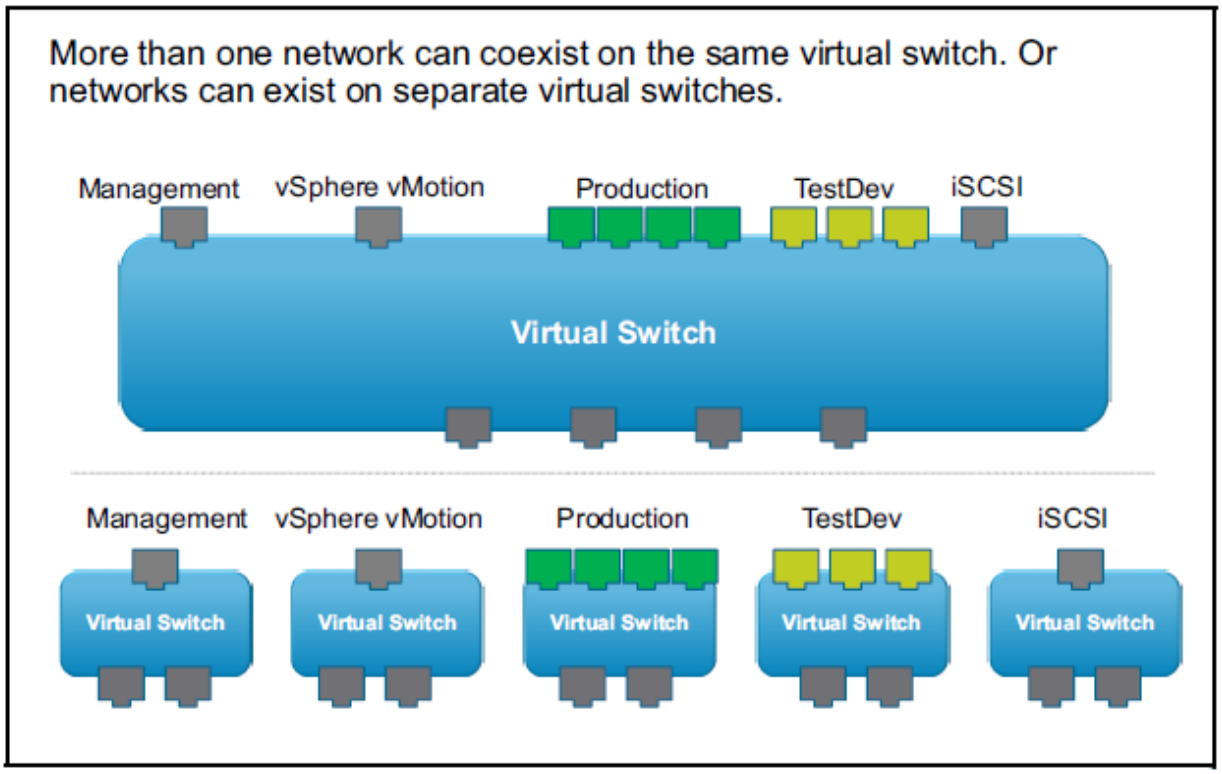
## Virtual Switch Connection Examples

Slide 5-8




در پیکربندی و ایجاد vSwitch در صورتی که Uplink های سرور فیزیکی محدود باشد می توانیم از یک vSwitch استفاده کنیم و تمامی Uplinkهای سرور را به آن اختصاص دهیم و برروی این vSwitch می توانیم چندین Port Group برای ماشین های مجازی و چندین VMkernel Port برای کارهای دیگری مانند Management و یا vMotion و یا ISCSI ایجاد کنیم.

اما در صورتی که Uplink به تعداد کافی برروی سرور فیزیکی وجود داشته باشد می توانیم چندین vSwitch برروی سرور ایجاد کنیم و Uplink های سرور را میان vSwitch ها تقسیم کنیم و Port Group مربوط به ماشین های مجازی و VMkernel ها را میان آنها تقسیم کنیم این پیاده سازی نسبت به پیاده سازی بالا Performance بالاتری دارد و دلیل آن بخاط این است که پهنای باند بیشتری از Uplink ها در اختیار Port Group ها و VMkernel Port ها قرار می گیرد زمانی که شما یک Uplink را به یک vSwitch اختصاص می دهید پهنای باند این Uplink میان Port Group ها و VMkernel Port های این سوییچ Share می شود.

## Types of Virtual Switches

Slide 5-9

A virtual network supports these types of virtual switches:

- Standard switches:
  - Virtual switch configuration for a single host
- Distributed switches:
  - Virtual switches that provide a consistent network configuration for virtual machines as they migrate across multiple hosts

یک Virtual Network شامل دو نوع Virtual Switch می باشد:

- Standard Switch

یک Virtual Switch است که توسط یک ESXi Host ایجاد می شود.

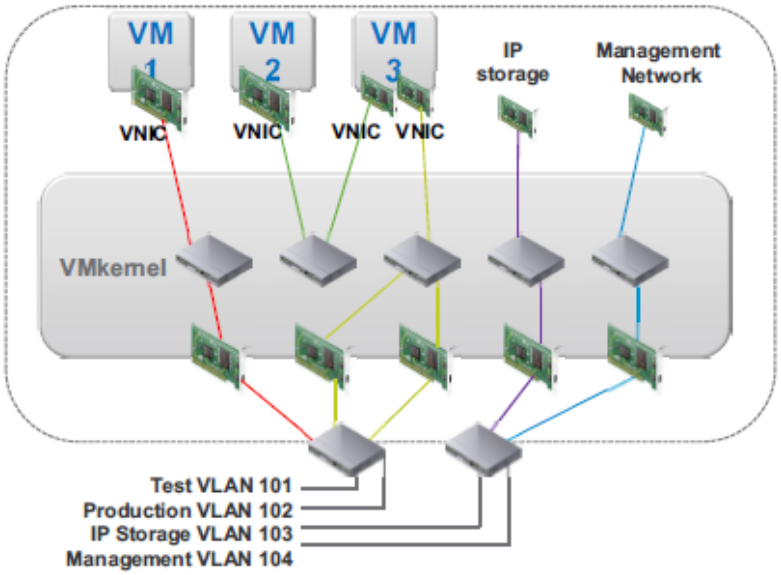
- Distributed Switch

یک Virtual Swich است که توسط vCenter Server ایجاد می شود و میان چندین ESXi Host مشترک می باشد.

## Standard Switch Components

Slide 5-10

A standard switch provides connections for virtual machines to communicate with one another, whether they are on the same host or a different host.




یک Standard Switch ارتباط میان ماشین های مجازی را با یکدیگر برروی یک Host یا یک Host دیگر برقرار می کند.

ارتباط یک Standard Switch با یک Standard Switch دیگر برروی یک Host یا Host های دیگر از طریق Uplink می باشد به عبارت دیگر در صورتی که یک Standard Switch شامل Uplink نباشد نمی تواند با سوییچ های دیگر ارتباط برقرار کند.

برروی یک Standard Switch پروتکل STP(Spanning Tree Protocol) وجود ندارد همانطوری که می دانید این پروتکل برای جلوگیری Loop لایه ۲ در سوییچ های فیریکی استفاده می شود در سوییچ های مجازی به دلیل اینکه زمانی که یک Broadcast وارد پورت سوییچ می شود آن را به پورت های دیگر ارسال نمی کند لذا Loop در این سوییچ ها ایجاد نمی شود.

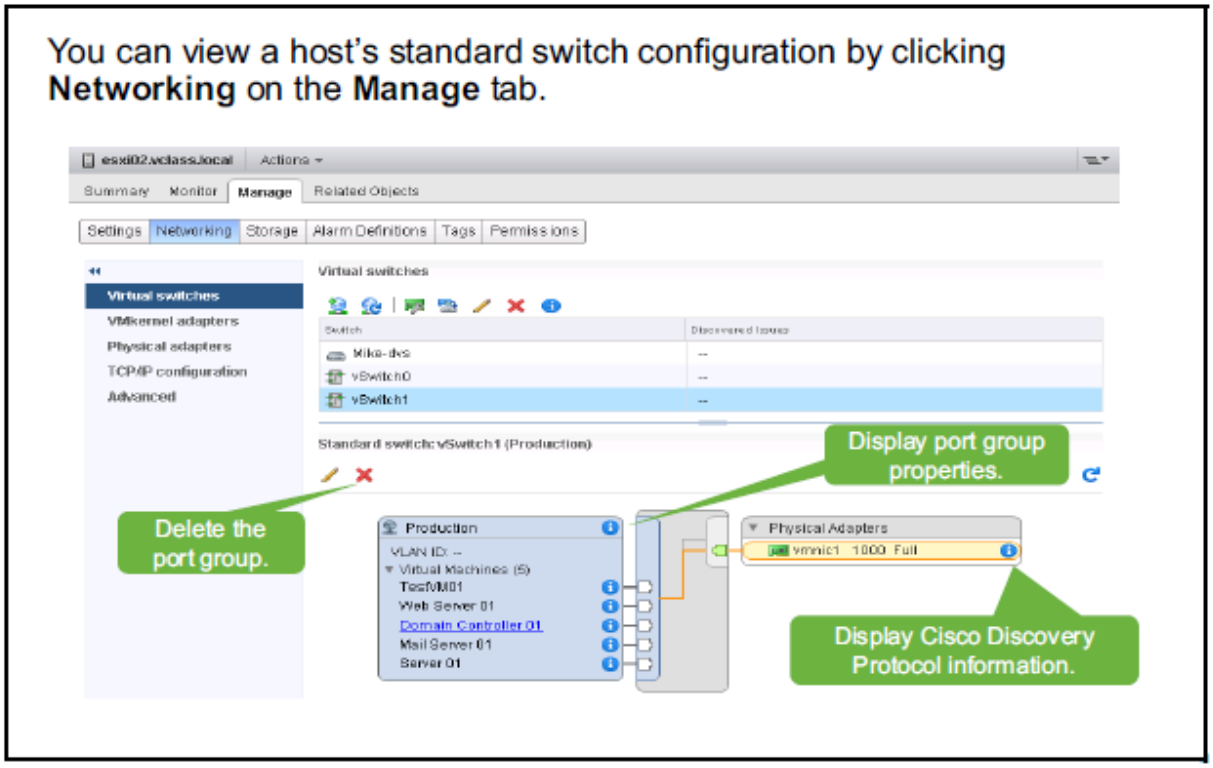
شما نمی توانید یک پورت سوییچ مجازی را مستقیما به کارت شبکه مجازی یک ماشین مجازی اختصاص دهید برای این منظور حتما بایستی از Port Group استفاده شود شما می توانید برروی یک Port Group تنظیمات مربوط به VLAN,Trunk,Security,QOS را انجام دهید.

برروی یک Standard Switch پروتکل CDP(Cisco Discovery Protocol) نیز وجود دارد وظیفه این پروتکل شناسایی Cisco Device هایی که مستقیما به سرور متصل می باشند.

برروی سوییچ های فیزیکی بهتر از Trunk یا Etherchannel استفاده شود و بهتر است برروی این پورت ها پیکربندی Port Fast استفاده شود.

## Viewing the Standard Switch Configuration

Slide 5-11




برای پیکربندی و یا مشاهده یک Host Standard Switch شما می توانید برروی یک Host کلیک کرده و سپس در Manage Tab وارد قسمت Networking شوید در این قسمت با کلیک برروی قسمت Virtual Switch می توانید تمامی Virtual Switch را مشاهده و یا پیکربندی کنید.

به صورت پیش فرض در این صفحه یک Standard Switch با نام vSwitch0 وجود دارد که برروی آن یک Virtual Machine Port Group با نام VM Network و یک VMkernel Port با نام Management Network وجود دارد .

## About VLANs

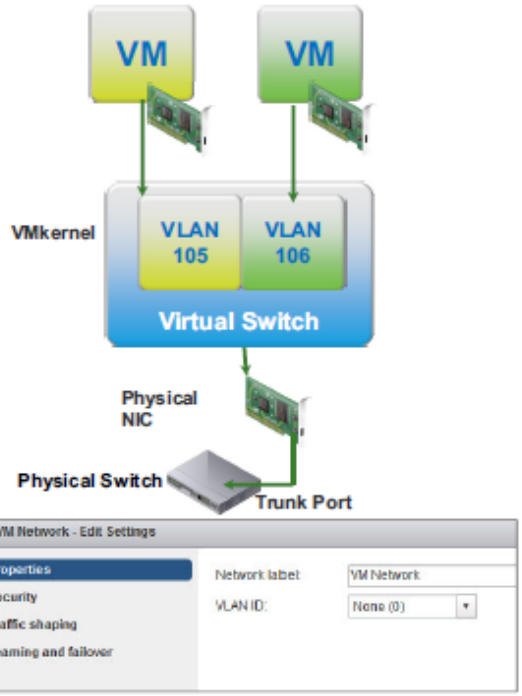
Slide 5-12

ESXi supports 802.1Q VLAN tagging.

Virtual switch tagging is one of the tagging policies supported:

- Packets from a virtual machine are tagged as they exit the virtual switch.
- Packets are untagged as they return to the virtual machine.
- Effect on performance is minimal.

ESXi provides VLAN support by giving a port group a VLAN ID.




یک ESXi Host می تواند 802.1Q VLAN Tagging را ساپورت کند.

یک VLAN برروی یک Port Group تعریف می شود سپس VMkernel تمامی Packet هایی که Tag یا unTag هستند از طریق سوییچ عبور می دهد.

یک VLAN ID بایستی برروی یک Port Group اختصاص داده شود به صورت زیر می باشد:

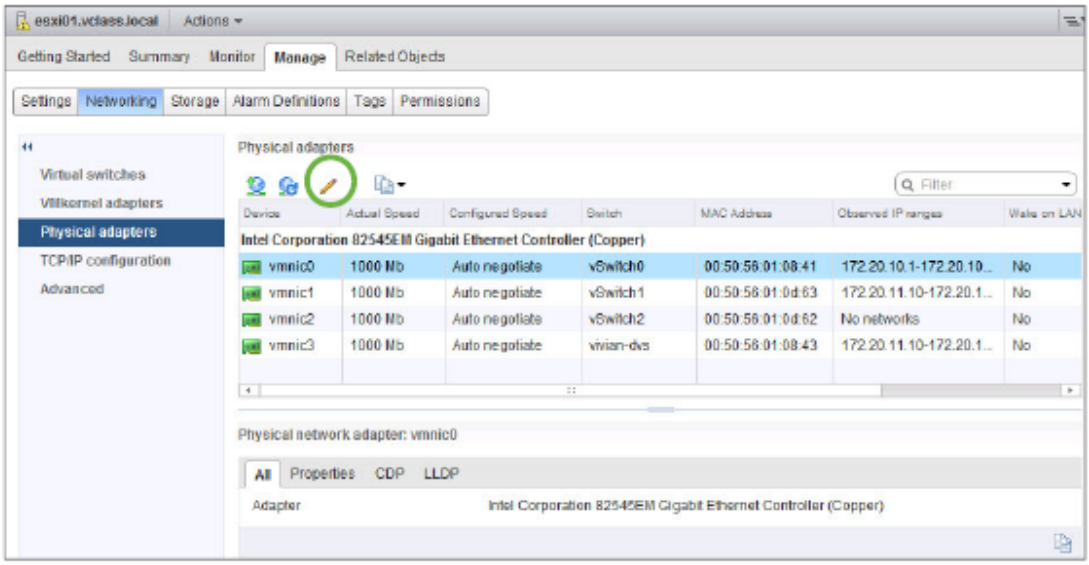
- VLAN ID 0
  این VLAN ID به معنی Untag می باشد.
- VLAN ID 4095
  به معنی تمامی VLAN ها یا همان Trunk می باشد.
- VLAN ID 1-4094
  تمامی VLAN ID هایی می باشد که می توان به یک Port Group اختصاص داد.

تمامی ماشین های مجازی که به یک VLAN ID تعلق دارند فقط می توانند با ماشین های مجازی که در همان VLAN ID هستند ارتباط داشته باشند .در صورتی که نیاز باشد که ماشین های مجازی با یک VLAN ID بتوانند ماشین های مجازی دیگر VLAN ID را ببینند بایستی این کار از طریق سوییچ فیزیکی و از طریق Interface Vlan انجام شود.

## Network Adapter Properties

Slide 5-13

A physical adapter can become a bottleneck for network traffic if the adapter speed does not match application requirements.




برای مشاهده کارت های شبکه فیزیکی یک سرور یا Physical Adapters می توانید برروی Host کلیک کرده سپس وارد قسمت Manage شده و از این قسمت وارد قسمت Networking شوید سپس در این قسمت برروی Physical Adapters کلیک کنید در این قسمت شما می توانید تمامی کارت های شبکه فیزیکی سرور را مشاهده کنید و در صورتی که برروی یک کارت شبکه کلیک کنید و برروی مداد کلیک کنید می توانید تنظیمات مربوط به کارت شبکه مربوطه را مشاهده و یا تنظیمات مربوط به آن را تغییر دهید.

## Review of Learner Objectives

Slide 5-14

You should be able to meet the following objectives:

- Describe the virtual switch connection types
- Describe the components of a standard switch

## Lesson 2: Configuring Standard Switch Policies

Slide 5-15

در انتهای این درس با مطالب زیر آشنا خواهید شد:

- توصیف قابلیت های امنیتی که می توان برروی Port Group اعمال کرد.
- توصیف قابلیت Traffic Shaping برروی Port Group
- توصیف قابلیت های NIC Teaming و Failover برروی Port Group یک VSS

## Learner Objectives

Slide 5-16

By the end of this lesson, you should be able to meet the following objectives:

- Describe the security of a standard switch port group
- Describe the traffic shaping of a standard switch port group
- Describe the NIC teaming and failover of a standard switch port group

## Network Switch and Port Policies

Slide 5-17

Policies set at the standard switch level apply to all of the port groups on the standard switch. The exceptions are the configuration options that are overridden at the standard port group.

Available network policies:

- Security
- Traffic shaping
- NIC teaming and failover

Policies are defined at these levels:

- Standard switch level:
  - Default policies for all the ports on the standard switch.
- Port group level:
  - Effective policies: Policies defined at this level override the default policies set at the standard switch level.

به صورت پیش فرض تمامی Policy ها از یک Standard Switch Level به تمامی Port Group ها روی Standard Switch به ارث می رسند .

به صورت کلی ما دو Object زیر را برای اعمال Policy ها در یک Standard Switch داریم:

- Standard Switch Level
- Port Group Level

مجموعه ایی از Policy هایی که می توان به Port Group Level یا Standard Switch Level اعمال کرد در میان آنها مشترک است و این تنظیمات به صورت پیش فرض از Standrad Switch Level به Port Group Level به ارث می رسد مگر اینکه یک Port Group بخواهد که رفتار را تغییر دهید که برای این منظور بایستی برروی Policy مورد نظر تیک Override را برروی Port Group بزنیم.

مجموعه ایی از Policy هایی که می توان به Port Group یا Standard Switch اعمال کرد شامل موارد زیر می باشد:

- Security
- Traffic Shaping
- Nic Teaming and Failover

نکته:

یک Standard Switch شامل Mac Address Table نمی باشد ولی تغییرات مربوط به Mac Address ماشین های مجازی را تشخیص می دهد و برای این کار از Configuration File ماشین مجازی استفاده می کند.

## Configuring Security Policy

Slide 5-18

Administrators can define security policies at both the standard switch level and the port group level:

- **Promiscuous mode**: Allows a virtual switch or port group to present all traffic regardless of the destination.
- **MAC address changes**: Accept or reject inbound traffic when the MAC address has been altered by the guest.
- **Forge transmits**: Accept or reject outbound traffic when the MAC address has been altered by the guest.


مدیر شبکه می تواند Security Policy ها را روی هر دو Standard Switch Level یا Port Group Level به صورت زیر انجام دهد:

- Promiscuous mode

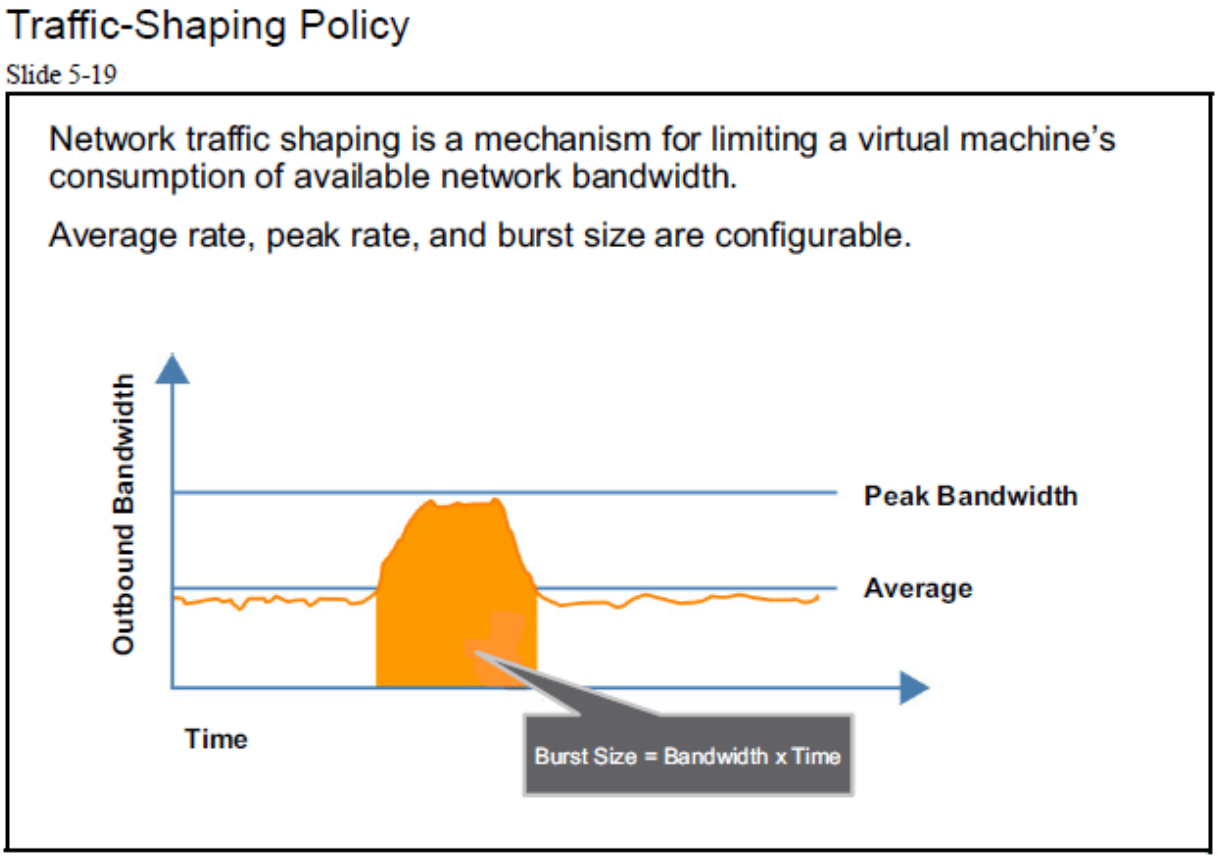
با استفاده از این قابلیت یک سوییچ مجازی یا Port Group می تواند ترافیک تمامی پورت ها را دریافت کند این قابلیت بیشتر برای موارد مانیتورینگ و IDS/IPS استفاده می شود.

- MAC address changes

در صورتی که ماشین مجازی Mac Address خود را تغییر داده باشد تمامی Inbound Traffic به سمت ماشین مجازی می تواند Reject یا Acceptشود.

- Forge transmits

در صورتی که ماشین مجازی Mac Address خود را تغییر داده باشد تمامی Outbound Traffic از ماشین مجازی می تواند Reject یا Accept شود.




پهنای باند کارت شبکه یک ماشین مجازی میتواند توسط Network Traffic Shaper کنترل شود.

زمانی که شما از یک Standard Switch برای اعمال Network Traffic Shaper استفاده می کنید عملیات Shape می تواند فقط در جهت Outbound انجام شود.

یک Traffic Shaping شامل قسمت های زیر می باشد:

- Average Rate

پهنای باندی است که برای کارت شبکه یک ماشین مجازی گارانتی شده است .

- Peak Rate

ماکزیمم پهنای باند موجود می باشد که در صورتی که آزاد باشد یک ماشین مجازی می تواند از آن استفاده کند.

- Burst Size

مدت زمانی است که یک ماشین مجازی می تواند از پهنای باند آزاد Peak استفاده کند و طبق فرمول زیر محاسبه می شود:

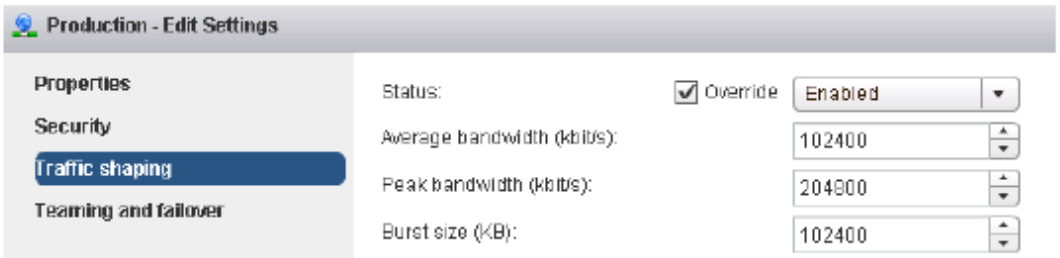
Burst Size = Bandwidth x Time

Configuring Traffic Shaping

Slide 5-20

A traffic-shaping policy is defined by average bandwidth, peak bandwidth, and burst size. You can establish a traffic-shaping policy for each port group and each distributed port or distributed port group:

- Traffic shaping is disabled by default.
- Parameters apply to each virtual NIC in the standard switch.
- On a standard switch, traffic shaping controls only outbound traffic.

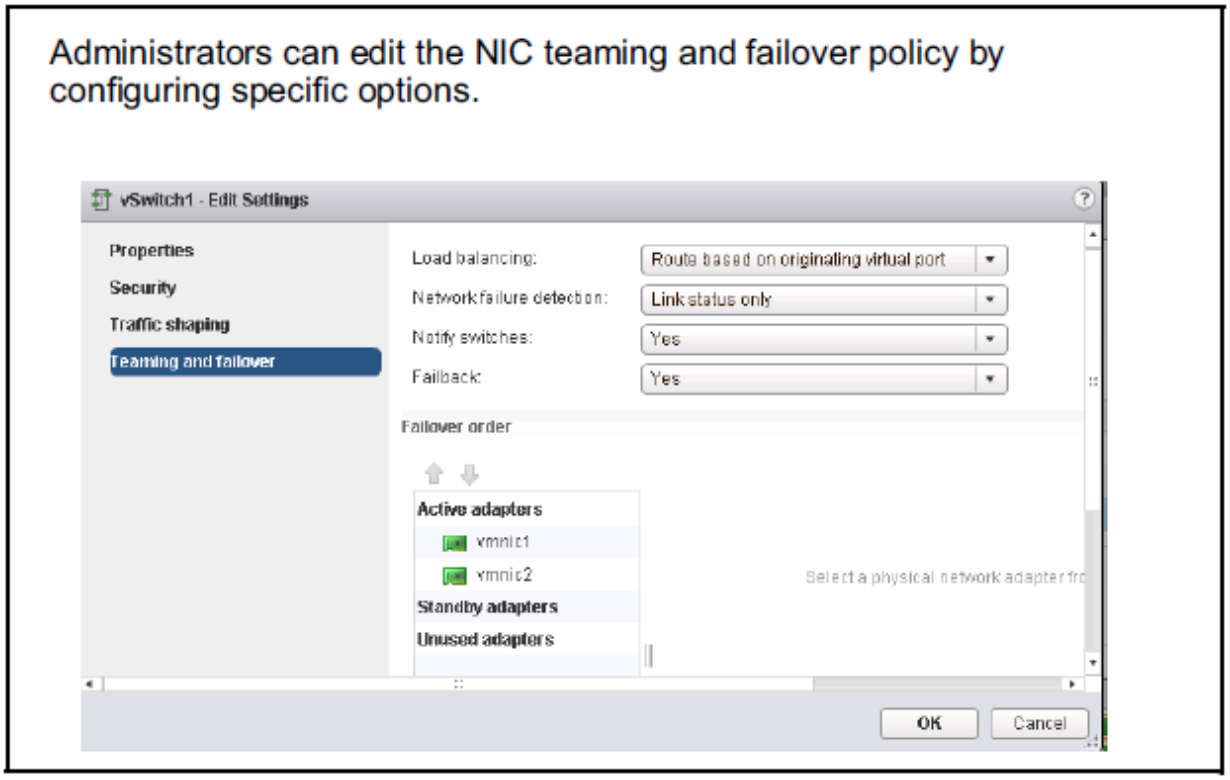



به صورت پیش فرض Traffic Shaping غیرفعال می باشد.

تمامی تنظیمات به تمامی Virtual NIC ها اعمال می شود.

## NIC Teaming and Failover Policy

Slide 5-21




NIC Teaming and Failover به شما این قابلیت را می دهند که چطور ترافیک شبکه را میان کارت های فیزیکی شبکه سرور Distribute کنید و چطور Reroute Traffic در زمانی که یک کارت شبکه فیزیکی Fail می شود.

در قسمت NIC Teaming and Failover ما گزینه های زیر را خواهیم داشت:

- Load Balancing

زمانی که برروی یک Port Group برروی یک سوییچ بیشتر از Uplink وجود داشته باشد می توان برای این Port Group روشی برای Loadbalance انتخاب کرد.

- Network Failure Detection

نحوه تشخیص Network Failure را مشخص می کند.

- Notify Switches

ارسال Notify به سوییچ فیزیکال می باشد .

- Failback

قابلیت Failback به شما این امکان را می دهد که در صورتی که مشکل لینک اصلی حل شود آیا دوباره از آن استفاده شود یا نه

در قسمت Failover Order می توان رفتار کارت شبکه های فیزیکی یک Port Group را مشخص کرد که این رفتار را می توان به صورت زیر دسته بندی کرد:

- Active Adapter

تمامی کارت شبکه هایی که در این قسمت قرار می گیرند در جهت ارسال و دریافت اطلاعات شرکت می کنند و می توانند در عملیات Loadbalance شرکت کنند.

- Standby Adapter

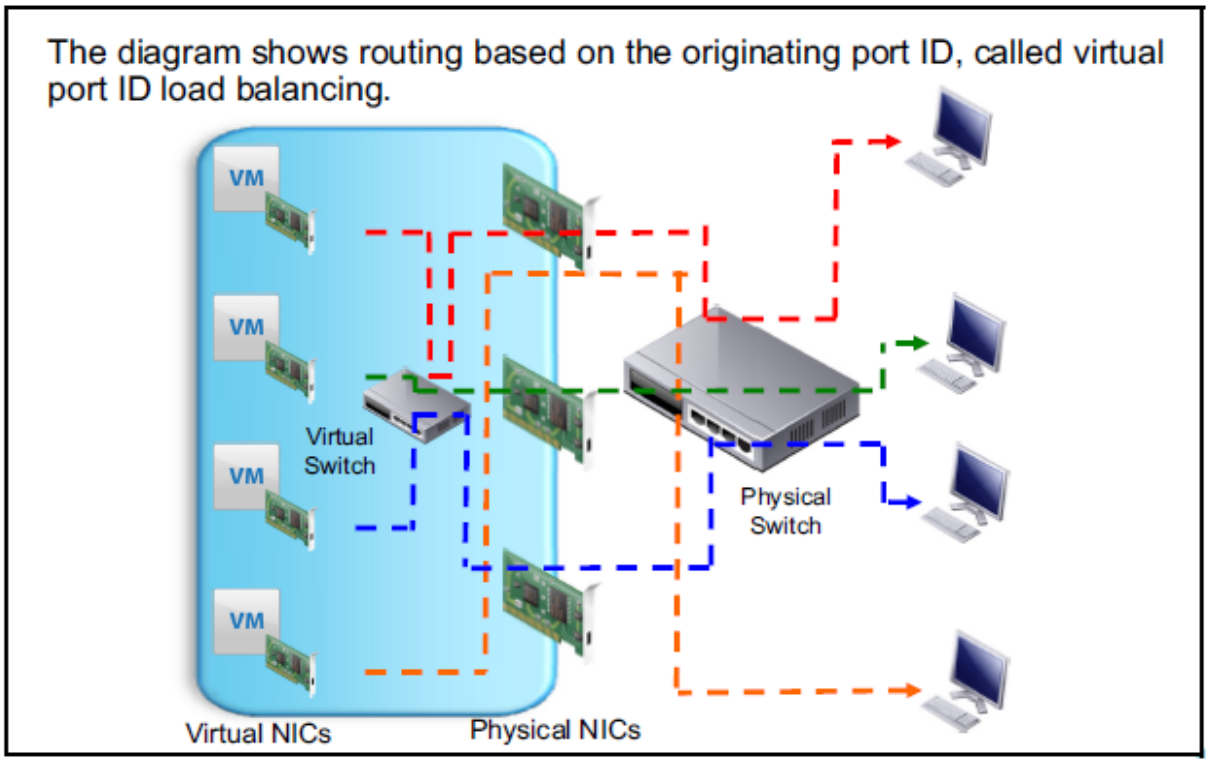
کارت شبکه هایی که در این قسمت قرار می گیرند در حالت Standby هستند و تا زمانی که کارت شبکه های موجود در قسمت Active Adapter در حال سرویس باشند وارد عمل نمی شوند این قسمت برای زمانی در نظر گرفته می شود که بخواهید عملیات Failover را برروی Port Group راه اندازی کنید.

- Unused Adapter

کارت شبکه هایی که در این قسمت قرار می گیرند قابل استفاده توسط این Port Group نیستند و Port Group های دیگر هم نمی توانند از آن استفاده کنند در واقع کارت شبکه هایی که در این قسمت قراردارند رزو می باشند برای مثال کابل کارت شبکه متصل نمی باشد.

## Load-Balancing Method: Originating Virtual Port ID

Slide 5-22

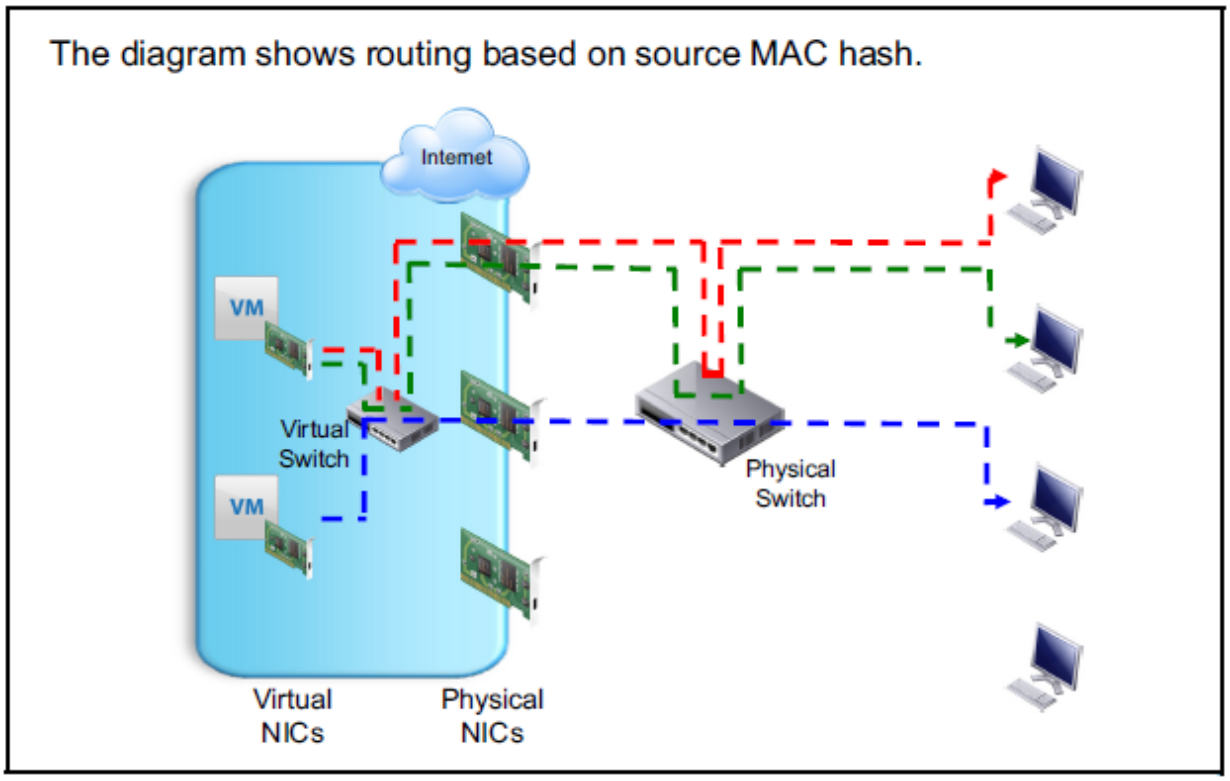



یکی از روش های Loadbalancing که می توان برای یک Port Group استفاده کرد و به صورت پیش فرض استفاده می شود Orginating Virtual Port ID می باشد که براساس Virtual Port ID می باشد زمانی که یک ماشین مجازی به یک Port Group متصل می شود از Port Group یک Virtual Port ID می گیرد براساس VPID و نسبت به تعداد کارت های فیزیکی یک Port Group عملیات Round Robin برای تقسیم بار شبکه استفاده می شود.

در این روش ترافیک یک ماشین مجازی همیشه از یک کارت شبکه فیزیکی ارسال یا دریافت می شود.

## Load-Balancing Method: Source MAC Hash

Slide 5-23




در این روش از Source Mac Hash ماشین مجازی استفاده می شود به عبارت دیگر Source Mac ماشین مجازی در یک الگوریتم Hashing قرار می گیرد و آخرین بیت آن برای یا صفر است یا یک که در صورتی که صفر باشد ماشین مجازی از اولین کارت شبکه فیزیکی استفاده می کند و در صورتی که یک باشد از دومین کارت شبکه فیزیکی استفاده می کند تعداد بیت های آخر در Source Mac Hash بستگی به تعداد کارت های شبکه فیزیکی دارد برای مثال اگر ۲ تا کارت شبکه فیزیکی داشته باشیم یک بیت آخر Source Mac Hash برای Load Balancing استفاده می شود و در صورتی که ۴ تا کارت شبکه فیزیکی داشته باشیم ۲ بیت از Source Mac Hash برای Load Balacing استفاده می شود این روش Overhead کمی دارد ولی در این روش