

A decorative graphic consisting of a light gray circle on the left side, partially overlapping a horizontal bar. The bar has a dark gray left half and a light gray right half. Large black square brackets are positioned on the left and right sides of the bar, framing the main title text.

Virtualios infrastruktūros sauga

**Tinklai ir tinklų sauga virtualioje
infrastruktūroje**

[Virtualus tinklas]

Kompiuterių tinklas virtualioje infrastruktūroje kuriamas naudojant fizinius ir virtualius komponentus.

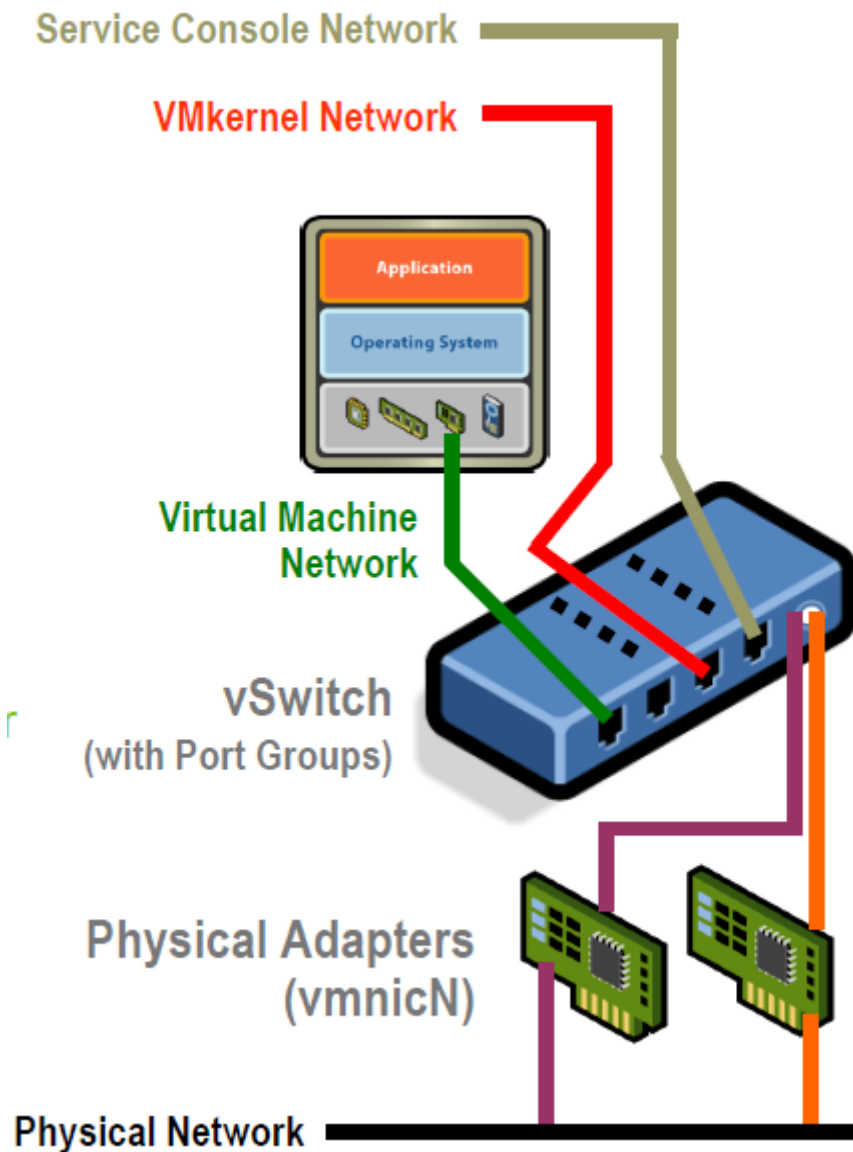
Fiziniai komponentai:

- Tinklo plokštės
- Komutatoriai
- Maršrutizatoriai

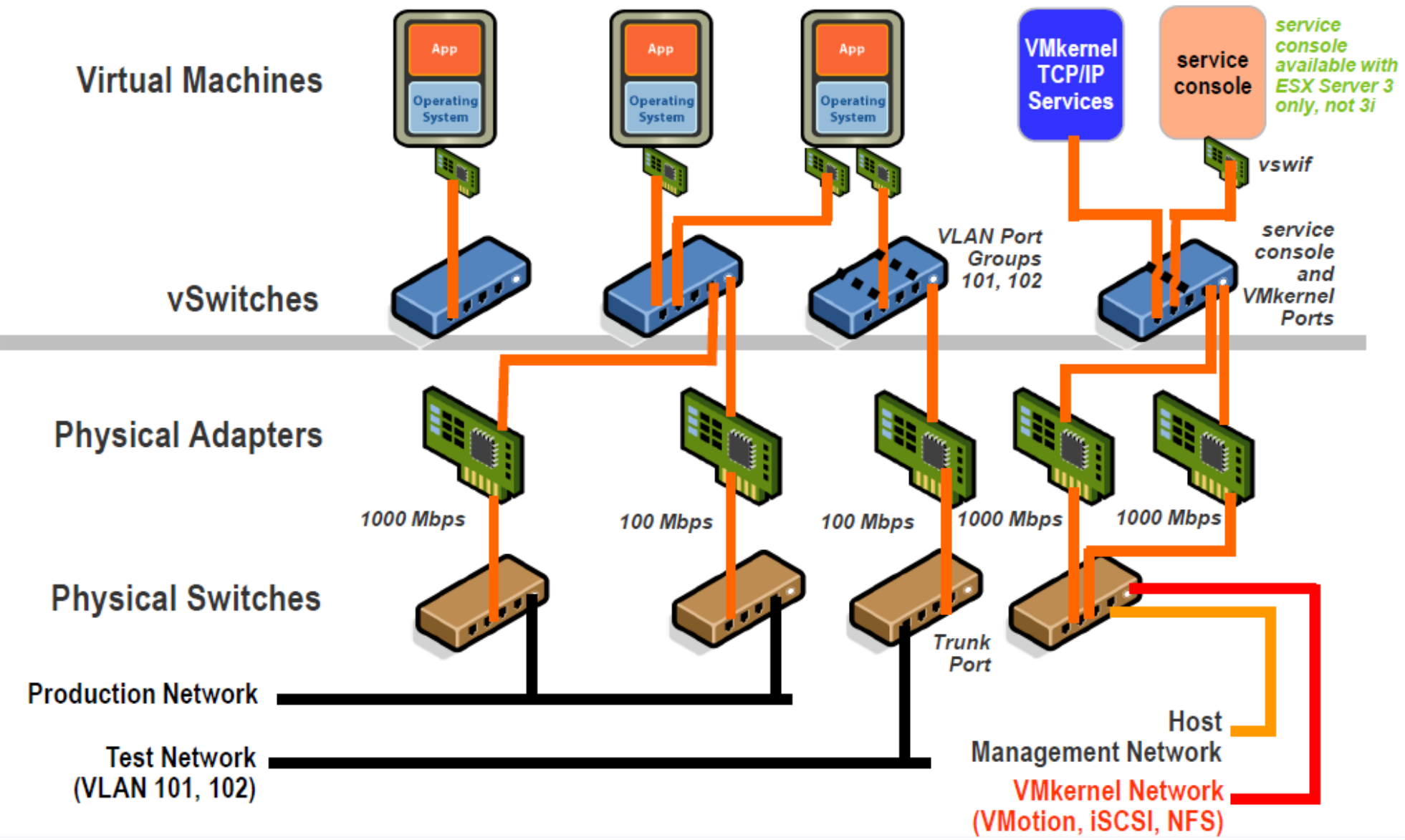
Virtualūs komponentai:

- Virtualios tinklo plokštės (vNIC)
- Vmkernel NIC (vmknic)
- Virtualūs komutatoriai
 - VM prievadai
 - vmkernel prievadai

Tinklo komponentai



Tinklo infrastruktūra



[Virtualios mašinos pajungimas]

Galimi trys būdai, kaip prijungti VM į tinklą:

- Naudoti VM prievadus
- Naudoti vmkernel prievadus
- Naudoti Service Console arba Management Network prievadus.

[Virtualūs NIC]

- vNIC – tai VM virtualios tinklo plokštės.
- VMkernel priklauso tinklo modulis, kuris dar vadinamas vmknics.

Vmware ESX gali emuliuoti tokias tinklo plokštes:

- AMD PCNET32, e1000 (*native*)
- vmxnet (paravirtualizuota)
- vmxnet2 (e1000) (paravirtualizuota)

Paravirtualizuota greitesnė nei *native*. VM gali turėti daugiausiai 4 vNIC.

[Virtualus komutatorius]

Virtualus komutatorius – tai VMkernel modulis, kuris suteikia tinklinį ryšį ESX serveriui. Tai 2 lygmens (Layer2) pagal OSI modelį įrenginys.

Virtualaus komutatoriaus pagalba galime prisijungti prie:

- valdymo tinklo – nuotoliniam prisijungimui prie ESX
- VM tinklo, kuriame užtikrinamas ryšys tarp VM
- IP saugyklos (NAS, iSCSI)
- Išorinio tinklo

Virtualus komutatorius kuriamas:

Configurations -> Networking lange.

[Virtualaus tinklo infrastruktūra]

Virtual Switch: vSwitch0

[Remove...](#) [Properties...](#)



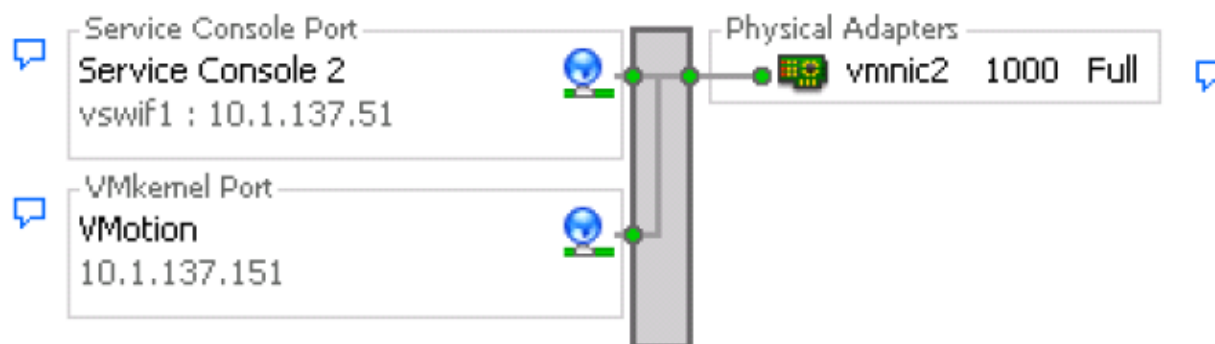
Virtual Switch: vSwitch1

[Remove...](#) [Properties...](#)



Virtual Switch: vSwitch2

[Remove...](#) [Properties...](#)



[Virtualus komutatorius]

- Du ar daugiau virtualių komutatorių negali būti pajugti prie vienos fizinės tinklo plokštės.
- Komutatorius gali turėti 2 ir daugiau fizinių tinklo plokščių ir jas grupuoti (pvz. **nic teaming**) tam kad užtikrinti automatinį paketų paskirstymą ir padidintų patikimumą.
- Tinklo komutatorius, neturintis priskirtos nei vienos fizinės tinklo plokštės, suformuoja vidinį tinklą ESX serverio viduje, leidžiantį VM komunikuoti neišeinant į išorę.

[Virtualus komutatoriaus prievadai]

- Kiekviena virtuali tinklo plokštė (vNIC, service console, vmknic) yra prijungiama prie atitinkamos prievadų grupės.
- Grupių tipai: VM ir VMkernel. (ESX 3.5 papildomai turi Service Console, kuri nuo ESX v.4.0 nebenaudojama)
- Prievadų grupės tipas nustatomas kuriant ją.
- Prievadų grupė kuriama, norint sudaryti atskirą VLAN (802.1q).
- VM „mato“ viena kitą, jei jų vNIC yra toje pačioje prievadų grupėje.
- VLAN ID galimi nuo 0 iki 4095.

[Virtualus komutatorius]

vSwitch valdo prievadų grupę, tačiau neturi galimybės konfigūruoti atskiro prievado.

vSwitch turi visas žinomas Layer 2 apsaugas:

- packet sniffing,
- MAC spoofing,
- srauto ribojimą.

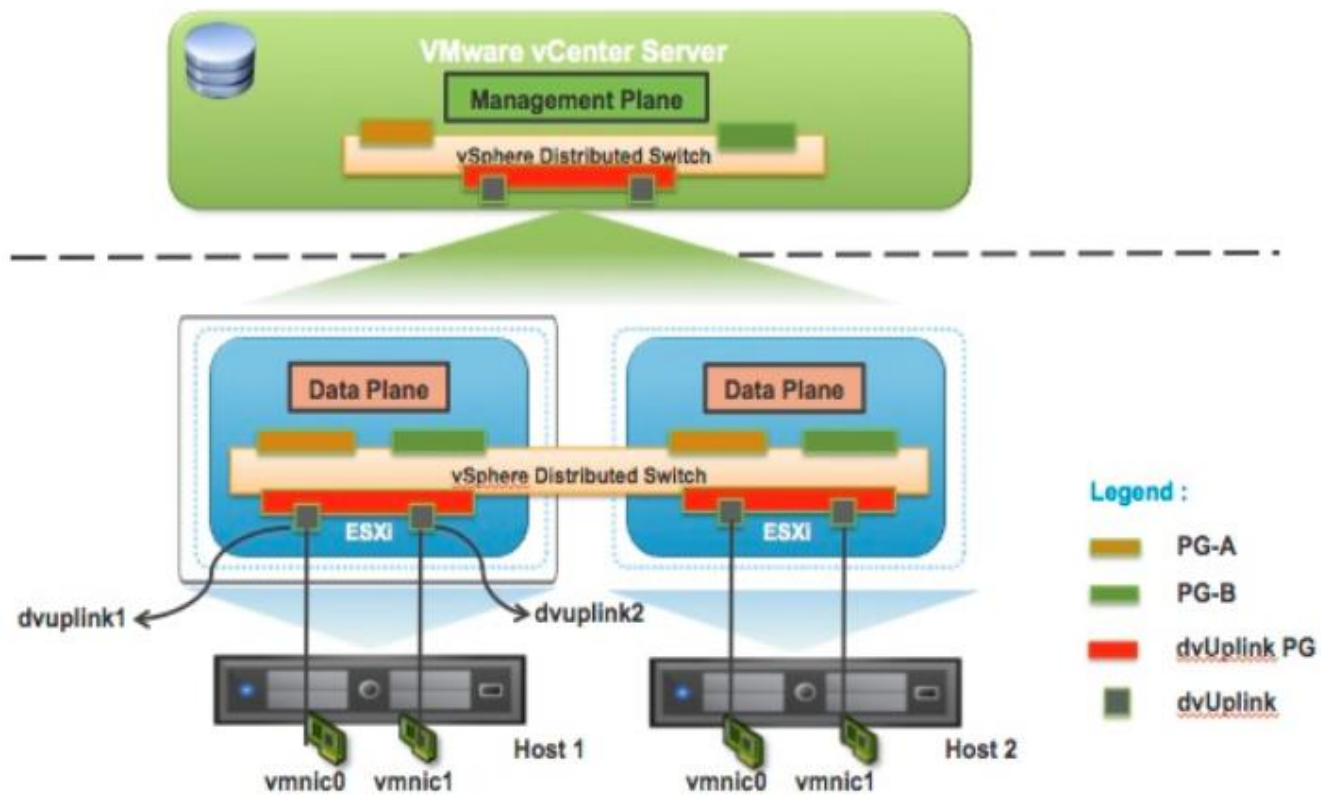
Nuo aukštesnio lygio (Layer 3) grėsmių turi būti apsisaugota naudojant VM vidines ugniasienes arba kitas priemones.

[Paskirstytas virt.komutatorius]

Distributed Virtual Switch (DVS) suteikia sistemos administratorius prieigą valdant tinklą.

- Centralizuotas vSwitch prievadų konfigūravimas, prievadų vardų suteikimas, filtravimas ir t.t.
- Link Aggregation Control Protocol (LACP) – suderina ir automatiškai konfigūruoja jungčių agregaciją tarp ESX serverių ir fizinių komutatorių.
- Tinklo monitoringas
 - Palaiko RSPAN ir ERSPAN protokolus nuotolinei tinklo analizei
 - IPFIX Netflow v. 10
 - SNMP v3

[Paskirstytas virt.komutatorius]



[Prijungimų tikrinimas]

Norint patikrinti ar teisingi fizinių tinklo plokščių ir virtualių komutatorių nustatymai, galima naudoti konsolės komandas (prisijungus per ssh):

```
> esxcfg-nics -l
```

```
> esxcfg-vswitch -l
```

esxcfg-nics komanda parodo fizinės tinklo plokštės MAC adresą ir sąryšį tarp fizinės ir virtualios tinklo plokštės *vmnic*.

[VLAN kūrimas]

Norint izoliuoti tarpusavyje virtualias mašinas, reikia sukurti prievadų grupes su nustatytais VLAN reikšmėmis.

VLAN leidžia sukurti daug loginių LAN fiziniame tinklo segmente.

VLAN leidžia:

- Padidinti saugumą t.y. nusiųsti paketą į teisingą segmentą;
- Padidina našumą, nes VLAN turi savo transliavimo domeną;
- Sumažinti kainą, nes nereikalingi fiziniai komutatoriai.

VLAN apibrėžia IEEE 802.1Q standartas, pagal kurį formuojami papildomi laukai kadre:

indikacinis 802.1Q (2 bytes) + VLAN ID (2 bytes)

[VLAN kūrimas]

VLAN kuriami tinklo komutatoriuose grupuojant:

- **prievadus**
- **tinklo įrenginių MAC adresus.**

Prievadų grupavimo atveju vieno VLAN prievadams suteikiamas tas pats VLAN ID. Paketas iš vieno VLAN niekada nepereina į kitą VLAN.

Grupuojant MAC adresus, komutatoriaus konfigūracijoje turi būti surašyti visų įrenginių MAC adresai, kurie priklausys konkrečiam VLAN.

Toks grupavimas retai naudojamas dėl didelio rankinio darbo kiekio.

[VLAN tipai]

Naudojami tokie VLAN tipai:

- Numatytasis (default) VLAN
- Gimtasis (native) VLAN
- Duomenų (data) VLAN

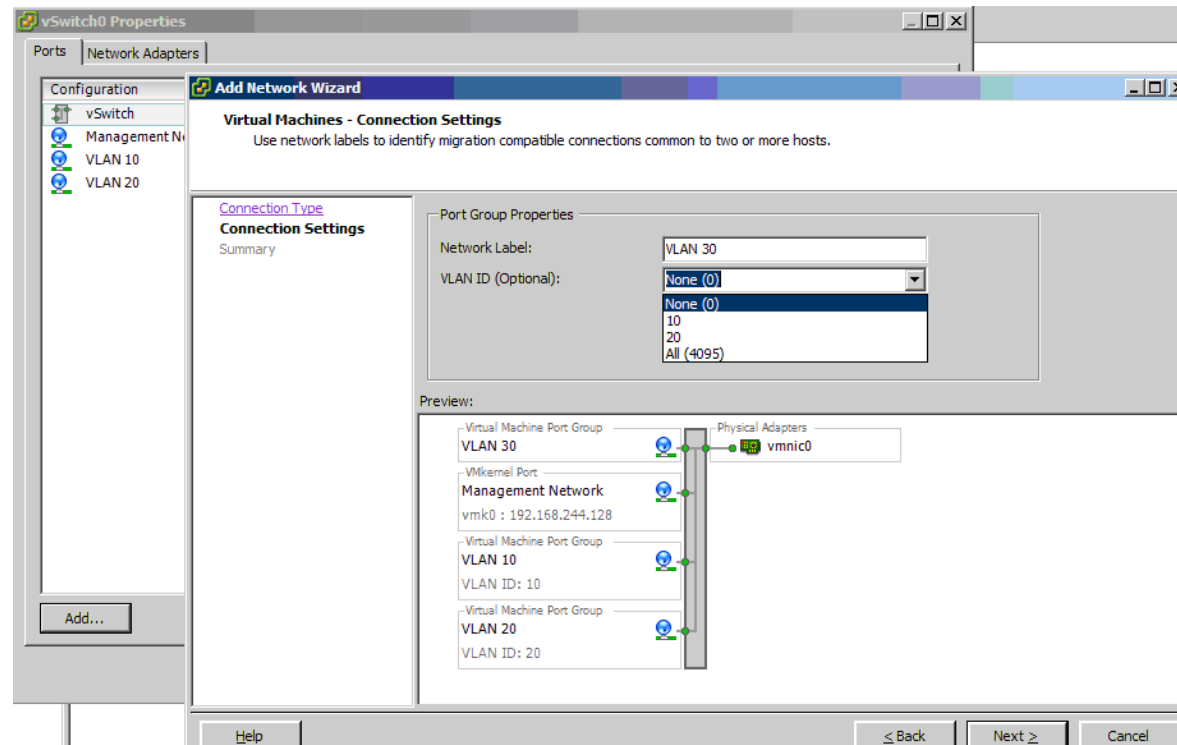
Numatytasis VLAN priskiriamas visiems komutatoriaus prievadams pirmą kartą užsikrovus sistemą. Numatytojo VLAN ID lygus 1 ir negali būti keičiamas (skaičius).

Gimtasis VLAN priskiriamas prie 802.1Q trunk port. 802.1Q trunk port persiunčia srautą, einantį iš bet kurio VLAN (tagged traffic) ir srautą, kuris nepriklauso jokiam VLAN.

Duomenų VLAN naudojamas vartotojų duomenų perdavimui.

[VLAN kūrimas]

VLAN kūrimas atliekamas pasirenkame virtualiųjų mašinių prievadų tipą ir nurodome pavadinimą ir „VLAN ID” reikšmę.



[VLAN konfigūravimas]

1. Sukuriami visi nurodyti virtualūs prievadai ir priskiriama VLAN ID reikšmė.
2. VM pajungimas prie VLAN atliekamas pasirinkus VM nustatymuose tinklo plokštę ir priskyrus jai atitinkamą VLAN. Analogiškai priskiriam tinklo plokštę komutatoriaus prievadų grupei ir kai nėra naudojami VLAN.

VM pajungimas prie VLAN

The screenshot displays the VMware ESXi 5.0.0 interface. At the top, the title bar reads "esx50 VMware ESXi, 5.0.0, 469512". Below it, a navigation bar includes tabs for "Getting Started", "Summary", "Virtual Machines", "Resource Allocation", "Performance", "Configuration", "Local Users & Groups", "Events", and "Performance".

The main area features a table of virtual machines:

Name	State	Provisioned Space	Used Space	Host CPU - MHz	Host Mem - MB
Windows 7 32 bit	Powered Off	22,16 GB	7,58 GB	0	0
Asta	Powered Off	24,12 GB	7,58 GB	0	0
MUbuntu1srv	Powered Off	11,14 GB	7,55 GB	0	0
MUbuntu2dsk	Powered Off	5,61 GB	5,00 GB	0	0
TEST	Powered Off	4,64 GB	2,64 GB	0	0

Below the table, the "Virtual Machine Properties" window for "Windows 7 32 bit" is open. It shows the "Hardware" tab with a list of devices:

Hardware	Summary
Memory	2048 MB
CPUs	2
Video card	Video card
VMCI device	Restricted
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk
CD/DVD drive 1	/vmfs/devices/cdrom/...
Network adapter 1	Testas2
Floppy drive 1	Client Device

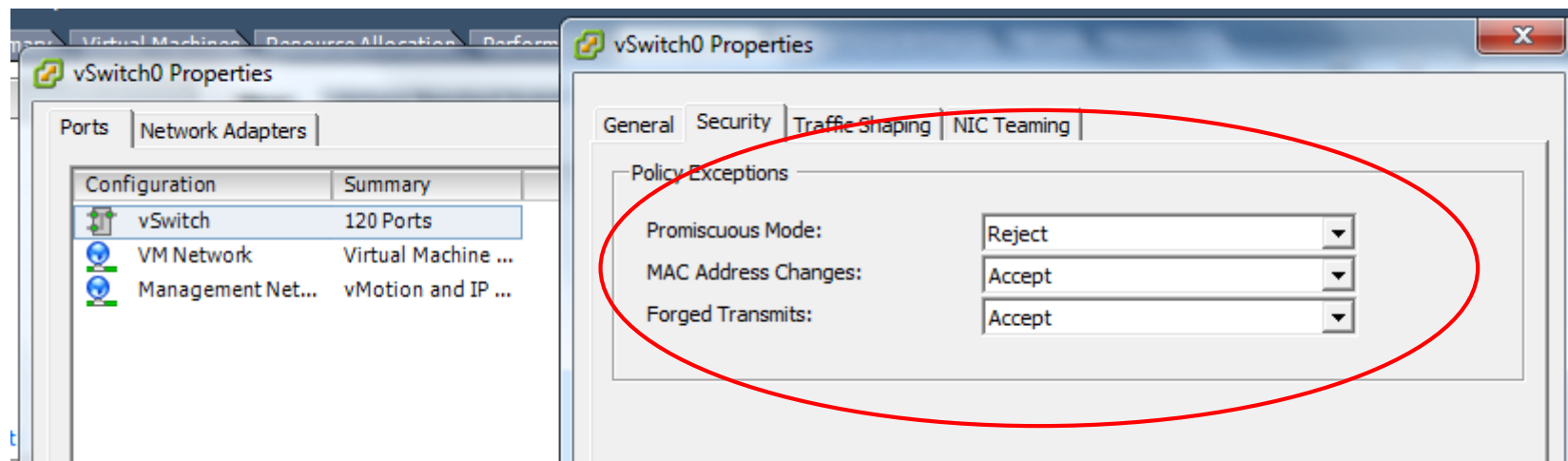
The "Network adapter 1" configuration is shown on the right. It includes the following settings:

- Device Status:** Connected, Connect at power on
- Adapter Type:** Current adapter: E1000
- MAC Address:** 00:0c:29:93:08:a5, with radio buttons for Automatic and Manual
- DirectPath I/O:** Status: Not supported
- Network Connection:** Network label: Asta, NAT, VM Network, VSwitchMantas, VSwitchTomkevicius

[Virtualaus komutatoriaus sauga]

Virtualaus komutatoriaus saugos nustatymai (Layer 2) išeinančiam srautui:

- Allow Promiscuouse Mode
- Allow MAC address Change
- Allow Forged Transmit



[Virtualaus komutatoriaus sauga]

Promiscuous Mode

- Reject – VM tinklo adapterio nustatymas į promiscuous režimą nedaro įtakos adapterio darbui
- Accept – VM tinklo adapterį nustatymas į promiscuous režimą leidžia tikrinti visus tinkle keliaujančius kadrus (IDS, Sniffer).

MAC address Change

- Reject – jei VM tinklo adapterio MAC adresas pakeičiamas į kitą nei nustatyta .vmx faile, kadrai atmetami.
- Accept - VM tinklo adapterio MAC adreso keitimas leidžiamas ir nesukelia jokių ribojimų.

Forged Transmit

- Reject — bet kurie išeinantys kadrai su skirtingu MAC adresu, nei nustatyta adapteryje atmetami.
- Accept — nefiltruojama ir visi išeinantys kadrai yra praleidžiami.

[Prievadų grupės sauga]

Komutatoriaus saugos nustatymai paveldimi prievadams, nors priedų grupėms gali būti perrašomi analogiškai trijų tipų saugos nustatymai tik su skirtingomis reikšmėmis:

- Allow Promiscuous Mode
- Allow MAC address Change
- Allow Forged Transmit

The image shows two overlapping windows from a vSphere interface. The background window is 'vSwitch0 Properties' with the 'Network Adapters' tab selected. It shows a table of network adapters and a list of effective policies. The foreground window is 'VM Network Properties' with the 'Security' tab selected. A red oval highlights the 'Policy Exceptions' section in the foreground window.

Configuration	Summary
vSwitch	120 Ports
VM Network	Virtual Machine ...
Management Net...	vMotion and IP ...

Port Group Properties

Network Label: VM Network
VLAN ID: None (0)

Effective Policies

Security

Promiscuous Mode: Rej
MAC Address Changes: Acc
Forged Transmits: Acc

Traffic Shaping

Average Bandwidth: --
Peak Bandwidth: --

VM Network Properties - Security

Policy Exceptions

Promiscuous Mode: Reject
MAC Address Changes: Accept
Forged Transmits: Accept

[Srauto valdymo principai]

Tinklo srauto valdymas gali būti daromas tik **išeinančiam** srautui.

Išeinantis srautas valdomas apibrėžiant:

- Vidutinį pralaidumą (Kbps)
- Maksimalų (peak) pralaidumą (Kbps)
- Pliūpsnio (burst) dydį apskaičiuojamą kaip KB

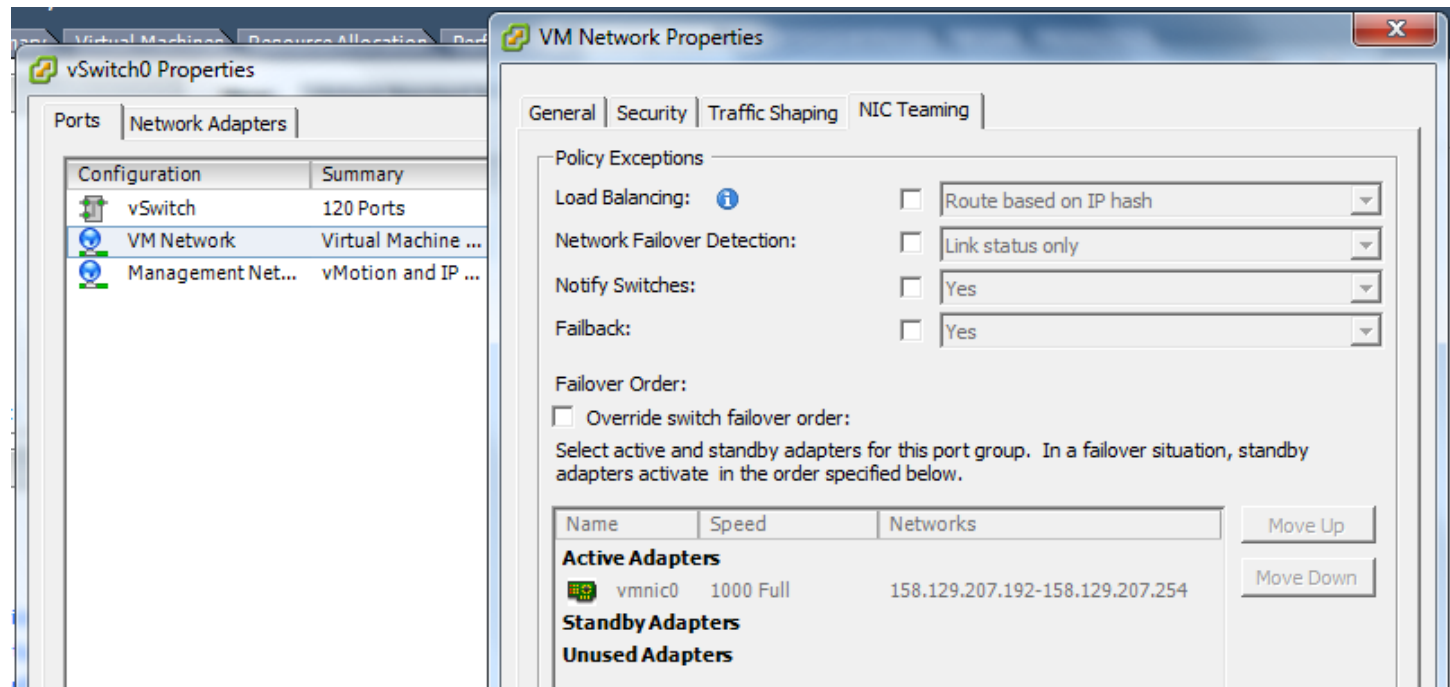
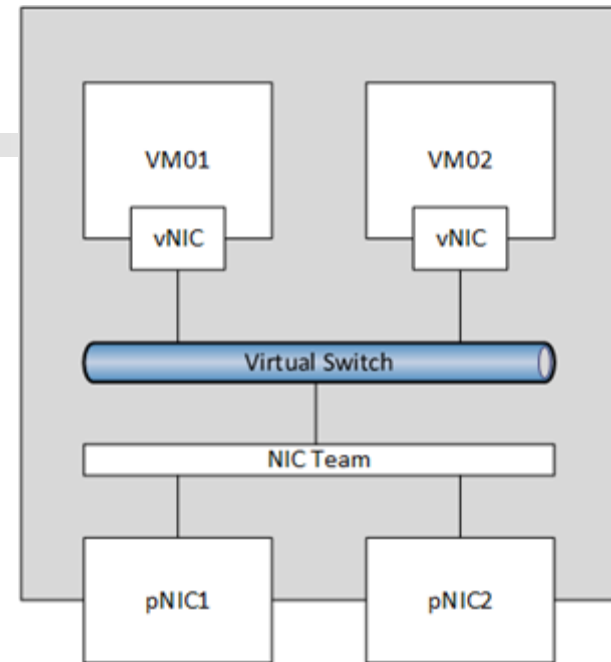
$$\text{Burst} = \text{Bandwidth} * \text{time}$$

Įėjimo srautas turi būti valdomas fiziniuose maršrutizatoriuose.

[pNIC grupės

Virtualus komutatorius gali turėti:

- Dedikuota pNIC (1 vnt.)
- Keletą dedikuotų pNIC
 - Apkrovos balansavimui
 - Patikimumo (failover) didinimui



[pNIC grupavimas]

Norint gauti apkrovos balansavimo ar padidinto patikimumo sistemas, keli pNIC priskiriami vienam virtualiam komutatoriui ir apjungiami į grupę (NIC teaming).

The screenshot shows the VMware vSphere Configuration interface for a host. The 'Configuration' tab is selected, and the 'Networking' section is expanded to show 'Virtual Switch: vSwitch0'. The 'View' is set to 'Virtual Switch'. The 'Networking' section displays a diagram of the vSwitch configuration. On the left, under 'Virtual Machine Port Group', there are two entries: 'VM Network' and 'Management Network' (with IP address vmk0 : 192.168.130.128). On the right, under 'Physical Adapters', there are two entries: 'vmnic1' and 'vmnic0', both with a speed of 1000 and status 'Full'. The diagram shows lines connecting the VM Network and Management Network to the vSwitch, which is then connected to the physical adapters. There are 'Remove...' and 'Properties...' buttons next to the vSwitch name.

localhost.localdomain VMware ESXi, 4.1.0, 348481 | Evaluation (60 days remaining)

Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions

Hardware

- Health Status
- Processors
- Memory
- Storage
- Networking
- Storage Adapters
- Network Adapters
- Advanced Settings
- Power Management

Software

- Licensed Features

View: Virtual Switch

Networking

Virtual Switch: vSwitch0 [Remove...](#) [Properties...](#)

Virtual Machine Port Group

- VM Network
- Management Network
vmk0 : 192.168.130.128

Physical Adapters

- vmnic1 1000 Full
- vmnic0 1000 Full

[Apkrovos balansavimas]

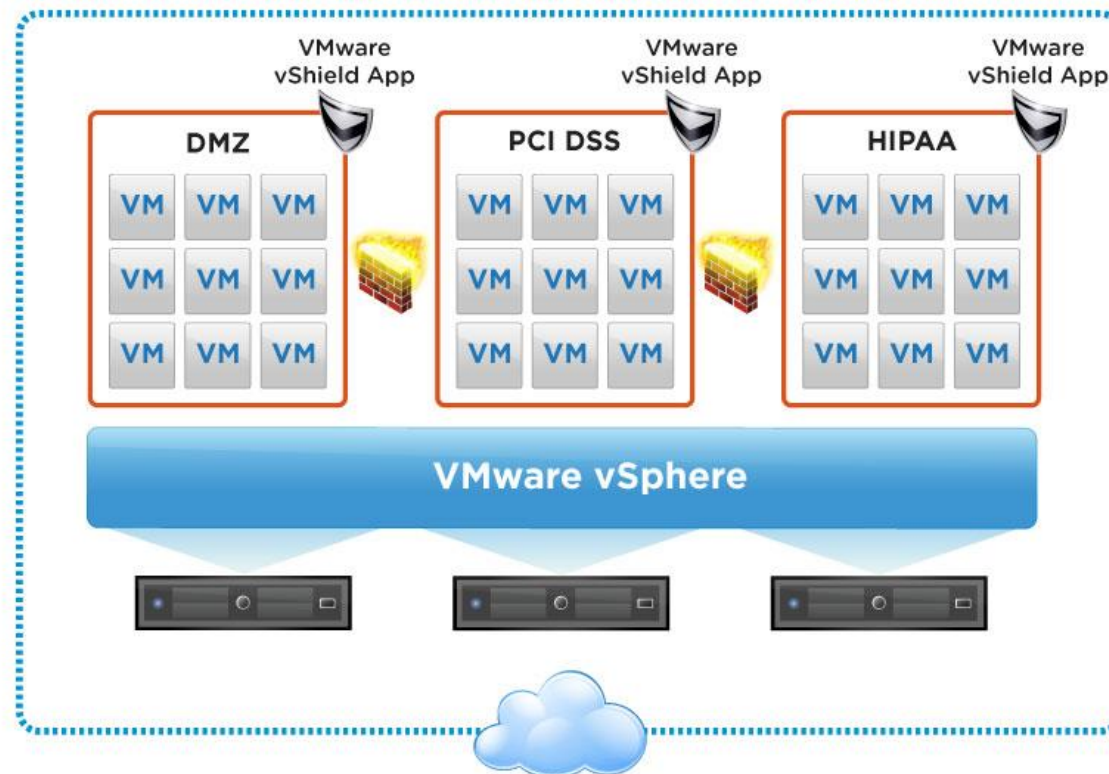
Balansuojant apkrovą, VMkernel nusprendžia per kurią pNIC IP paketas turi būti išsiųstas.

Balansavimui naudojami tokie maršrutizavimo algoritmai:

- pagal prievado ID (nesudaro CPU apkrovos)
- Pagal siuntėjo MAC hash (vidutinė CPU apkrova)
- Pagal IP hash (imlus CPU apkrovai, galimas didesnis išeinančio srauto pralaidumas per kelias pNIC, reikalingas 802.3ad palaikymas – link aggregation).

[Saugumo zonos]

Dėl lankstaus virtualių komutatorių konfigūravimo galimybių, virtualioje infrastruktūroje galimos įvairios saugumo zonos.



[Tinklo gedimų detektavimas]

- Tinklo gedimus aptinka VMkernel, kuri stebi:
 - Sujungimo (link) būseną
 - Srauto apkrovimą (beaconing)
- Gedimai yra apeinami (failover) konfigūruojant tinklo nustatymus:
 - Apkrovos balansavimą
 - Padidintą patikimumą
 - Atstatymo procedūras (failback) t.y. kai pNIC vėl prijungiama prie tinklo.

Tinklo gedimų detektavimas

The screenshot displays the VMware vSphere configuration interface for a vSphere Standard Switch (vSwitch0). The main window shows the vSwitch configuration, including a list of network adapters connected to it. A dialog box titled "vSwitch0 Properties" is open, showing the "NIC Teaming" tab. The "Network Failover Detection" dropdown menu is highlighted with a red circle, and its value is set to "Link status only".

vSwitch0 Properties - Network Adapters

Configuration	Summary
vSwitch	120 Ports
VM Network 3	Virtual Machine ...
VM Network 2	Virtual Machine ...
VM Network	Virtual Machine ...
Management Net...	vMotion and IP ...

vSwitch0 Properties - NIC Teaming

Policy Exceptions:

- Load Balancing: Route based on the originating virtual port ID
- Network Failover Detection: **Link status only**
- Notify Switches: Yes
- Failback: Yes

Failover Order:

Select active and standby adapters for this port group. In a failover situation, standby adapters activate in the order specified below.

Name	Speed	Networks
Active Adapters		
vmnic0	1000 Full	192.168.44.1-192.168.44.1
vmnic1	1000 Full	192.168.44.1-192.168.44.1
Standby Adapters		
Unused Adapters		

Adapter Details:

Name:
Location:
Driver: