# Operatsioonisüsteemi ja teenuste administreerimine

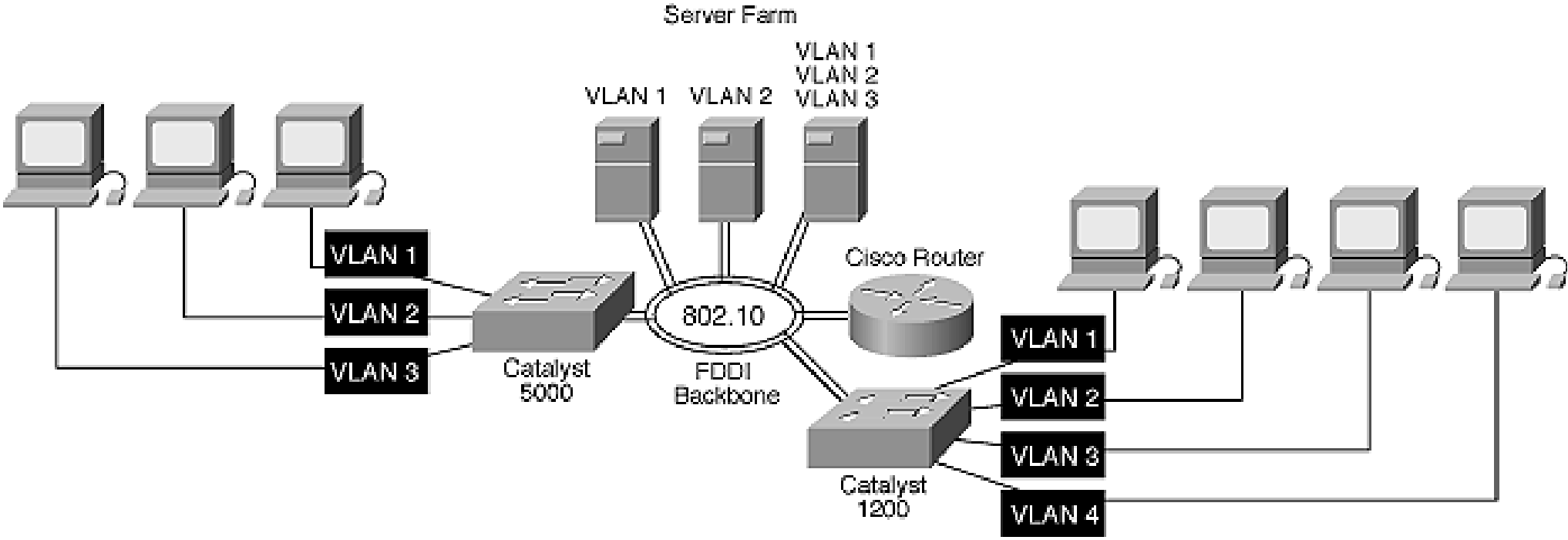
- Virtualiseerimine
- Konteinerid

# Virtualiseerimine

Virtualiseerimine on süsteemihalduses üldine trend

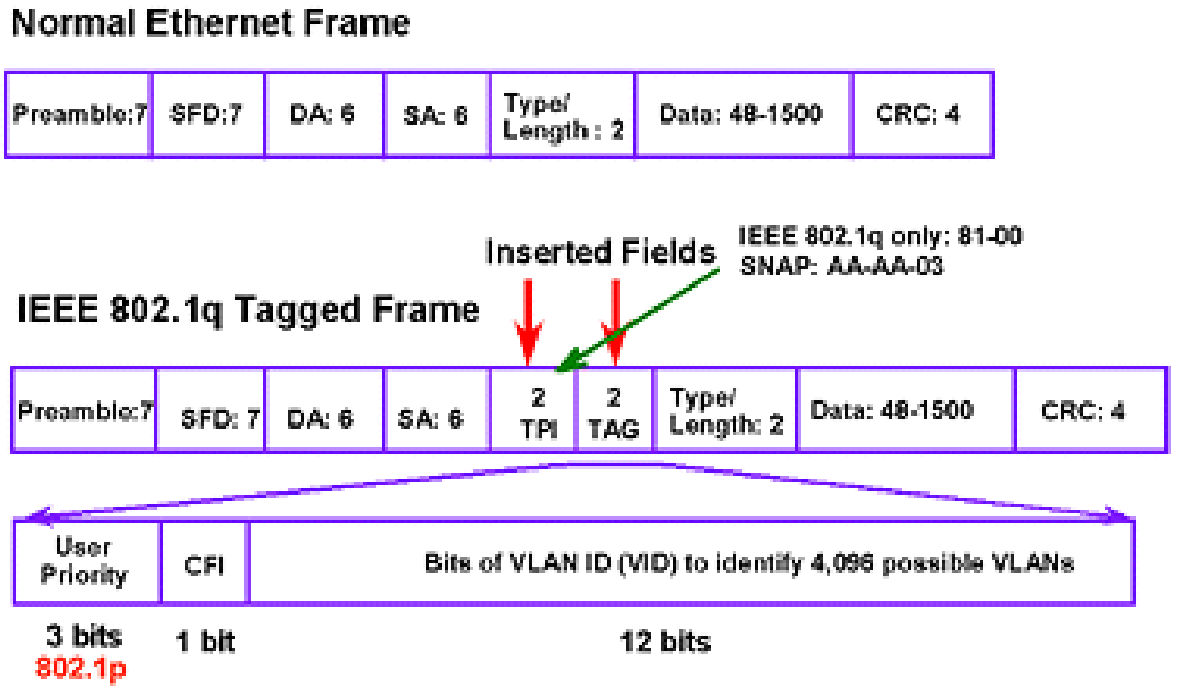
- Võrkude virtualiseerimine
  - VPN – firma sisevõrk IP tasandil üle avaliku võrgu
  - VLAN – virtuaalne võrk Etherneti tasandil
- Kettahalduse virtualiseerimine
  - SAN, NAS, RAID, LVM
- Ressursside virtualiseerimine OS-s
  - virtuaalmälu, protsessori aja jagamine, võrguliidesed
- Teenuste tasemel virutaliseerimine
  - virtuaalsed veebiserverid, meiliserverid
- Protsesside kapseldamine
  - Java, sandboxes (Chrome, Adobe)
- Serverite virtualiseerimine

# VLAN näide

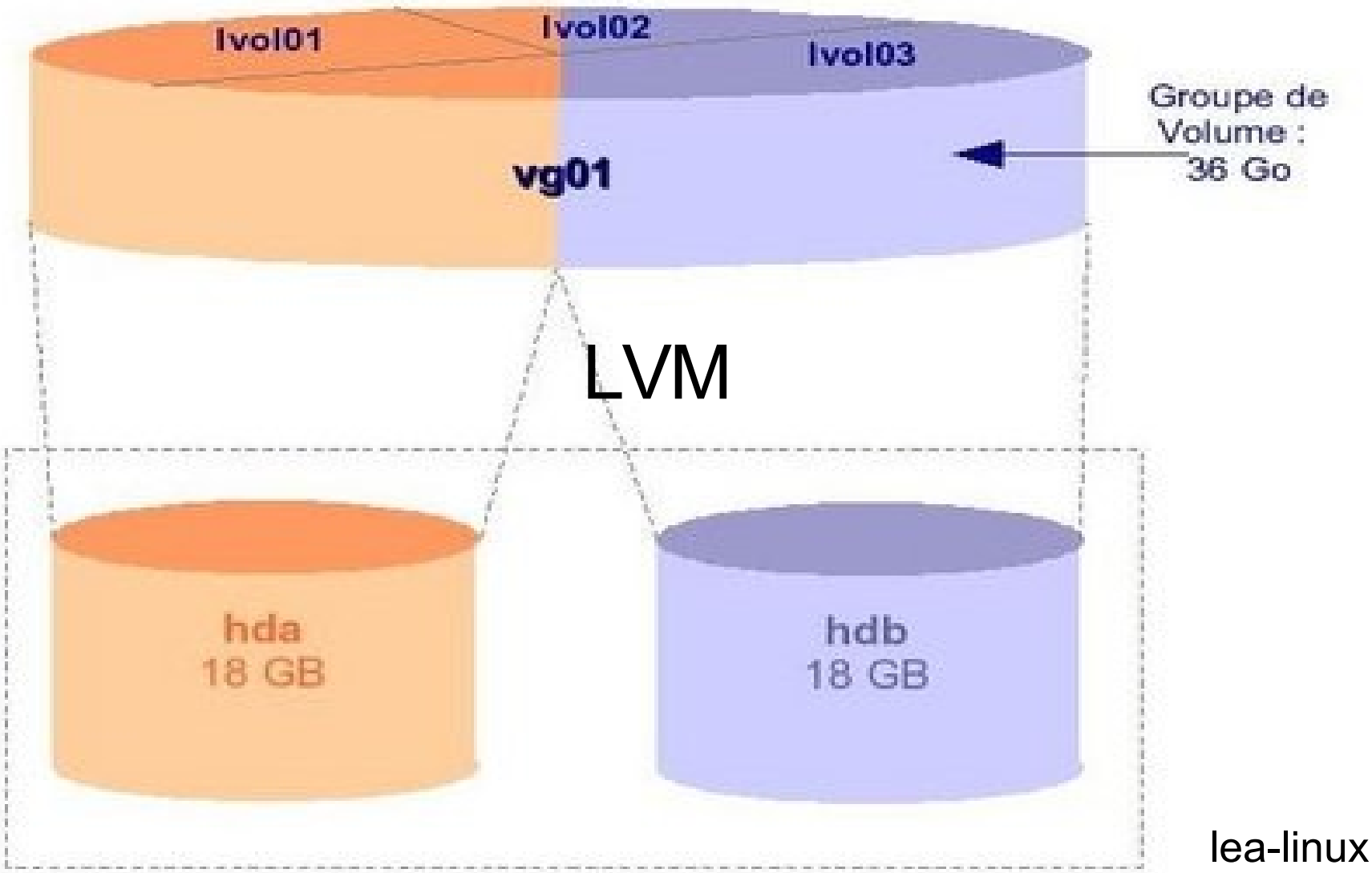

Server Farm
VLAN 1
VLAN 2
VLAN 3
VLAN 1
VLAN 2
VLAN 3
Cisco Router
802.10
FDDI
Backbone
Catalyst
5000
Catalyst
1200
VLAN 1
VLAN 2
VLAN 3
VLAN 4

# 802.1q VLAN tagging

- 802.1q märgendamine võimaldab
  - defineerida VLAN-i, kus seadmed asuvad eri switchide küljes
  - seadmed kuuluvad korraga mitmesse VLAN-i
- Kõik võrguseadmed ei aktsepteeri 802.1q pakette!
- Muudab Etherneti paketi päist
  - TPI - 2 baiti
  - TAG – 2 baiti
    - prioriteet
    - VLAN ID 1-4096

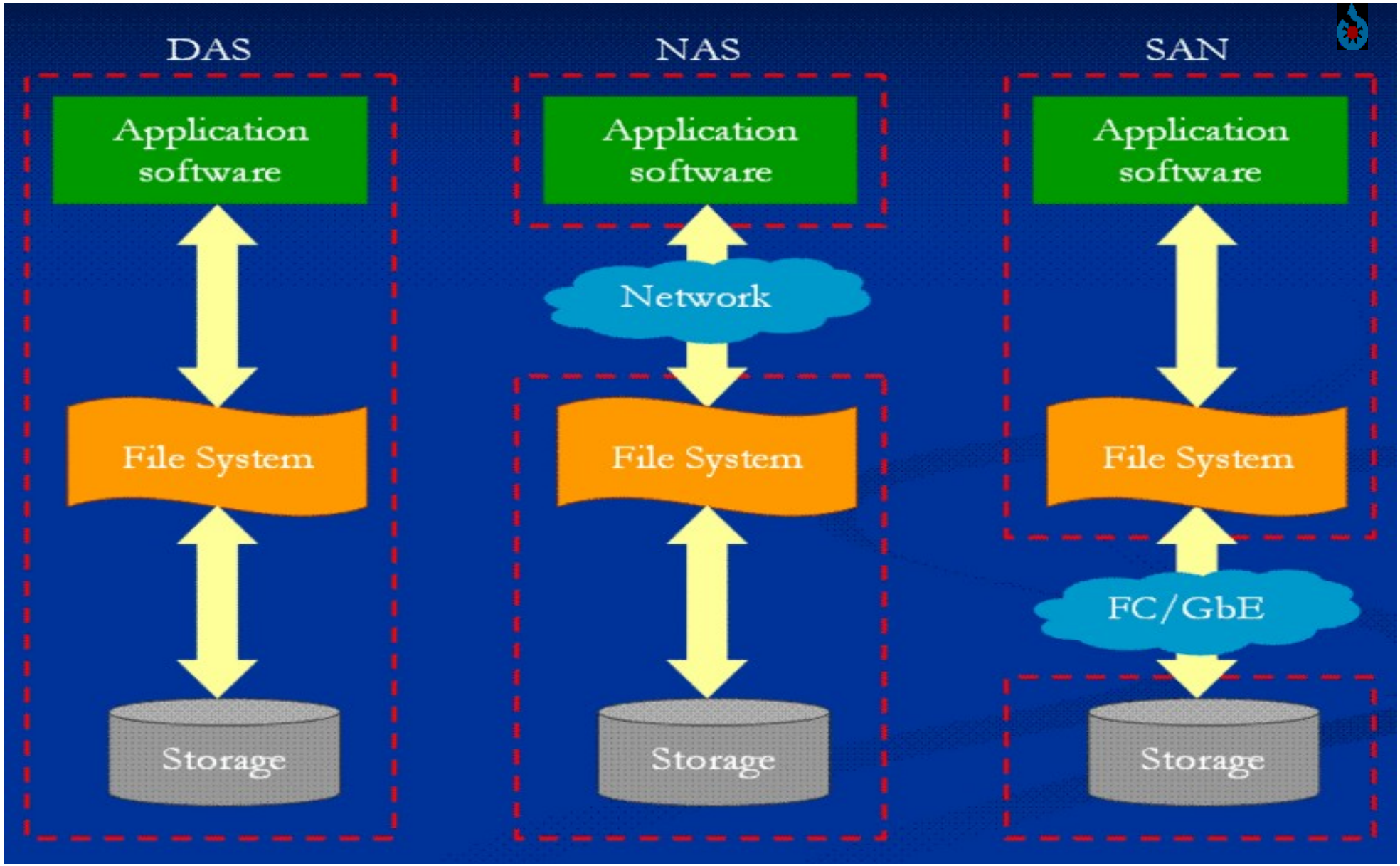


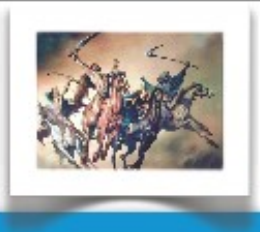
# LVM




lea-linux.org

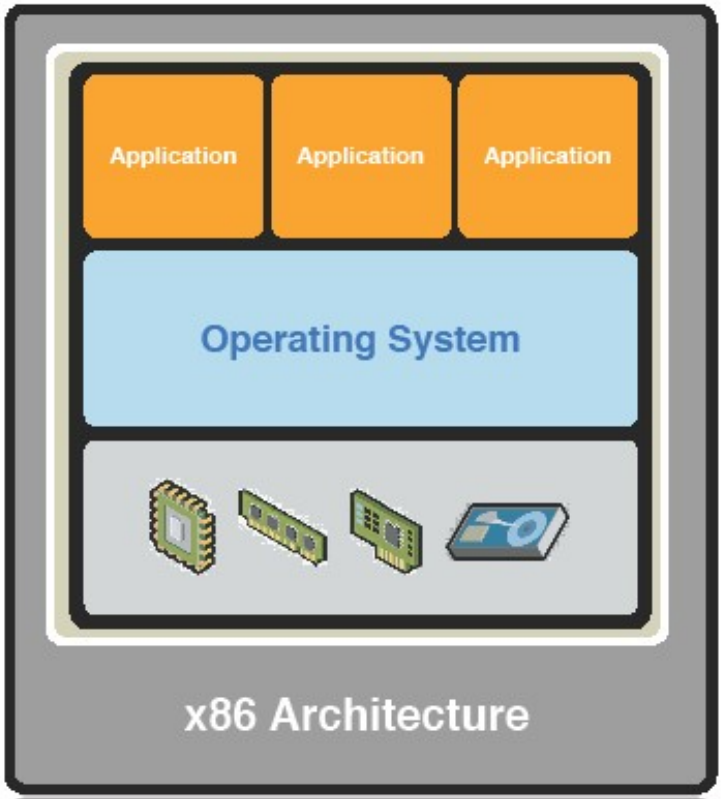
# DAS-NAS-SAN


DAS
Application software
File System
Storage
NAS
Application software
Network
File System
Storage
SAN
Application software
File System
FC/GbE
Storage

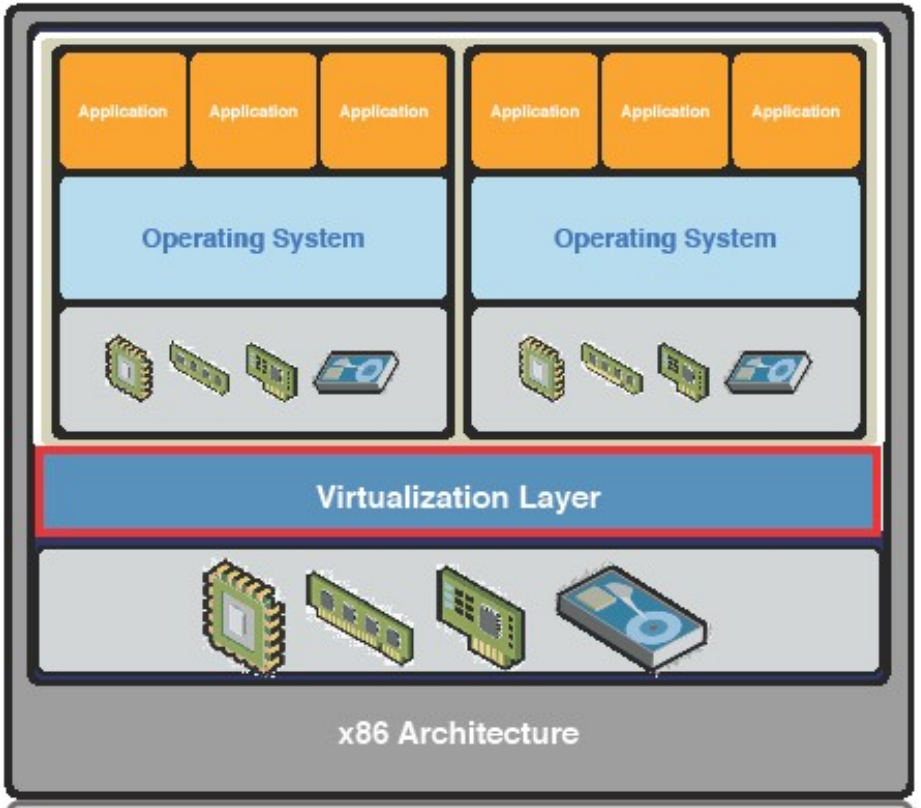


# x86 Virtualization* Overview

## From This




## To This




*Represents "Type 1" or Bare Metal "Server" Virtualization

# Isoleerimine

Virtualiseerimise fundametaalne olemus

- Tarvara isoleerimine
  - Erinevad versioonid
  - Erinevad teegid (DLL hell)
- Turvakontektstide isoleerimine
  - Teenused eraldi
  - Erinevad kasutajate ja haldajate baasid
- Jõudluse isoleerimine
  - Ressursside dünaamiline jagamine

# Miks?

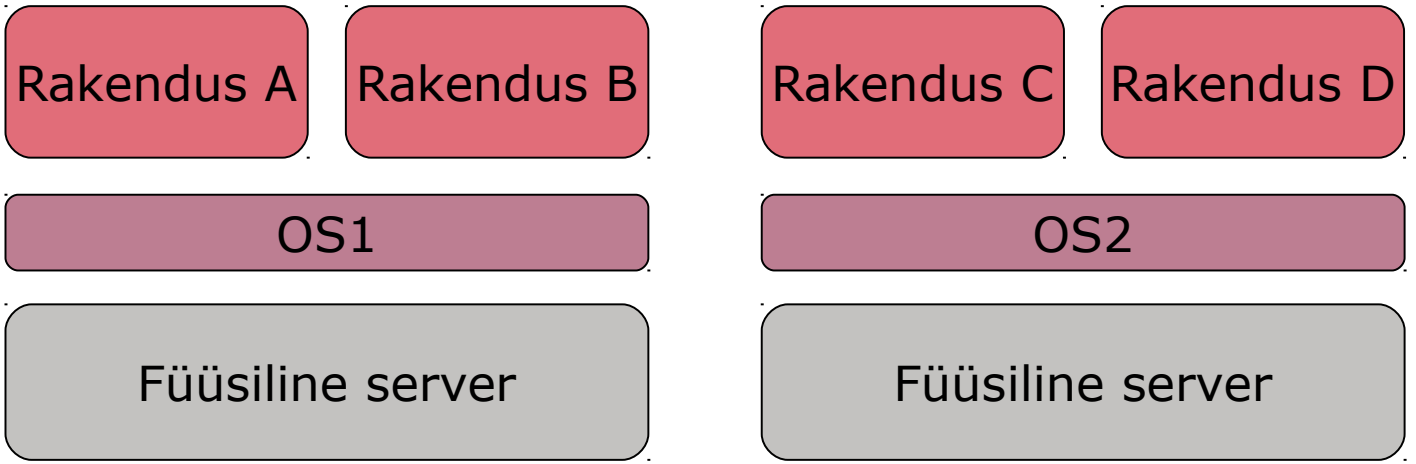
- Sest virtualiseerimine võimaldab:
  - suurendada rakenduste turvalisust (iga rakenduse jaoks oma virtuaalmasin);
  - loob uusi võimalusi nii serverites (uus server vähem kui 10 minutiga) kui tööjaamades (erinevate operatsioonisüsteemide samaaegne kasutamine);
  - suurendada riistvara kasulikku koormatust ning kohandada ressursse vastavalt koormusele;
  - vähendada sõltuvusi riistvarariketest;
  - hoida kokku kulusid (toide, jahutus, riiulipind).

# Virtuaalmasinate kasutajad

- Serverimajutusega tegelev teenusepakkuja
- Ettevõtja/IT juht, kes peab servereid hankima ja käideldavuse tagama
- Tarkvara kasutajatugi
- Tarkvara arendaja ja testija
- Demo, õpetajad
- Teistel asjahuvilised

# Levinud olukord

- Hulk reaalseid servereid



# Virtualiseermine

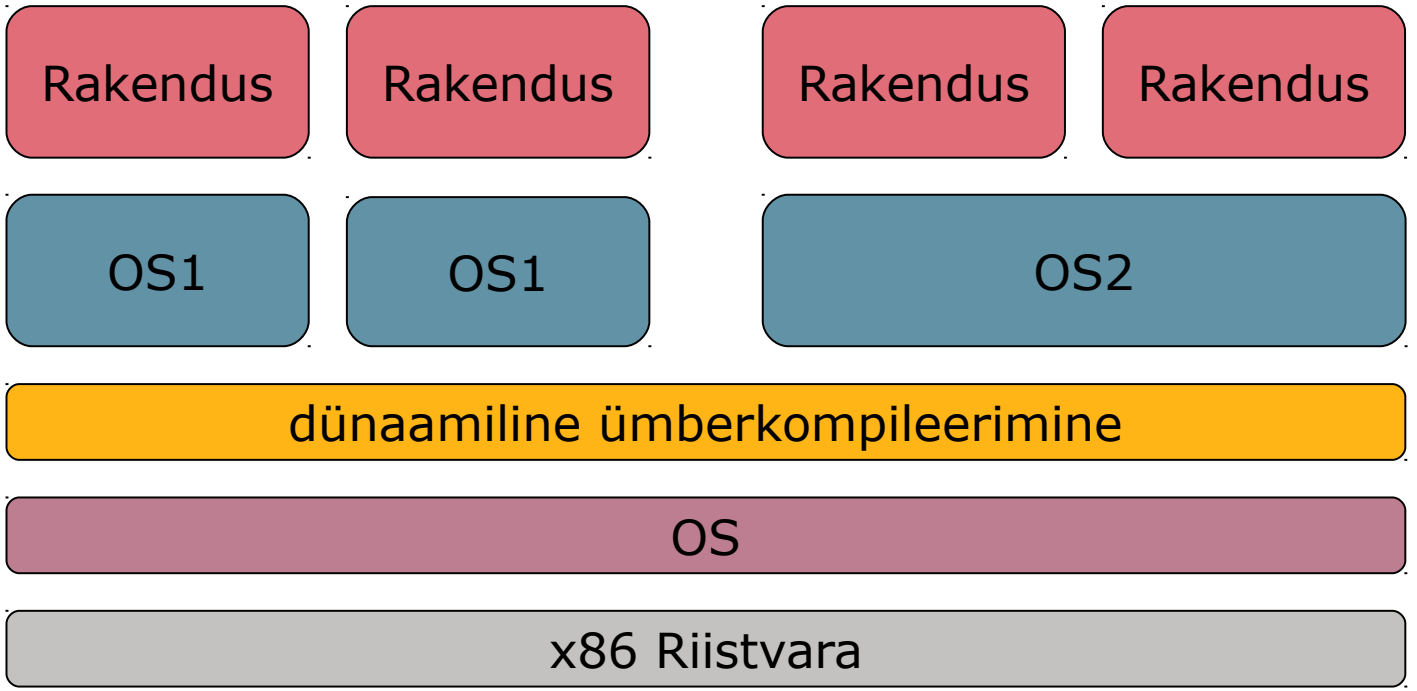
- Igal virtuaalarvutil on oma failipuu, eraldi juurkasutaja (administraator).
- Virtuaalmasinale saab ette anda kasutatava protsessoriressursi, mälu hulga jt ressursipiiranguid
- Virtualiseerimine võimaldab ühes füüsilises masinas kasutada korraga erinevaid operatsioonisüsteeme.

# Virtualiseerimise variandid

- „Raskekaalulised“ lahendused (virtuaalmasinal on oma tuum):
  - riistvara tarkvaraline emuleerimine (Qemu, UML);
  - dünaamiline ümberkompileerimine (VmWare, Hyper-V);
  - paravirtualiseerimine (Xen, VmWare);
  - riistvara toega virtualiseerimine (KVM, VmWare, Xen);
- „Kergekaalulised“ lahendused (virtuaalmasin kasutab peremehe tuuma):
  - konteinervirutaliseerimine (vServer, OpenVZ, LXC)
  - chroot, jail

# Dünaamiline ümberkompileerimine

- OS1 ja OS2 võivad olla Windowside, Linuxite või BSDde „karbiversioonid“.



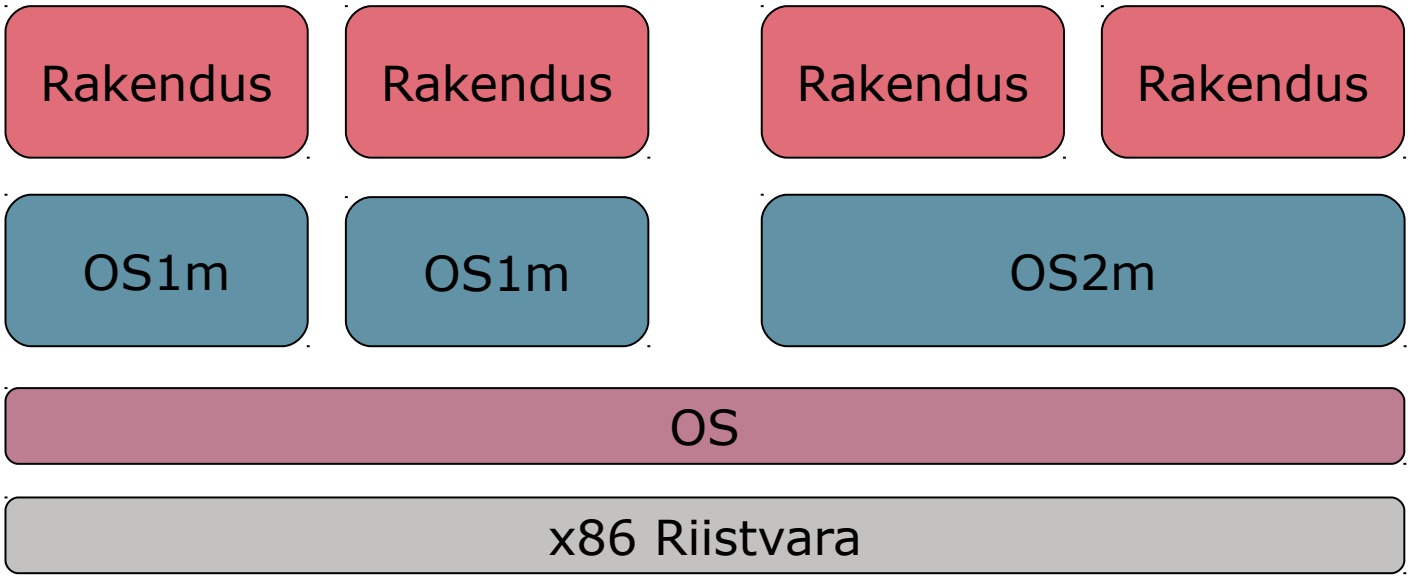
# Eelised/Puudused

- Eelised
  - virtuaalmasinas kasutatav operatsioonisüsteem on muutmata kujul.
- Puudused
  - võivad esineda dünaamilisest ümberkompileerimisest tingitud jõudlusprobleemid

Näiteid:
QEmu, VMware Workstation/Server, Virtual PC/Server, Parallels

# Paravirtualiseerimine

- OS1 ja OS2 on modifitseeritud vältimaks dünaamilist ümberkompileerimist.



# Protsessoritootjate tugi

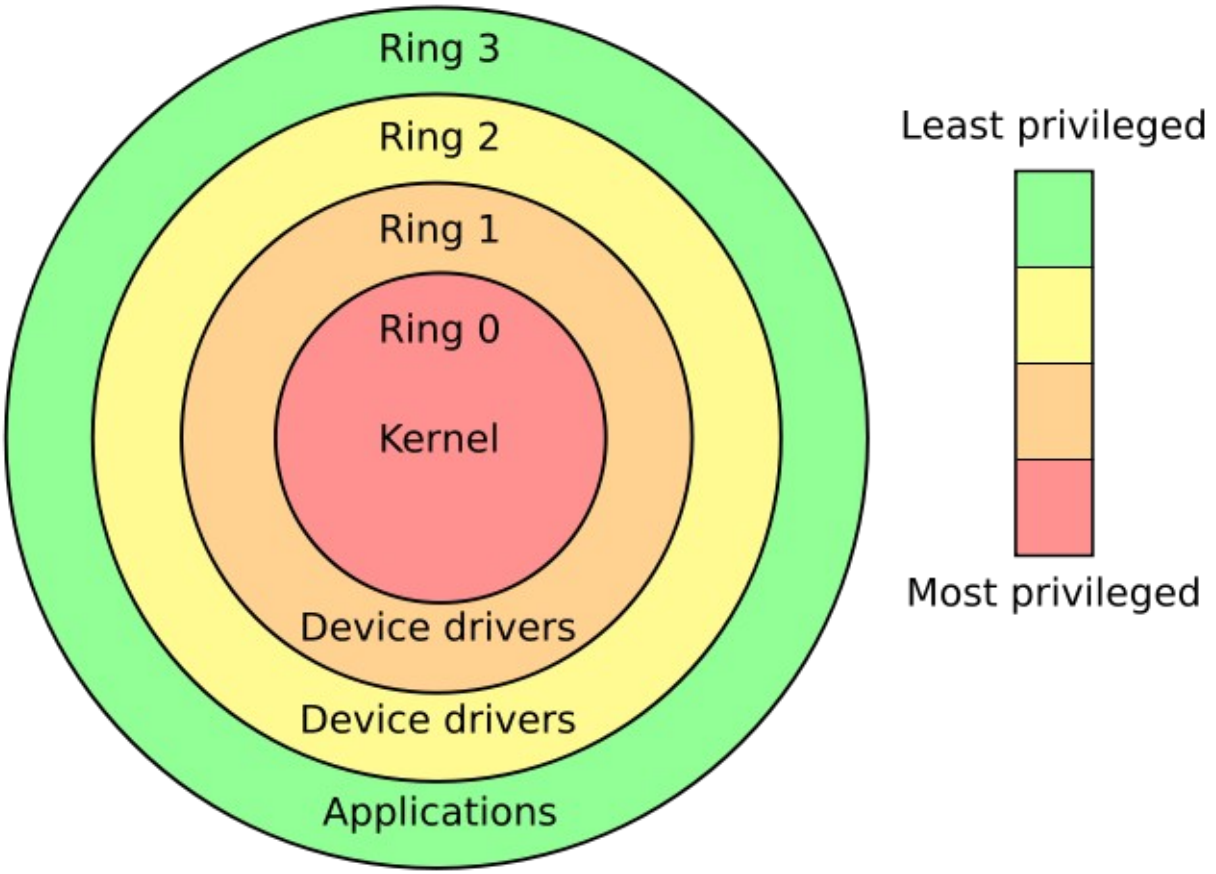


Vältimaks virtuaalmasina OS-i dünaamilist (ja staatilist) ümberkompileerimist on nii AMD kui ka Intel välja töötanud hüperviisorrežiimi võimaldavad riistvaralaiendused.

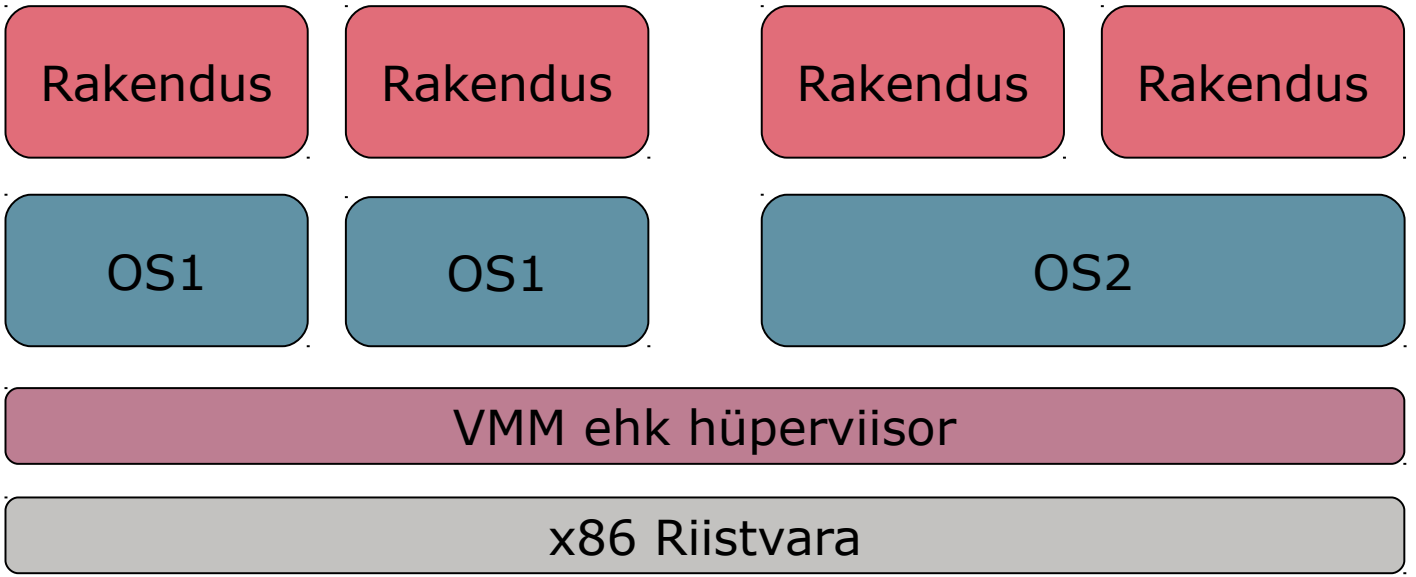
- AMD
  - AMD-V virtualiseerimis-tehnoloogia
  - RVI
- Intel
  - Virtualization Technology VT-i, VT-x, jt
  - EPT

# Processor modes

- Hypervisor mode (-1)
- Protected mode (0)
- User mode (>0)



# Hüperviisorlahendus



# Konteinervirutaliseerimine

- võimaldab ühes Linuxi serveris käigus hoida mitmeid Linux servereid
- kõik virtuaalmasinad kasutavad ühist tuuma
- virtuaalmasinatel on oma failisüsteem
- virtuaalmasinad võivad pärineda erinevatest distributsioonidest (eeldusel, et suudavad olemasoleva tuuma peal töötada)
- praktiliselt puudub jõudluse kadu
- virtuaalmasinate kaupa saab piirata kasutatavaid ressursse
- virtuaalmasinaid saab hallata sõltumatult, aga ka otse *host* masina käsurealt, kuna kõigi virtuaalmasinate failisüsteemid on *host* failisüsteemi osad
- Vahendid: LXC, Vserver, OpenVZ, Virtuozzo

# Eelised, puudused võrreldes raskekaaluliste lahendustega

- Eelised
  - õhuke virtualiseerimiskiht, jõudluse minimaalne kadu
  - dünaamiline mälu ümberjagamine
  - ühine haldus
- Puudused
  - väiksem eraldatus – ühine tuum
    (turva)probleemid tuumas mõjutavad kõiki *guest*-e
  - ei võimalda erinevaid operatsioonisüsteeme
  - probleemid rakendustega, mis vajavad tuuma poolt erikohtlemist (lisamoodulid)
    näiteks Kerberos autentimisega NFS, Bind
  - ilma oluliste lisaprivileegideta ei saa virtuaalmasinate all failisüsteeme monteerida

# Konteinervirtualiseerimise lahendused

- LXC
  - kõige kergekaalulisem
  - *libvirt* tugi
- Vserver
  - kergekaalulisem
  - parem ühilduvus teiste tuuma taseme modifikatsioonidega
  - parem ühilduvus Debian põhiste distributsioonidega
- OpenVZ
  - detailsem ressursihaldus
  - *checkpoint* (elusa migreerimise) tugi
  - võrgukihi täielik virtualiseerimine
    - tulemüür igas virtuaalmasinas
    - virtuaalne võrk virtuaalmasinate vahel
  - parem dokumentatsioon
  - parem tugi RPM põhistele distributsioonidele
- Virtuozzo – OpenVZ kommertsversioon

# chroot, BSD jail

- Kõige kergekaalulisemad konteinerid
- Ei moodusta omaette operatsioonisüsteemi
- Mingi teenusele/protsessile piiratakse ligipääs ainult mingile failisüsteemi osale
- Turvaprobleemid
  - avatud failisangad jäävad avatuks ka peale *chroot*-i
  - aktiivset kataloogi ei muudeta
  - puuduvad ressursipiirangud

# Checkpointing

- Võimaldab salvestada virtuaalmasina hetkeseisu
- Kasutatakse
  - varundamiseks
  - elusaks migreerimiseks
  - muudatuste tagasivõtmise võimaldamiseks
- Variandid
  - ainult mälu seisu salvestamine
    - failisüsteemi hetkeseis tuleb fikseerida sõltumatult
    - elusaks migreerimiseks tuleb virtuaalmasin failisüsteemi replikeerimiseks külmutada
  - mälu ja failisüsteemi hetkeseisu salvestamin
    - võimaldab praktiliselt nähtamatut elusat migreerimist
    - võimaldab töötava süsteemi varundamist
    - virtuaalmasina erinevate konfiguratsioonide puud näiteks SP1 uuendustega ja ilma, SP2 uuendustega ja ilma

# *Ballooning*

- Virtuaalmasine mäluhaldus
- *Balloon* protsess virtuaalmasinas
  - täidab *guest* opsüsteemilt vaba mälu
  - annab selle mälu *host* opsüsteemile (VMM-ile)

# Libvirt

- Ühine virtualiseerimisliides mitmetele virtualiseerimistehnoloogiatele
  - VmWare, Parallels, MS Hyper-V
  - KVM/Qemu
  - OpenVZ, LCX, UML
- Võrkude virtualiseerimine
  - bridging, NAT, jt
- Ketaste virtualiseerimine
  - NFS, LVM, iSCSI, jt

# Virtualiseerimise tegevused

- virtuaalmasina loomine *template*-st
- virutaalmasina *start-stop*
- virtuaalmasina *suspend-resume*
- *snapshot*-i tegemine
- virtuaalmasina migreerimine
- seadme lisamine-eemaldamine
- võrgukonfiguratsioon
- protsessori ja mälu ressursihaldus
- infopäringud, statistika

# Kokkuvõte

- Virtualiseerimine võimaldab hoida kokku kulusid.
- Virtualiseerimine võimaldab suurendada turvalisust.
- Virtualiseerimine teeb võimaldab dünaamili lahendusi.
- Virtualiseerimine võimaldab dünaamilisemat süsteemihaldust