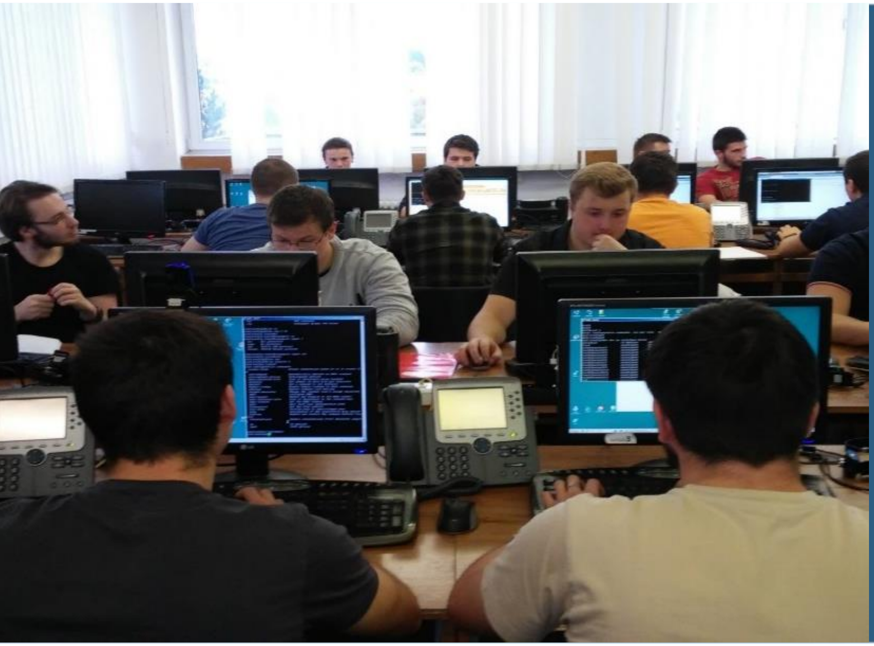
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Virtualizácia
Cloud Computing
SDN

Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Cisco
Networking Academy

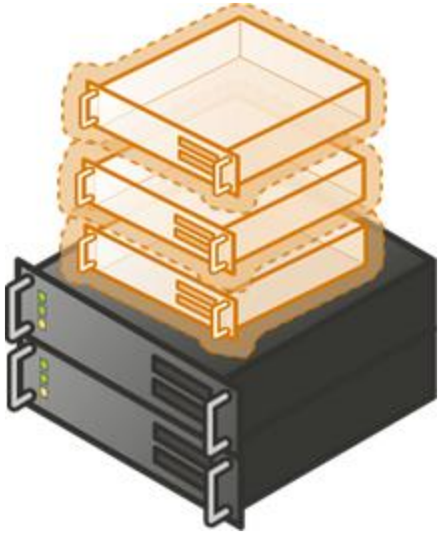


Virtualizácia

Virtualizácia

- Spúšťanie logicky oddelených programov (OS) na jednom fyzickom zariadení
- Fyzický stroj – host
- Virtuálny stroj – guest (virtual machine - VM)

- Každá VM má
  - „pocit“, že beží na vlastnom HW
  - Vlastnú vRAM
  - Vlastný priestor na HDD
  - Vlastnú MAC a IP



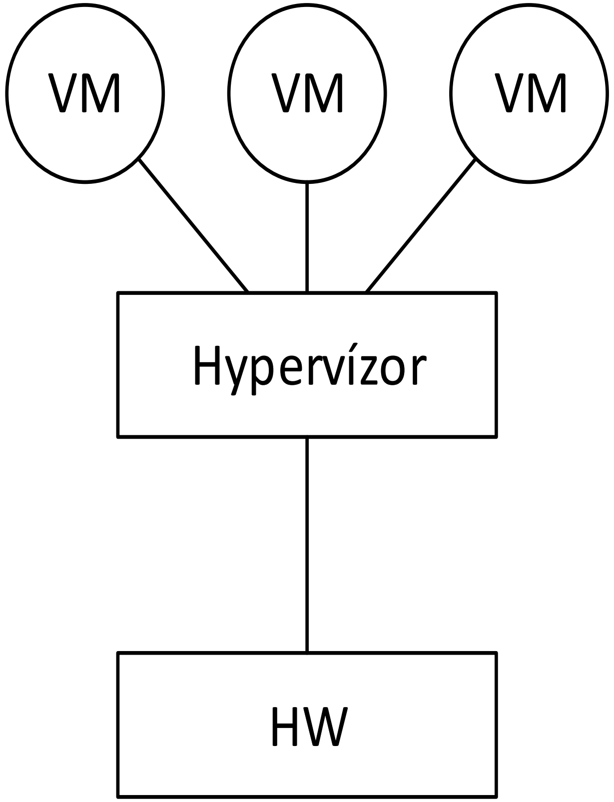
Hypervízor (VMM)

- Program prideľujúci zdroje VM sa nazýva **hypervízor**
- Niekedy aj Virtual machine monitor
- Hypervízor má neobmedzenú kontrolu nad VM
- Dokáže
  - Spúšťať VM
  - Vypínať VM
  - Pridávať/odoberať zdroje
  - Meniť množstvo zdrojov

- Pomocou hypervízora dokážeme administrátorsky pristupovať k jednotlivým VM (prístup na konzolu)

Hypervízor – 1. typ

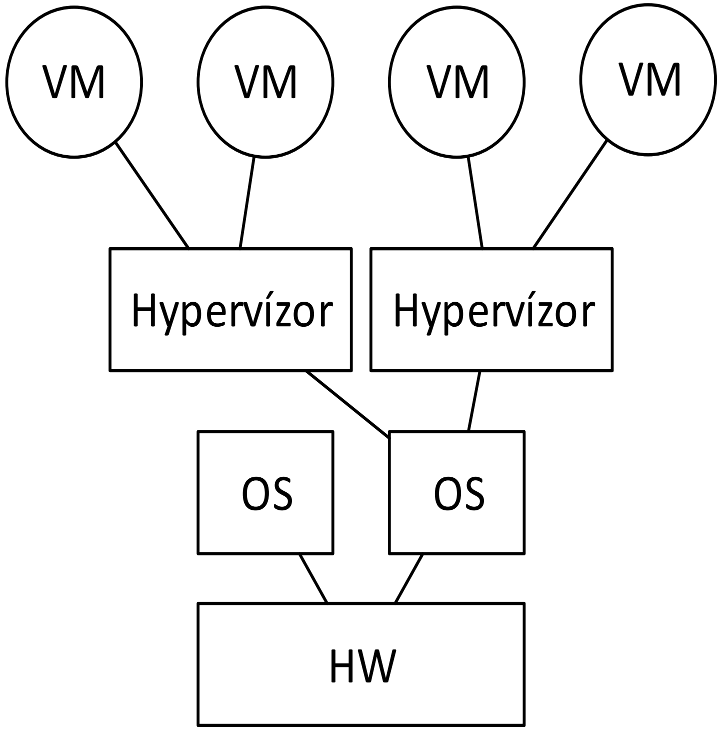
- Nazývaný aj natívny (bare metal)
- Beží priamo nad HW
- Manažment cez externý program (web)
- Príklad:
  - Citrix XenServer (Citrix XenCenter)
  - VMware ESX (Vmware vSphere Client)



Typ1
Native (bare metal)

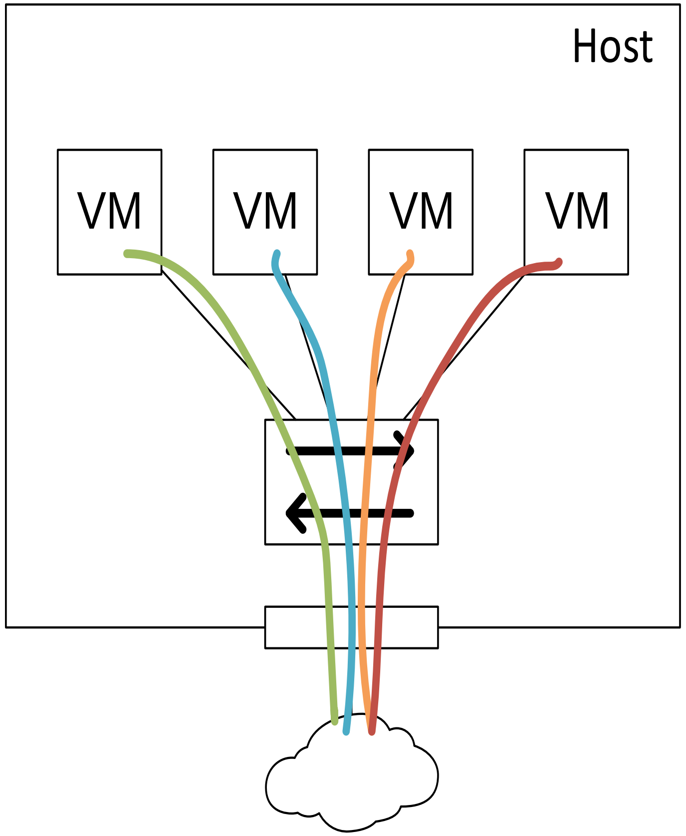
Hypervízor – 2. typ

- Nazývaný aj hosted
- Beží nad OS
- Manažment priamo cez OS (GUI, CLI)
- Príklad:
  - Oracle Virtualbox
  - VMware Workstation / Player
  - KVM / QEMU
  - Windows Virtual PC

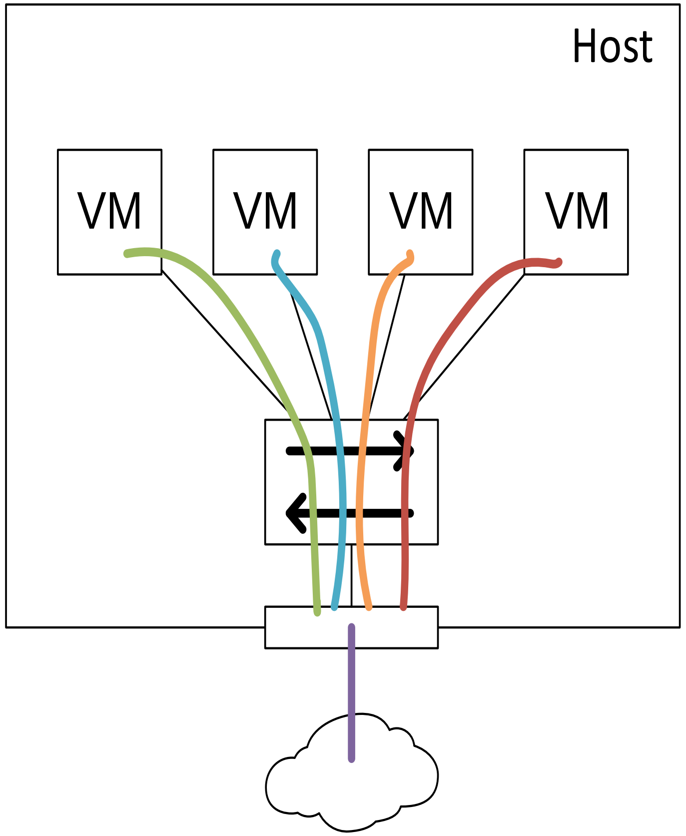


Typ2
Hosted

Sieť vo virtualizácii

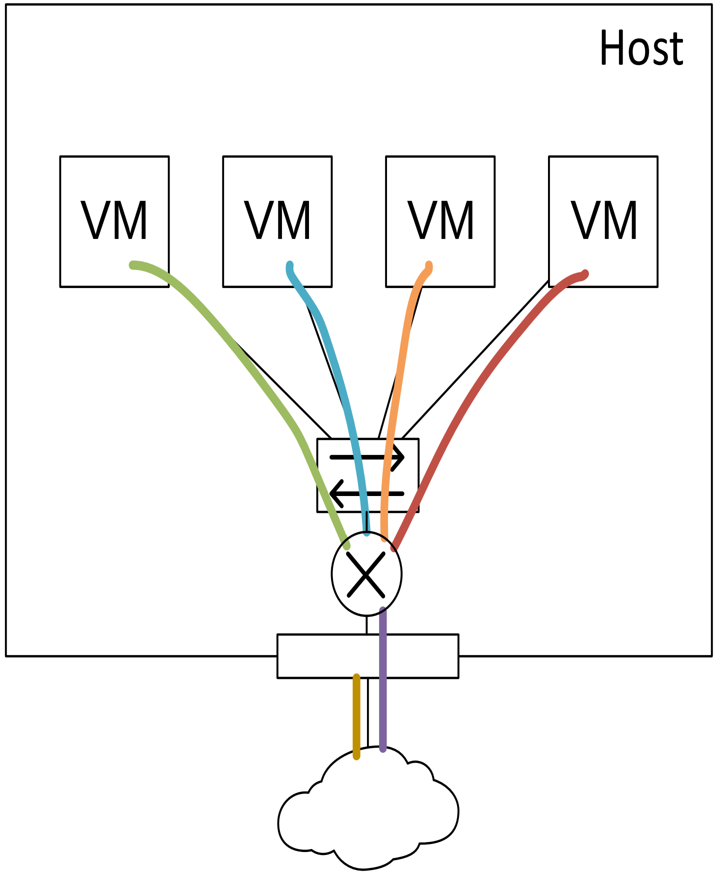


Priame pripojenie VM do siete

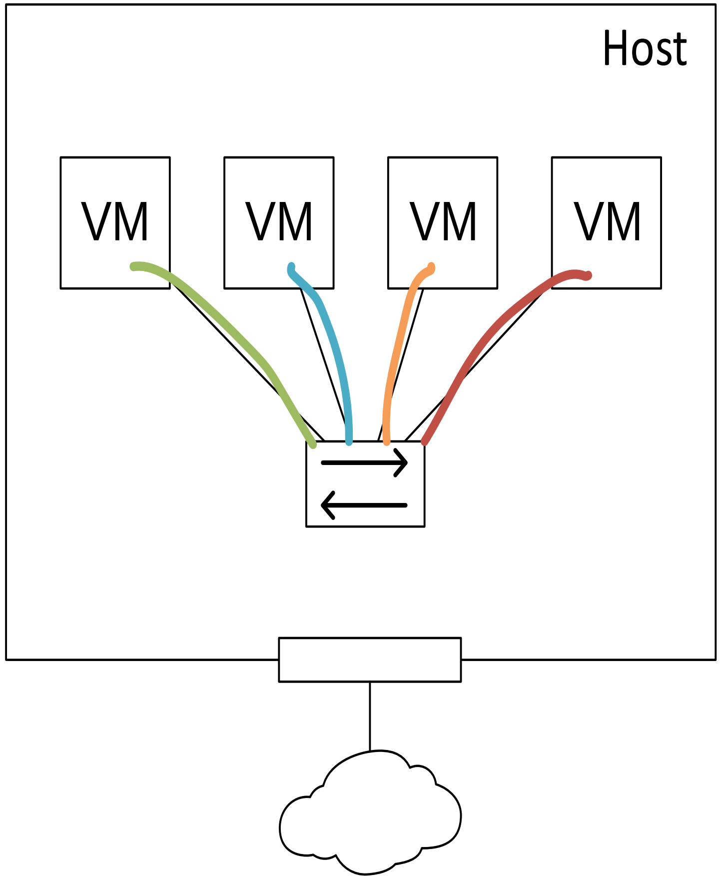


Preklad adries
(NAT)

Sieť vo virtualizácii



Virtuálna sieť



Lokálna (izolovaná) sieť

Kontajnerová virtualizácia

- Virtualizovaná je jedna, prípadne sada aplikácií
  - Nie celý operačný systém
  - Napr.:
    - Web server
    - Databázový server
- Kontajner je zvyčajne prichystaný so základnou konfiguráciou
- Všetky kontajnery na systéme zdieľajú jadro OS

Kontajnerová virtualizácia

- Výhody:
  - Izolácia procesov
    - Pr.: Ak hacknú web server, neovplyvnia databázový server
  - Jednoduchá migrácia
  - Možnosť prideľovať kvóty kontajnerom
    - CPU, RAM, HDD
- Nevýhody
  - Všetky kontajnery zdieľajú jedno jadro
  - Kontajner vytvorený v Linuxe nepôjde vo Windowse

Docker

- Kontajnerová virtualizácia pre Linuxové programy
- Architektúra x86_64, ARM
- Integrovaný v mnohých technológiách
  - AWS, OpenStack, Puppet

LXC

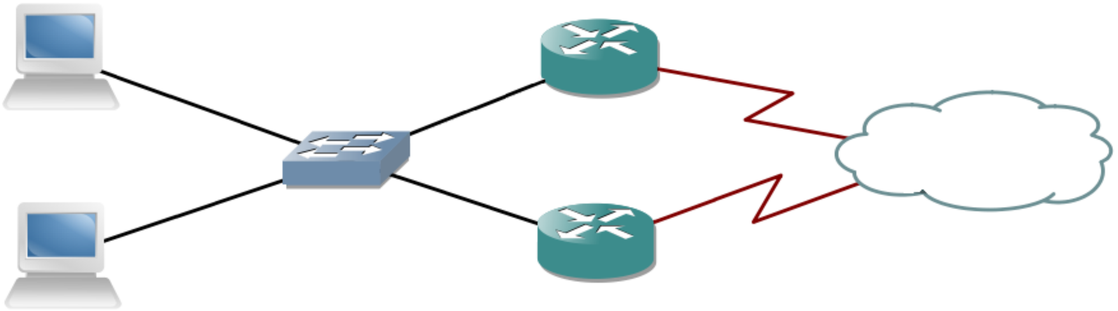
- Skratka pre Linux Container
- Na rozdiel od Docker-a, vie virtualizovať viac procesov v jednom kontajneri
- Vytvára „namespace“ v rámci OS
- Medzistupeň medzi Dockerom a virtualizáciou OS
  - Kontajnery zdieľajú jadro OS
  - Môžu sa tváriť ako samostatné OS (vlastná IP)
- LXD – hypervízor pre LXC kontajnery
  - Nie až tak stabilný ako LXC

Cloud Computing

Cloud Computing (CC)

- Zdieľaný výpočtový výkon na niekoľkých zariadeniach
- Zákazník platí za službu, nie za softvér
- Pre zákazníka sa javí ako nekonečný priestor

- Prečo slovo cloud?
- V diagramoch sieťových topológií sa obláčikom znázorňuje Internet, resp. niečo ďaleko, mimo vlastnej siete



Modely CC

- Privátny cloud
  - Využívaný jednou organizáciou pre vlastné potreby
  - OpenStack, VMware ESX/ESXi
- Komunitný cloud
  - Využívaný skupinou s rovnakým spoločným záujmom
    - Prepojenie univerzít v rámci jedného výskumu
- Verejný cloud
  - Ponúkaný verejnosti
  - Amazon Web Services, Microsoft Azure
- Hybridný cloud
  - Kombinácia predošlých

Služby v CC

- Softvér ako služba (SaaS)
- Platforma ako služba (PaaS)
- Infraštruktúra ako služba (IaaS)

- Podmnožiny služieb
  - FwaaS – Firewall
  - LBaaS – Load Balancer
  - DNSaaS – Domain Name Service
  - ...

- Čokoľvek ako služba (XaaS)

Software as a Service (SaaS)

- Aplikácie dostupné cez web rozhranie, alebo klientské aplikácie

- Úložný priestor
  - Google Drive
  - Dropbox
  - MS OneDrive
- Kancelárske prostredie
  - MS Office 365
- Informačný systém

Platform as a Service (PaaS)

- Spravidla prostredia určené developerom
- Prostredia na beh vlastných aplikácií

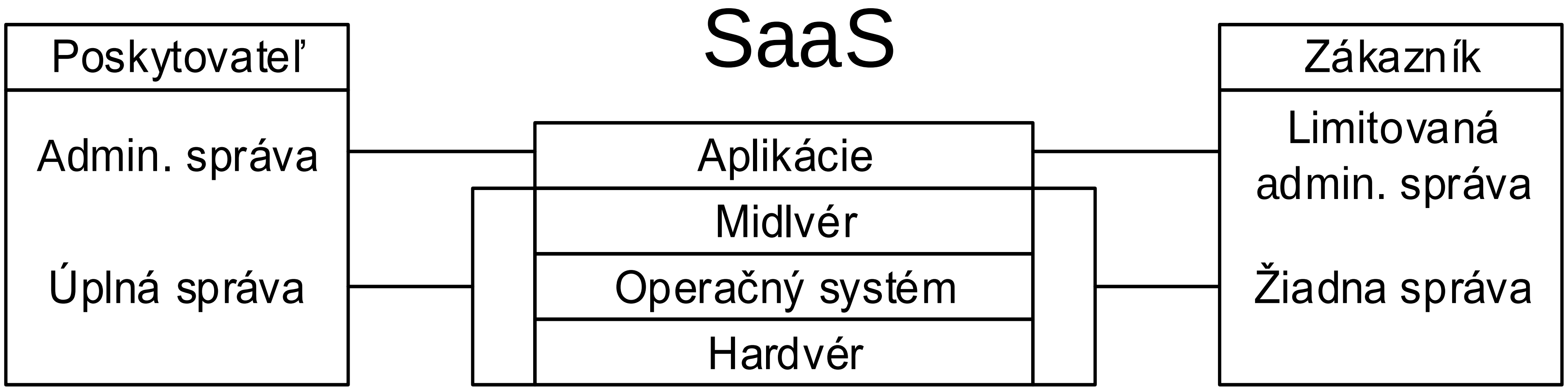
- Java virtual machine
- .net prostredia
- Databázy
- Autentifikácia, Autorizácia (AAA)

Infrastructure as a Service (IaaS)

- Poskytovateľ poskytuje „len konektivitu“
- Celková administrácia prostredia je na zákazníkovi

- Priestor pre vlastné virtuálne mašiny
- Virtuálne siete
- Firewall-ing
- Rozkladanie záťaže

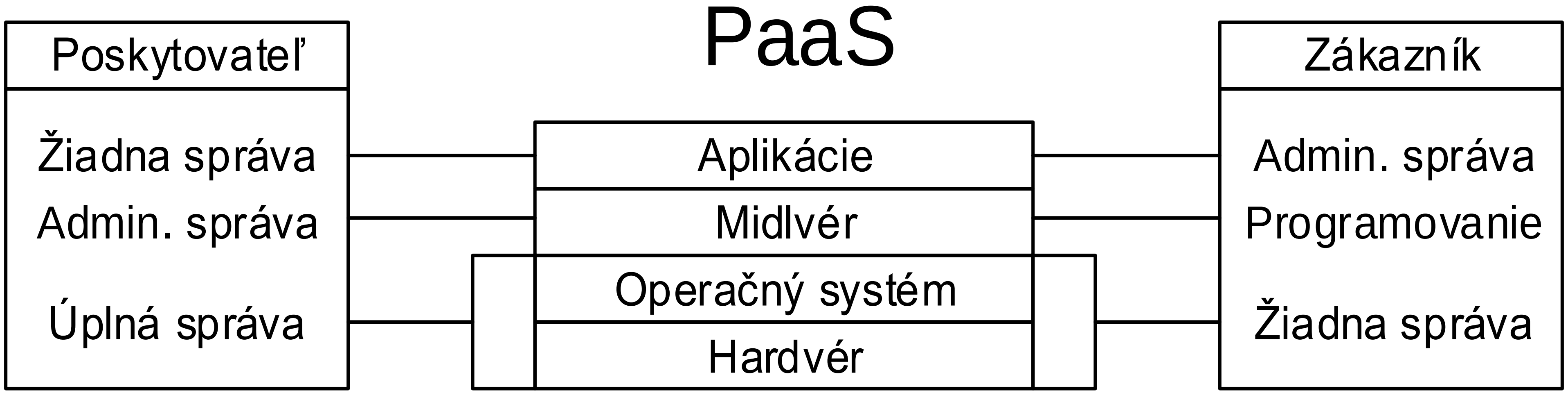
Kompetencie v CC prostredí



SaaS

Poskytovateľ		Zákazník
Admin. správa	Aplikácie	Limitovaná admin. správa
Úplná správa	Midlvér Operačný systém Hardvér	Žiadna správa

Kompetencie v CC prostredí



PaaS

Poskytovateľ

Žiadna správa

Admin. správa

Úplná správa

Aplikácie

Midlvér

Operačný systém

Hardvér

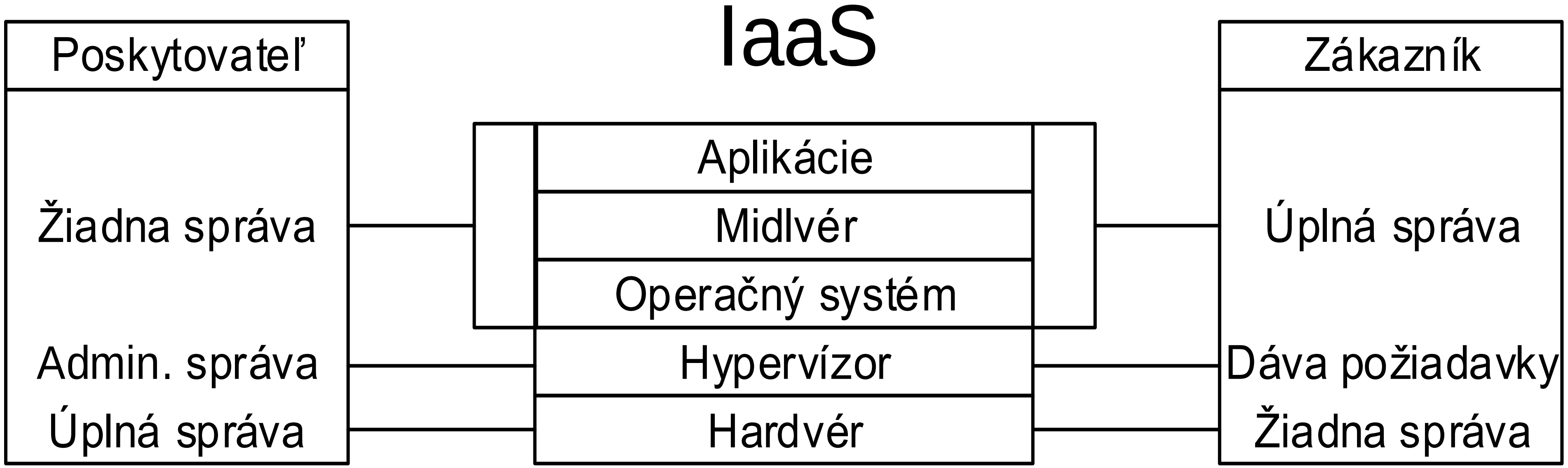
Zákazník

Admin. správa

Programovanie

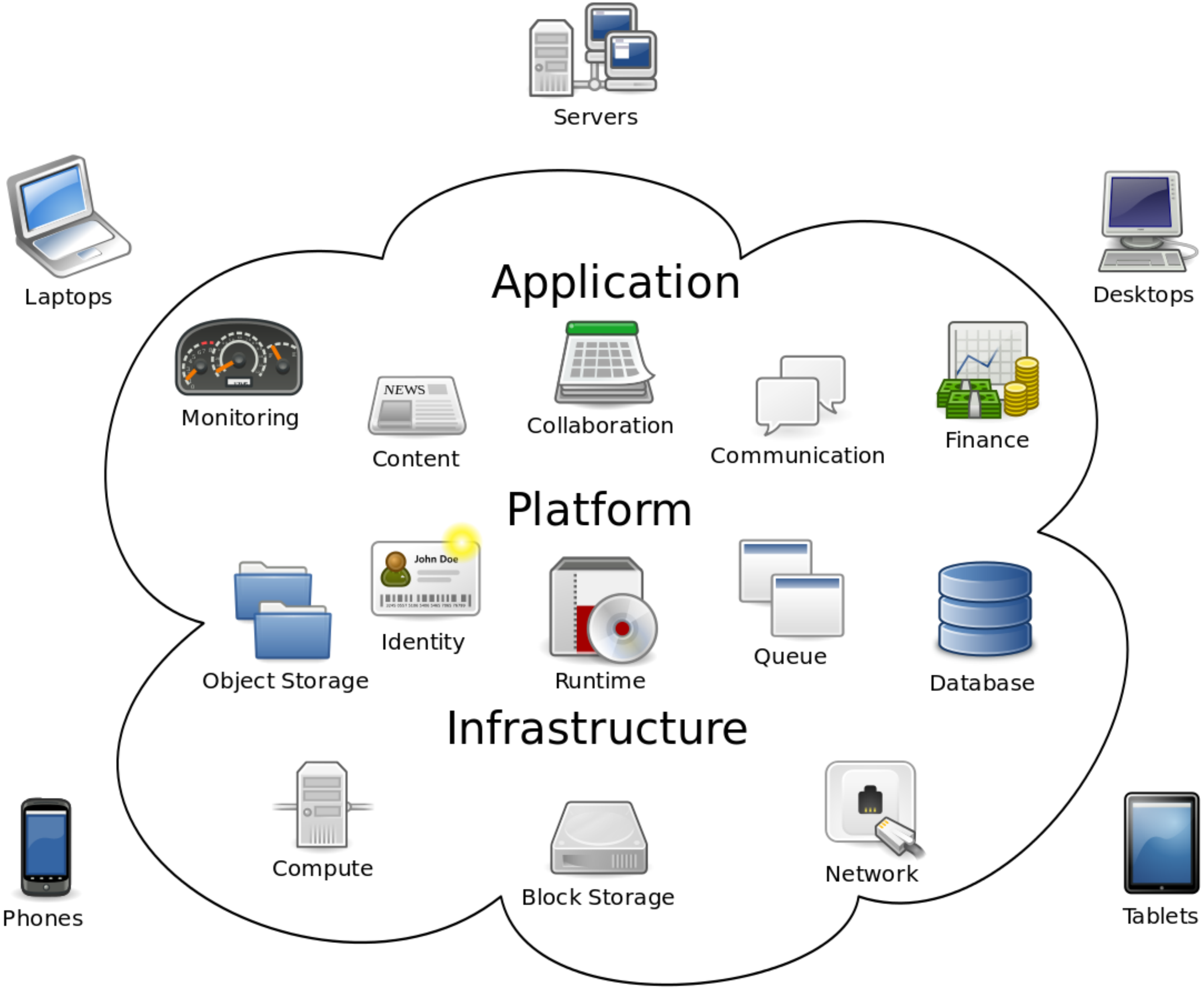
Žiadna správa

Kompetencie v CC prostredí



IaaS

Poskytovateľ		Zákazník
Žiadna správa	Aplikácie Midlvér Operačný systém	Úplná správa
Admin. správa	Hypervízor	Dáva požiadavky
Úplná správa	Hardvér	Žiadna správa



Cloud computing

https://sk.wikipedia.org/wiki/Cloud_computing#/media/File:Cloud_computing.svg

Poskytovatelia verejného cloudu

- AWS – Amazon Web Services (64% trhu v r. 2017*)
- DigitalOcean
- Google cloud
- Microsoft Azure

* http://assets.rightscale.com/uploads/pdfs/RightScale-2018-State-of-the-Cloud-Report.pdf

Orchestrácia

- Inými slovami automatizácia
- Najsilnejšia zbraň cloudu
- Dovoľuje automatizovane spravovať niekoľko zariadení naraz
- Veľmi často nasadzovaná vo virtuálnych prostrediach
- Je potrebné odlíšiť použitie
  - Automatizácia koncových zariadení
  - Automatizácia „deployment-u“

Softvérovo definované siete

Čo je SDN?

- Virtualizácia sieťových funkcií
- Programovo centrálne riadená sieť
- Striktné oddelenie riadiacej a dátovej roviny
- Otvorené programovacie API sieťových prvkov

Prečo SDN?

- Súčasné siete sú postavené na hierarchickom dizajne
- Funguje v nich množstvo režijných protokolov (STP, OSPF, IGMP, ...)
- Takéto siete sú funkčné, stabilné, no statické
    - Častý pohyb zariadení v sieti nemajú v láske

Virtualizácia na vzostupe

- V súčasných dátových centrách sú 10-tky tisíc fyzických serverov
- 1 fyzický server ≠ 1 virtuálny server
- Dynamické prostredie so stovkami tisíc serverov
  - STP musí šalieť ☺
  - Premiestnenie servera do inej časti siete (VLAN, ACL, QoS)

Organizovanie SDN siete

- Riadiaca rovina je v samostatnom aktívnom prvku – kontroléri
- Kontrolér je centrálny riadiaci prvok celej siete
- Dátová rovina je distrbuovaná v niekoľkých zariadeniach
- Konunikácia medzi kontrolérom a dátovými časťami – riadiace protokoly

Architektúra SDN

- RFC 7426
- Control plane (Riadiaca rovina)
  - Rozhoduje o ceste datagramu v celej sieti
  - Dodáva preposielacie tabuľky zariadeniam
  - Zodpovedá za aplikovanie rozhodnutí do dátových zariadení
  - Môže sa zaujímať o operačné údaje siete (stavy portov, ...)

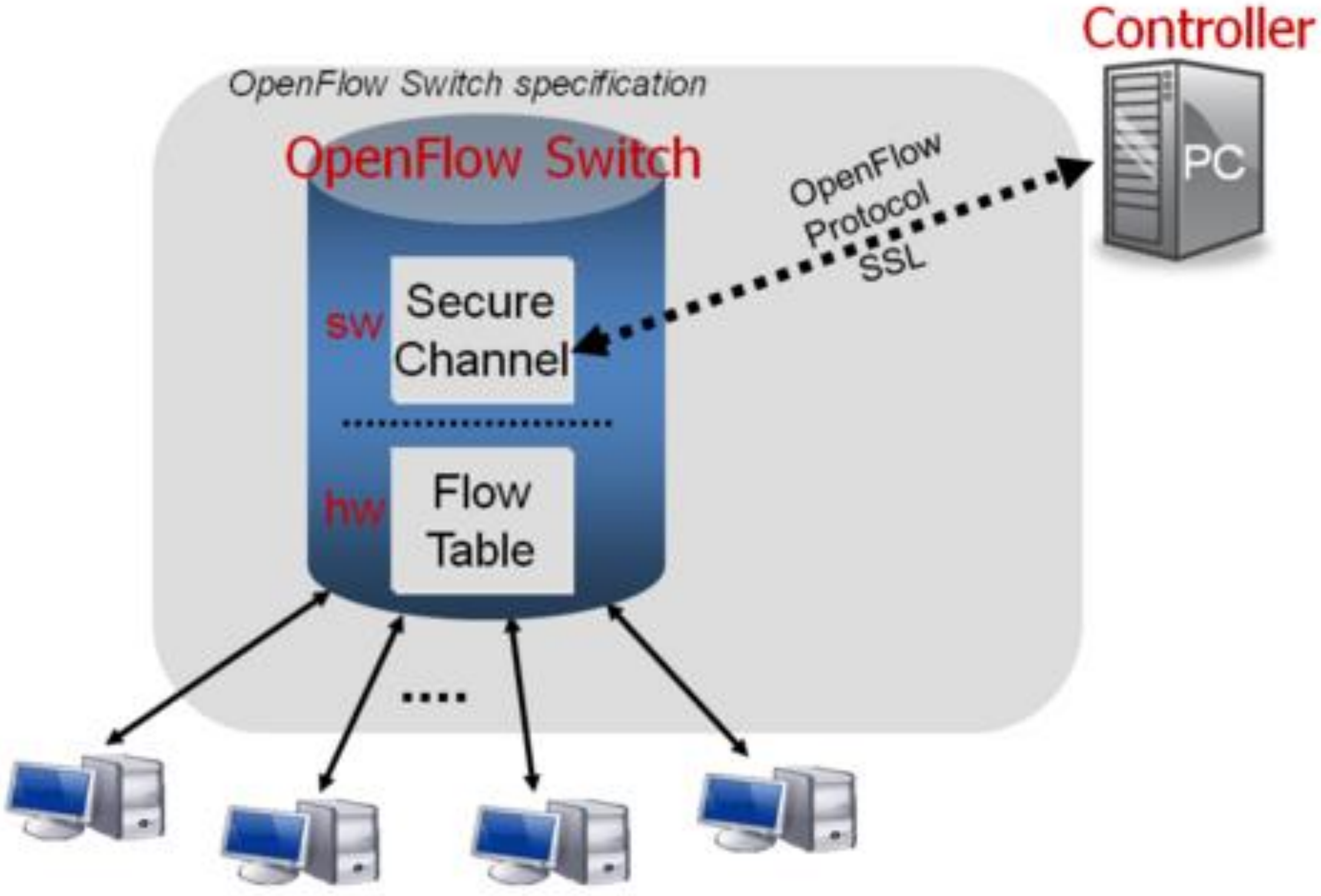
Architektúra SDN

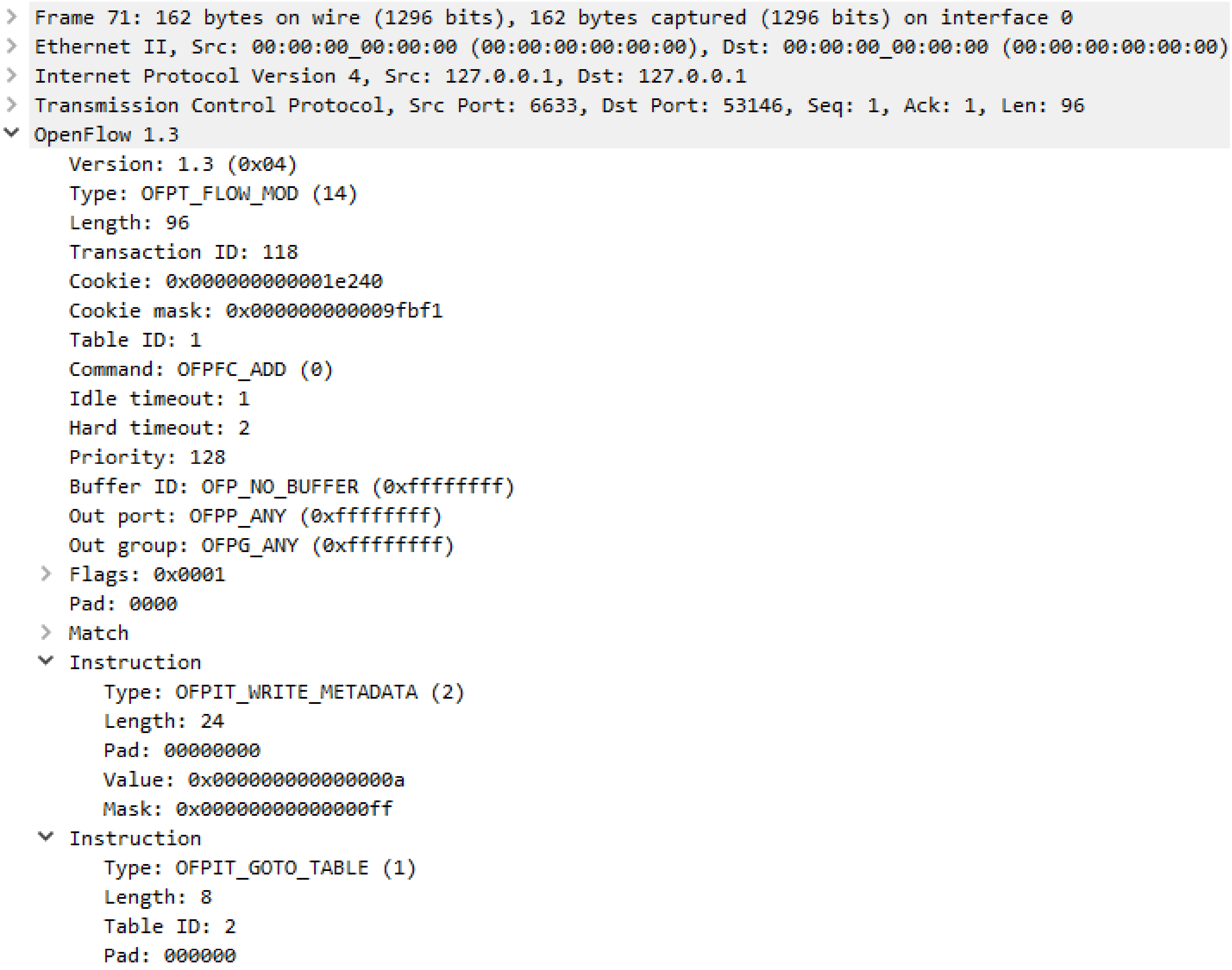
- Forwarding plane (Dátová rovina)
  - Zodpovedá za spracovanie datagramov
  - Založená na inštrukciách od riadiacej vrstvy
- Management plane
  - Zodpovednosť za monitoring a konfiguráciu aktívnych prvkov

Protokol OpenFlow

- Prvé štandardizované rozhranie medzi riadiacou a preposielacou časťou (control a forward)
- Môže manipulovať so zariadeniami bez ohľadu na to, či sú virtuálne, alebo fyzické
- Je implementovaný na oboch stranách SDN infraštruktúry (control aj data plane)

Protokol OpenFlow





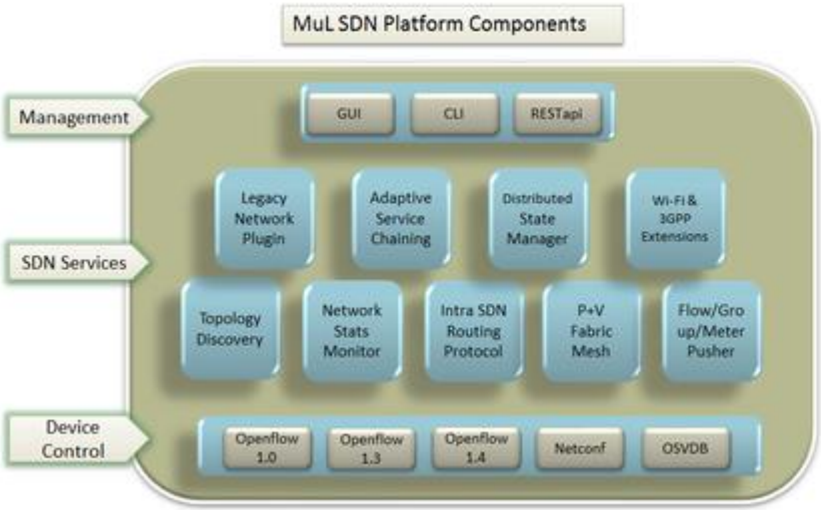
```
> Frame 71: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 6633, Dst Port: 53146, Seq: 1, Ack: 1, Len: 96
v OpenFlow 1.3
    Version: 1.3 (0x04)
    Type: OFPT_FLOW_MOD (14)
    Length: 96
    Transaction ID: 118
    Cookie: 0x000000000001e240
    Cookie mask: 0x000000000009fbf1
    Table ID: 1
    Command: OFPFC_ADD (0)
    Idle timeout: 1
    Hard timeout: 2
    Priority: 128
    Buffer ID: OFP_NO_BUFFER (0xffffffff)
    Out port: OFPP_ANY (0xffffffff)
    Out group: OFPG_ANY (0xffffffff)
  > Flags: 0x0001
    Pad: 0000
  > Match
  v Instruction
      Type: OFPIT_WRITE_METADATA (2)
      Length: 24
      Pad: 00000000
      Value: 0x000000000000000a
      Mask: 0x00000000000000ff
  v Instruction
      Type: OFPIT_GOTO_TABLE (1)
      Length: 8
      Table ID: 2
      Pad: 000000
```

SDN kontroléry

- POX
  - Nástupca NOX
  - Programovaný v Pythone, veľa API
  - Prehľadná dokumentácia, Webové GUI
- OpenDayLight
  - Modulárny kontroler pre Linux
  - Programovaný v Jave (Maven, REST API, ...)

SDN kontroléry

- OpenMUL
  - Programovaný v C
  - Modulárny, otvorené API



SDN prepínače

- Open vSwitch
  - Najrozšírenejšia implementácia L3 prepínača
  - Používaný v rôznych projektoch (Xen, KVM, OpenStack)
  - Plná podpora OpenFlow 1.3
  - Veľa funkcií
    - Zber dát (NetFlow, IPFIX)
    - Zrkadlenie prevádzky (SPAN, RSPAN)
    - Tunelovanie (GRE, VxLAN, STT, LISP)

SDN prepínače

- Indigo Virtual Switch
  - OpenSource pre Linux a KVM
  - Plná podpora OpenFlow protokolu
- Cisco Virtual Topology Forwarder
  - L3 prepínač pre x86 procesory
  - Veľa funkcií
    - L2, L3 prepínanie (IPv4, IPv6), VxLAN

Hardvérové zariadenia s podporou SDN

- Brocade MLX smerovače
- HP prepínače (2920, 3500, 5400, 8200)
- Cisco
  - Smerovače so systémom IOS-XE, IOS-XR, NX-OS
  - Prepínače Nexus 3000, 6000, Cat 4500E
- Juniper smerovače a prepínače
- Mikrotik

ŽILINSKÁ UNIVERZITA · UNIVERSITAS SOLNENSIS

MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7