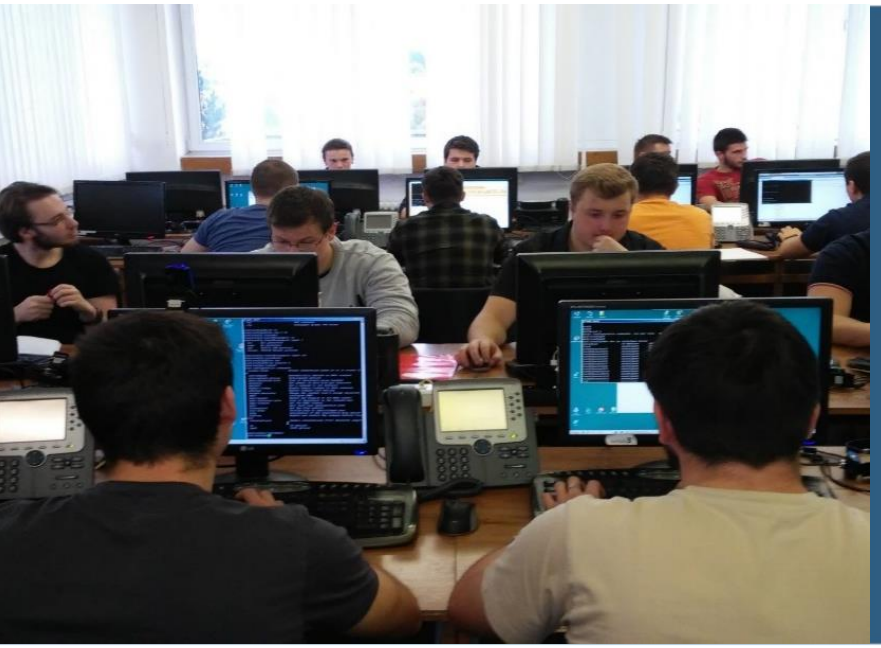
MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Virtualizácia
Cloud Computing
SDN
SD-WAN

Marek Moravčík

Vytvorené v rámci projektu KEGA 026TUKE-4/2021

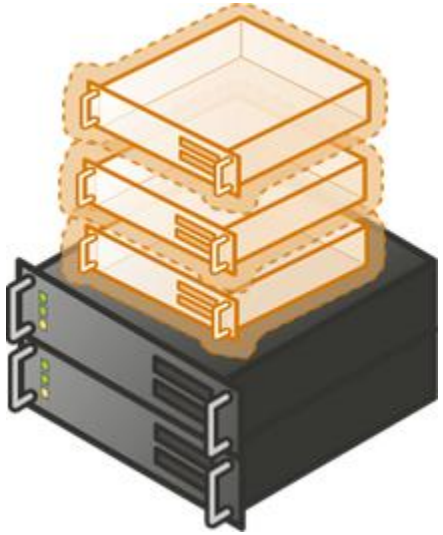


Virtualizácia

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



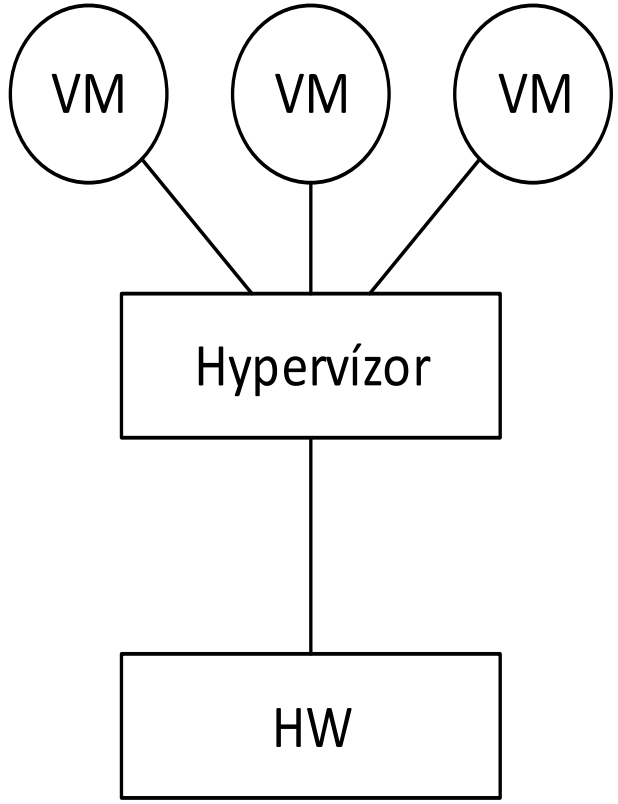
Hypervízor (VMM)

- 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

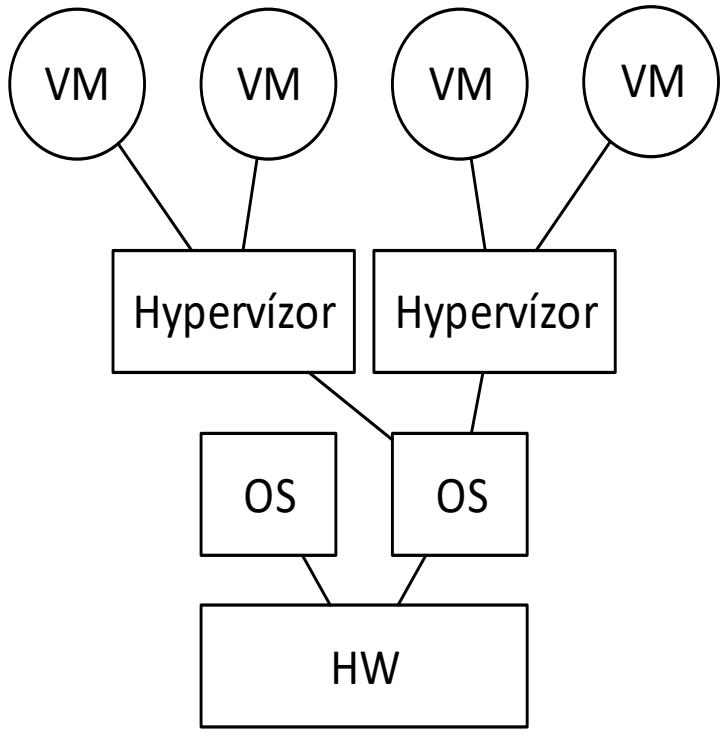
- Nazývaný aj natívny (bare metal)
- Beží priamo nad HW
- Manažment cez externý program (web)
- Príklad:
  - Citrix XenServer (Citrix XenCenter)
  - VMware ESX (Vmware vSphere Client)



Typ1
Native (bare metal)

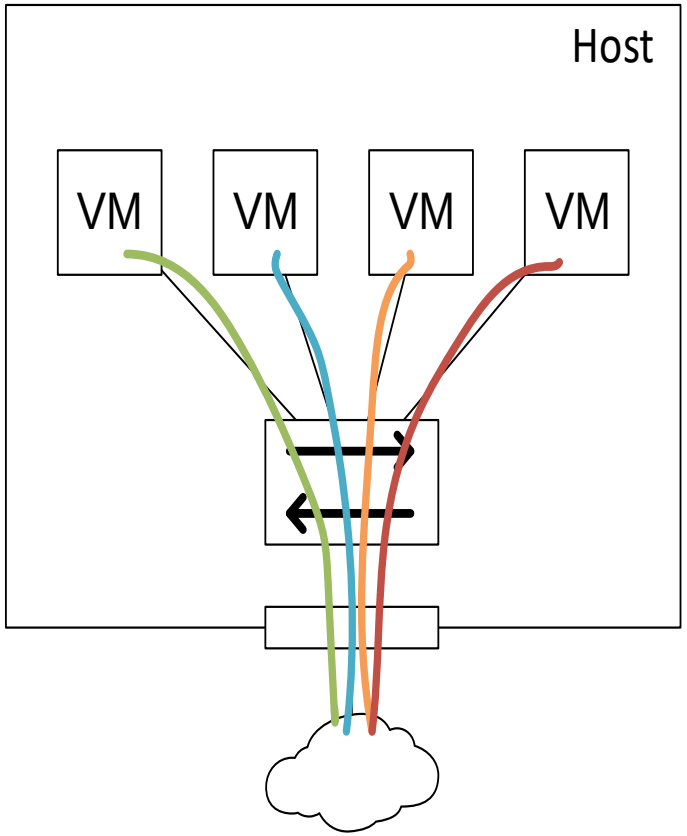
Hypervízor – 2. typ

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

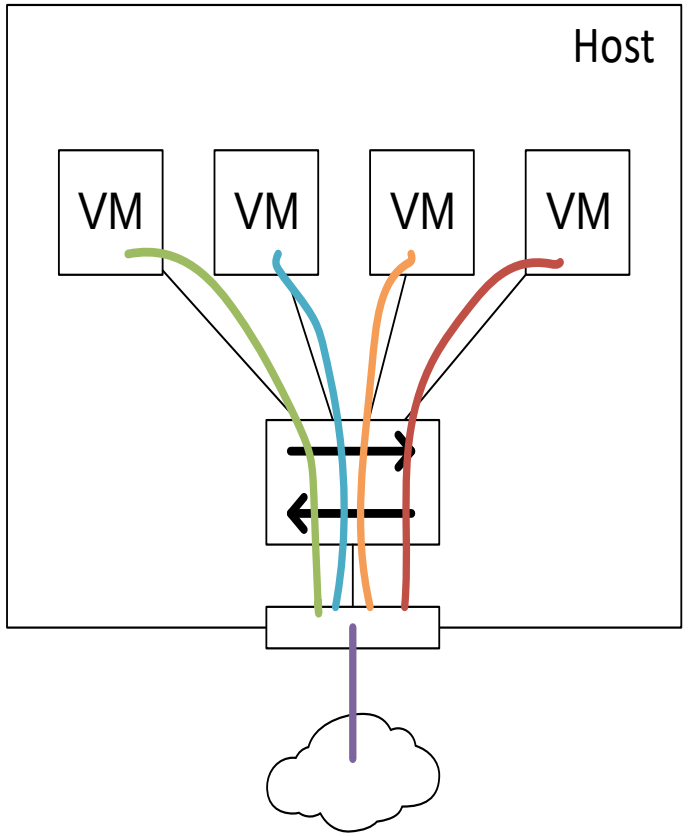


Typ2
Hosted

Sieť vo virtualizácii

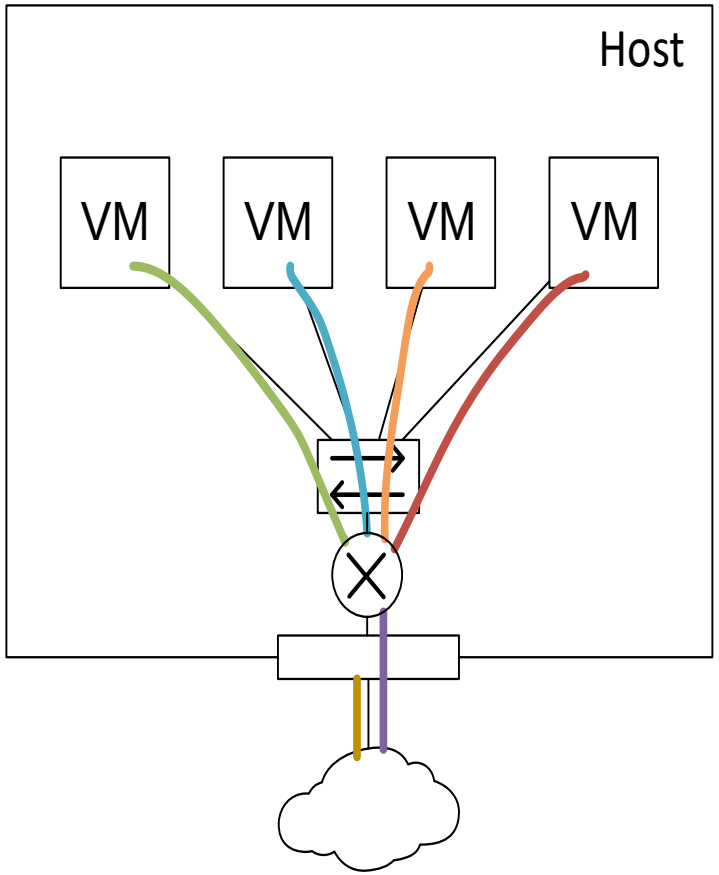


Priame pripojenie VM do siete

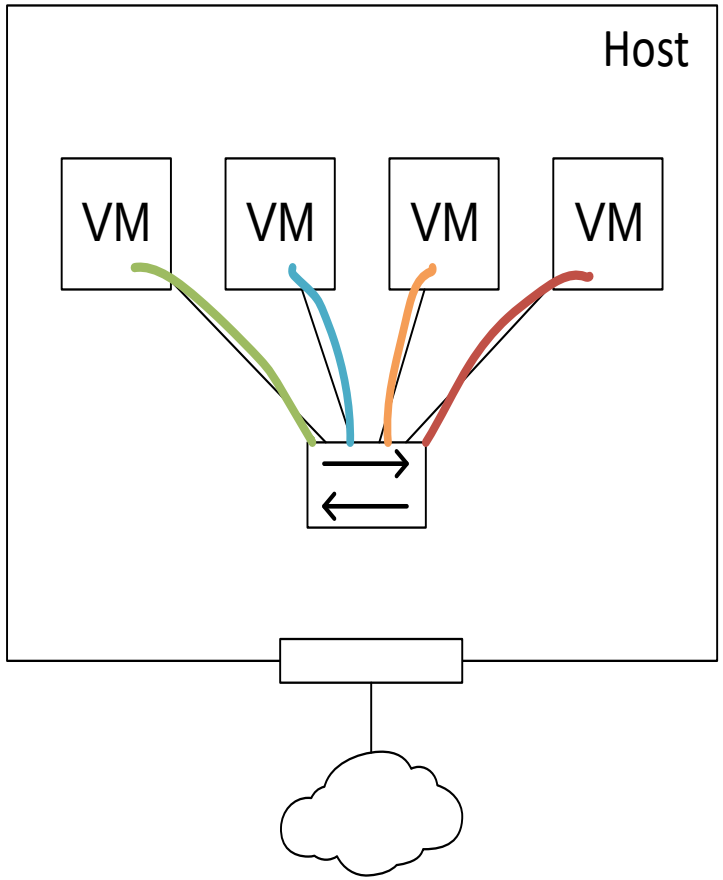


Preklad adries (NAT)

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, s390x, ppc64le
- Integrovaný v mnohých technológiách
  - AWS, OpenStack, Puppet

LXC

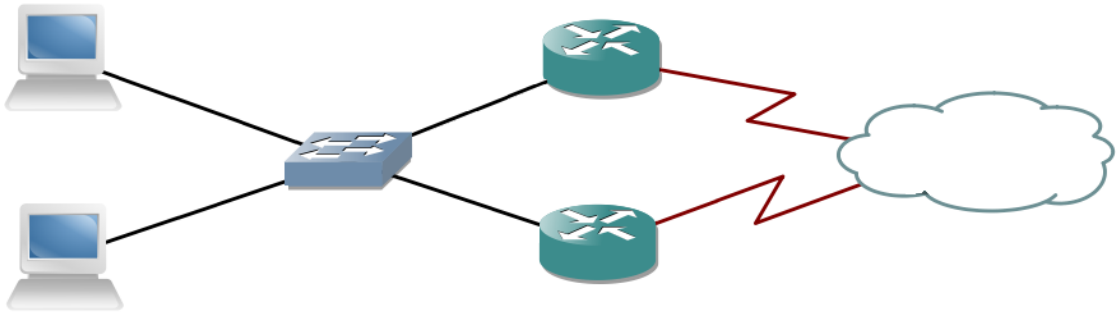
- Skratka pre Linux Container
- Na rozdiel od Docker-a, vie virtualizovať viac procesov v jednom kontajneri
- Vytvára „namespace“ v rámci OS
- Medzistupeň medzi Dockerom a virtualizáciou OS
  - Kontajnery zdieľajú jadro OS
  - Môžu sa tváriť ako samostatné OS (vlastná IP)
- LXD – hypervízor pre LXC kontajnery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

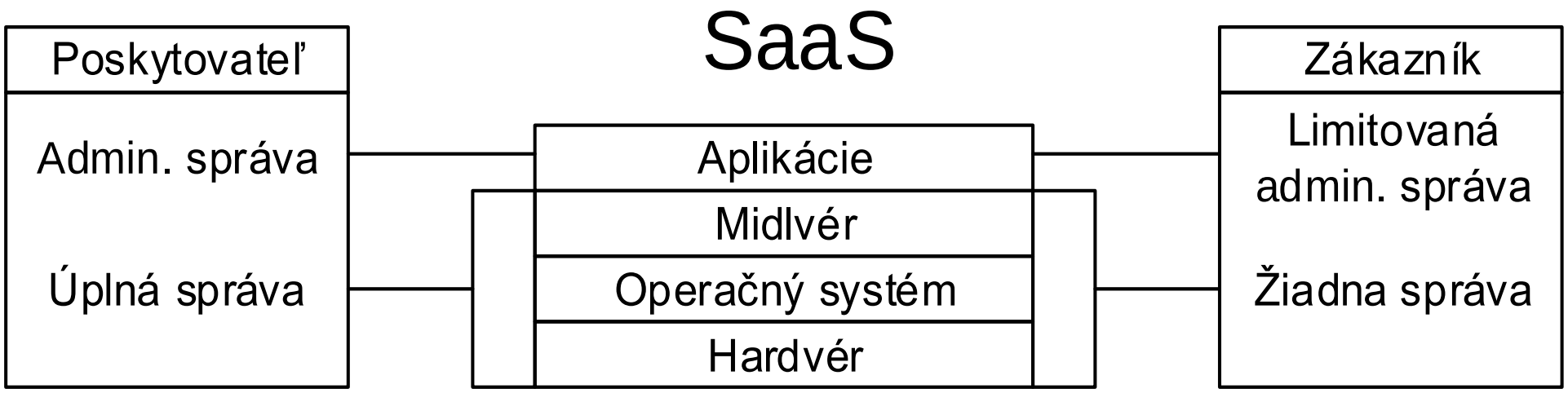
- Čokoľvek ako služba (XaaS)

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

Kompetencie v CC prostredí

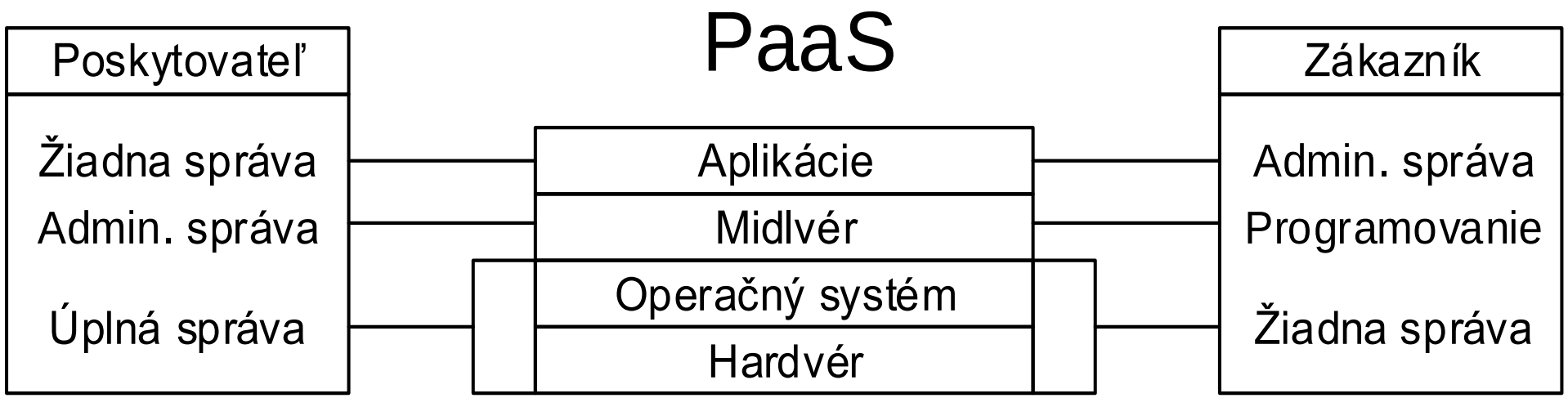


Platform as a Service (PaaS)

- Spravidla prostredia určené developerom
- Prostredia na beh vlastných aplikácií

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

Kompetencie v CC prostredí

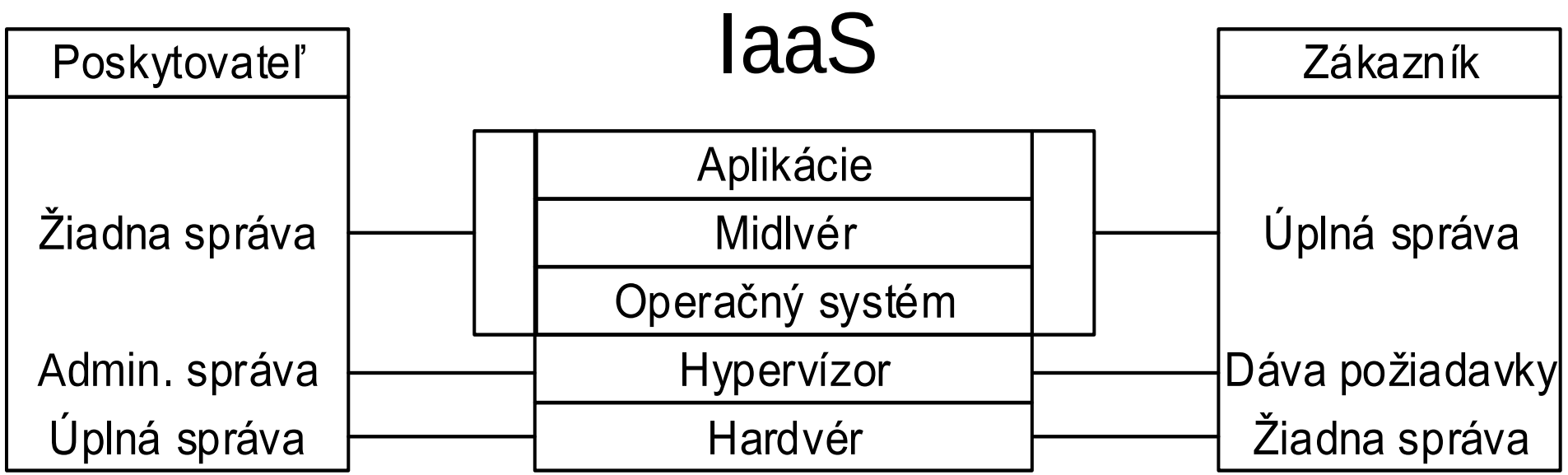


Infrastructure as a Service (IaaS)

- 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



Poskytovatelia verejného cloudu

- Amazon Web Service
- Microsoft Azure
- Google Cloud Platform
- DigitalOcean

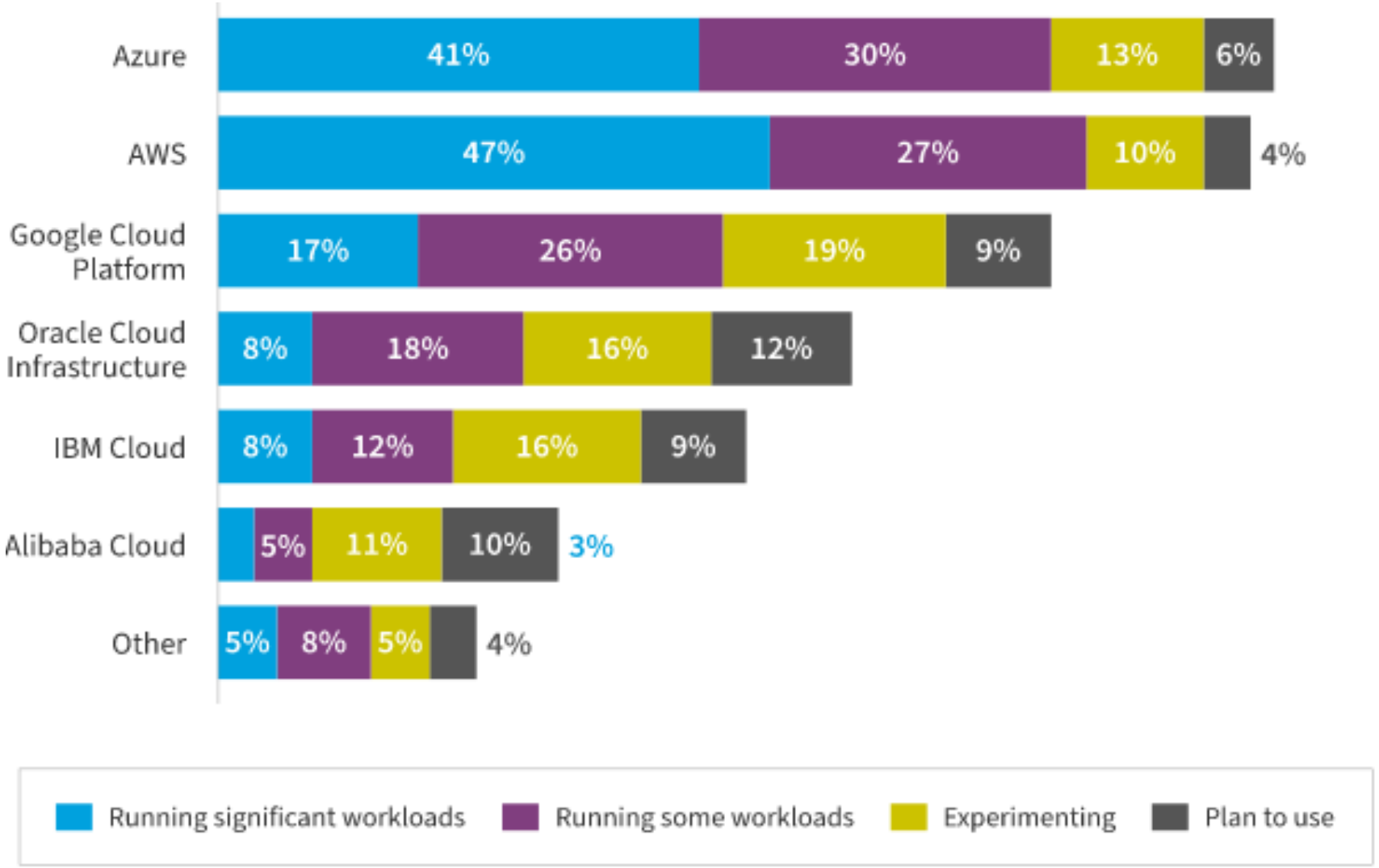
Google Cloud Platform

DigitalOcean

Alibaba Cloud

IBM Cloud

What public cloud providers does your organization use? (2023)



* https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks

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? Prečo SDN?

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

- 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 ☺
  - Premiestnenie servera do inej časti siete (VLAN, ACL, QoS)

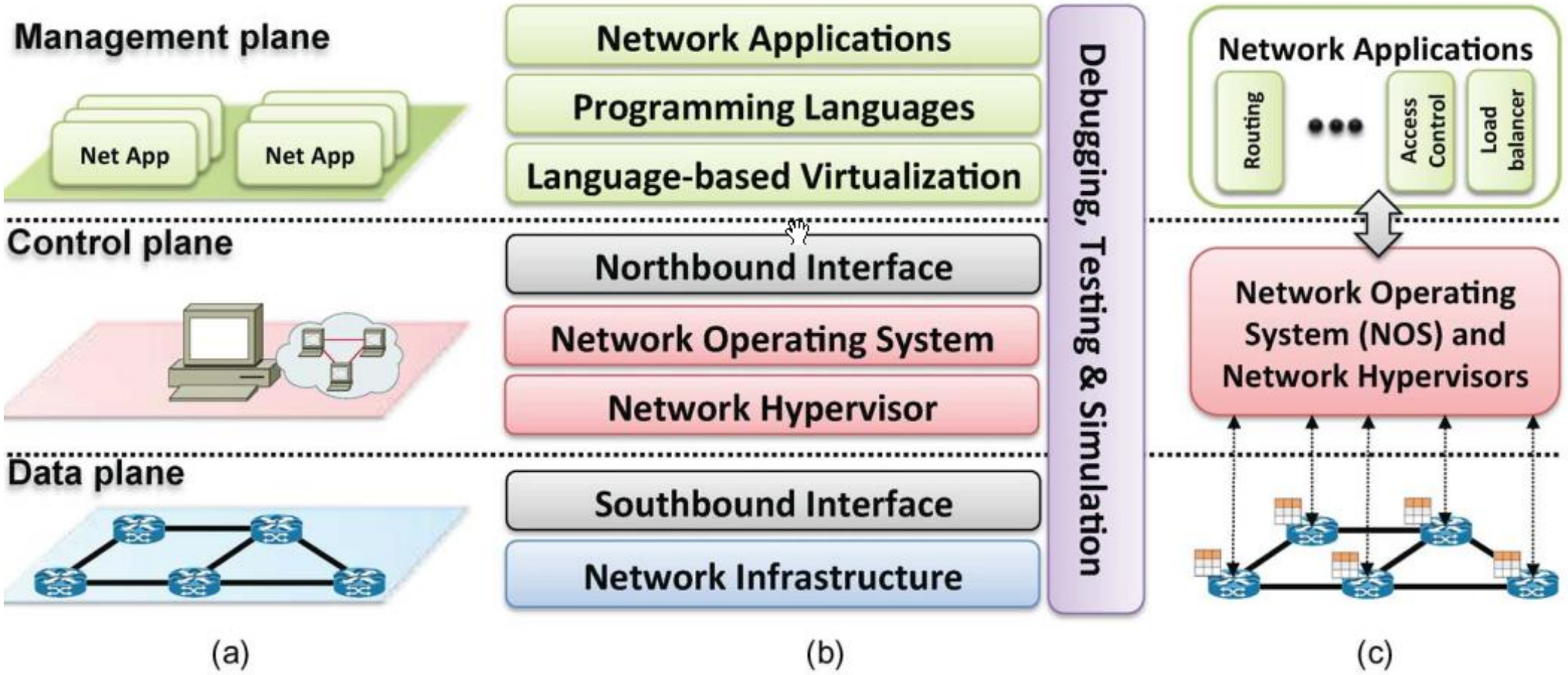
Organizovanie SDN siete

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

Architektúra SDN



Protokoly v SDN

- Pre northbound takmer výlučne RestAPI
- Pre southbound zvyčajne OpenFlow
  - Nie je jediným štandardom, v súčasnosti sú dostupné (či sa vyvíjajú) aj alternatívne otvorené:
    - NetConf
    - LISP
    - XMPP
    - BGP
    - MPLS-TP
    - OVSDB
  - a proprietárne:
    - Cisco OpFlex
    - Fortinet

Štandardizácia v SDN

SDO	Working Group	Focus	Outcomes
ONF	Architecture & Framework	SDN architecture, defining architectural components and interfaces	SDN Architecture [51]
	Northbound Interfaces	Definition of standard NBIs for SDN controllers	
	Testing and Interoperability	Specification of OpenFlow conformance test suites	Conformance tests [52]
	Extensibility	Development of extensions to OpenFlow protocol, producing specifications of the OpenFlow switch (OF-WIRE) protocol	OF-WIRE 1.4.0 [53]
	Configuration & Management	OAM (operation, administration, and management) capabilities for OF protocol, producing specifications of the OF Configuration and Management (OF-CONFIG) protocol	OF-CONFIG 1.2 [54] OpenFlow Notifications Framework [55]
	Forwarding Abstractions	Development of hardware abstractions and simplification of behavioral descriptions mapping	OpenFlow Table Type Patterns [56]
	Optical Transport	Specification of SDN and control capabilities for optical transport networks by means of OpenFlow	Use cases [57] Requirements [58]
	Wireless & Mobile	Specification of SDN and control capabilities for wireless and mobile networks by means of OpenFlow	
	Migration	Methods to migrate from conventional networks to SDN-based networks based on OpenFlow	Use cases [59]
	Market Education	Dissemination of ONF initiatives in SDN and OpenFlow by releasing White Papers and Solution Briefs	SDN White Paper [60]
IETF	Application-Layer Traffic Optimization (ALTO)	Provides applications with network state information	Architectures for the coexistence of SDN and ALTO [61]
	Forwarding and Control Element Separation (ForCES)	Protocol specifications for the communication between control and forwarding elements.	Protocol specification [30]
	Interface to the Routing System (I2RS)	Real-time or event driven interaction with the routing system in an IP routed network	Architecture [62]
	Network Configuration (NETCONF)	Protocol specification for transferring configuration data to and from a device	NETCONF protocol [63]
	Network Virtualization Overlays (NVO3)	Overlay networks for supporting multi-tenancy in the context of data center communications (i.e., VM communication)	Control plane requirements [64]
	Path Computation Element (PCE)	Path computation for traffic engineering and path selection based on constrains	ABNO framework [65] Cross stratum path computation [66]
	Source Packet Routing in Networking (SPRING)	Specification of a forwarding path at the source of traffic	OpenFlow interworking [67] SDN controlled use cases [68]
	Abstraction and Control of Transport Networks (ACTN) BoF	Facilitate a centralized virtual network operation	Virtual network controller framework [69]

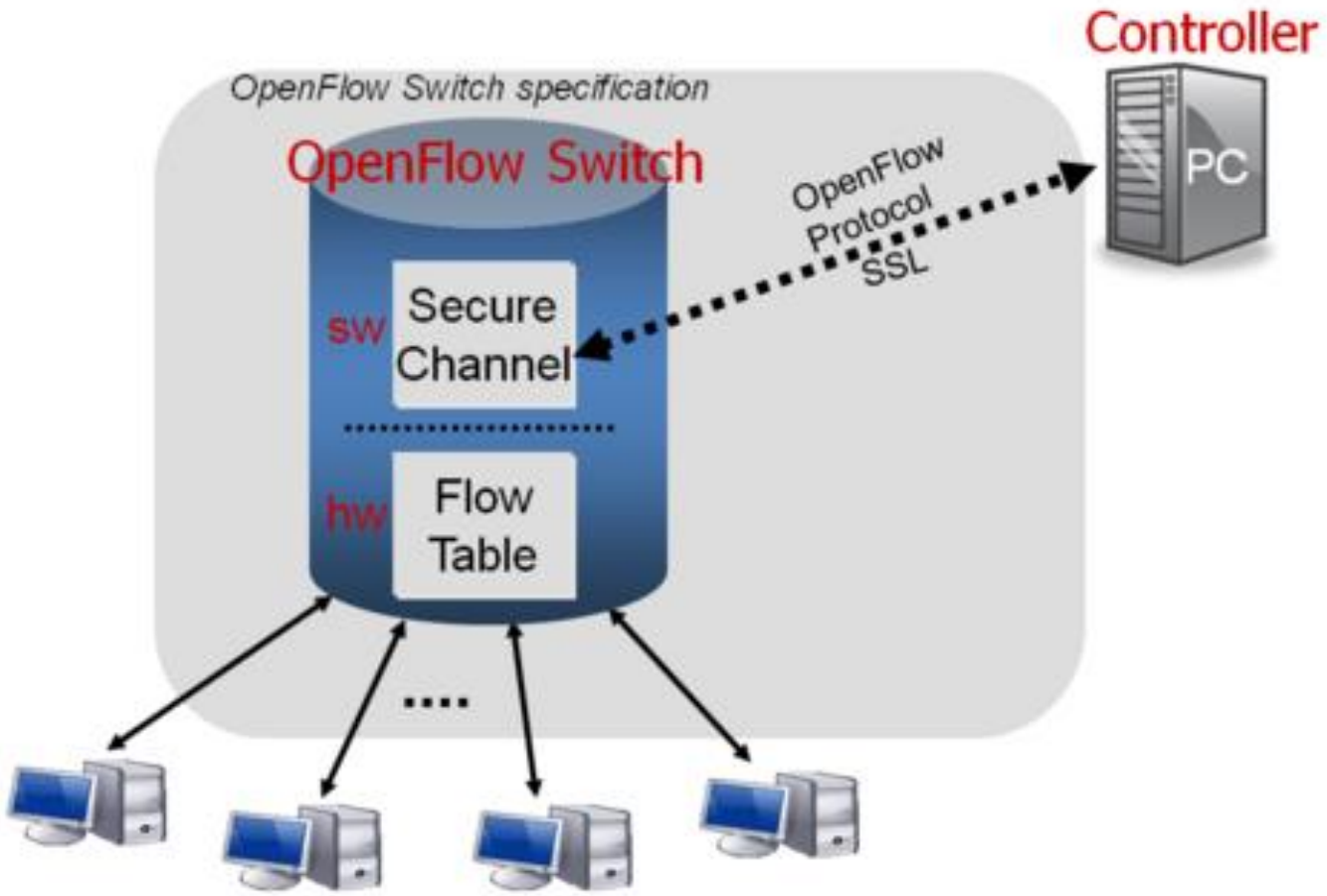
Štandardizácia v SDN (2)

IRTF	Software-Defined Networking Research Group (SDNRG)	Prospection of SDN for the evolution of Internet	SDN operator perspective [70] SDN Architecture [71] Service / Transport separation [72]
ITU-T	SG 11	Signalling requirements using SDN technologies in Broadband Access Networks	Q.Supplement-SDN [73] Q.SBAN [74]
	SG 13	Functional requirements and architecture for SDN and networks of the future	Recommendation Y.3300 [75]
	SG 15	Specification of a transport network control plane architecture to support SDN control of transport networks	
	SG 17	Architectural aspects of security in SDN and security services using SDN	
BBF	Service Innovation and Market Requirements	Requirements and impacts of deploying SDN in broadband networks	SD-313 [76]
MEF	The Third Network	Service orchestration in Network as a Service and NFV environments	
IEEE	802	Applicability of SDN to IEEE 802 infrastructure	
OIF	Carrier WG	Transport SDN networks	Requirements for SDN enabled transport networks [77]
ODCA	SDN/Infrastructure	Requirements for SDN in cloud environments	Usage model [78]
ETSI	NFV ISG	Orchestration of network functions, including the combined control of computing, storage and networking resources	NFV Architecture [79]
ATIS	SDN Focus Group	Operational aspects of SDN and NFV	Operation of SDN [80]

Protokol OpenFlow

- Prvé štandardizované Southbound API
- Rozhranie medzi riadiacou a preposielacou časťou (control a data)
- 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, ...)
- 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

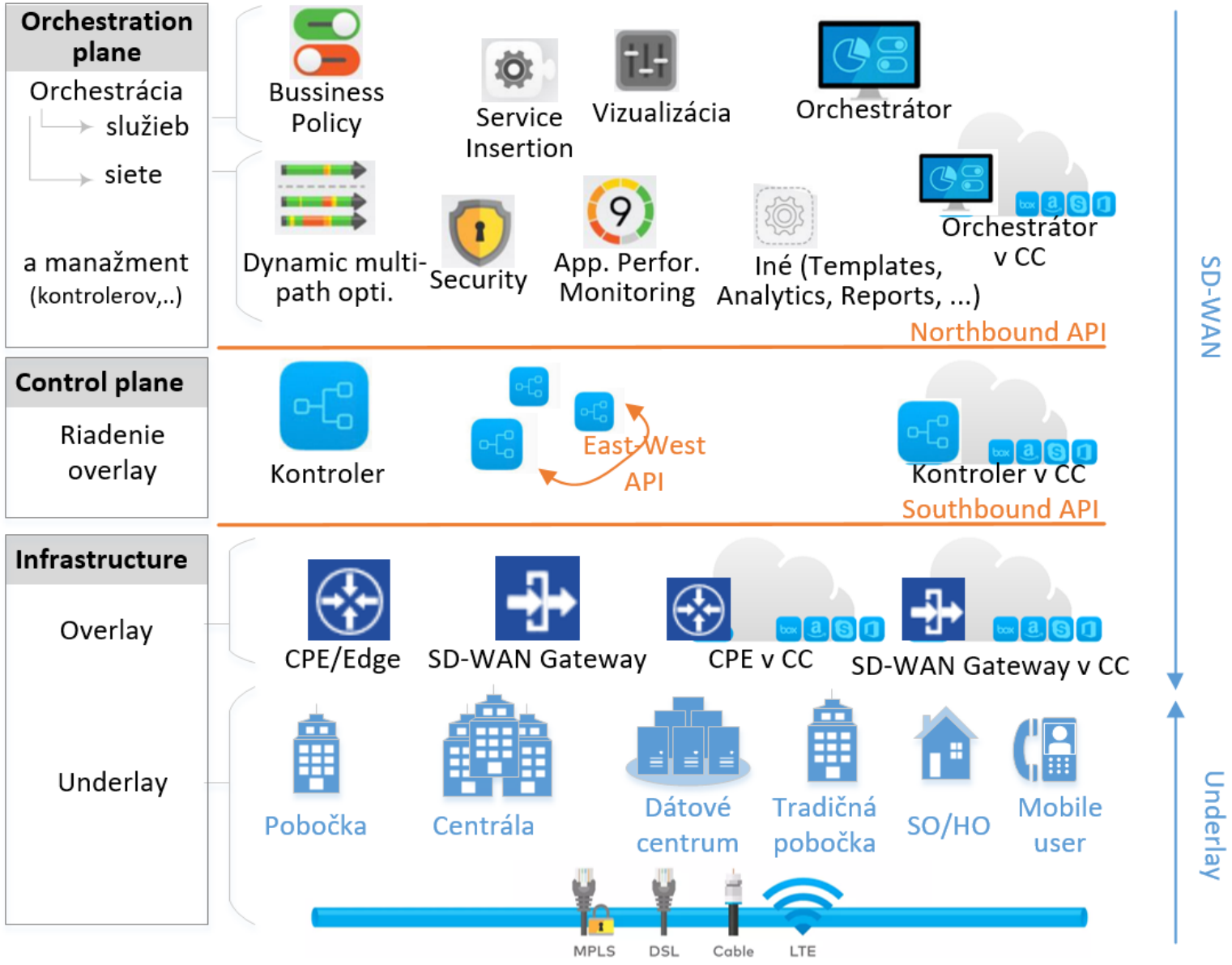
- Brocade MLX smerovače
- HP prepínače (2920, 3500, 5400, 8200)
- Cisco
  - Smerovače so systémom IOS-XE, IOS-XR, NX-OS
  - Prepínače Nexus 3000, 6000, Cat 4500E, Cat 9000
- Juniper smerovače a prepínače
- Mikrotik

Softvérovo definované rozľahlé siete SD-WAN

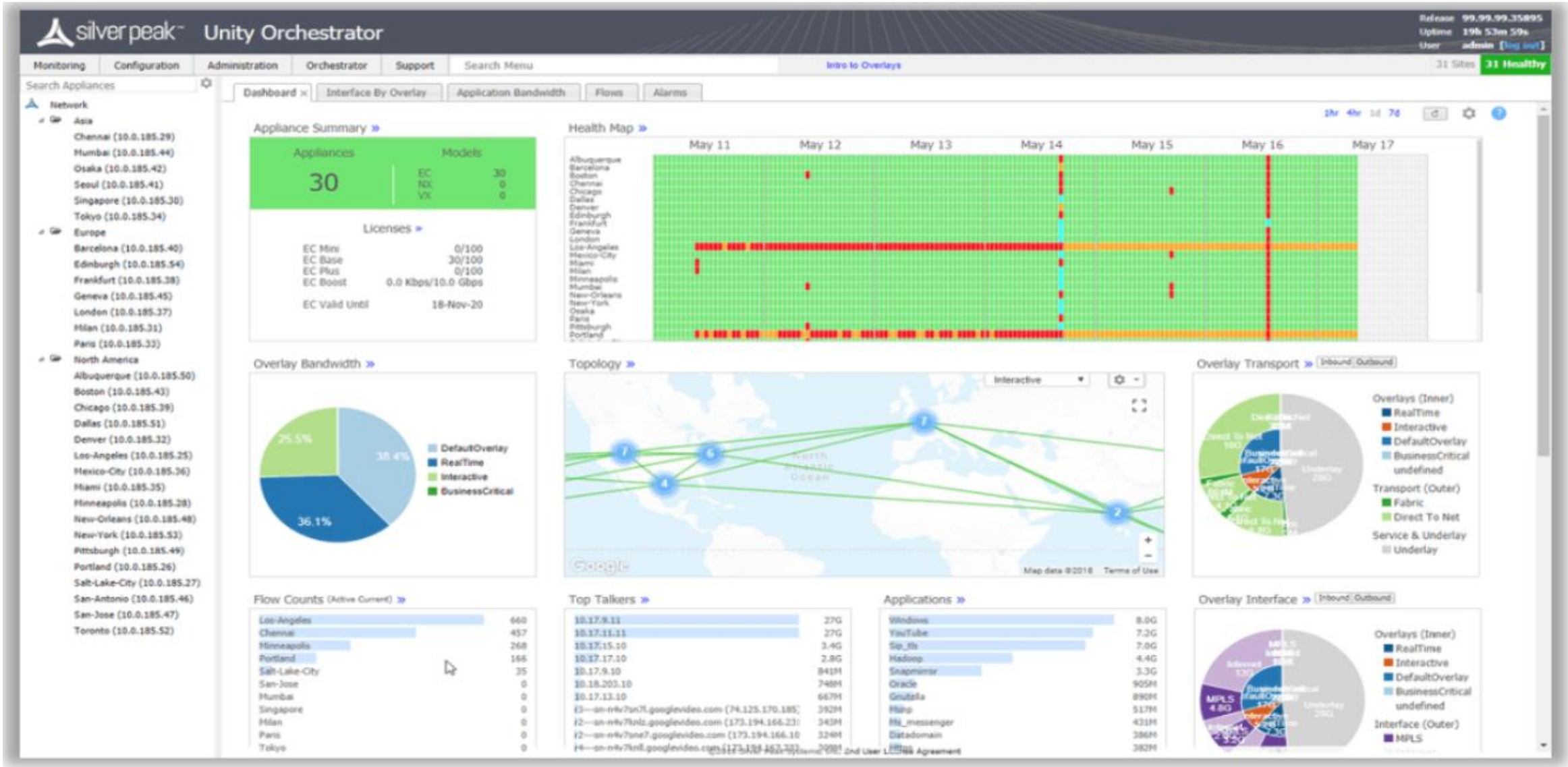
SD-WAN

- Použitie paradigmy SDN na WAN siete
- Kontrolér + CPE (Customer Premises Equipment) zariadenia
- Centrálny dashboard
  - Prehľad o stave fyzických a logických liniek
    - Oneskorenie, stratovosť, jitter, ...

Architektúra SD-WAN



Dashboard


silverpeak Unity Orchestrator
Release 99.99.99.35895
Uptime 19h 53m 59s
User admin [log out]
Monitoring
Configuration
Administration
Orchestrator
Support
Search Menu
Intro to Overlays
31 Sites
31 Healthy
Search Appliances
Network
Asia
Chennai (10.0.185.29)
Mumbai (10.0.185.44)
Osaka (10.0.185.42)
Seoul (10.0.185.41)
Singapore (10.0.185.30)
Tokyo (10.0.185.34)
Europe
Barcelona (10.0.185.40)
Edinburgh (10.0.185.54)
Frankfurt (10.0.185.38)
Geneva (10.0.185.45)
London (10.0.185.37)
Milan (10.0.185.31)
Paris (10.0.185.33)
North America
Albuquerque (10.0.185.50)
Boston (10.0.185.43)
Chicago (10.0.185.39)
Dallas (10.0.185.51)
Denver (10.0.185.32)
Los-Angeles (10.0.185.25)
Mexico-City (10.0.185.36)
Miami (10.0.185.35)
Minneapolis (10.0.185.28)
New-Orleans (10.0.185.48)
New-York (10.0.185.53)
Pittsburgh (10.0.185.49)
Portland (10.0.185.26)
Salt-Lake-City (10.0.185.27)
San-Antonio (10.0.185.46)
San-Jose (10.0.185.47)
Toronto (10.0.185.52)
Dashboard
Interface By Overlay
Application Bandwidth
Flows
Alarms
Appliance Summary
Appliances
30
Models
EC 30
NX 0
VX 0
Licenses
EC Mini 0/100
EC Base 30/100
EC Plus 0/100
EC Boost 0.0 Kbps/10.0 Gbps
EC Valid Until 18-Nov-20
Health Map
May 11
May 12
May 13
May 14
May 15
May 16
May 17
Overlay Bandwidth
25.5%
38.4%
36.1%
DefaultOverlay
RealTime
Interactive
BusinessCritical
Topology
Interactive
Map data ©2018
Terms of Use
Overlay Transport
Inbound Outbound
Overlays (Inner)
RealTime
Interactive
DefaultOverlay
BusinessCritical
undefined
Transport (Outer)
Fabric
Direct To Net
Service & Underlay
Underlay
Flow Counts (Active Current)
Los-Angeles 660
Chennai 457
Minneapolis 268
Portland 166
Salt-Lake-City 35
San-Jose 0
Mumbai 0
Singapore 0
Milan 0
Paris 0
Tokyo 0
Top Talkers
10.17.9.11 27G
10.17.11.11 27G
10.17.15.10 3.4G
10.17.17.10 2.8G
10.17.9.10 841M
10.18.203.10 748M
10.17.13.10 667M
Applications
Windows 8.0G
YouTube 7.2G
Sip_tls 7.0G
Hadoop 4.4G
Snapmirror 3.3G
Oracle 905M
Gnutella 890M
Http 517M
Ms_messenger 431M
Datadomain 386M
382M
Overlay Interface
Inbound Outbound
Overlays (Inner)
RealTime
Interactive
DefaultOverlay
BusinessCritical
undefined
Interface (Outer)
MPLS

CPE

- Fyzické alebo virtuálne zariadenie
- Fyzické
  - Univerzálne CPE
    - GrayBox
    - WhiteBox
  - Uzavreté CPE – BlackBox
- Virtuálne
  - On premise virtuálka
  - Obraz v Cloude (AWS, Azure, ...)
- Je na hranici siete, zvyčajne má viac WAN pripojení
  - Ethernet, MPLS, LTE, ...

White Box

Intel Atom C2000

Siete v SD-WAN

- Delí sa na 2 časti – Underlay a Overlay
- Underlay
  - Fyzická sieť prepájajúca CPE zariadenia a kontrolér
  - Rôzne typy L1
  - Rôzni poskytovatelia konektivity
- Overlay
  - Logická sieť nad Underlay
  - Zvyčajne mesh point-to-point sietí (full mesh, hub and spoke)
  - Tunely bývajú šifrované (IPsec)

Výrobcovia SD-WAN zariadení

- Cisco/Viptela
  - Cisco 4000, ASR 1000, Viptela vEdge 1000, ENCS 5100
- Nokia/Nuage
  - Nokia smerovače, Nuage NSG 7850, NSG-v 7850
- Fortinet
  - Firewally FortiGate – FG 30, 50, 90, FortiManager
- Versa Networks
  - VersaFlex VNF V100
- VMware VeloCloud
  - Najmä virtuálky v rozšírení NSX
- Riverbed
- SilverPeak

Európsky ISP používajúci SD-WAN

- Benestra
  - Nuage
- British Telecom
  - Viptela
- Telefonica
  - Nuage
- Vodafone
  - Juniper Contrail
- Telia/Sonera
  - Najskôr Nuage, prechod na Viptelu

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť.

Vytvorené v rámci projektu KEGA 026TUKE-4/2021