HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

BMEVIHIMA00 Hálózati technológiák integrációja

SDN, NFV

Áttekintő kép

Jakab Tivadar
jakab@hit.bme.hu

Budapest,
2021.04.21.

MŰEGYETEM 1782

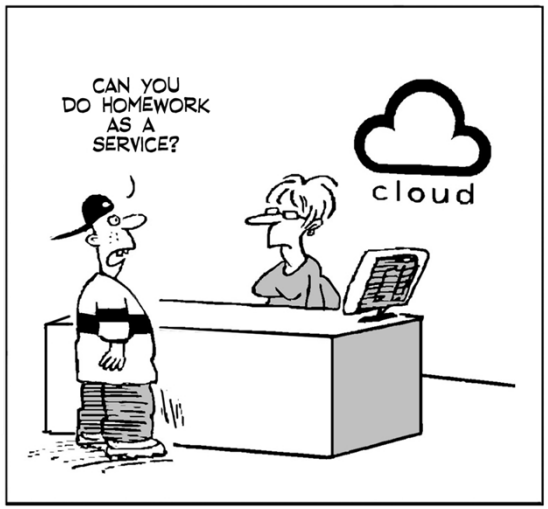
TARTALOM

- Hagyományos architektúrák és korlátaik
- Szoftver alapú hálózatok (SDN)
- Hálózati funkciók virtualizálása
- Források és feldolgozási szempontok

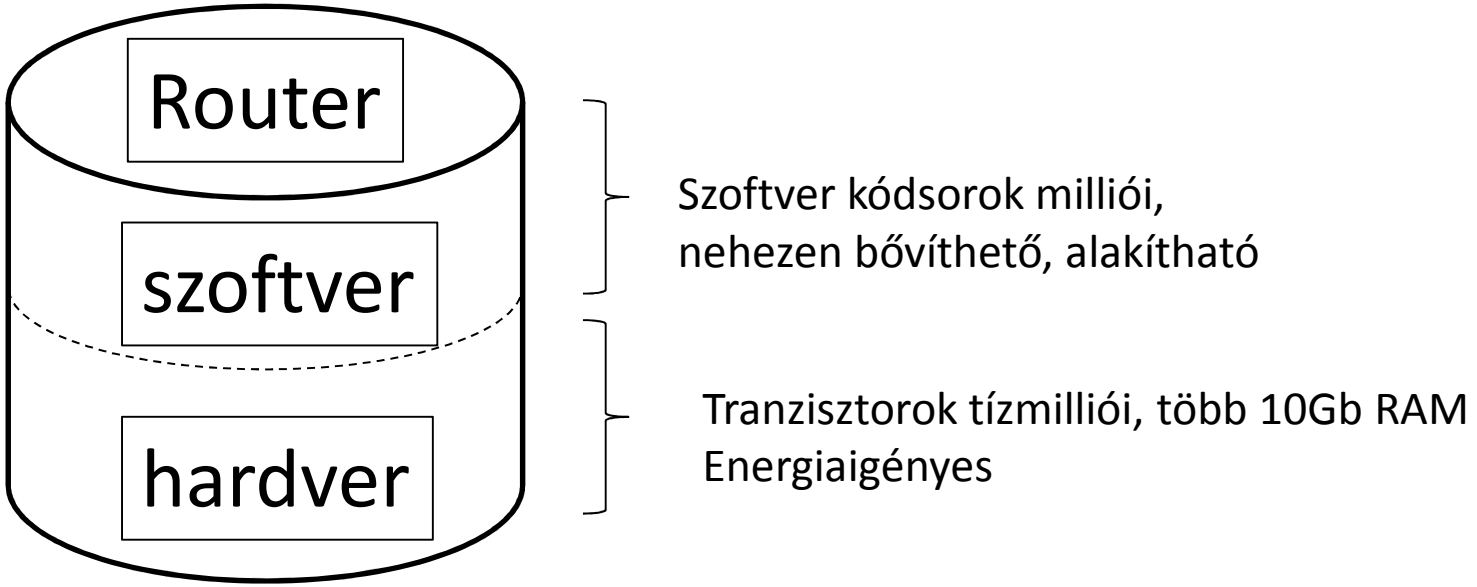
Mottó

To virtualize anything effectively, we have to virtualize everything from resources to services to functions... even to the users themselves. That's the big step because infinite flexibility is only a short distance from chaos.

Forrás: http://www.cloudnfv.com/WhitePaper.pdf

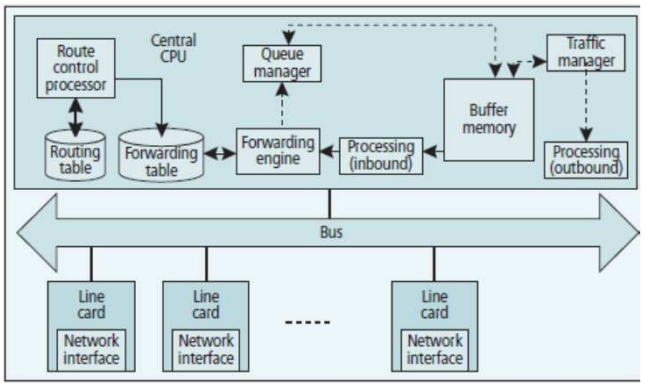


HAGYOMÁNYOS HÁLÓZATOK ARCHITEKTÚRÁJA



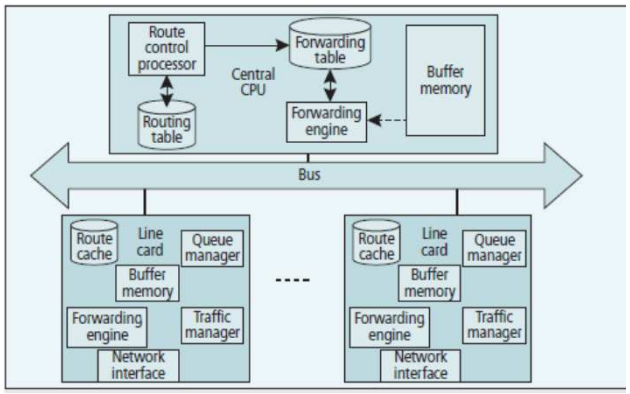
- Vertikális integráció (célhw+célsw): komplex funkciók, protokollok (OSPF, BGP, QoS, forgalomvezérlés / traffic engineering, NAT, tűzfalak, …)

ROUTEREK ARCHITEKTURÁLIS FEJLŐDÉSE



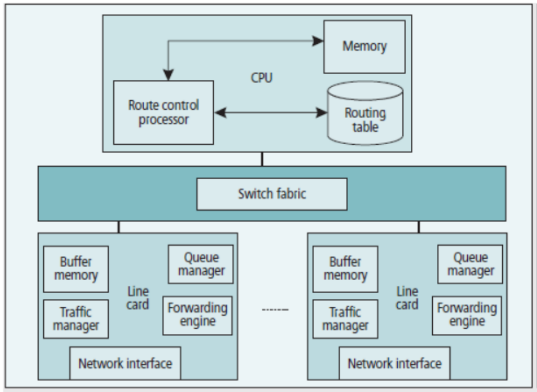
Első generációs router

- Egy CPU
- Közös buszra kapcsolódó interfészkártyák
- Kommersz valós idejű op. rsz.
- Szoftverben implementált funkciók: kapcsoló, sorok menedzselése, forgalom menedzselése L2/L3 feldolgozás
- A CPU-t megosztva használta
  - a csomagtovábbítás
  - a routing protokollok
  - a routing tábla frissítések
  - a menedzsment funkciók



Második generációs router

- Több intelligencia a vonali kártyákon
  - Processzor, memória, továbbításhoz cache
  - Lehetővé téve bizinyos forwarding operációkat
- A vezérlés és a menedzsment továbbra is a CPU-n maradt

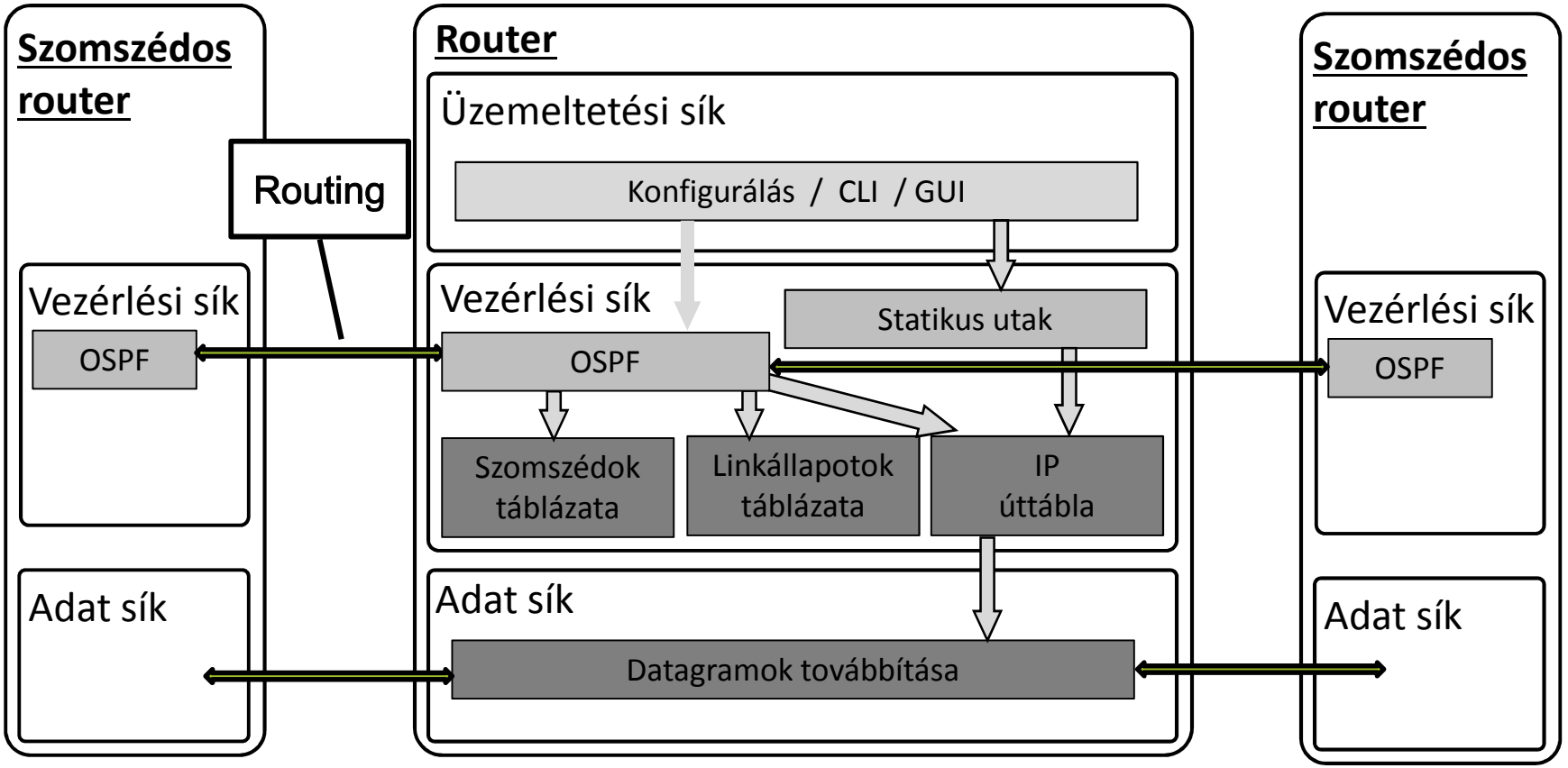


Harmadik generációs router

- Funkciók szigorú szétválasztása
  - Forwarding: hardwer alapú
  - Control: software alapú
- A vezérlés és a menedzsment továbbra is a CPU-n maradt
- A közös busz helyett kapcsolómező a továbbítás sebességének növelésére

Forrás: Kim-Khoa Nguyen et al., Enabling Infrastructure as a Service (IaaS) on IP Networks: From Distributed to Virtualized Control Plane, IEEE Communications Magazine • January 2013, https://ieeexplore.ieee.org/document/6400450

HÁLÓZATI SÍKOK



- **Üzemeltetési sík**: az eszköz beállításainak kezelése (konfigurálás) és működésének felügyelete
- **Vezérlési sík**: a beérkező információk alapján folyamatosan döntéseket hoz a csomagtovábbítás módjáról – merre menjen a forgalom
- **Adatsík**: a vezérlési síktól kapott utasítások alapján dönt a csomagok sorsáról (továbbítás a megfelelő irányba / eldobás)

Forrás: https://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html

A HAGYOMÁNYOS ARCHITEKTÚRA KORLÁTAI

- A gyártóspecifikus vertikális integráció (monolit hw – op.rsz – hálózati funkciók) miatt
  - a fejlesztések időigényesek, sokszor rugalmatlanok, adott alkalmazáshoz szükségtelen funkciókat is tartalmaznak
  - a különböző gyártók eszközeinek közös rendszerben történő üzemeltetése bonyolult és rosszul automatizálható,

    gyártóspecifikus CLI-k, scriptek (minden eszközt másként) <-> integrált üzemeltető sw rendszer (minden funkciót hasonlóan, egyformán)
  - az üzemeltetés skálázhatósága rossz
- Ennek következményeként bár az alapvető hálózati funkció (célcím alapú L3 továbbítás jól működik),

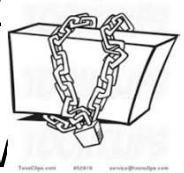
A HAGYOMÁNYOS ARCHITEKTÚRA KORLÁTAI

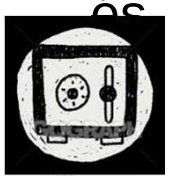
- Bár az alapvető hálózati funkció (célcím alapú L3 továbbítás jól működik), a gyártóspecifikus vertikális integráció korlátainak következményeként
  - nem elég jól működik
    - a célcím alapú L2 továbbítás: pl. STP korlátai)
    - a L3 forgalomvezérlés (Traffic Engineering): pl. a dinamikus erőforrás lefoglalás problémái miatt (pakolási probléma)
    - a nagyméretű folyamok (elephant flow) továbbítása (statisztika: a folyamok ~5%-a a link sávszélességének ~40%-át is elfoglalhatja)
  - gyakorlatilag nem nagyon működik
    - az elosztott an megvalósuló policyk összehangolása (pl. QoS és hálózatbiztonság)
    - policy alapú (L3 és L4 forrás, nyelő) routing magvalósítása
    - biztonsági funkciók hatékony beillesztése a továbbítási útvonalba

A HAGYOMÁNYOS HÁLÓZATOK MEGÚJÍTÁSÁNAK KORLÁTAI

Az innováció korlátai

- Eszközökbe zárt hálózati funkciók (spec hw. + zárt
- Gyártóspecifikus (zárt) sw interfészek
- Lassú protokollszabvány folyamatok
- A gyártók innovációs kapacitásai és üzleti megfontolásai határozzák meg a folyamatok irányát és sebességét





Az üzemletetés korlátai

- Költséges, rosszul skálázódó, lassú folyamatok (hálózati mérnök, CLI, scriptek)

- A konfigurációs hibák okozzák a legtöbb működési zavart

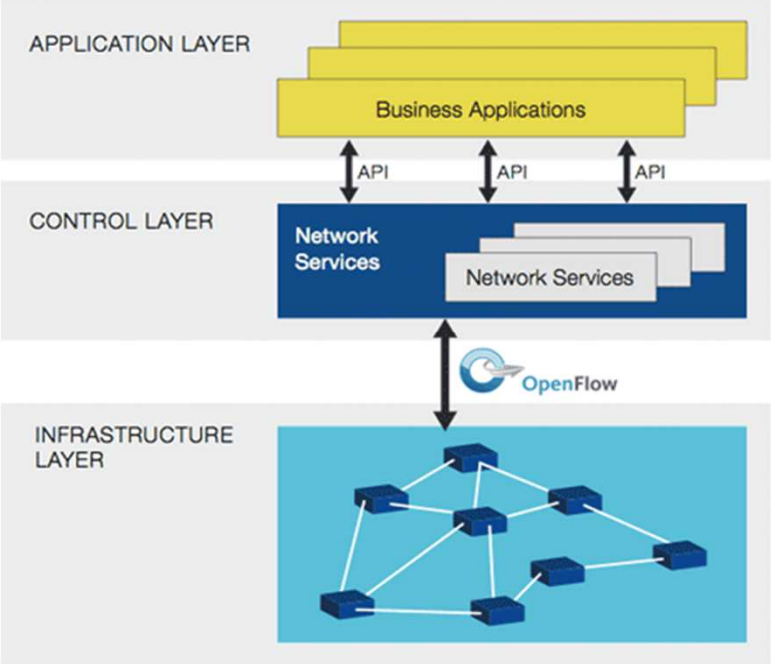
- Szoftverhibák az eszközökben (router sw-e: több millió kódsor. frissítés: ismert hibák ismer cserélése)

- Kritikus hálózati szegmensek
  - Adatközpontok hálózati megoldásai
  - Otthoni hálózatok

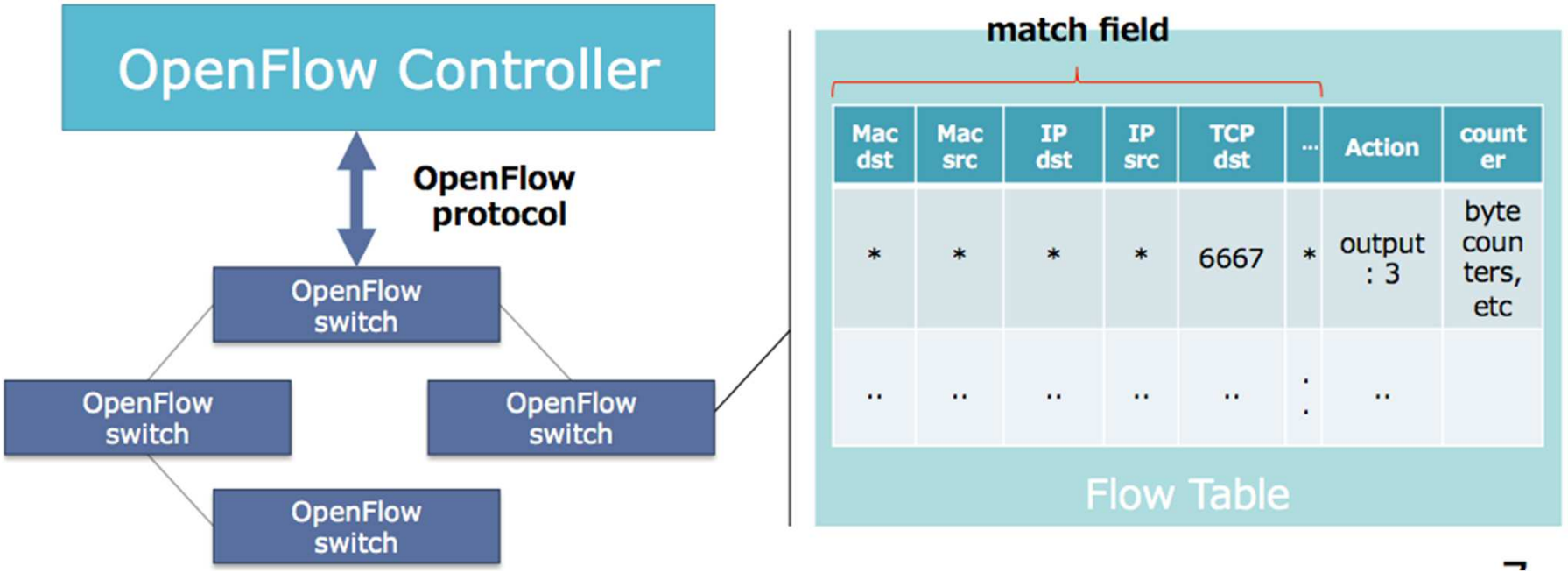
A HÁLÓZATI ARCHITEKTÚRA FEJLŐDÉSI IRÁNYAI

- Szoftver alapú hálózatok
  - erőforrások szoftver alapú vezérlése
  - hatékony kivételkezelés a továbbításban
- Hálózati funkciók virtualizálása
  - az erőforrások egy részének a rugalmasság növelésére fordítása
  - a hálózati funkciók minél nagyobb hányadának tisztán szoftver alapú (nem kell speciális hw) megvalósítása

ÁLTALÁNOS ARCHITEKTÚRA

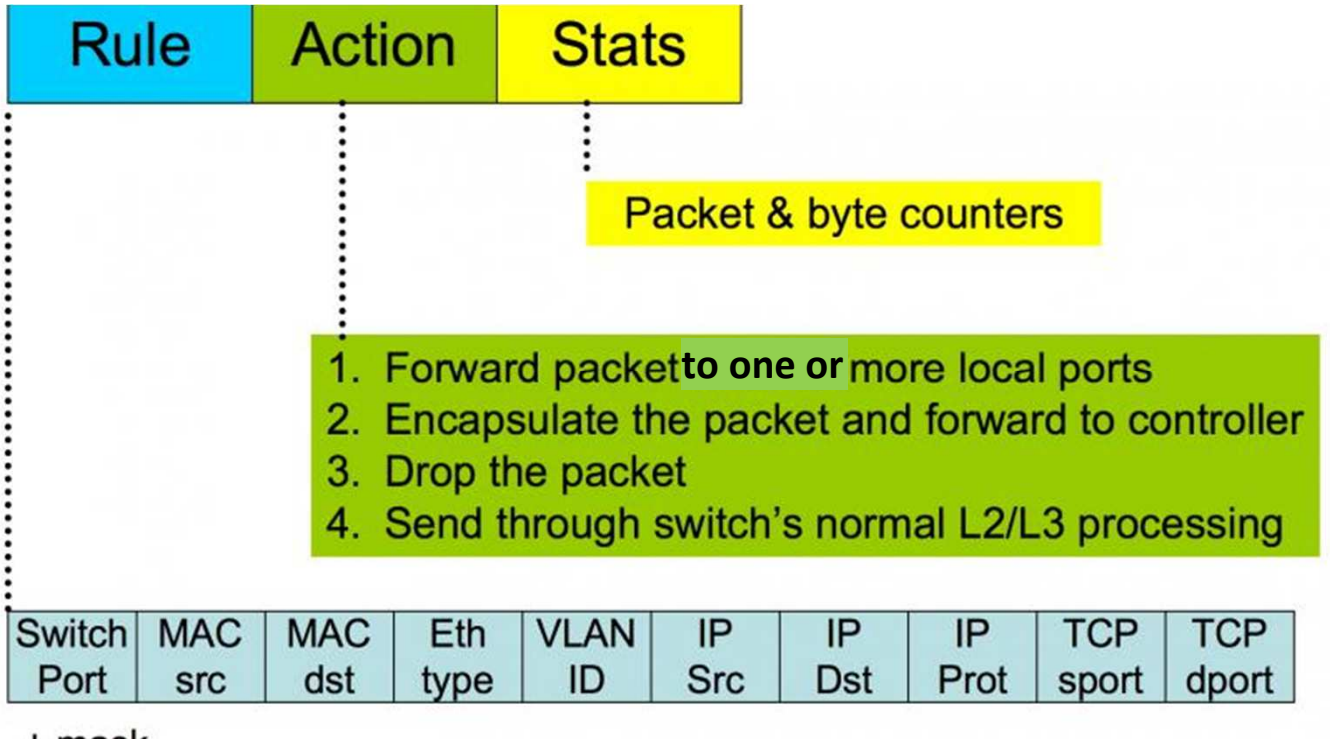


OPENFLOW



- Az SDN megvalósításának egyik meghatározó technológiája
- Nyílt interfész a vezérlési sík és adat sík között

OPENFLOW



- L2, L3 és L4 fejléc adatok alapján integrált továbbítási szabályok

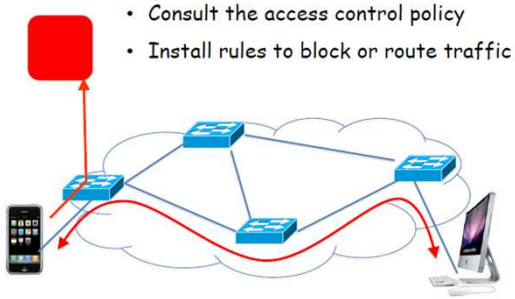
TOVÁBBÍTÁSI SZABÁLYOK
EGY PÉLDA

	Input Port	Source MAC	Dest MAC	Ether Type	VLAN ID	Source IP@	Dest IP@	IP Proto	IP SrcPort	IP DstPort
MASKS										
Ethernet Switching	*	*	12:2E	*	*	*	*	*	*	*
IP Routing	*	*	*	*	*	*	1.2.3.4	*	*	*
App Firewall	*	*	*	*	*	*	*	*	*	443
Flow Switching	Port6	12:2E	17:FF	0800	VLAN7	1.2.3.4	4.3.2.1	06	11317	80
VLAN + App	*	*	*	*	VLAN7	*	*	*	*	80
Port + Ethernet + IP	Port6	12:2E	*	0800	*	*	4.3.2.1	06	*	*

OPENFLOW ALKALMAZÁSI PÉLDÁK

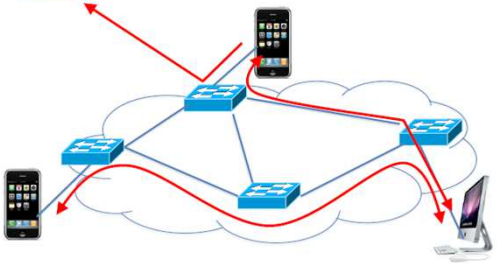
E.g.: Dynamic Access Control

- Inspect first packet of a connection
- Consult the access control policy
- Install rules to block or route traffic



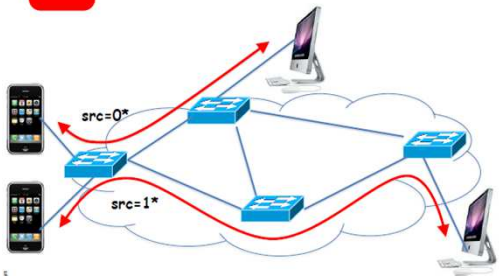
E.g.: Seamless Mobility/Migration

- See host send traffic at new location
- Modify rules to reroute the traffic

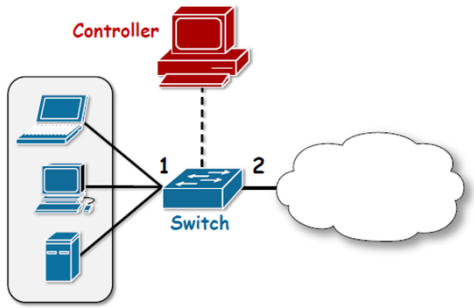


E.g.: Server Load Balancing

- Pre-install load-balancing policy
- Split traffic based on source IP



In-depth Example: Simple Repeater

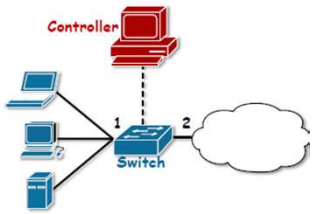


- Simple Network Repeater
  - forward packets received on port 1 out 2 and vice versa

Simple Repeater

Controller (POX) (Pseudo)-Program

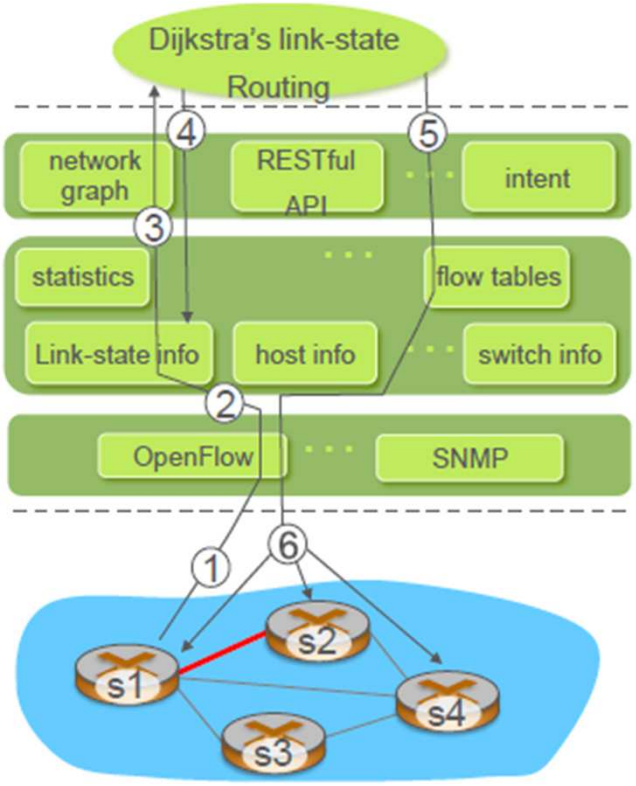
```
def handle_packetIn(packet):
    out_port = 2
    if packet.in_port == 2:
        out_port = 1
    flow_mod = ofp_flow_mod()
    flow_mod.match = ofp_match()
    flow_mod.match.in_port = \
        packet.in_port
    action = ofp_action_output()
    action.out_port = out_port
    flow_mod.action = [ action ]
    flow_mod.buffer_id = \
        packet.buffer_id
    send(flow_mod)
```



Flow Table

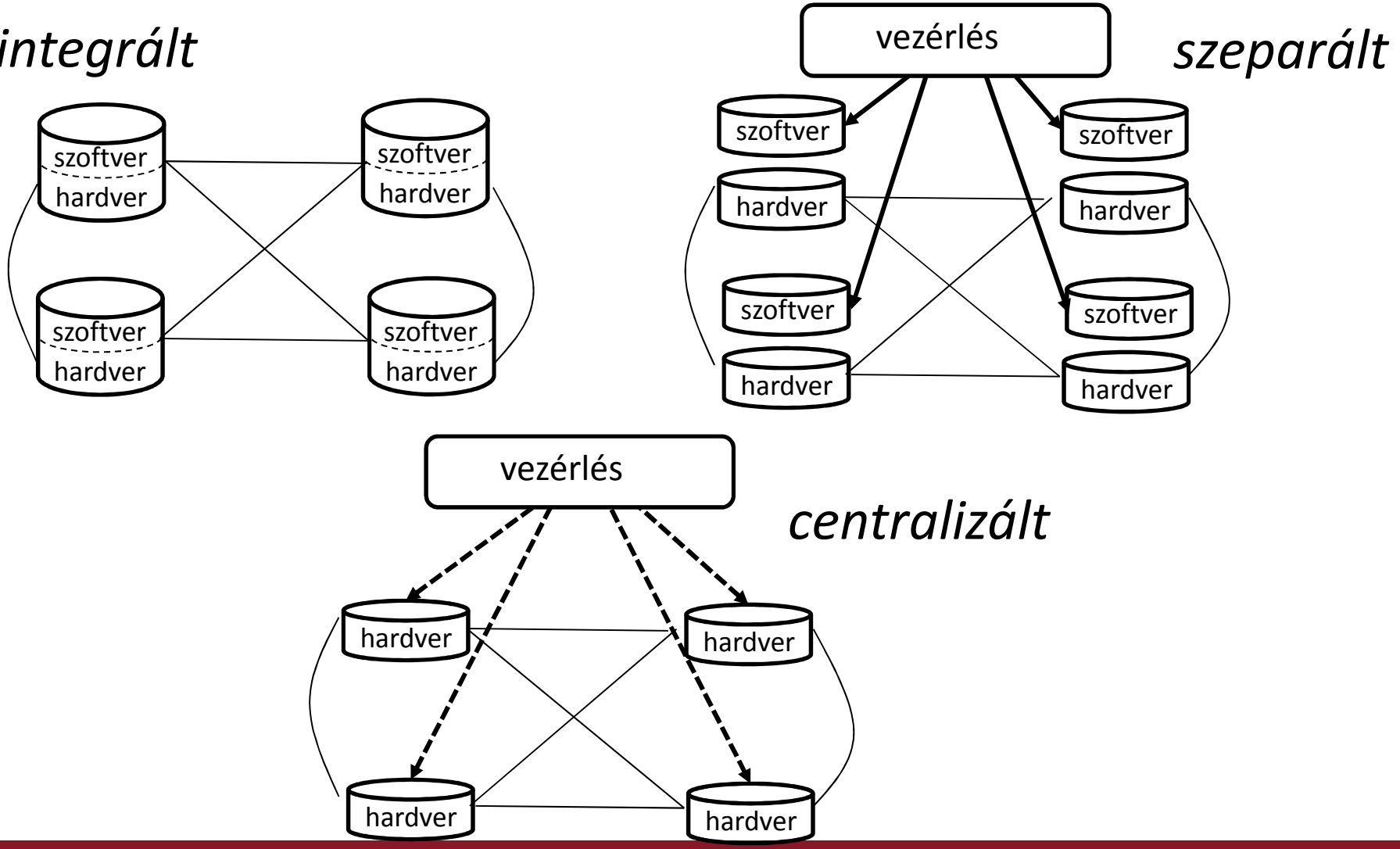
Priority	Pattern	Action	Counters
DEFAULT	IN_PORT:1	OUTPUT:2	(0,0)
DEFAULT	IN_PORT:2	OUTPUT:1	(0,0)

OPENFLOW VEZÉRLÉSI ÉS ADAT SÍK KÖZTI EGYÜTTMŰKÖDÉSI PÉLDA

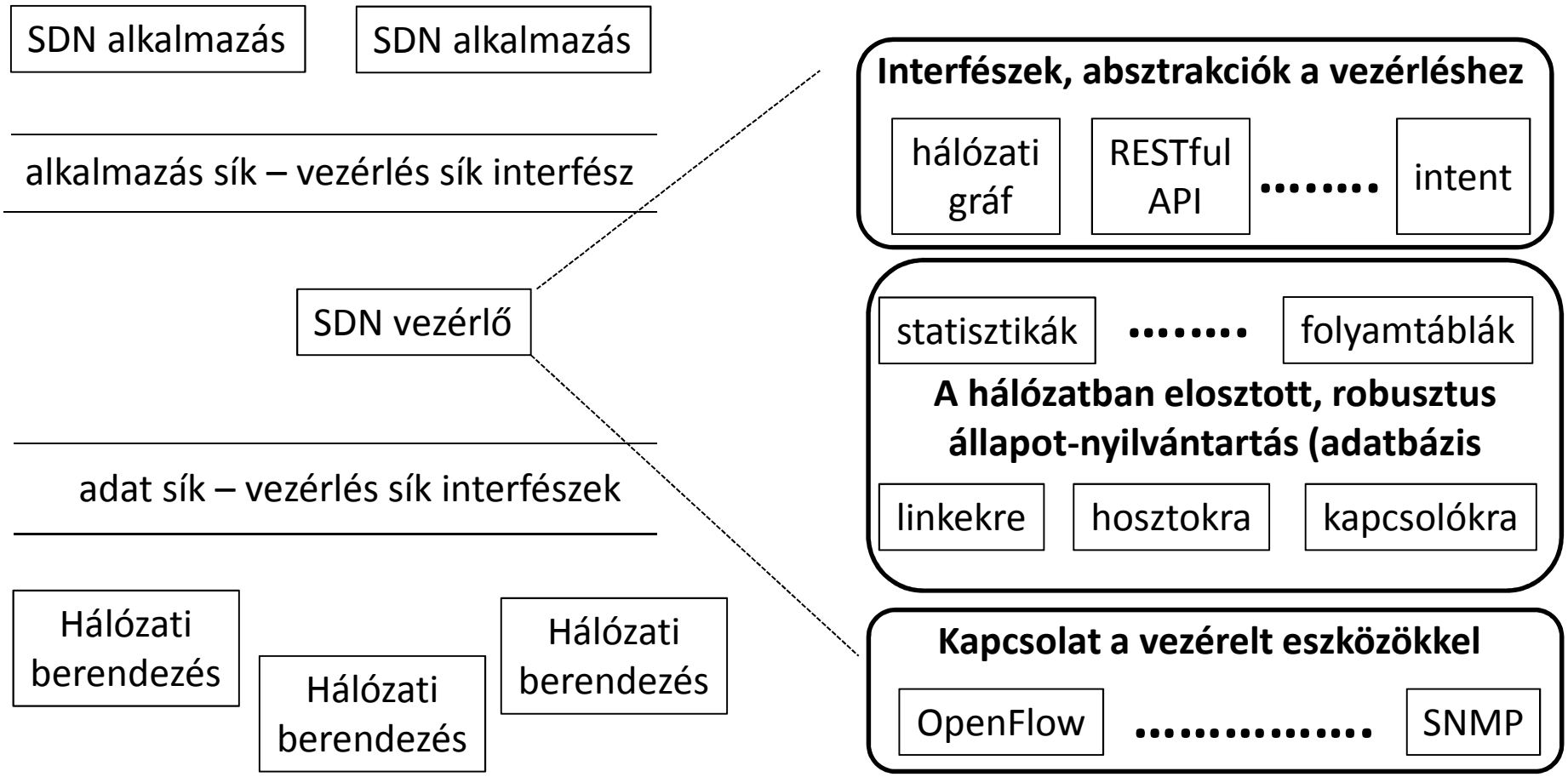


1. S1, experiencing link failure using OpenFlow port status message to notify controller
2. SDN controller receives OpenFlow message, updates link status info
3. Dijkstra's routing algorithm application has previously registered to be called when ever link status changes. It is called.
4. Dijkstra's routing algorithm access network graph info, link state info in controller, computes new routes
5. link state routing app interacts with flow-table-computation component in SDN controller, which computes new flow tables needed
6. Controller uses OpenFlow to install new tables in switches that need updating

SDN
A VEZÉRLÉSI ÉS ADATSÍK SZÉTVÁLASZTÁSA



SDN ARCHITEKTÚRA



SDN ARCHITEKTÚRA - ADATSÍK

- Adat sík
  - Forgalomtovábbító eszközök
    - Gyors, egyszerű kapcsolóeszközök hardverben megvalósított forgalomtovábbítási képességekkel
    - A kapcsolótábla tartalmát a vezérlő biztosítja
    - API a kapcsolótábla vezérléséhez (pl. OpenFlow):
    - Protokoll a vezérlővel folyó kommunikációhoz (p. OpenFlow)
  - Néhány protokollt is képesek futtatni (pl. ARP, LLDP)
  - Jól definiált interfészeken kommunikálnak a vezérlési síkkal
    - Funkcióik szoftveresen vezérelhetők
    - Képességeiket hirdetik
    - Eseményekről jelzést adnak

SDN ARCHITEKTÚRA
VEZÉRLÉSI SÍK

- Vezérlési sík
  - Logikai értelemben központosított
  - Alapvető funkciói
    - A topológiára és a hálózati állapotokra vonatkozó információk kezelése
    - Eszközök felderítése
    - Forgalomtovábbítási út meghatározása
    - Biztonsági funkciók
  - A vezérlők koordinálása
  - Interfész az alkalmazási sík felé

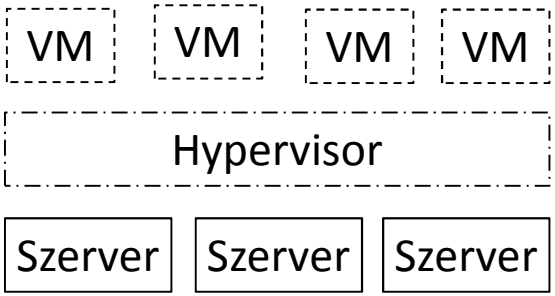
SDN ARCHITEKTÚRA ALKALMAZÁSI SÍK

- Alkalmazási sík
  - Meghatározzák a hálózattól kért erőforrásokat és működést az üzleti és policy szempontoknak megfelelően
  - Vezérlési alkalmazások alapvető funkciói
    - Alacsony szintű funkciókra (vezérlő API) alapozott komplex megoldások
    - Routing/forwarding, access control, terhelésmegosztás (load balancing)
  - Szükséges lehet az elosztott vezérlők működésének összehangolása (*orchestration*)
  - Megfelelő program nyelvek támogatják a fejlesztését

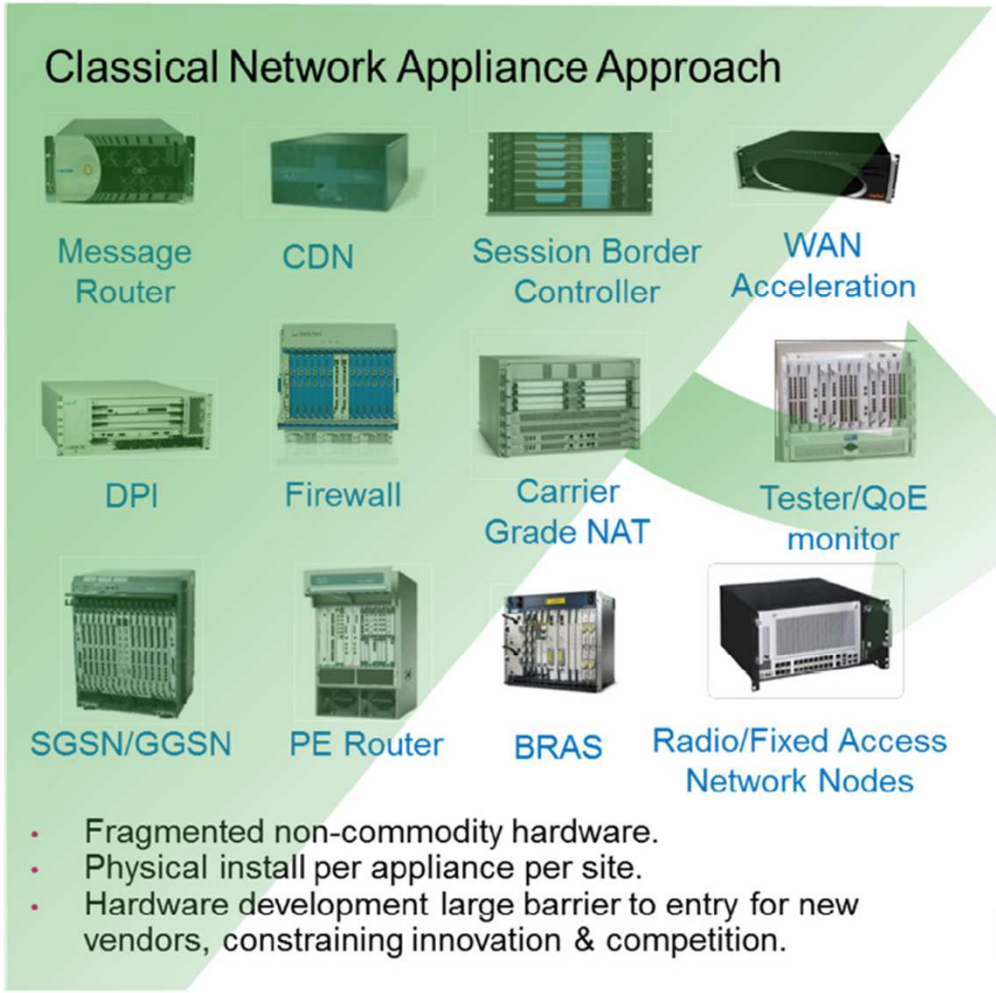
SDN ÖSSZEGZÉS

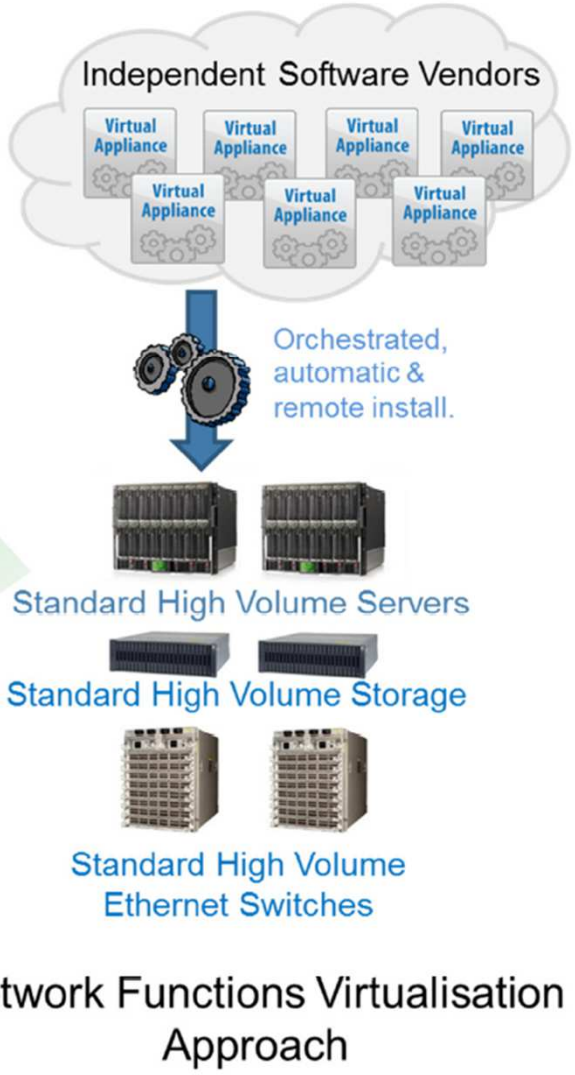
- vezérlési sík és adatsík szétválasztása összetett továbbítási szabályok érvényesítésére
- architektúra
  - három réteg: infrastruktúra (hálózati eszközök és linkek), vezérlés (, alkalmazások a továbbítási szabályok meghatározására
- centralizált vezérlés (egy/több centralizált vezérlő)
- jól definiált nyílt API
- csomagjellemzőkre alapozott továbbítási szabályok
  - L2, L3, L4 header alalpú szabályok:
  - MAC src addr, dst addr, Eth type, VLAN ID,
  - MAC src addr, dst addr, prot
  - src port, dst port

- Hálózati funkciók virtualizálása
  - Hardver és szoftver szétválasztása (COTS szerverek)
  - Hálózat funkciók rugalmas, jól skálázható és automatizálható (szoftverből vezérelhető) létrehozása
  - Hálózati szolgáltatások dinamikus létesítése, telepítése, skálázása
  - Virtualizált funkciók gyors, egyszerű mozgathatósága
  - Kódok újrahasznosíthatósága
- Hálózati funkciók virtualizálása
  - Hálózati funkciók szoftver alapon
  - Moduláris hálózati funkciók
  - Implementálás virtuális gépekben (COTS szerverek, hypervisor)
  - Jól definiált API-k a szoftvermodulok között

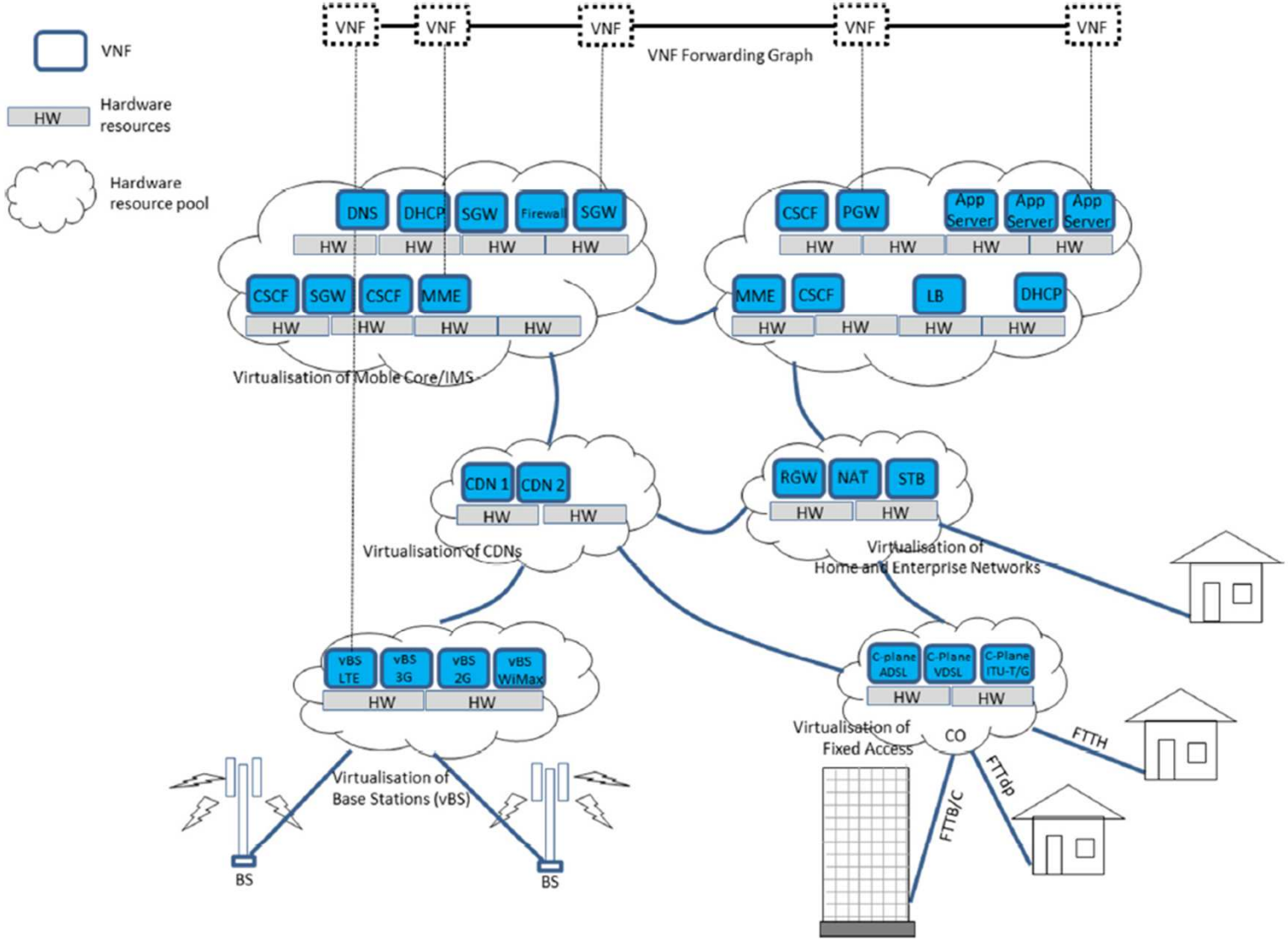


HÁLÓZATI FUNKCIÓK VIRTUALIZÁLÁSA





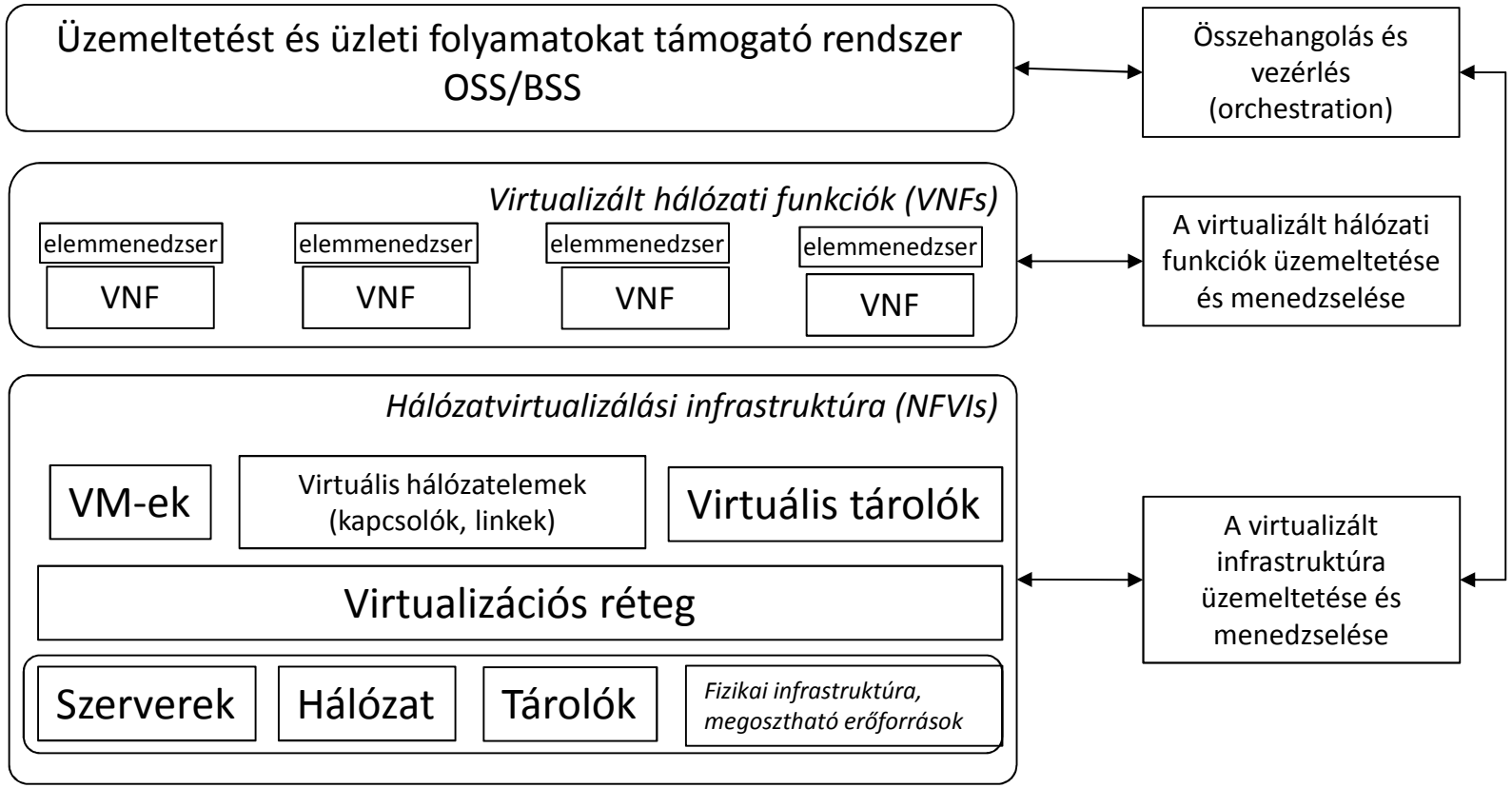
HÁLÓZATI FUNKCIÓK VIRTUALIZÁLÁSA: ALKALMAZÁSI PÉLDÁK



EGYSZERŰSÍTETT ETSI NVF ARCHITEKTÚRA

- Hálózati funkciók virtualizálása
  - Hardver és szoftver szétválasztása (COTS szerverek)
  - Hálózat funkciók rugalmas, jól skálázható és automatizálható (szoftverből vezérelhető) létrehozása
  - Hálózati szolgáltatások dinamikus létesítése, telepítése, skálázása
  - Virtualizált funkciók gyors, egyszerű mozgathatósága
  - Kódok újrahasznosíthatósága
- Hálózati funkciók virtualizálása
  - Hálózati funkciók szoftver alapon
  - Moduláris hálózati funkciók
  - Implementálás virtuális gépekben (COTS szerverek, hypervisor)
  - Jól definiált API-k a szoftvermodulok között

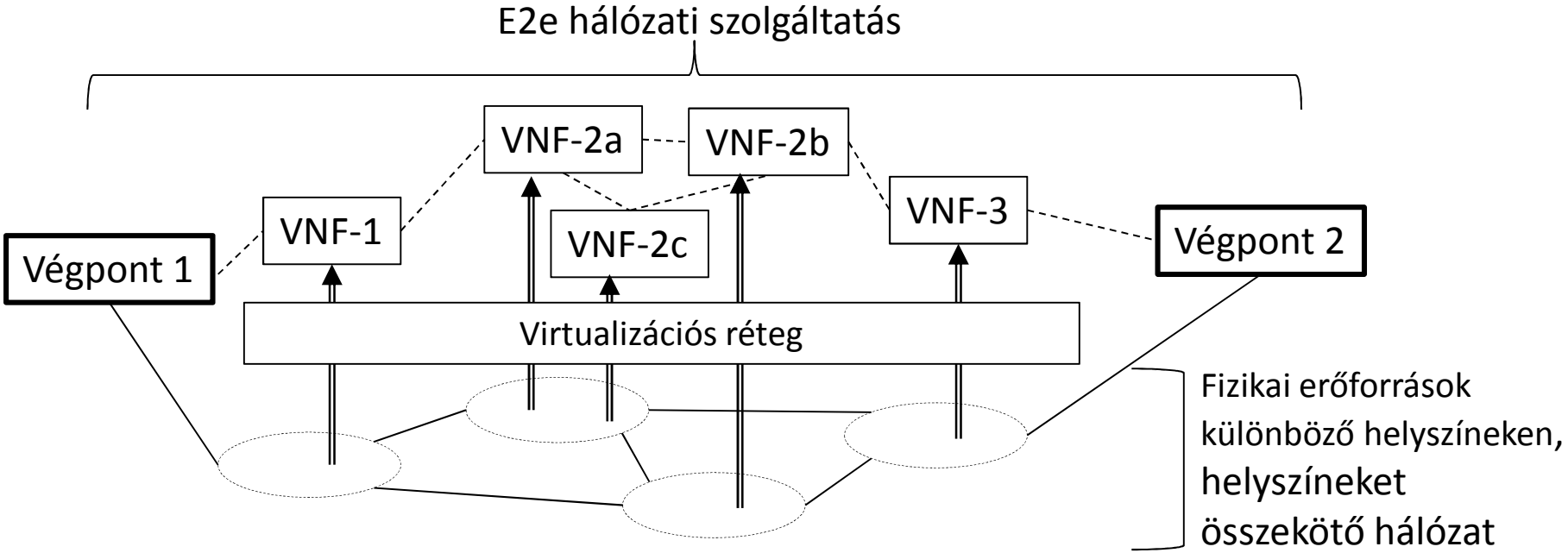
EGYSZERŰSÍTETT ETSI NVF ARCHITEKTÚRA



EGYSZERŰSÍTETT ETSI NVF ARCHITEKTÚRA

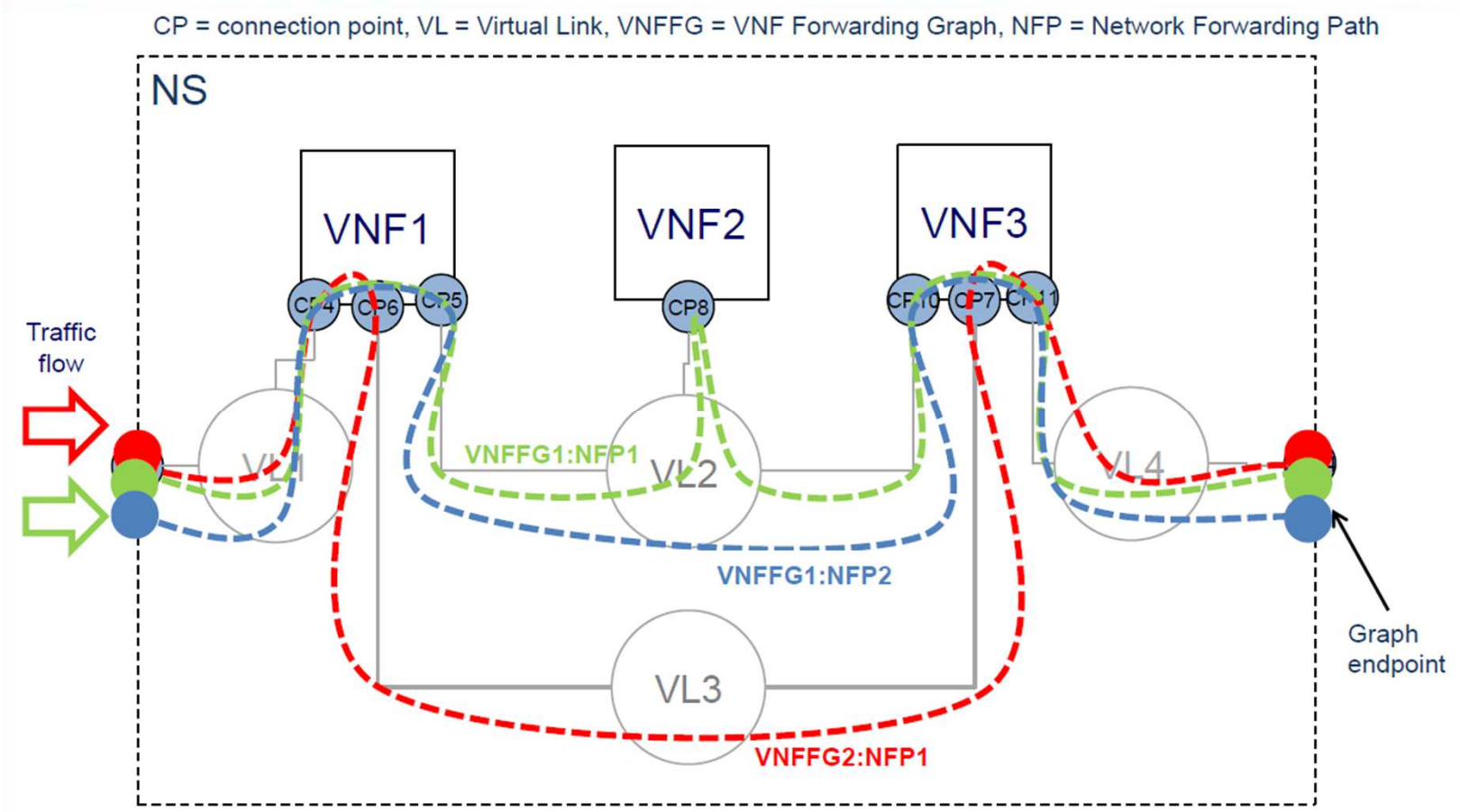
- Funkcionális blokkok
  - Üzemeltetés és üzleti folyamatokat támogató rendszer (Operations and Business Support Systems – OSS/BSS)
    - szolgáltatások, számlázás, minőség-ellenőrzés, fejlesztés, stb.
  - Elemmenedzser
    - Egy vagy néhány (azonos típusú) virtualizált hálózati funkció alapvető menedzselési eszközei
  - Virtualizált hálózati funkció
    - Több komponensből is állhat, amelyek különböző VM-eken lehetnek megvalósítva
    - Pl. egy otthoni hálózat egyik eleme: Otthoni átjáró (Residential Gateway)
  - Hálózati infrastruktúra
    - Adatközponton (hálózati helyen) belül a számítási és tárolási infrastruktúra elemeinek összekapcsolására
    - Transzporthálózat a hálózati helyek összekapcsolására
  - Hardver erőforrások
    - COTS szerverek, tárolók
  - Virtualizációs réteg és virtualizált erőforrások
    - Szétválasztja és ezzel függetleníti a VNF-et megvalósító szoftvert és a kiszolgáló erőforrásokat, ezzel függetleníti a hardver és a szoftver életciklusát
    - Lehetővé teszi, hogy a VNF-et megvalósító szoftver különböző hardver erőforrásokon is megvalósulhasson
    - Indokolt esetekben a VM-eknek lehet közvetlen hozzáférése egyes hardver erőforrásokhoz (pl. hálózati kártyák - NIC) a jobb teljesítmény érdekében
    - Ugyanakkor a VM-nek szabványos hozzáférést kell biztosítania az erőforrásokhoz a VNF-ek számára
  - A virtualizált infrastruktúra üzemeltetése és menedzselése
    - Ellenőrzi és kezeli a VNF és az azt kiszolgáló erőforrások együttes működését (nyilvántartás, erőforrás-lefoglalás/felszabadítás, hibamenedzsment, stb.)
  - A VNF-ek menedzselése
    - A VNF-ek élettartama alatt a létehozás, frissítés, lekérdezés, skálázás, leállítás feladatait látja el
  - Összehangolás és vezérlés (orchestration)
    - A hálózatvirtualizálási infrastruktúra és a szoftvererőforrások kezelésével hálózati szolgáltatásokat valósít meg

HÁLÓZATI SZOLGÁLTATÁS NFV KÖRNYEZETBEN



- Hálózati funkciók láncolása komplex (több hálózati funkciót is magában foglaló) szolgáltatások kialakítására
- Az egyes virtuális funkciók megvalósítása az infrastruktúrán el van fedve az e2e szolgáltatás elől, kivéve ha valamilyen speciális előírás (policy constraint) szükségessé teszi (pl. helyfüggő szolgáltatás megvalósítása)
- Az egyes funkciók különböző földrajzi helyeken valósíthatók meg
- Továbbítási gráf a funkciók megfelelő sorrendű bejárásához(pl. tűzfal, NAT, terhelésszétosztás)

HÁLÓZATI SZOLGÁLTATÁS NFV KÖRNYEZETBEN

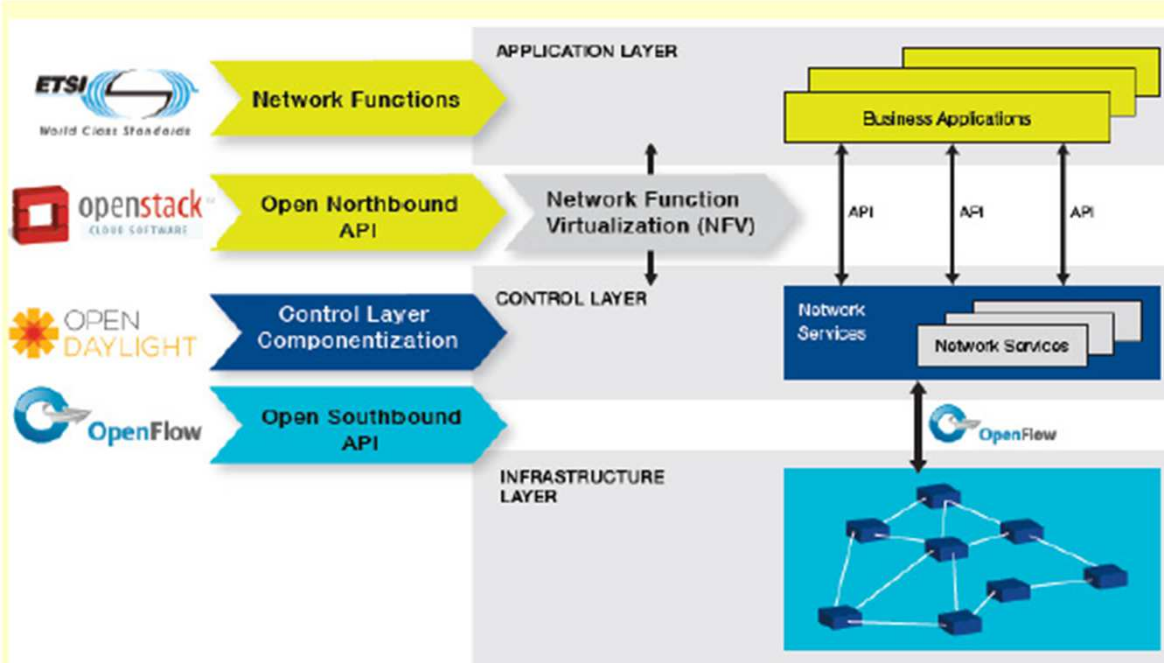


NFV ÖSSZEGZÉS

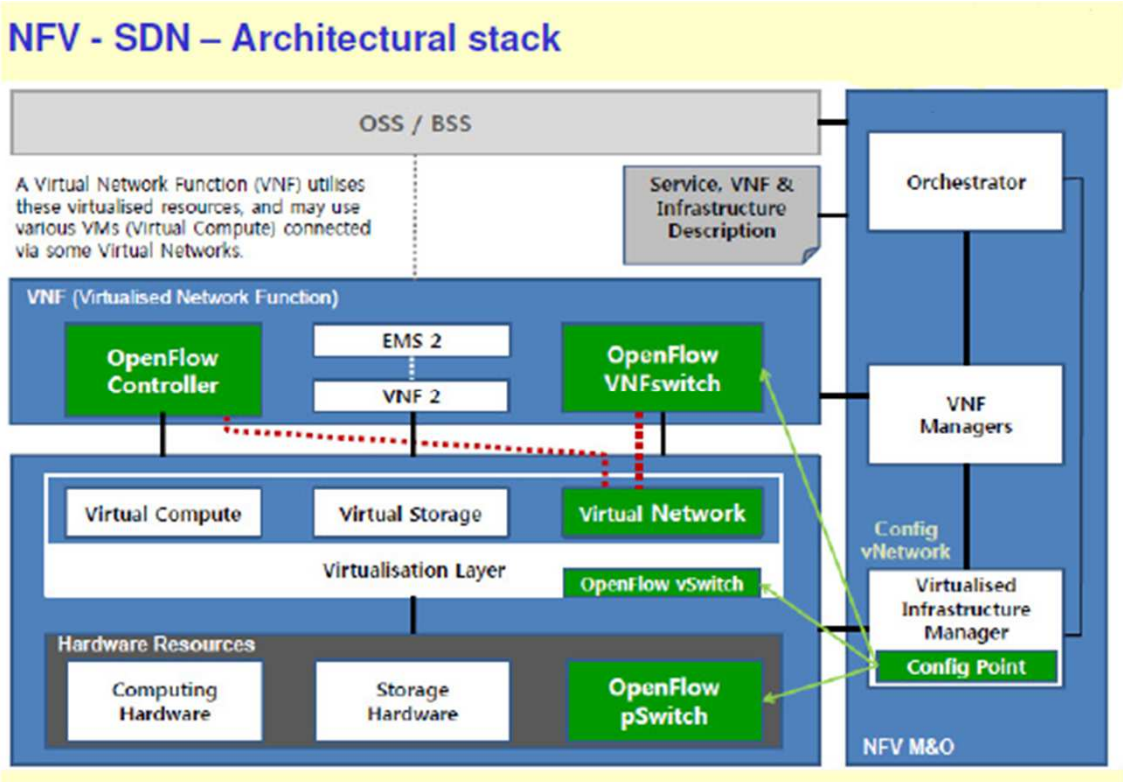
- Hálózati funkciók szoftver alapon
- Moduláris hálózati funkciók
- Implementálás virtuális gépekben (COTS szerverek, hypervisor)
- Jól definiált API-k a szoftvermodulok között

- Skálázhatóság (példányosítás)
- Nyílt platformokon
- Szoftverkomponensek újrafelhasználhatósága
- Szoftver alapú üzemeltetés (programozhatóság, automatizálhatóság)

NFV –SDH


ETSI
World Class Standards
Network Functions
openstack
CLOUD SOFTWARE
Open Northbound API
OPEN DAYLIGHT
Control Layer Componentization
OpenFlow
Open Southbound API
APPLICATION LAYER
Business Applications
Network Function Virtualization (NFV)
API
API
API
CONTROL LAYER
Network Services
Network Services
OpenFlow
INFRASTRUCTURE LAYER

NFV –SDH


NFV - SDN – Architectural stack
OSS / BSS
A Virtual Network Function (VNF) utilises these virtualised resources, and may use various VMs (Virtual Compute) connected via some Virtual Networks.
Service, VNF & Infrastructure Description
Orchestrator
VNF (Virtualised Network Function)
OpenFlow Controller
EMS 2
VNF 2
OpenFlow VNFswitch
VNF Managers
Virtual Compute
Virtual Storage
Virtual Network
Config vNetwork
Virtualisation Layer
OpenFlow vSwitch
Virtualised Infrastructure Manager
Config Point
Hardware Resources
Computing Hardware
Storage Hardware
OpenFlow pSwitch
NFV M&O

IRODALMAK ÉS FELDOLGOZÁSI SZEMPONTOK

A tárgy honlapjára felkerültek az NFV témakörrel (5.) kapcsolatos források lapján a következőek a célkitűzések a Network Function Virtualization (NFV) témakörben:

- **NFV főbb motivációk, célok megismerése, megértése,**

  Forrás:

  Driving digital transformation in networks and operations | SDN NFV World Congress 2018

  Adan Pope, Cienna, https://www.youtube.com/watch?v=TTILQPCOox8

  (ehhez sajnos nem találtam meg az előadás anyagát pdf-ben)

- **SDN (Service Defined Network) és NFV viszonyának, kapcsolódásának megismerése, megértése**

  Források: honlap (http://www.hit.bme.hu/~jakab/edu/HTI20.htm)

  1.c.ii és 1.c.iii (két Ivan Pepelnjak előadás)

  5.b.ii (Marie-Paule Odini ETSI NFV turorial) és

  a kapcsolódó ETSI NFV tanulmány:

  Report on SDN Usage in NFV Architectural Framework

- **az ETSI NFV architektúra áttekintése**

  Források:(http://www.hit.bme.hu/~jakab/edu/HTI20.htm)

  5.b.i (Dr. Raquel Morera tutorial, az architektúra a lényeges, nem az interfészek részletei)

- **ETSI MANO** (csak áttekintés jelleggel, amennyi az 5G menedzsment megértéséhez kell)

  Források:(http://www.hit.bme.hu/~jakab/edu/HTI20.htm)

  6.c.iii (Uwe Rauschenbach: NFV MANO Part 1: Overview and VNF Lifecycle Management)

  6.c.iv (Jeremy Fuller: NFV MANO Part 2: Network Service Lifecycle Management)

IRODALMAK ÉS FELDOLGOZÁSI SZEMPONTOK

- **Biztonsági vonatkozások** (érdeklődőknek)

  Lehetséges források :(http://www.hit.bme.hu/~jakab/edu/HTI20.htm)

  További ETSI előadások

  6.c.v Security Challenges and Opportunities in SDN/NFV and 5G Networks

- **alkalmazási vonatkozások áttekintése egy kiválasztott példa alapján**

  Lehetséges források:

  ETSI (válogatott tanulmányok: http://www.hit.bme.hu/~jakab/edu/HTI19/ETSI_NFV_2019_RepTab_v3.htm)

  Report on Acceleration Technologies & Use Cases

  (https://docbox.etsi.org/ISG/NFV/Open/Publications_pdf/Specs-Reports/NFV-IFA%20001v1.1.1%20-%20GS%20-%20Acceleration%20-%20UCs%20report.pdf)

  Virtualizálás a mobil hálózatban

  6.f.i SDN/NFV-Based Mobile Packet Core Network Architectures: A Survey

  (Van-Giang Nguyen et. al., IEEE Comm. Surveys and Tutorials Vol. 19, No. 3)

  (http://www.hit.bme.hu/~jakab/edu/litr/NFV/SDN_NFV-Based%20Mobile%20Packet%20Core%20NetworkArchitectures%20-%20A%20Survey__IEEE07892961.pdf)