

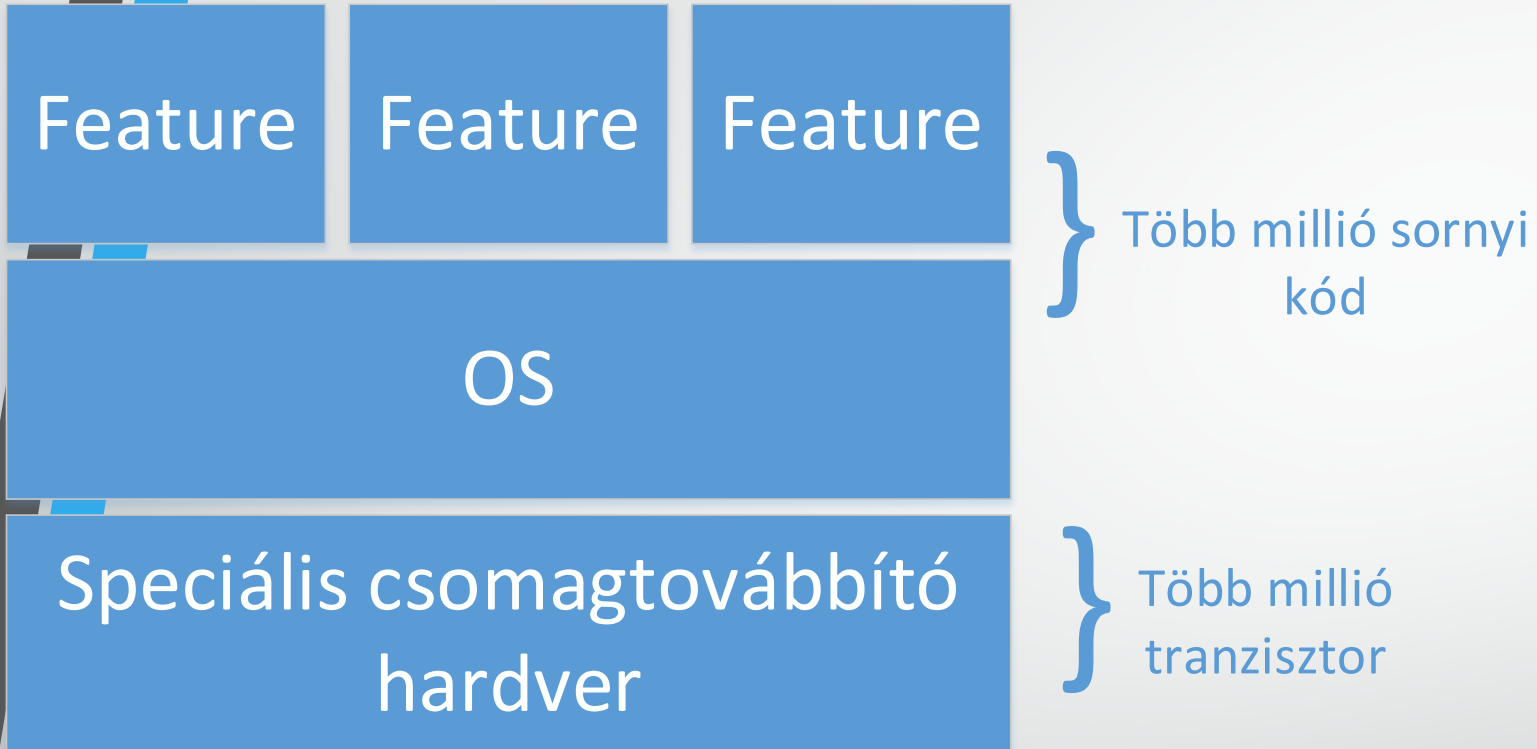
# IP alapú kommunikáció

7. Előadás – SDN

Kovács Ákos

- A meglévő hálózatok limitációi:
  - Nehéz a valóssal megegyező kísérleteket végezni nagy rendszeren
  - A fejlesztés stagnál -> drága eszközök
  - A hálózatok régóta változatlanok
- Zárt rendszerek
  - Nehéz kollaborálni mivel nincsenek nyílt platformok a vendorok között
  - A fejlesztés csak az egyes eszközgyártóknál vagy azok csoportjánál valósul meg
  - Hatalmas az akadály az új ötletek előtt

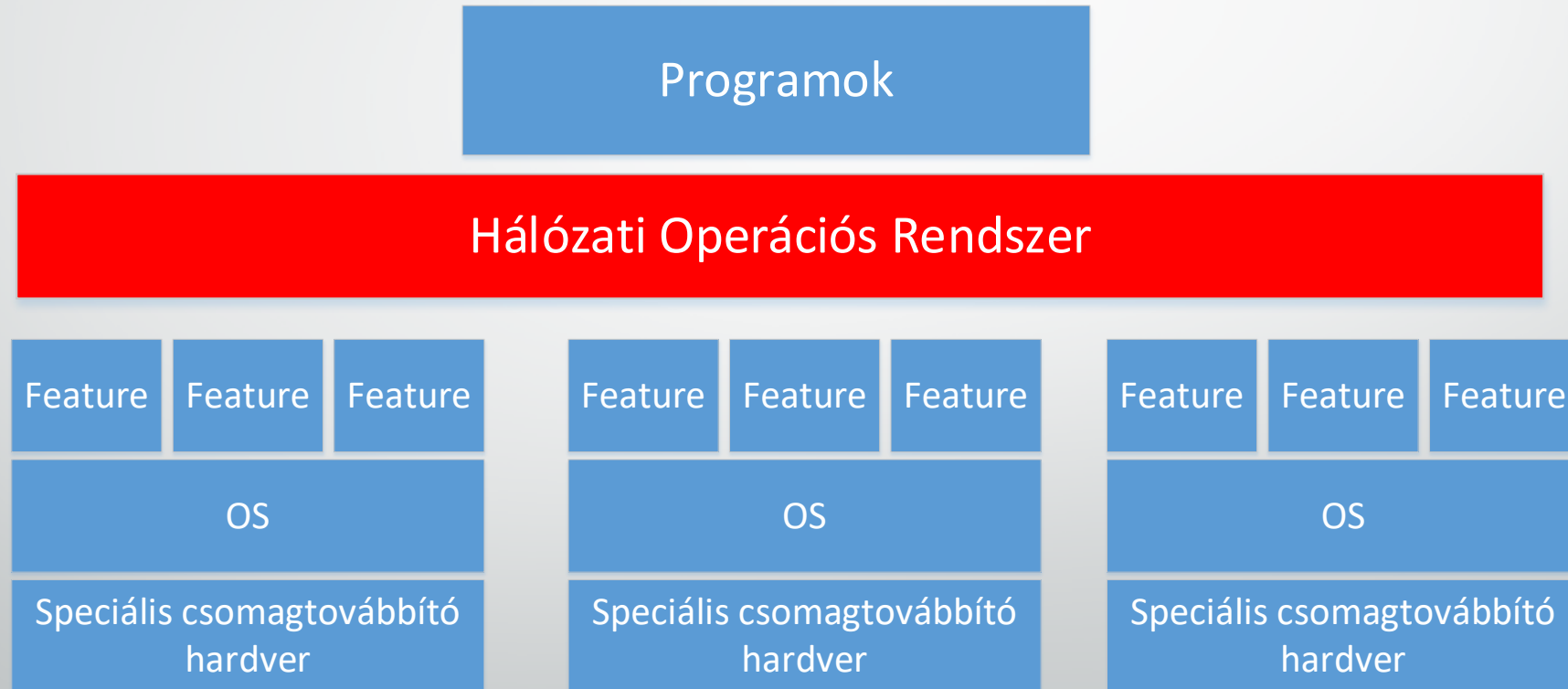
# Software Defined Network



- Egy csomó komplex funkció pl.: OSPF, BGP, MPLS, TE, NAT.....

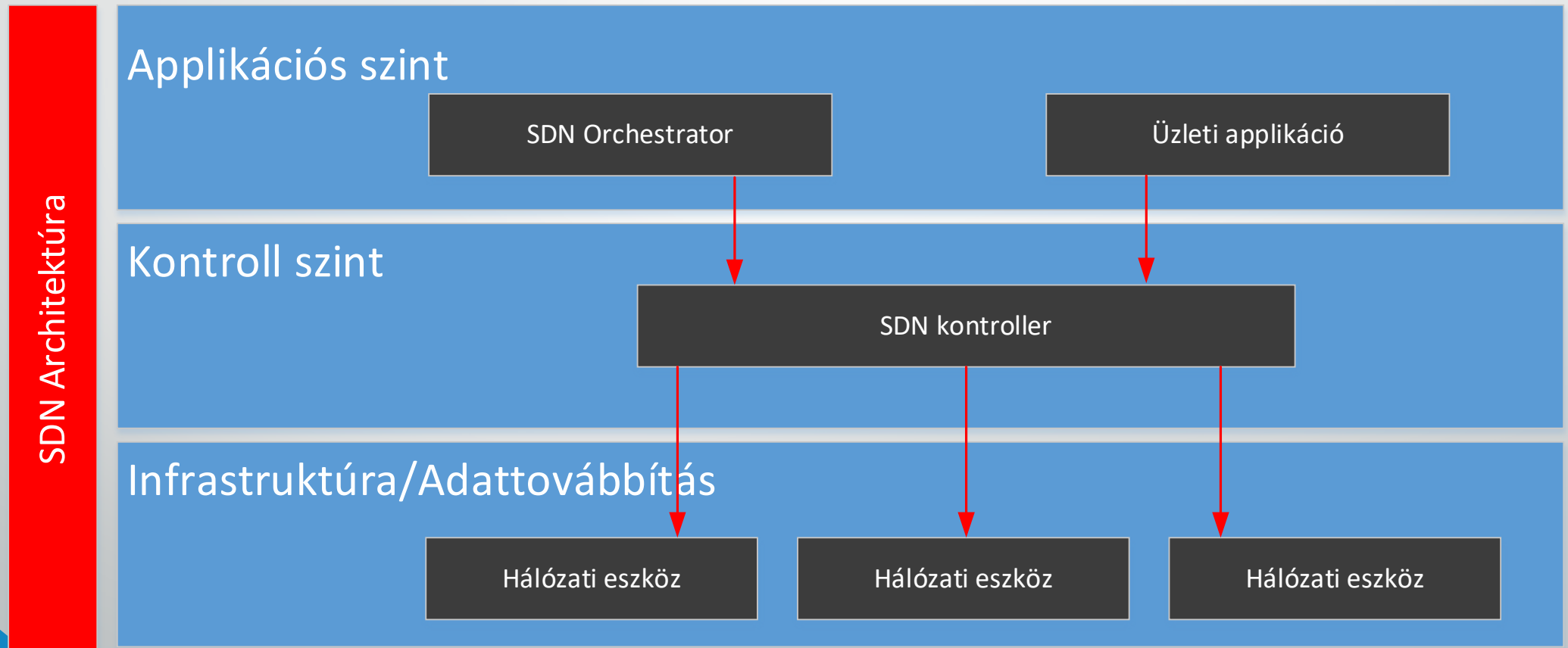
Nem lehet csak úgy változtatni!!!

- Az alapötlet:



- Data Plane:
  - A csomagok feldolgozása a lehető legnagyobb sebességgel, a csomagok állapota és végpontjai alapján pl.: IP, TCP, Ethernet stb.
- Control Plane
  - Eldönti hogyan és merre továbbítsuk a csomagot, routing, TE, tűzfal stb.
- Válasszuk külön ezt a kettőt, a control plane az agy, mely dönt, a data plane az izom mely végrehajtja.
- Ez egy olyan architektúra melyben nem egy/több hálózati eszközt menedzselünk hanem egy egész hálózatot

- Az SDN architektúrában, a adattovábbítás és a döntési szint különálló valamint az applikációktól teljesen elkülönítve működik



- **Infrastruktúra:**
  - Ez a réteg tartalmazza a fizikai és virtuális hálózati eszközöket, minden eszköz ebben a rétegben Openflow képes eszköz
- **Kontroll szint:**
  - Ebben a szintben található a központosított döntési szint mely megállapítja az egyes csomagok továbbítási paramétereit, ez a szint OpenFlow protokollal kommunikál az alsóbb réteggel
- **Applikációs szint**
  - Itt találhatóak meg a különböző szolgáltatások, valamint az orchestrator, mely egy globális betekintést nyújt a hálózatba

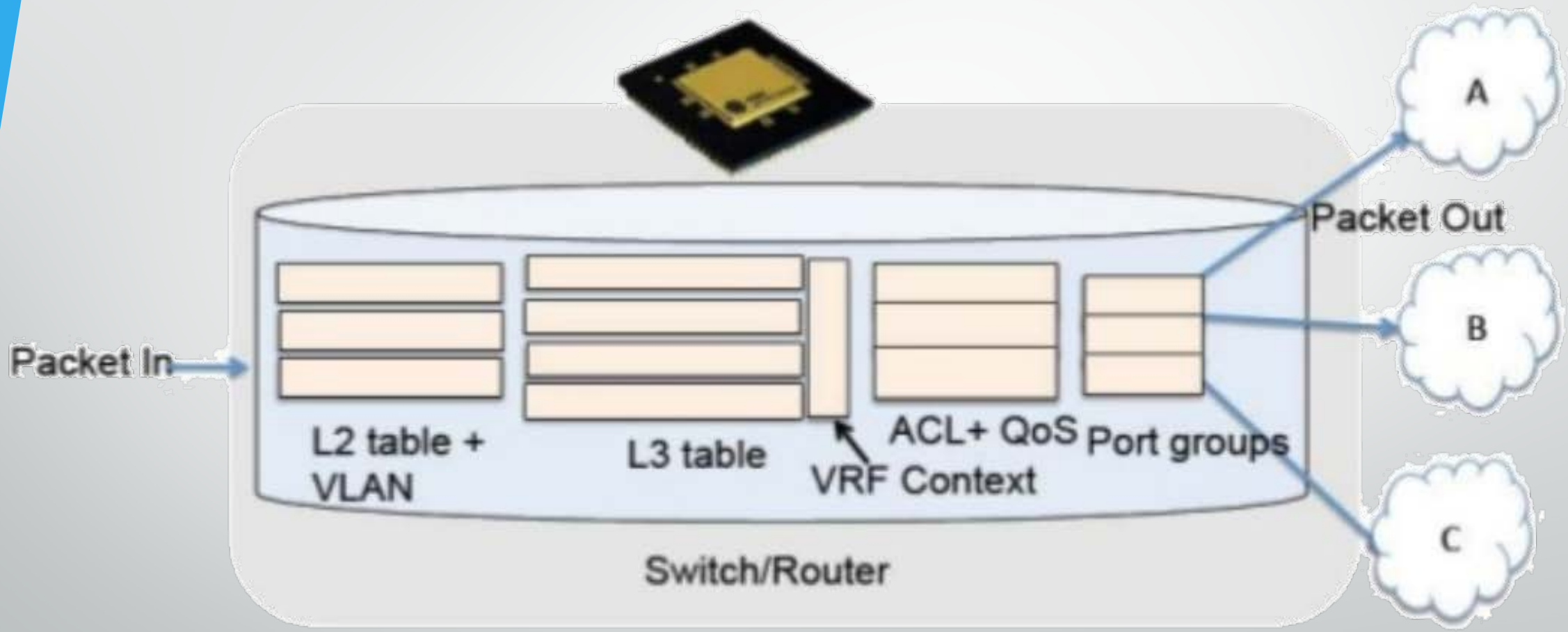


- OpenFlow protokoll

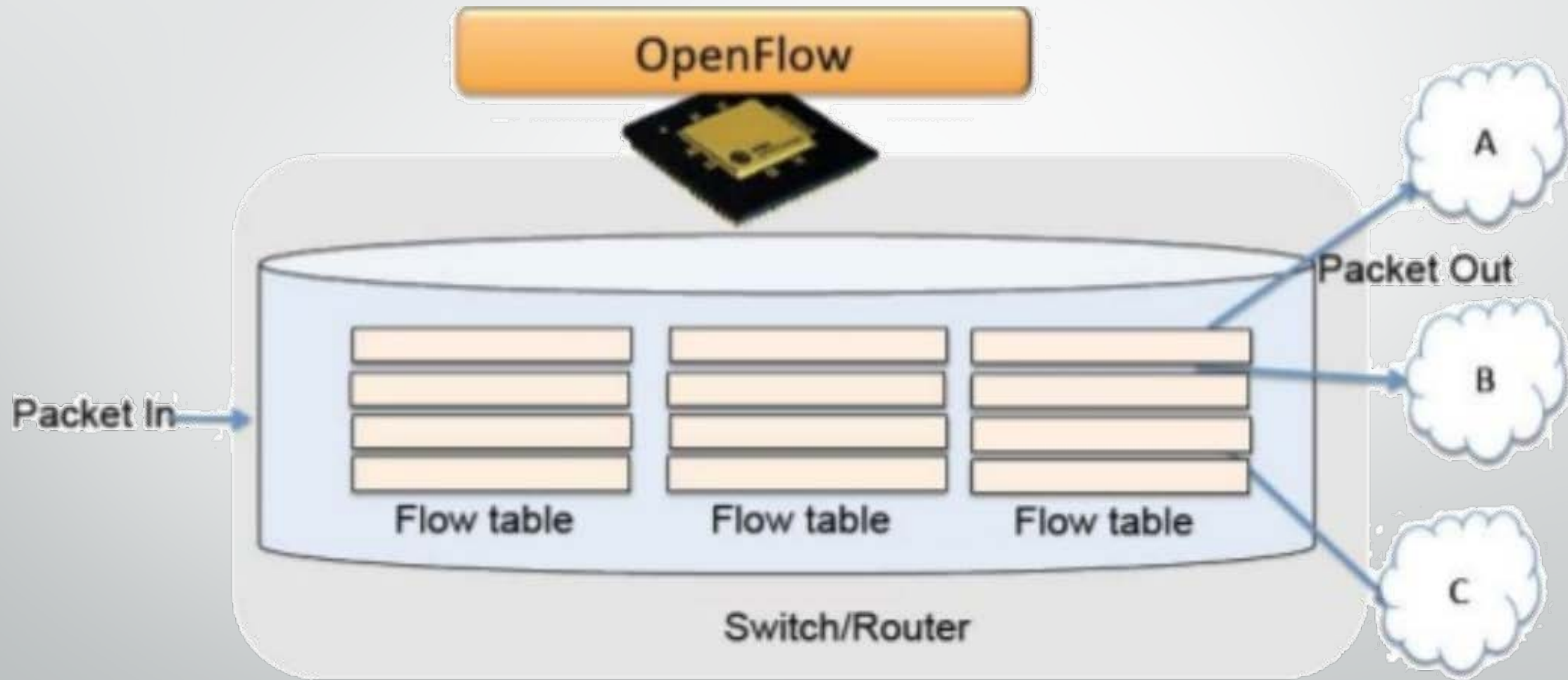
- Az Openflow egy API (Application Programming Interface) mely megteremti a standardizált felületet a SDN eszközökön
- Ez a protokoll képes beszélgetni az összes SDN eszközzel a hálózaton, figyeli/monitorozza az összes portot és tárolja az összes lehetséges útvonalat két végpont között
- Képes utasítani az eszközöket, hogy irányítsák a hálózati forgalmat un. Flow Table alapján, ez lehetőséget ad arra, hogy gyorsan reagáljunk az esetleges hibákra valamint akár user szinten irányíthassuk a forgalmat.



# Software Defined Network



# Software Defined Network



## OpenFlow

**OpenFlow Controller**

OpenFlow Protocol (SSL/TCP)



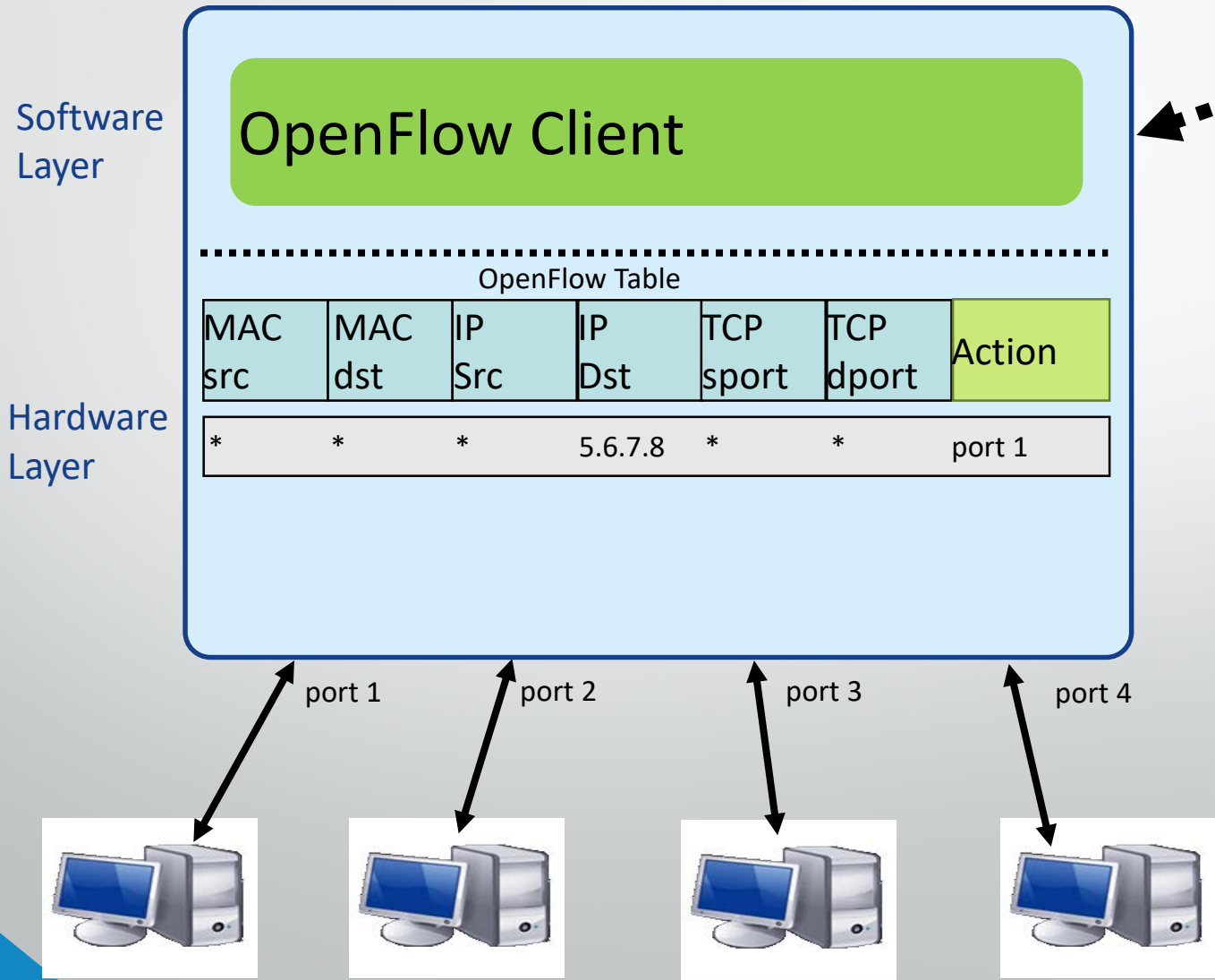
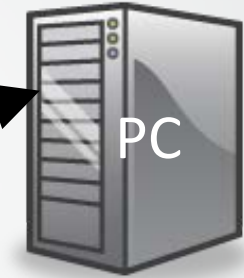
**Control Path**

**OpenFlow**

**Data Path (Hardware)**

## OpenFlow Switching

Controller



Példák flow entry-kre:

Switching

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:...	*	*	*	*	*	*	*	port6

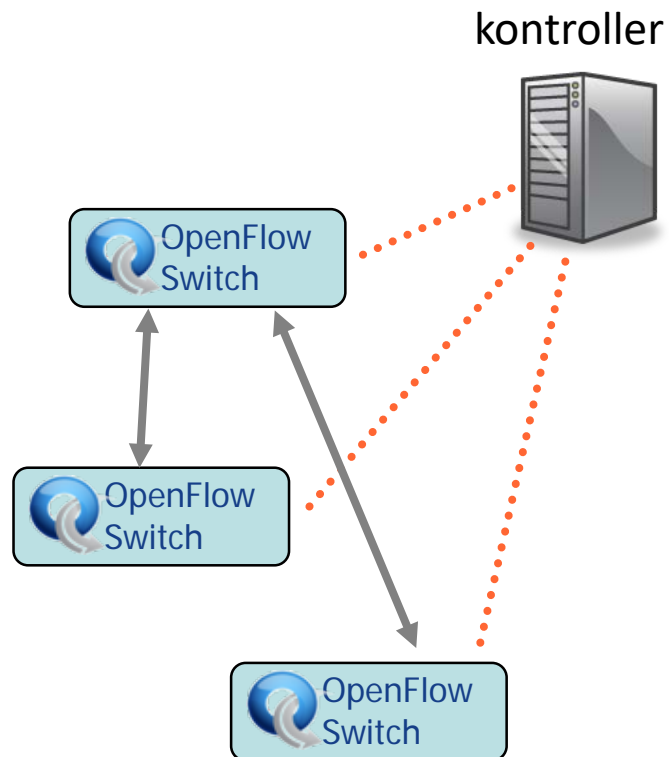
Routing

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	5.6.7.8	*	*	*	port6

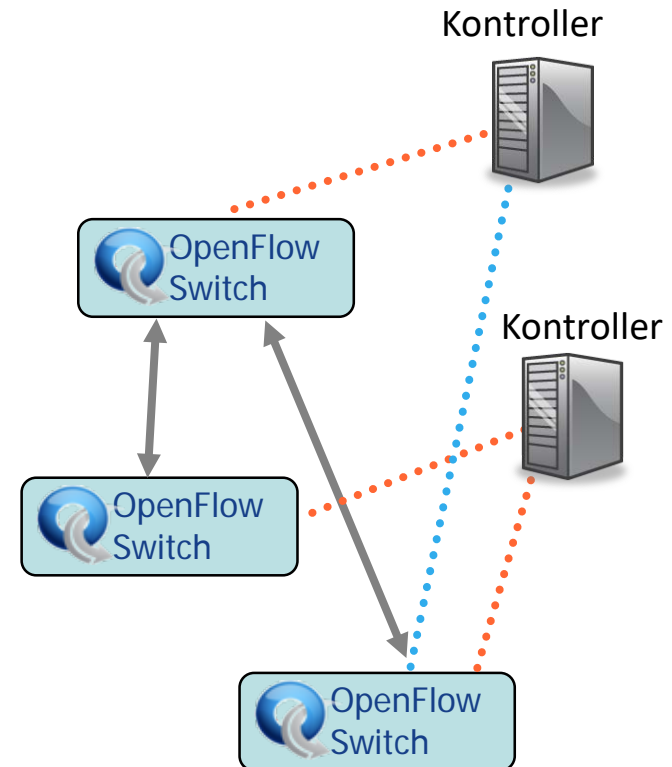
Firewall

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	*	*	*	*	*	*	*	22	drop

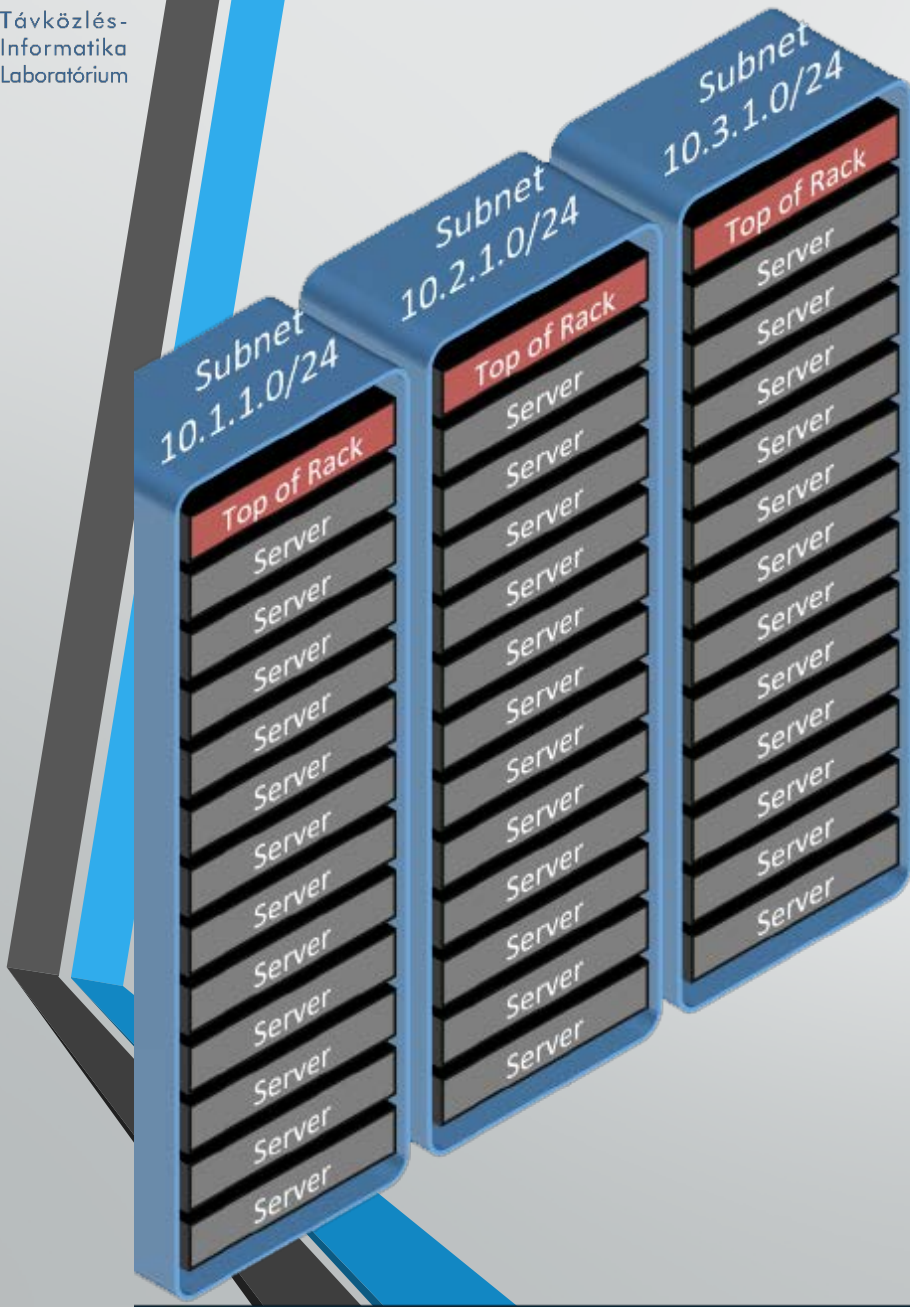
## Központosított kontrolller



## Elosztott Kontrolller



- Killer App: Virtualizált hálózatok
  - Képzelnünk el egy multi-tenant adatközpontot
  - Az előfizetők a saját hálózatukat maguk alakíthatják ki független az alapját adó rendszertől
  - Az adatközpont üzemeltetője nem is tud arról milyen rendszert üzemeltet, csak az adatfolyamok méretét látja



- Tipikus Adatközpont felépítés
- A szerverek egy rackben helyezkednek el
- Ezek Layer2-n vannak összekötve
- Beköltözik ide egy vállalat



# Software Defined Network



# Software Defined Network



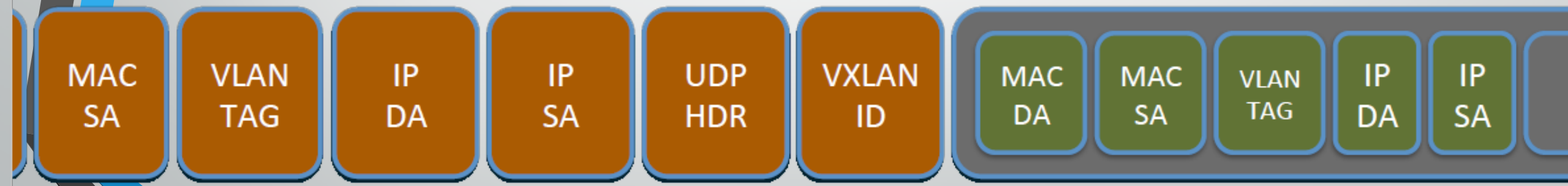
- Túlnő egy szekrényen
- Hogy éri el layer2-n a másik rendszert, feltéve, hogy több száz ilyen rack van több ezer előfizetővel?

- Megoldás: VXLAN
  - Hasonló koncepció mint a VLAN de:



$2^{12} = 4096$  VLAN

# Software Defined Network



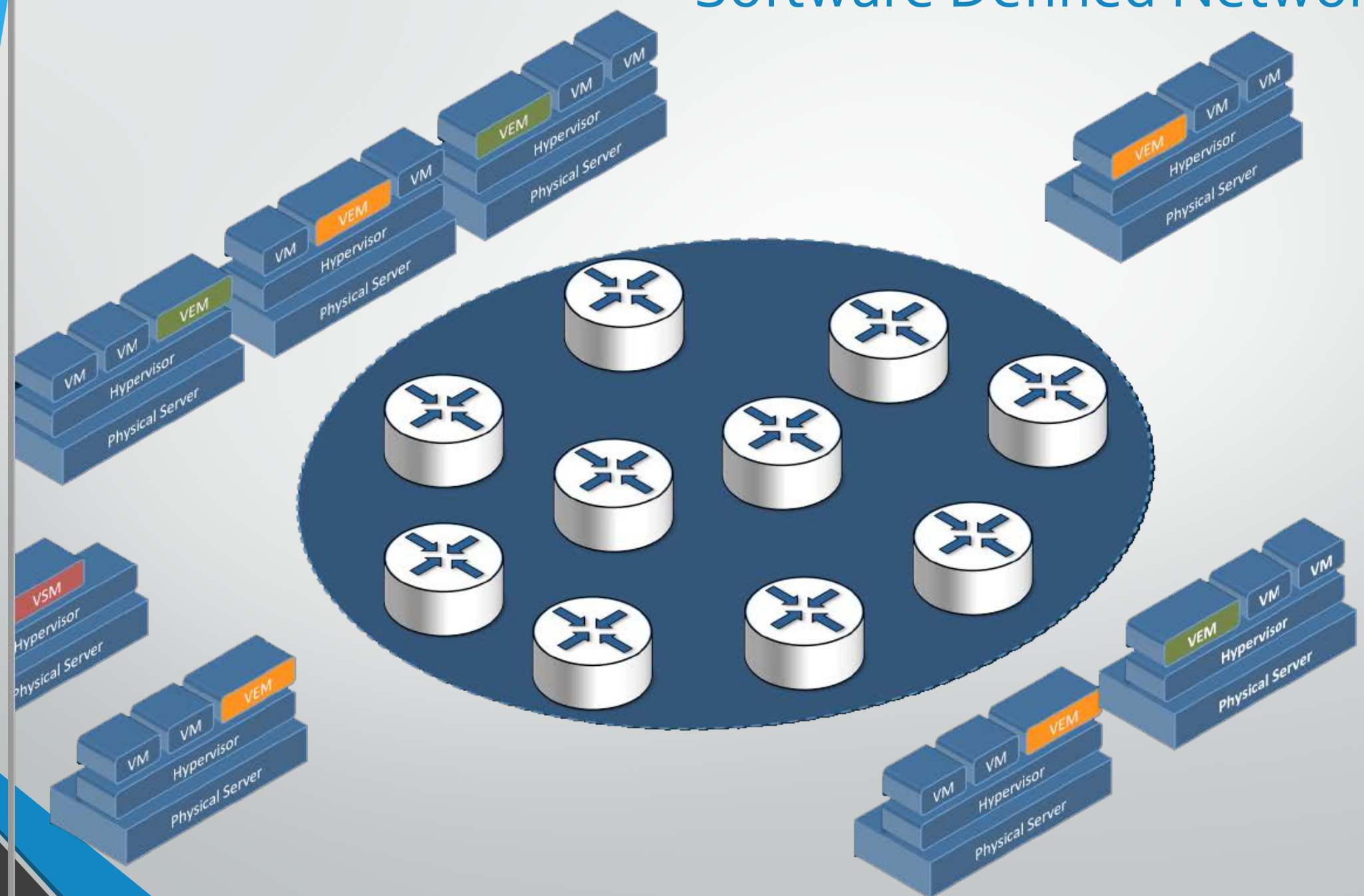
**Új Layer 2 Header**

**Új IP Header**

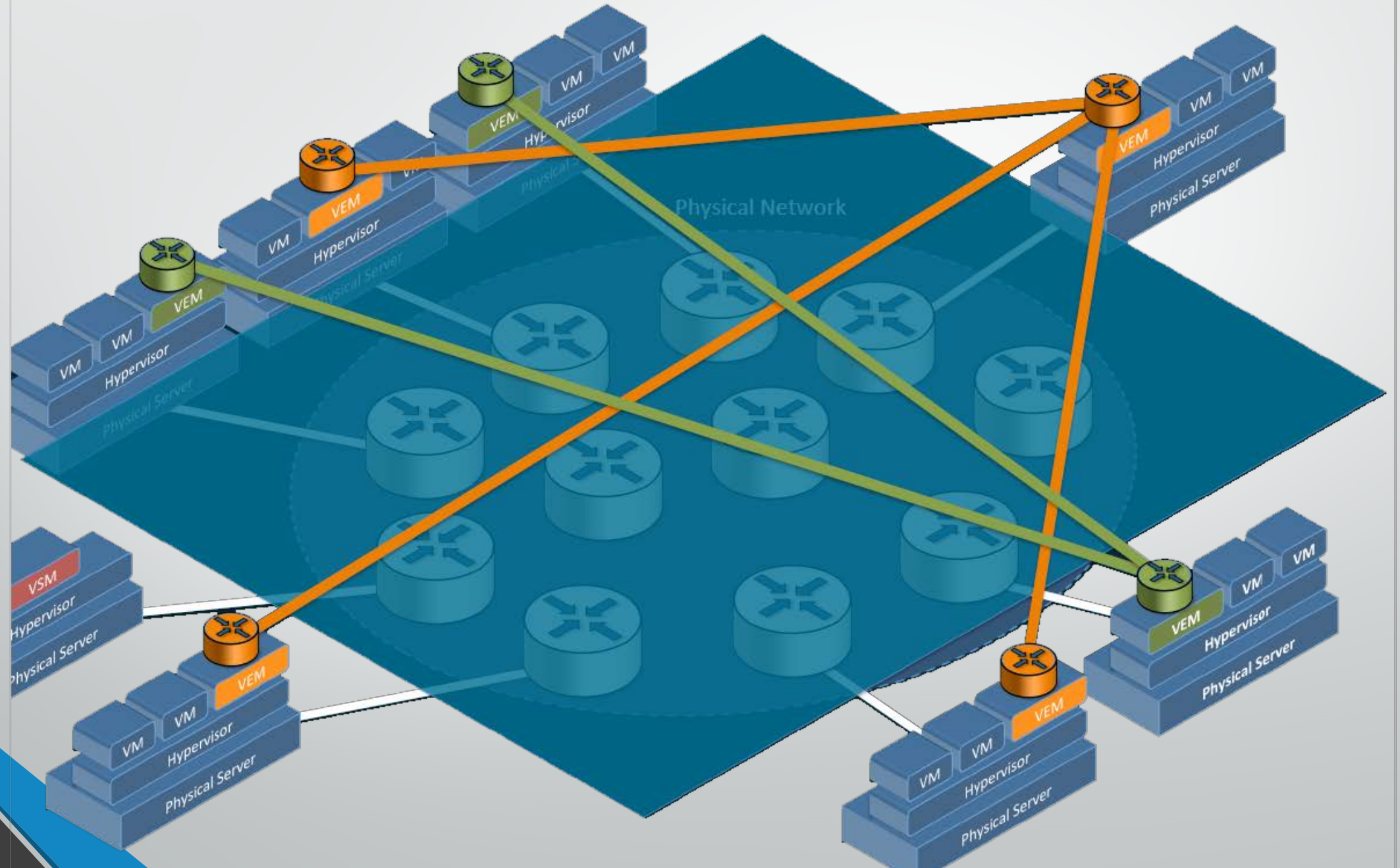
**VXLAN Header**

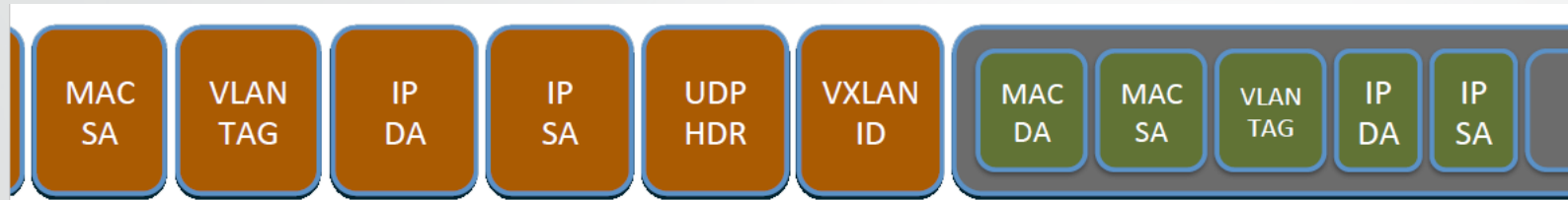
**UDP csomag**

# Software Defined Network



# Software Defined Network





- A VXLAN Headerben az ID 24 bites
- $2^{24} = 16,777,216$  VLAN
- Ezeket berakják egy UDP csomagba (4789-es port)
- Ezek gyakorlatilag tunnelek két végpont között melyek végpontjai lehetnek virtuális vagy fizikai switchportok

## Google's OpenFlow WAN

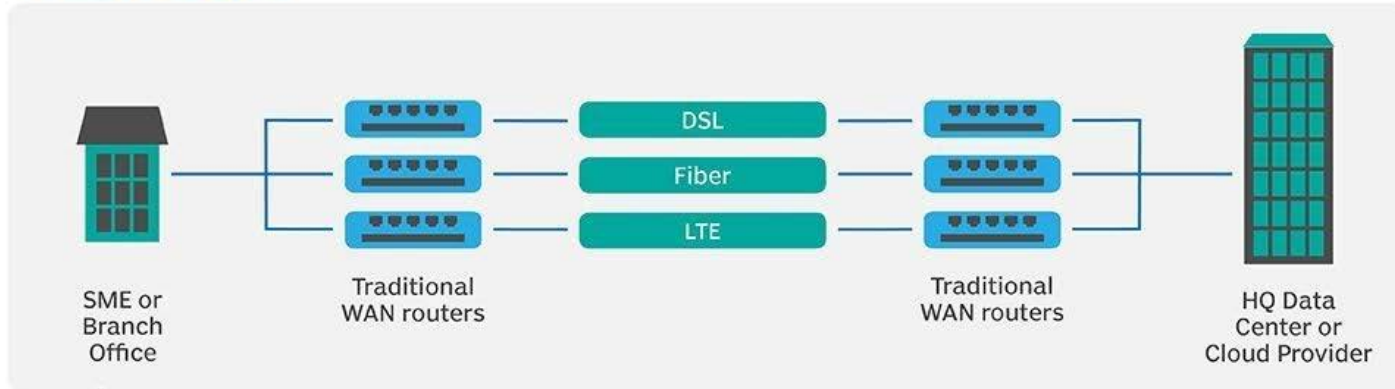




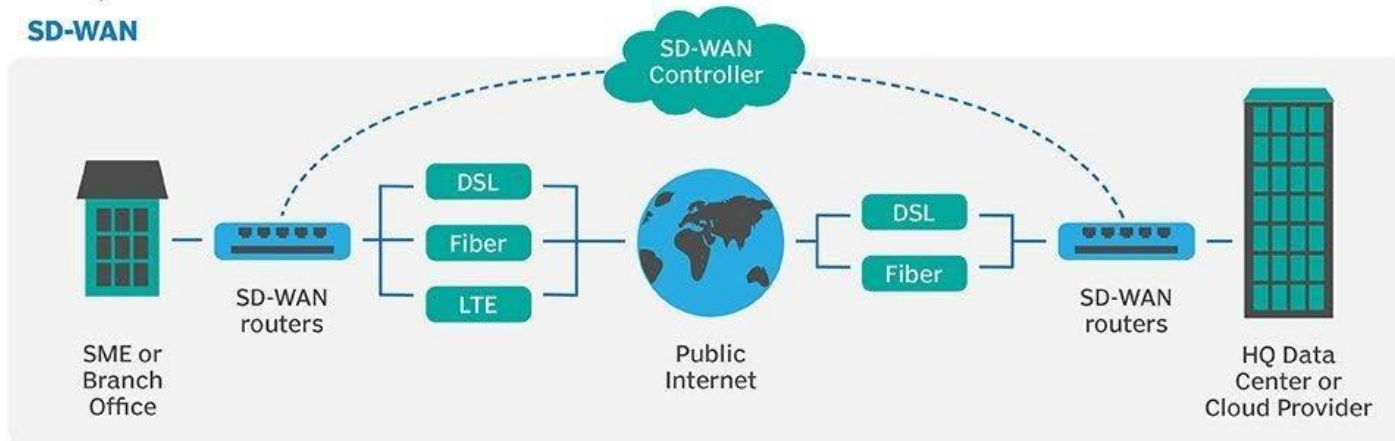
- Az SDN terminológia WAN-ra helyezve
  - Az SD-WAN lehetőséget ad a cégeknek, hogy üzletileg kritikus applikációk üzemeljenek nagy megbízhatósággal a low-cost normál internet előfizetésekkel.
- Garner szerint 2019 végéig a nagyvállalatok mintegy 30%-a bevezeti valamilyen szinten az SD-WAN-t.

## TRADITIONAL WAN VERSUS SD-WAN

### TRADITIONAL WAN



### SD-WAN



- Igények
  - Több csatlakozási pont pl.: MPLS, LTE, DSL
  - Dinamikus útvonal választás, load-balance, rugalmasság
  - Egységes, könnyen kezelhető interfész (UI)
  - VPN és egyéb third-party szolgáltatás támogatása, WAN optimizer, tűzfal

- Szolgáltatások
- **Rugalmasság** – egy rugalmas SD-WAN csökkenti a kiesés lehetőségét, valós idejű kiesés detektálás
- **QoS** – alkalmazás szintű prioritások, akár útvonalválasztás szinten is.
- **Security** – Általában ez kimerül abban, hogy IPSec-et használ
- **Alkalmazás optimalizálás** – ezt az egyes alkalmazások/szolgáltatások cache-elésével oldják meg

- Szolgáltatások II.
- **Telepítési lehetőségek** – A legtöbb ilyen termék virtualis vagy fizikai dobozban akár előre konfiguráltan kapható opcionálisan „a felhőben”
- **Adminisztráció** – egyszerűsített menedzsment az egyik legfontosabb kitétel az SD-WAN-nál.
- **Online-TE** – globális rálátással a kontrollernek könnyebb optimális útvonalat találni az éppen aktuális forgalmi trendeknek megfelelően.