



Felhő alapú hálózatok (VITMMA02) Hálózati megoldások a felhőben

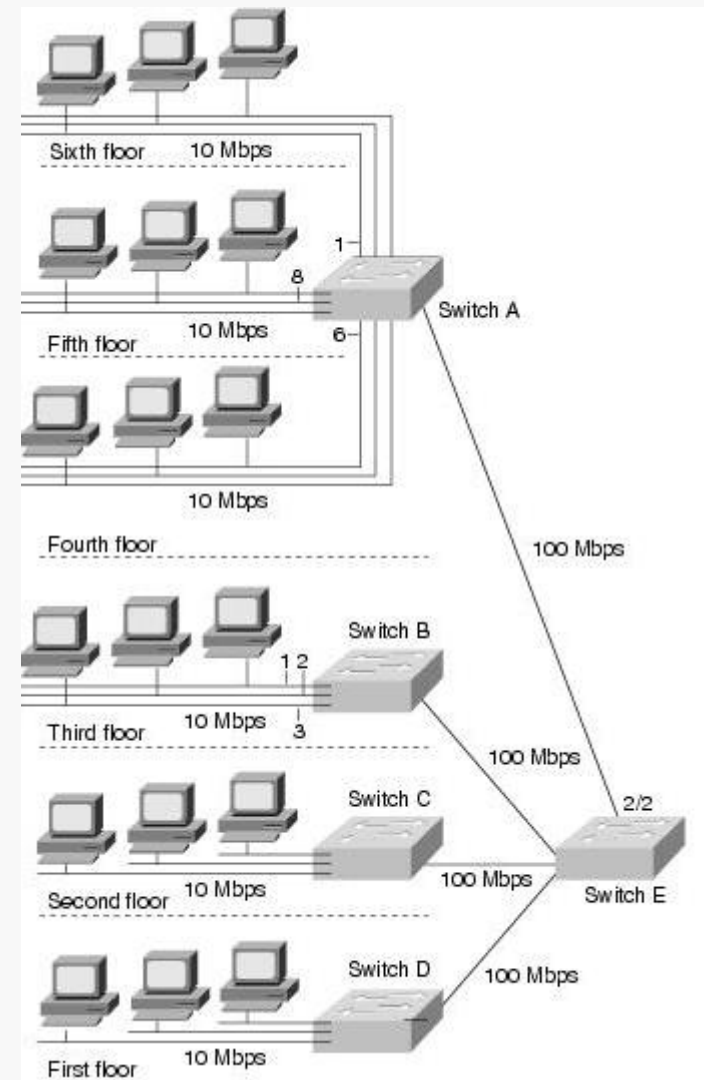
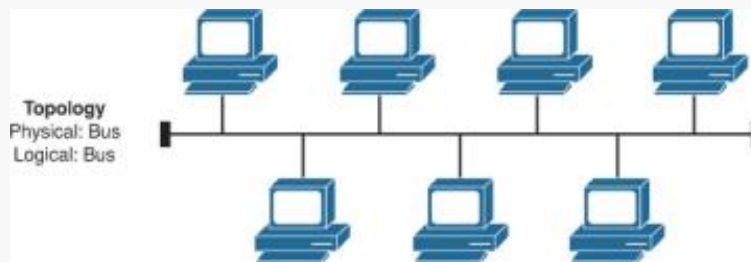
Dr. Maliosz Markosz

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Távközlési és Médiainformatikai Tanszék

2020. tavasz

Ethernet

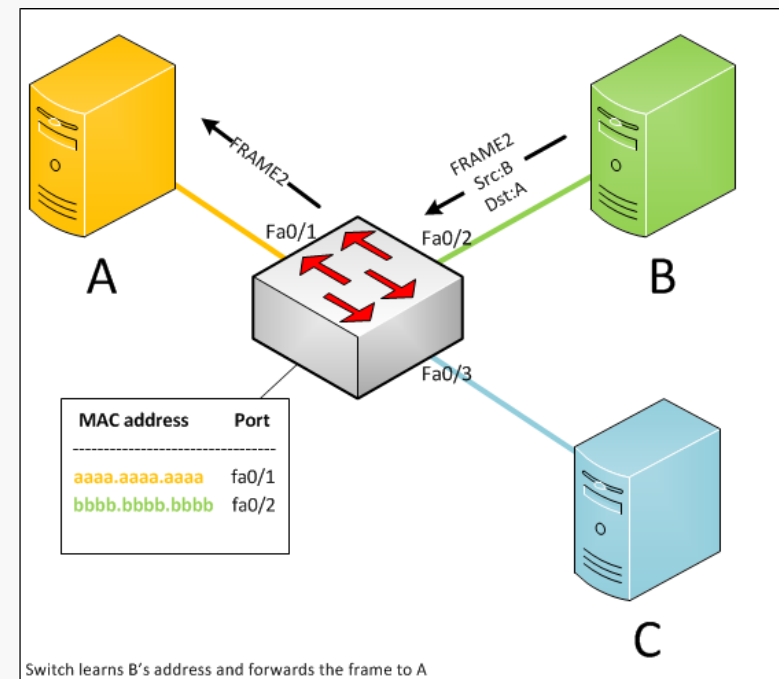
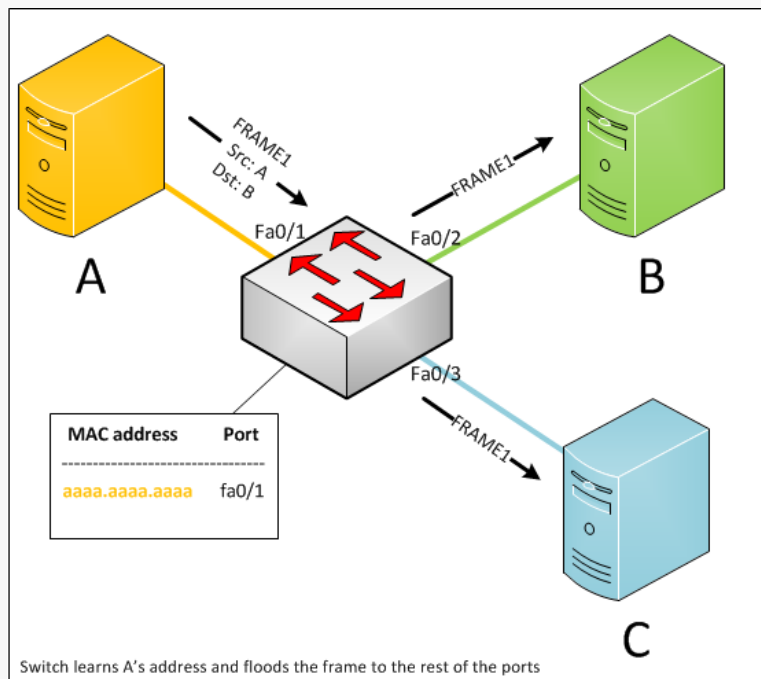
- » L2 hálózat
- » Ethernet bridging vagy switching: kapcsolt Ethernet
 - » osztott közeget emulál



Háttéranyag: <http://www6.ietf.org/edu/documents/82-RoutingBridgingSwitching-Perlman.pdf> 18-44 oldal

Ethernet

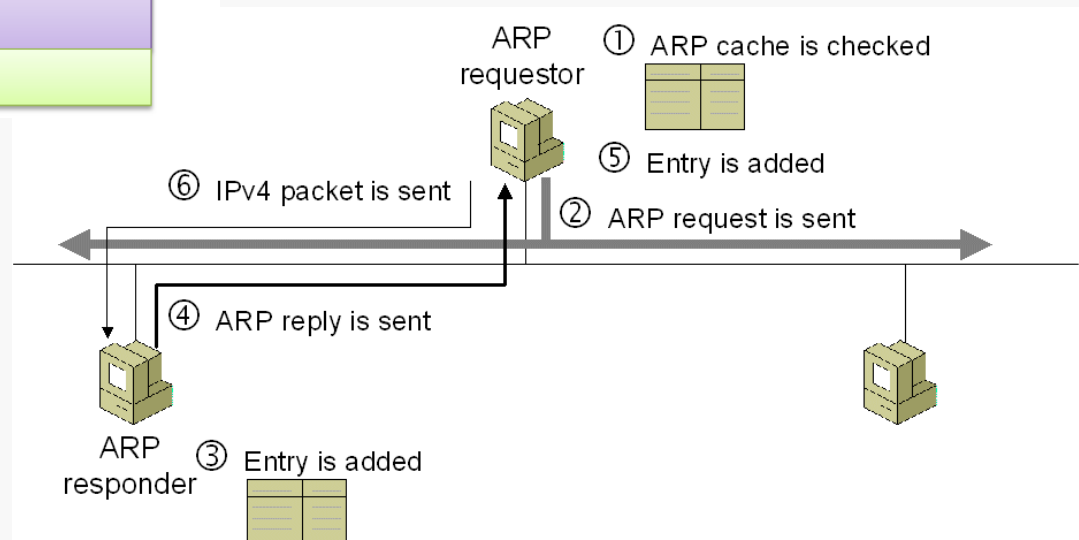
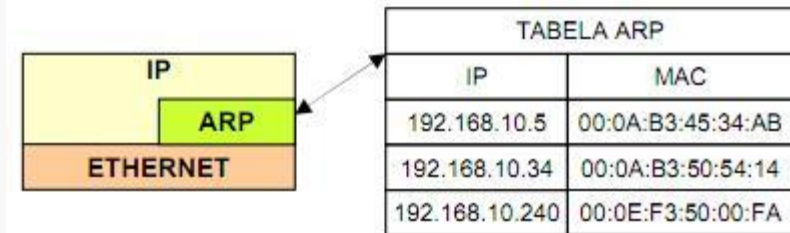
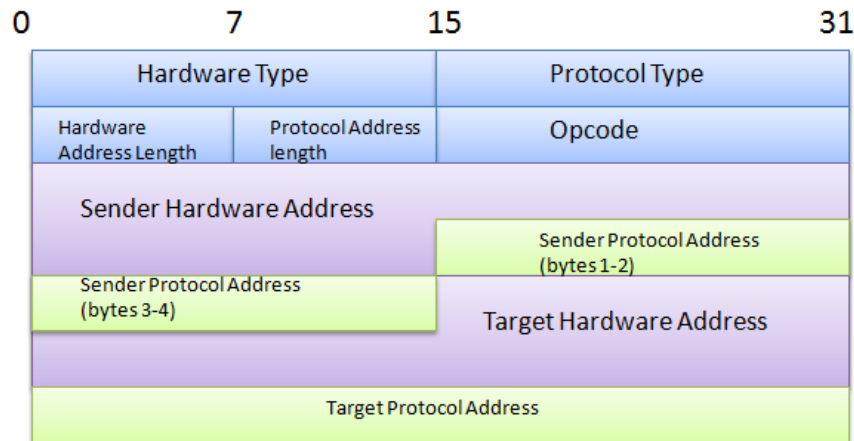
- » Spanning Tree Protocol (STP)
- » MAC cím tanulás
- » transparent bridging
- » elárasztás (flooding): broadcast, ismeretlen unicast és multicast csomagokra
- » hibalehetőségek: implementációs hiba, hibás konfiguráció
- » ha kialakul továbbítási hurok, a kapcsolók 100% CPU terhelését okozzák



IP cím MAC leképezés

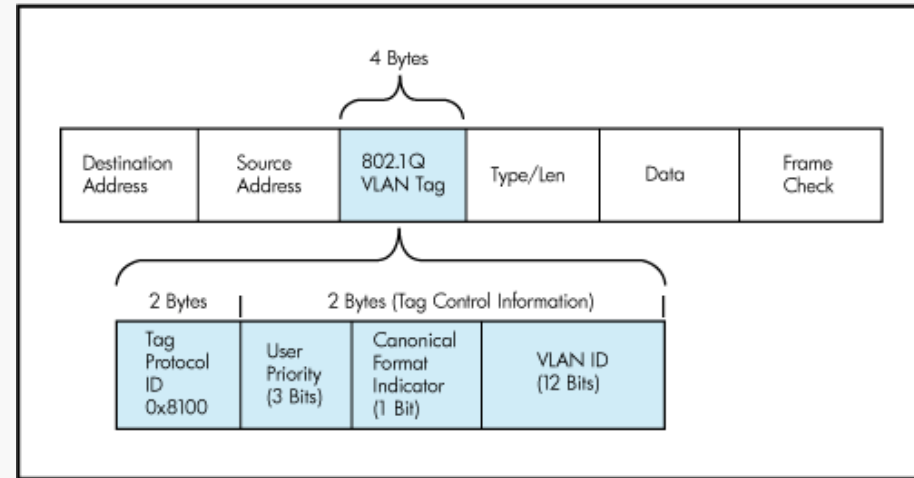
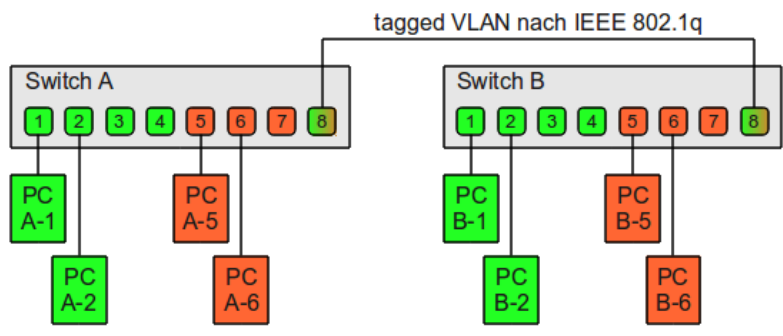
» Address Resolution Protocol (ARP)

ARP header



Izoláció: VLAN

- » Izolált virtuális hálózati szegmensek: VLAN-ok (IEEE 802.1Q)
 - » L3 nélkül
 - » skálázhatósági szempontból is jobb



- » Továbbítás VLAN ID és cél MAC alapján
- » Ethernet hálózati kártya
 - » MAC cím szűrés
 - » egy vagy néhány unicast és multicast címre képes szűrni, csak a neki címzetteket dolgozza fel
 - » VM-ek egy fizikai gépen
 - » számos VM (és hozzá tartozó MAC cím) egy fizikai gépen belül
 - » a hypervisor a fizikai hálózati kártyát általában „promiscuous mode”-ban (válogatás nélküli üzemmód) használja
 - » minden csomagot CPU segítségével dolgoz fel

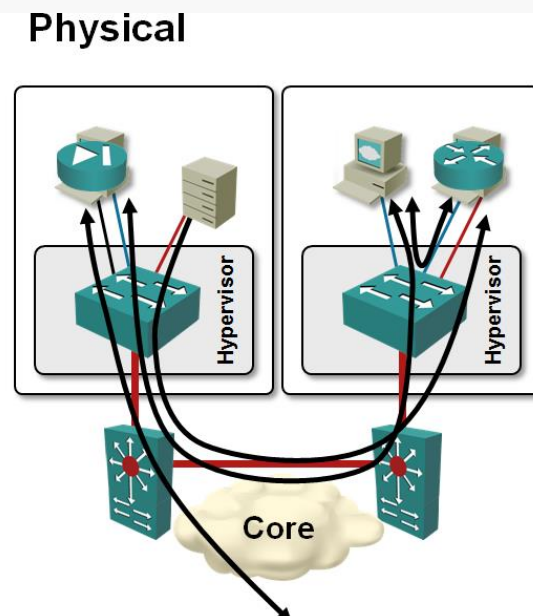
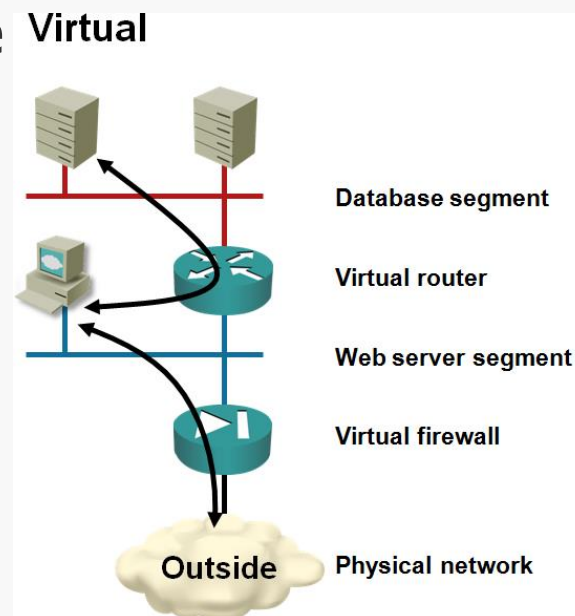


VLAN skálázhatósága

- » 4094 lehet egy Ethernet hálózatban
 - » 12 bites VID (0x000 és 0xFFF foglalt)
- » hypervisor hálózati kártya válogatás nélküli üzemmódban
 - » elárasztással küldött csomagok CPU általi feldolgozása
- » Jellemző megvalósítás
 - » összes VLAN az összes szerver hálózati kártyán
 - » hypervisor minden elárasztással küldött csomagot feldolgoz, még akkor is, ha nincs is aktív VM abban a VLAN-ban
 - » olyan mintha egy VLAN-unk lenne

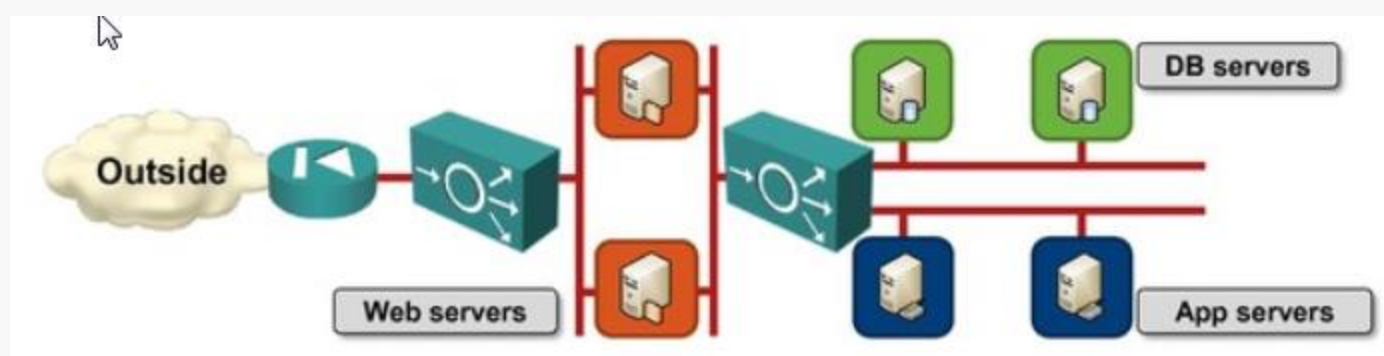
Virtuális hálózati architektúrák

- » Egy fizikai hálózat – sok virtuális hálózat
- » Sok ügyfél az adatközpontban
 - » minden ügyfélnek több VM
 - » mintha privát hálózaton lennének
 - » igazodás a változó igényekhez
- » Tunneling, encapsulation
 - » egy vagy több címke



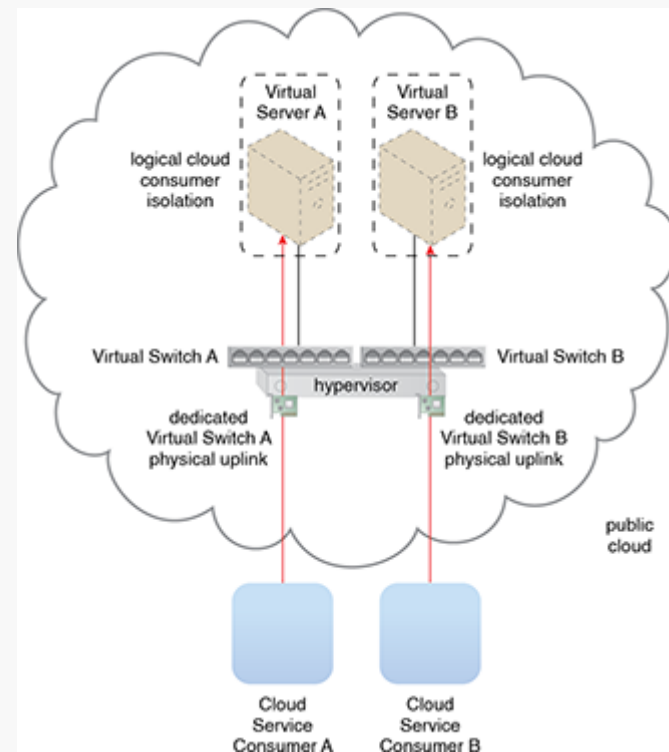
Web alkalmazás architektúra

- » Egy komplex alkalmazás hálózati funkciókat is igényel
 - » L2/L3 csomagtovábbítás több címtartományban
 - » tűzfal
 - » terheléselosztás
 - » NAT
 - » VPN hozzáférés



Web alkalmazások a felhőben

- » Több felhő kliens mellett minden alkalmazás szeparálva a többitől
 - » a meglévő hálózati kapcsolatok fenntartásával
 - » belső címzés
 - » hálózati szolgáltatások
 - » biztonsági modell
 - » virtuális szegmensek
 - » QoS





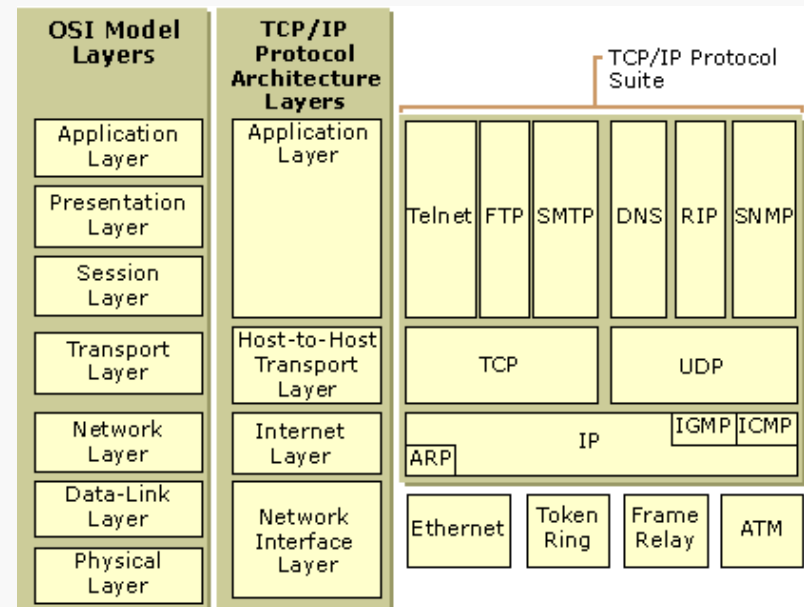
Virtuális hálózati architektúrák

- » A lényeges kérdés: skálázható?
- » A cél: skálázható infrastruktúra több ezer virtuális hálózat számára
- » Skálázhatóság
 - » áteresztőképesség növelése a terhelés növekedésével arányosan
 - » scaling up: vertikális skálázás
 - » nagyobb erőforrás (gyorsabb vagy több processzor, nagyobb vagy gyorsabb memória és merevlemez)
 - » felhő esetén az adott virtuális gép erőforrásait növeljük
 - » scaling out: horizontális skálázás
 - » újabb szerverek hozzáadása



Hálózat a felhőben

- » Internet
 - » világméretű, nagyon sok végpont, egész jól működik ☺
- » Adatközpont
 - » hasonló kihívások
 - » akár több milliós nagyságrendű VM (pl. AWS)
 - » exponenciális növekedés
 - » gyakran a sávszélesség a szűk keresztmetszet
- » Opciók
 - » Layer2
 - » kapcsolás – switching
 - » egyszerűbb, könnyen használható
 - » VM migrálásnál IP cím maradhat
 - » skálázhatóság?
 - » kis és közepes méretig
 - » jellemzően vállalati adatközpontokban
 - » Layer3 (Amazon, Facebook, stb.)
 - » útvonalválasztás – routing
 - » jól skálázódik
 - » tetszőleges méretű hálózat
 - » mégsem “kis Internet”



Hálózat a felhőben

» Opciók

» Layer2: Ethernet

- » független a MAC cím és az elhelyezkedés

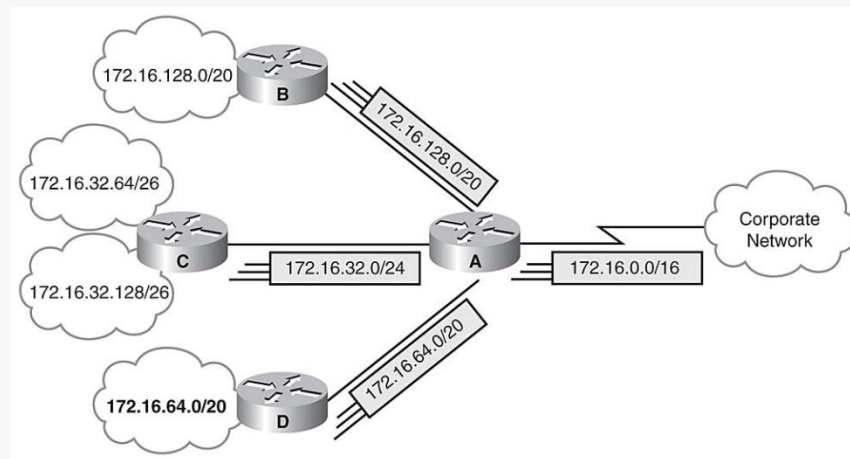
- » flat addressing

- » skálázhatósági korlát: összes MAC cím ismerete a kapcsolókban

» Layer3

- » hierarchikus címtér

- » aggregált útvonalválasztási információ





Hálózat a felhőben

- » Layer2: Ethernet
 - » könnyű konfigurálni, telepíteni: plug and play
 - » kb. 1000 szerverig
 - » kommunikáció a lokális szegmensen belül
 - » szegmensen kívüli forgalom: default gateway-nek
 - » az ügyfél a kapott IP cím tartományban szabad kezet kap
 - » új VM-ek indítása
 - » IP címek megváltoztatása
- » Spanning Tree Protocol
 - » nincs többutas lehetőség



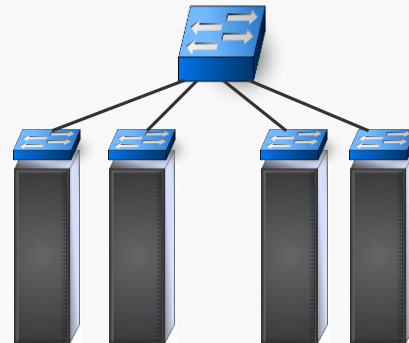
Hálózat a felhőben

» Layer3

- » minden hálózati eszköz útválasztó
 - » protokoll: Open Shortest Path First (OSPF) vagy Intermediate System to Intermediate System (IS-IS)
 - » topológia információ terjesztés
- » egy VM – egy L2 "hálózat"
 - » nincs L2 broadcast, multicast nehézkes
 - » nincs VLAN
 - » pl. Windows szerverek broadcast segítségével fedezik fel egymást
- » Equal Cost MultiPath (ECMP)
 - » jobb sávszélesség kihasználás
- » legrövidebb út
 - » Dijkstra algoritmus
- » VM mozgás bonyolultabb
 - » IP cím változás

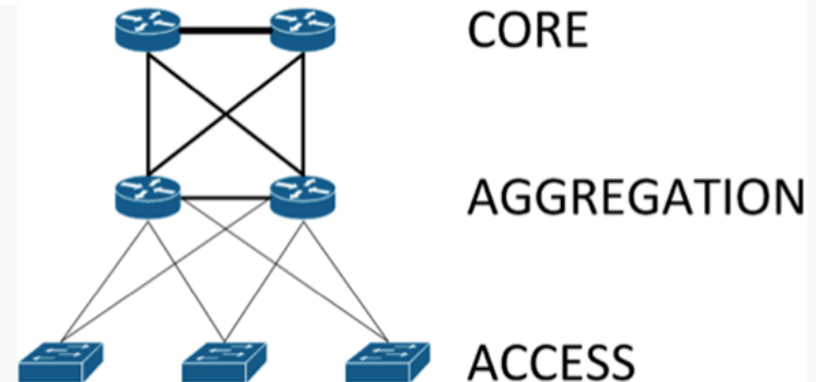
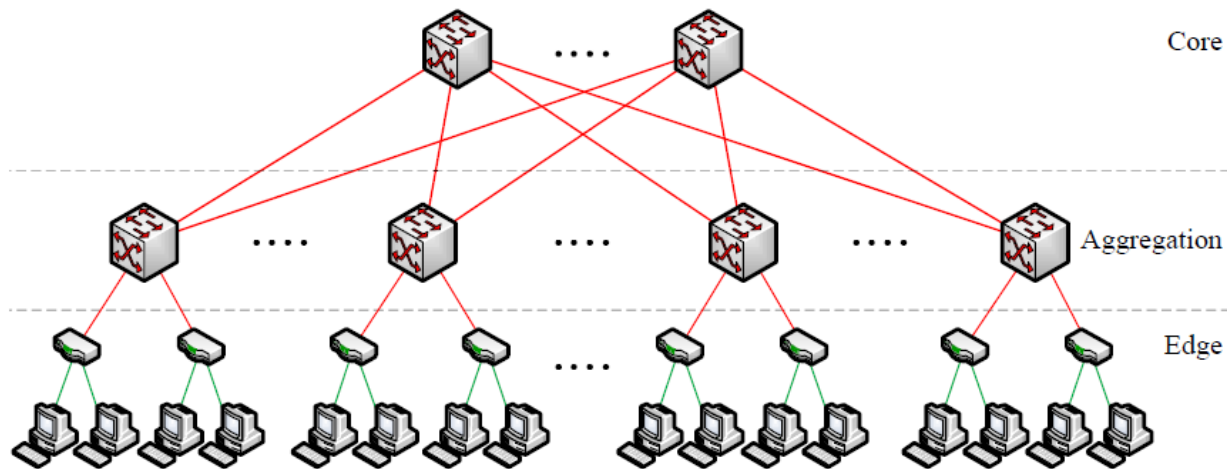
Hálózati topológiák

- » 3 szintű hierarchia: ToR, aggregáló, központi kapcsoló
- » lapos(abb) topológia, 2 szint: ToR és központi kapcsoló
 - » egy nagy kp.-i kapcsoló: költséges, limitált portszám
 - » pl. egy 128 portos GbE kapcsoló ára kb. 100-szorosa egy 48 portosénak



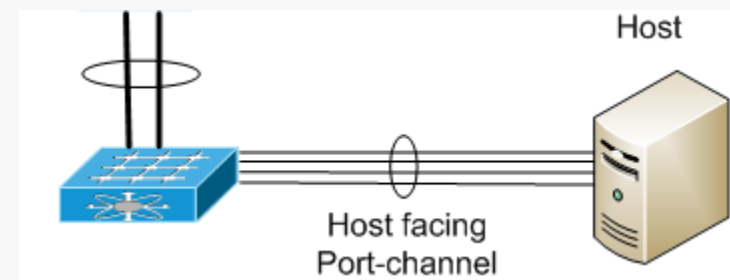
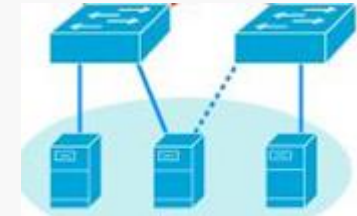
Hálózati topológiák

- » Redundancia és/vagy terheléselosztás
 - » kettős csillag



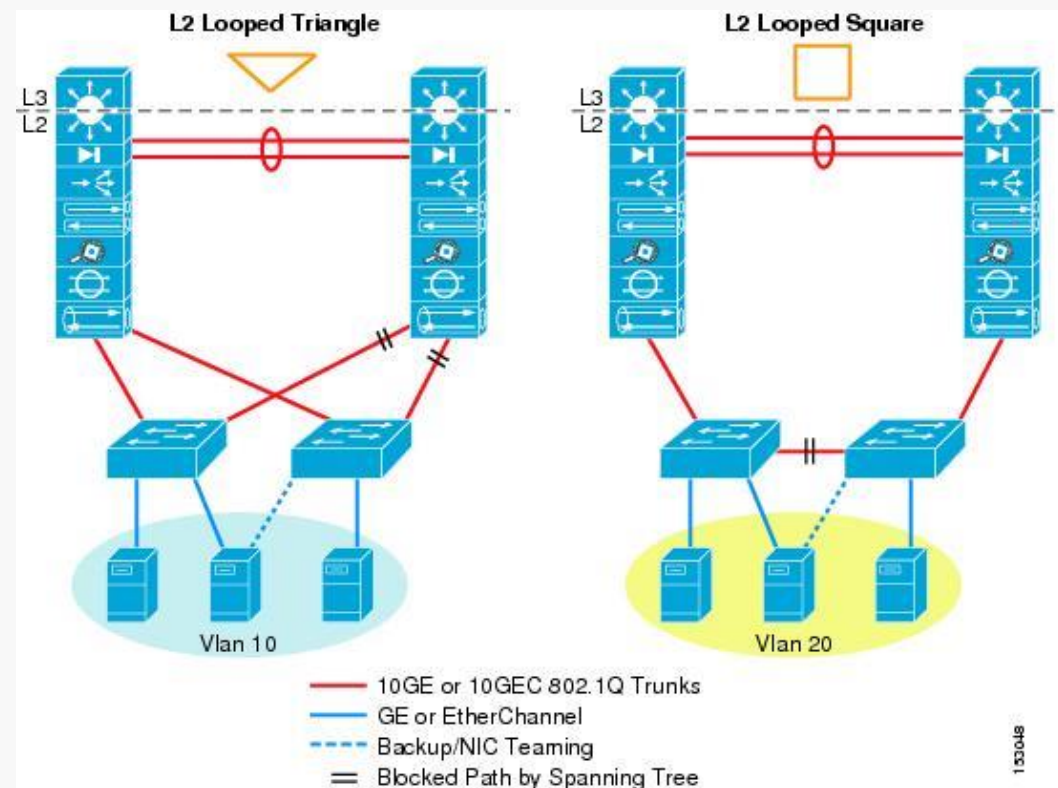
Szerver – ToR kapcsoló

- » Egyszeres kapcsolódás (single homed)
 - » 1 szerver – 1 kapcsoló
 - » rendelkezésre állás biztosítása külső mechanizmusokkal
 - » Single Point of Failure
 - » NIC, vezeték, kapcsoló port, kapcsoló
- » Többszörös kapcsolódás (multi homed)
 - » 1 szerver – 2 kapcsoló
 - » üzemi/tartalék
 - » egyidejű használat
 - » külön MAC, IP címek
- » Port-channel
 - » a kapcsolót konfigurálni kell
 - » logikailag egy kapcsolatot, fizikailag linkek aggregáltja
 - » 1 szerver – 1 kapcsoló
 - » 1 szerver – több kapcsoló
 - » virtuális port-channel
 - » külön fizikai kapcsolón végződnek
 - » megosztott vagy kommunikáló vezérlő síkok
 - » a kapcsolók is össze vannak kötve
 - » 2-nél több esetén gyűrűben



ToR – központi kapcsoló

- » Hurkolt topológia
 - » háromszög
 - » elterjedt megoldás
 - » az összeköttetések fele kihasználatlan
 - » több port a kp.-i kapcsolón
 - » négyzet
 - » kevésbé redundáns
 - » kevesebb port a kp.-i kapcsolón



ToR – központi kapcsoló

- » Hurokmentes topológia
 - » nincs szükség STP-re
 - » U
 - » ToR kapcsoló tranzitként viselkedik hiba esetén
 - » fordított U
 - » kevesebb ToR kapcsoló port
 - » nem megfelelő egyszerűs kapcsolódású szervereknek
 - » nincs hálózati szintű redundancia

