VPN

VPN Szolgáltatások

Moldován István

Budapest University of Technology and Economics

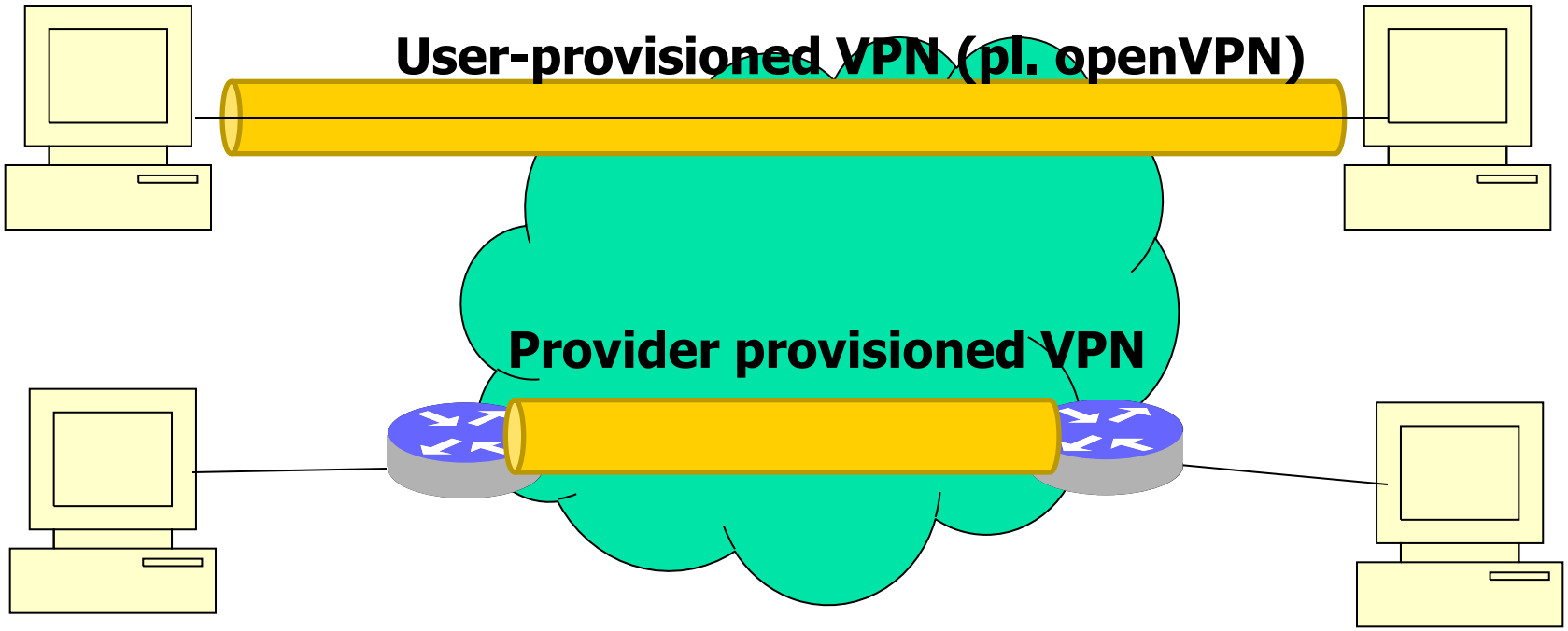
Department of
Telecommunications and Media Informatics

Virtuális Magánhálózatok

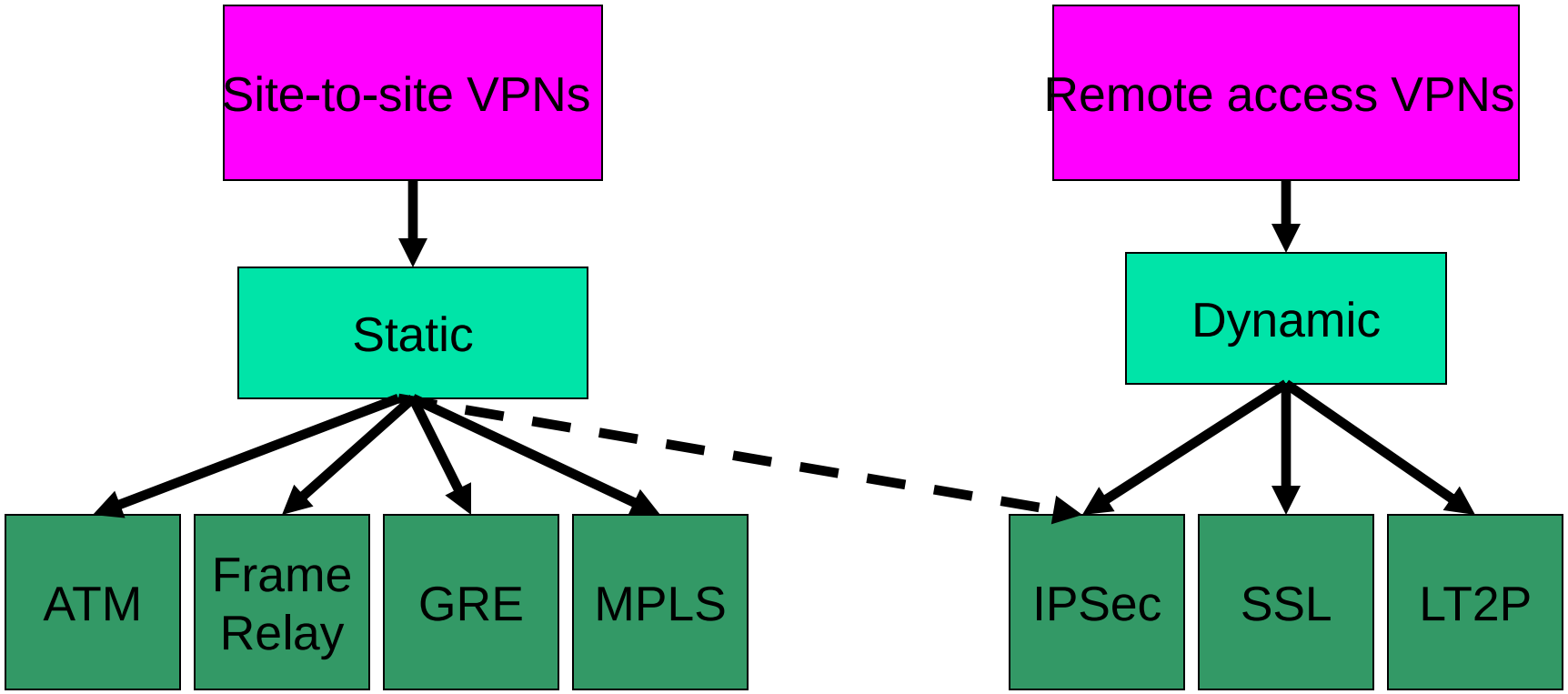
- Virtual Private Network (VPN)
- Két alapvető típus
  - User-space VPN
  - Provider Provisioned VPN (ppvpn)
- Mindkettő a hálózat erőforrásainak költséghatékony kihasználását célozza

L3-L2 VPNs

- L2 és L3 VPN példa



VPN típusok


Site-to-site VPNs
Remote access VPNs
Static
Dynamic
ATM
Frame Relay
GRE
MPLS
IPSec
SSL
LT2P

Provider-Provisioned VPN-ek

- A szolgáltató a saját infrastruktúráját osztja meg több virtuális hálózatot létrehozva
- A szolgáltatás biztonságos adatátvitelt biztosít a felhasználó számára
  - A titkosítást vagy forgalom elkülönítést a szolgáltató biztosítja
  - A szolgáltató garantálhatja a szolgáltatásban leírt minőséget is

PP-VPN típusok

- Layer 2 – TLS
  - Megvalósítható több szinten
    - L1: EoS
    - L2: VLAN, QiQ, MiM
    - L3: MPLS – VPWS, VPLS
- Layer 3 – IP VPN
  - Tunnelek segítségével
  - ATM, FR, IP-GRE, L2TP, MPLS…

PP-VPN szolgáltatások

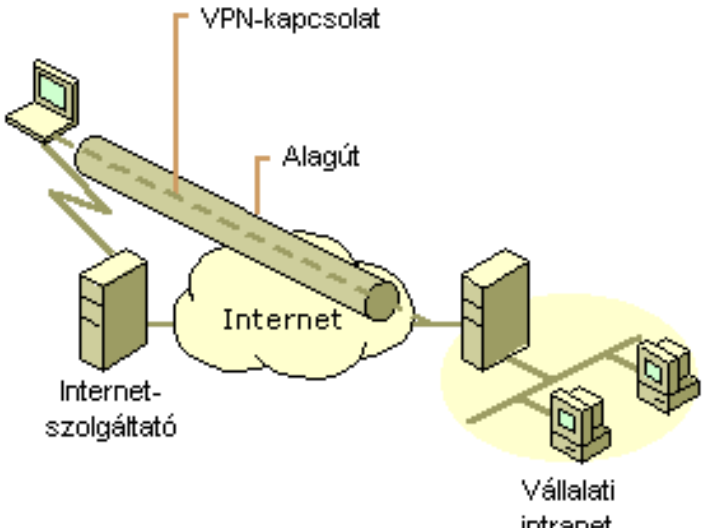
- L3 VPN – IPVPN, VPRN
  - IP szintű kapcsolatot biztosít a telephelyek között
  - A csomagok routing segítségével jutnak célba
- L2 VPN – VLL vagy PW
  - Pont-pont kapcsolat – bridging!
- L2 VPN – TLS, VPLS
  - Ethernet szintű kapcsolat a telephelyek közt
  - Bridging
    - A két telephely egyetlen LAN-t lát

Felhasználói VPN-ek

Felhasználói VPN

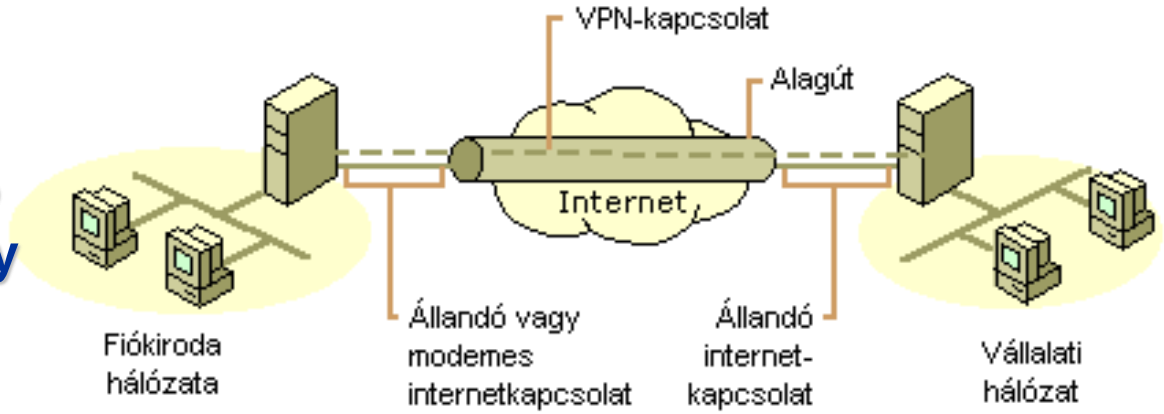
- Bérelt vonal – nem költséghatékony
- Internet – olcsó kommunikáció
  - Nem biztonságos!
- Megoldás: biztonságos kapcsolat kialakítása az Interneten kódolt alagutak használatával
  - Egy vagy több kliens használhat egy alagutat
  - A biztonságot a kódolás adja
  - Minőségbiztosítás az Internet szolgáltatótól függ…

VPN az ügyfél típusa szerint



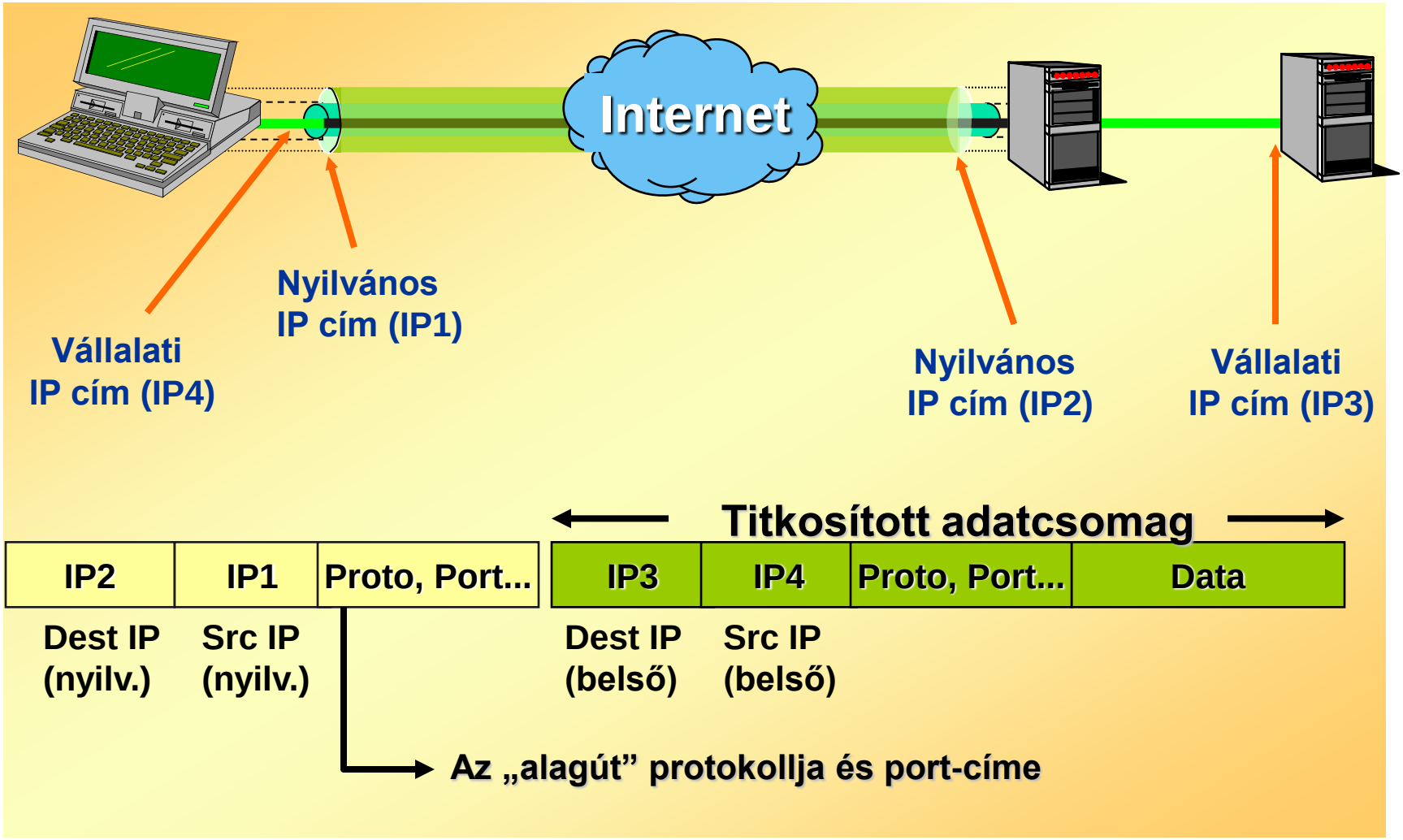
Ügyfél-kiszolgáló (Client-2-Router)

Kiszolgáló-kiszolgáló (Router-2-Router vagy LAN-2-LAN)



moldovan@tmit.bme.hu

Alagúthálózat



Alagútprotokollok: PPTP

- Point to Point Tunneling Protocol
- Azonosítás:
  - EAP (tanúsítvány), MS-CHAPv2, CHAP, PAP
- Titkosítás:
  - MPPE (Microsoft Point to Point Encryption) (= RC4)
- Kommunikáció:
  - PPTP Control Connection: TCP 1723 port
  - Adatforgalom (GRE): IP 47

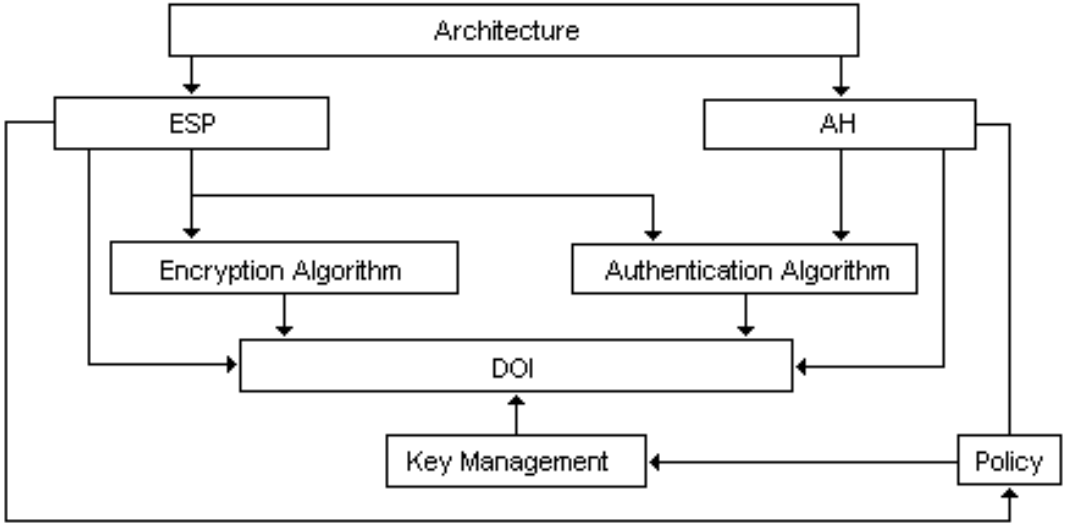
Alagútprotokollok: L2TP

- Layer 2 Tunneling Protocol (RFC 2661)
  - Cisco L2F alapokon nyugszik
  - UDP kommunikáció, 1701-es port
    - UDP – TCP forgalmat visz át, nem hatékony 2 szinten TCP
    - Az adat és a kontrollforgalomhoz egyaránt
    - Az IPSec titkosítás ezt a portot elrejti
- Azonosítás:
  - EAP, MS-CHAPv2, CHAP, PAP
- Titkosítás:
  - IPSec
- Kompatibilitás
  - Windows 2000-től beépítve
  - Windows 98/ME/NT4:

Alagútprotokollok: L2TP

- Az L2TP titkosítását az IPSec motor végzi
  - Automatikusan létrehozott IPSec Filter az UDP 1701-es portra
  - Tanúsítványalapú azonosítás
    - A sikeres csatlakozás feltétele hogy az ügyfél és a kiszolgáló rendelkezzen legalább egy, közös, mindkét fél által megbízott CA-tól származó, érvényes tanúsítvánnyal

IPSec



- RFC 2401, 2402, és 2406
- Vég-vég IP alapú adat titkosítás
- Nem NAT képes (IKE miatt, részleges megoldás van, checksum, ...)
- Részei:
  - Interenet Kulccsere (Internet Key Exchange)
    - UDP 500-as port
    - Paraméter egyeztetés
    - Kulccsere
  - Azonosító fejléc (Authentication Header AH)
    - Forrás azonosítás, integritás védelem
  - Biztonsági Tartalom Beágyazás (Encapsulating Security Payload ESP)
    - Azonosítás, integritás védelem, titkosítás

SSL VPN

- Felhasználói VPN
- Virtuális tunnel interfész használata
  - Routing vagy bridging
- SSL/TLS tehnológiát használ
  - Csak TCP felett
  - A biztonságért felelős az SSL protokoll
  - Kódolás, tanúsítvány kezelés
- Megvalósítások
  - Pl. OpenVPN

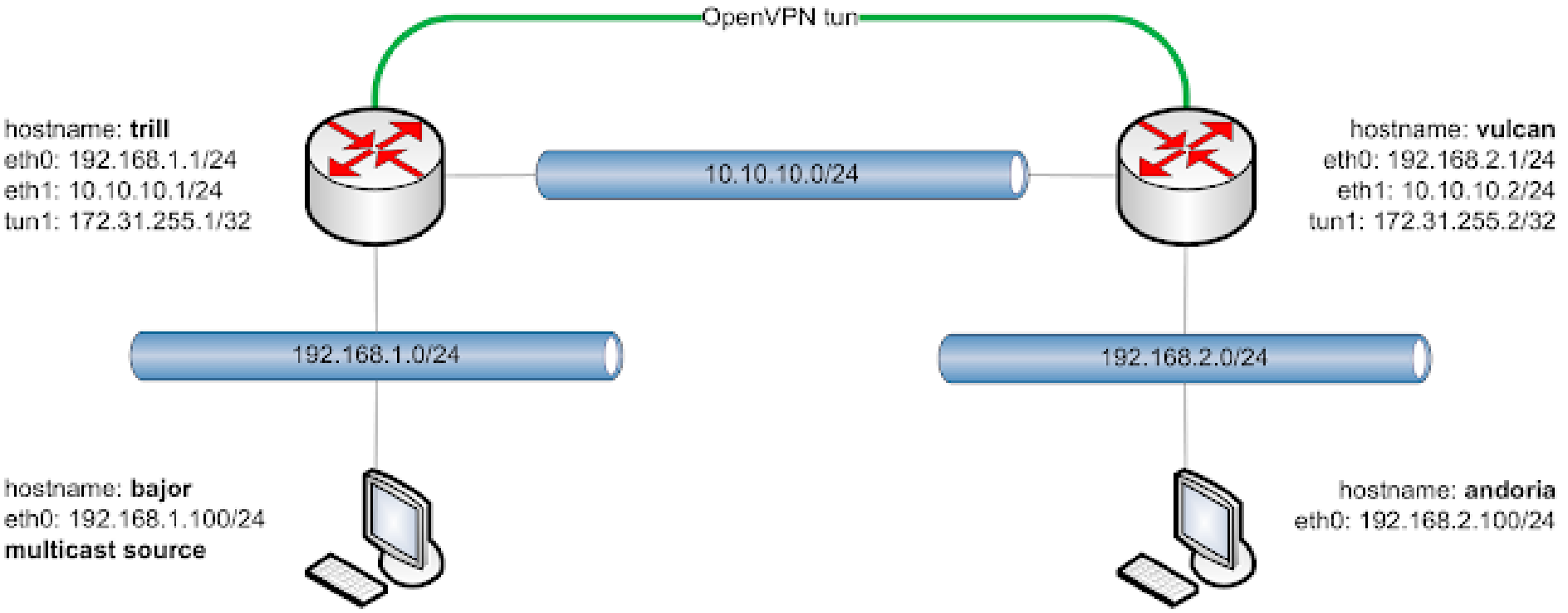
SSL VPN – működés

- A modern user-space VPN virtuális tun és tap interfészt ad a VPN végpontokon
- A forgalom a virtuális interfészre routolásával történik -> “tun0”
  - Ugyanúgy kezelhető mint egy valós interfész a célhálózat felé
  - Brctl – bridging megvalósítás
  - Tűzfalazható, stb.

User VPN – előnyök, hátrányok

- Mikor SSL és mikor IPSec VPN?
- Az SSL VPN egyszerűbb
  - Felhasználó által menedzselhető
  - Egyszerűen konfigurálható
  - TCP – nem támogat QoS-t, UDP-t
- Az IPSec VPN komplexebb
  - Adminisztrátor állíthatja be (root jog)
  - IP szintű – QoS támogatás lehetséges
  - Transzparens a felhasználó felé

Példa: OpenVPN



Szolgáltatói VPN-ek
Provider Provisioned VPN (PP-VPN)

PP-VPN - megvalósítás

- Különböző szintű alagutazási technológiával oldható meg
  - Akár az 1, 2 és 3. rétegben
- Legelterjedtebbek:
  - L2TP, GRE, MPLS : PPVPN
  - IPSec, SSL/TLS: user

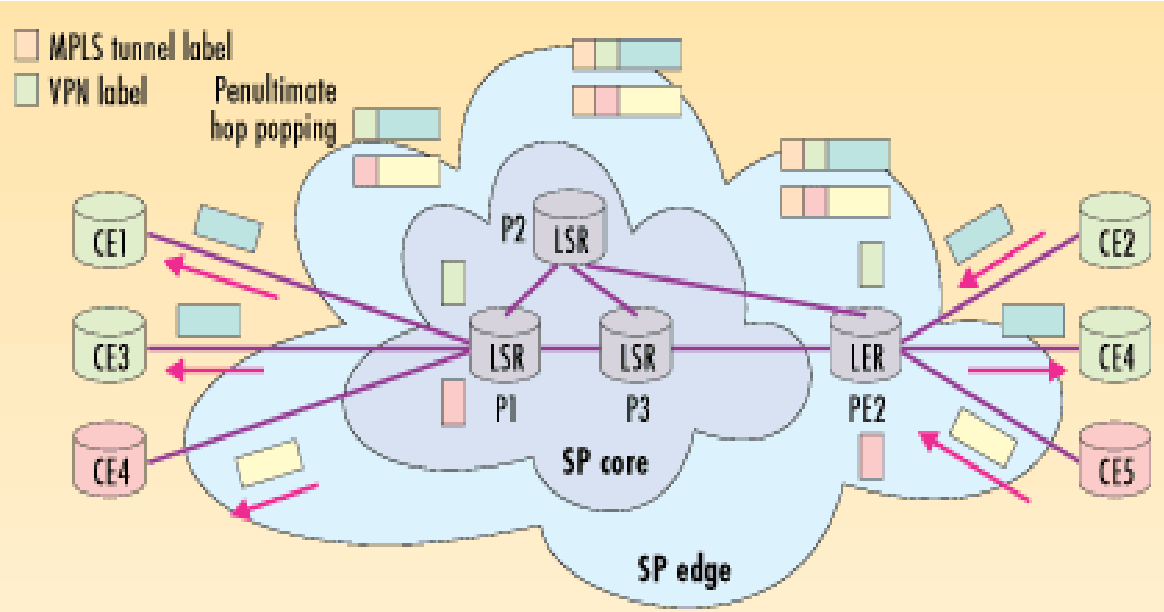


FIGURE 2: PP-VPNs have their own subset of terms and definitions, such as customer-edge devices (CEs) and provider-edge devices (PEs).

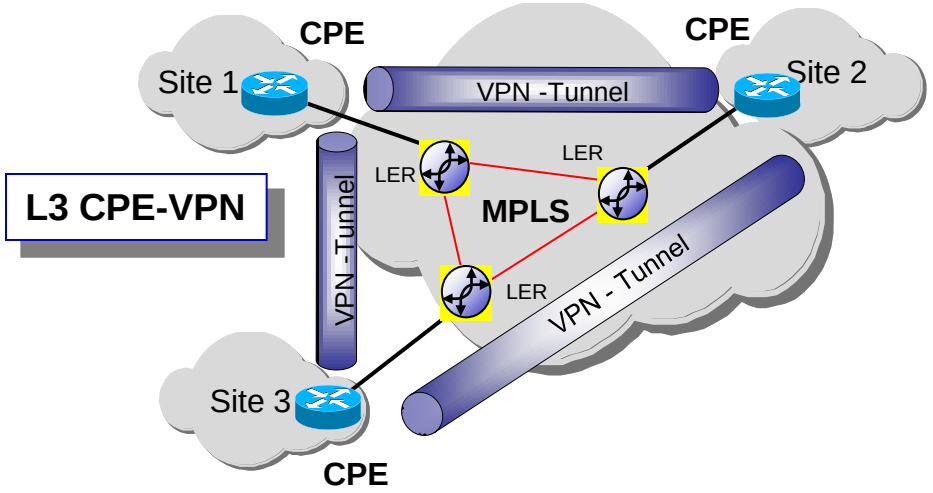
moldovan@tmit.bme.hu

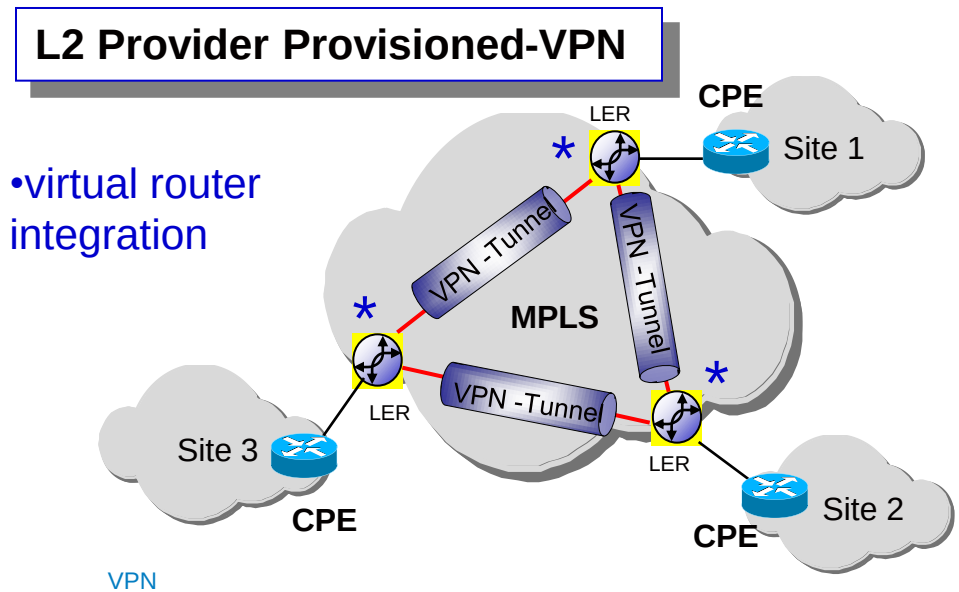
VPN szolgáltatások

- L3 VPN – IPVPN, VPRN
  - IP szintű kapcsolatot biztosít a telephelyek között
  - A csomagok routing segítségével jutnak célba
- L2 VPN – VLL vagy PW
  - Pont-pont kapcsolat
- L2 VPN – TLS, VPLS
  - Ethernet szintű kapcsolat a telephelyek közt
  - Bridging
    - A két telephely egyetlen LAN-t lát

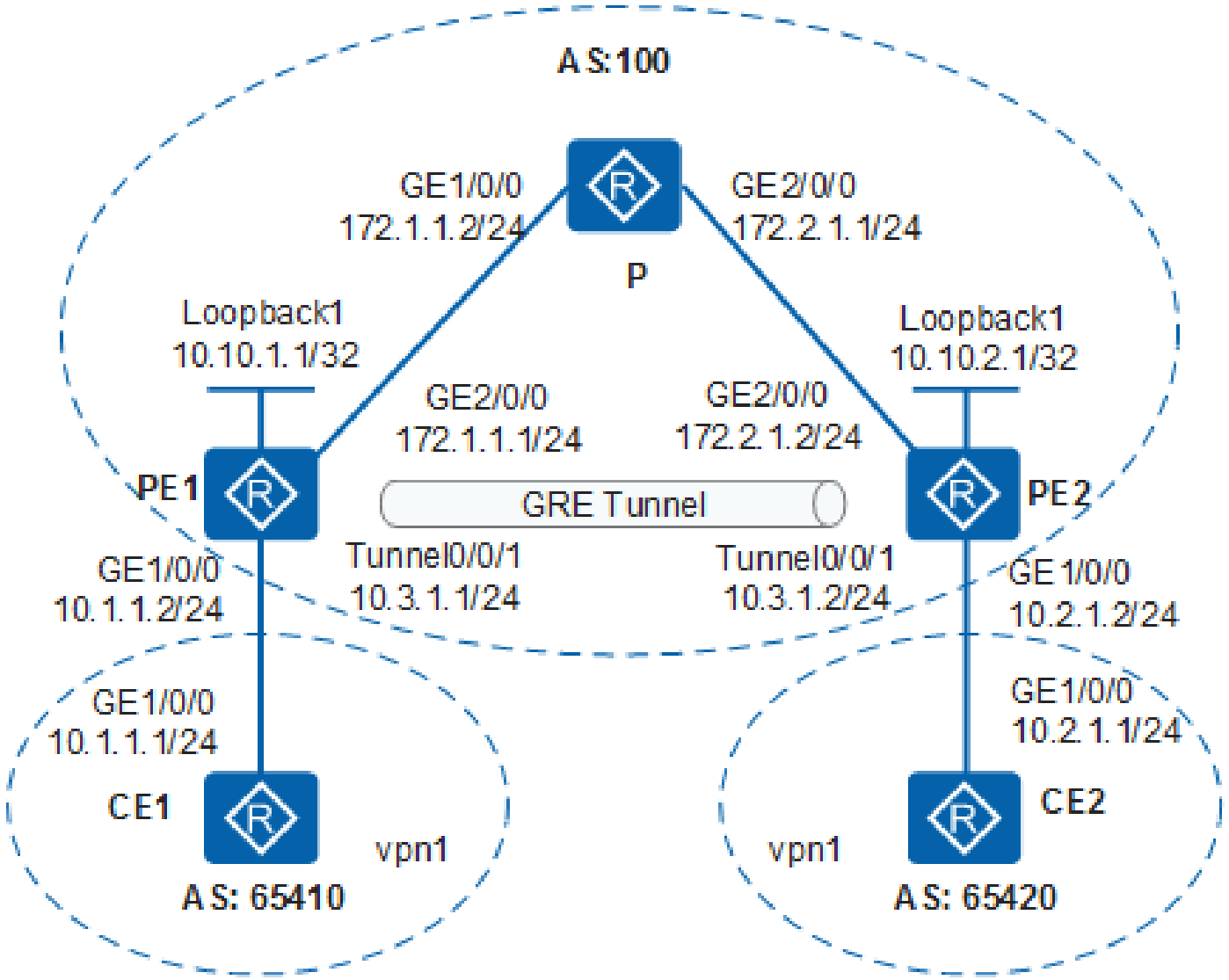
L3 (IP) VPN–alapvető modell

- **Self-Managed IP VPNs**
  - „overlay” model:
    - Customer Premise VPN solutions (CPE)
    - IPSec
- **Carrier-Managed IP VPNs**
  - A virtuális router modell
    - L2 & L3 Provider Provisioned VPN solution (PP)





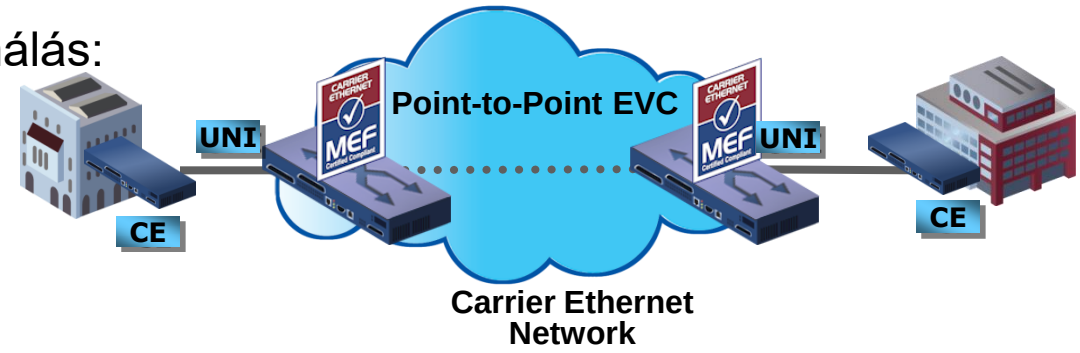
Példa: L3 (IP) VPN



Ethernet szolgáltatások

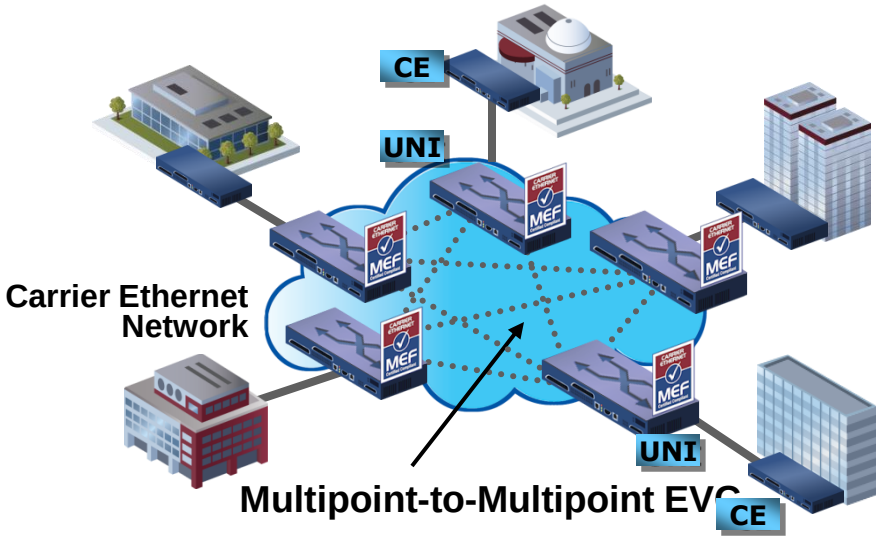
- E-Line Szolgáltatás – felhasználás:
  - Ethernet Private Line
  - Virtual Private Line
  - Ethernet Internet Access

E-Line szolgáltatás típus



- E-LAN Szolgáltatás – felhasználás:
  - Multipont L2 VPN-ek
  - Transzparens LAN Szolgáltatás
  - Alap az IPTV és Multicast szolgáltatásokhoz stb.

E-LAN szolgáltatás típus



MEF által hitelesített Carrier Ethernet termékek

UNI: User Network Interface, CE: Customer Equipment

Szabványosítás

Provider Bridges (Q-in-Q)
Provider Backbone Bridges (Mac-in-Mac)
Provider Backbone Transport (PBB-TE)

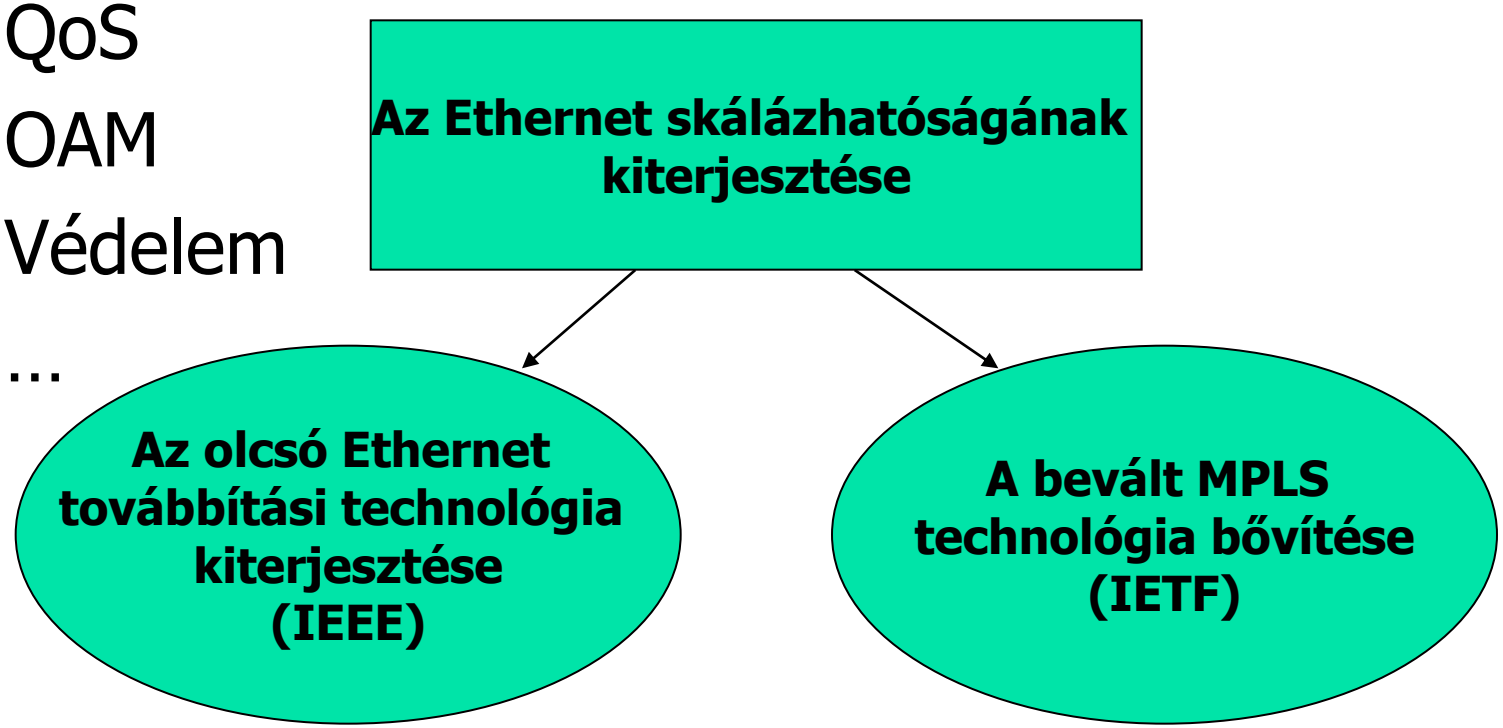
Pseudowire
Virtual Private LAN Service
Hierarchical VPLS

UNI specifikáció
Szolgáltatás Definíciók
Szolgáltatás specifikációk

UNI specifikáció– szolgáltató olda
Szolgáltatás Definíciók
T-MPLS

Kihívások

- Szolgáltatói tulajdonságok
  - Skálázhatóság
  - QoS
  - OAM
  - Védelem
  - …



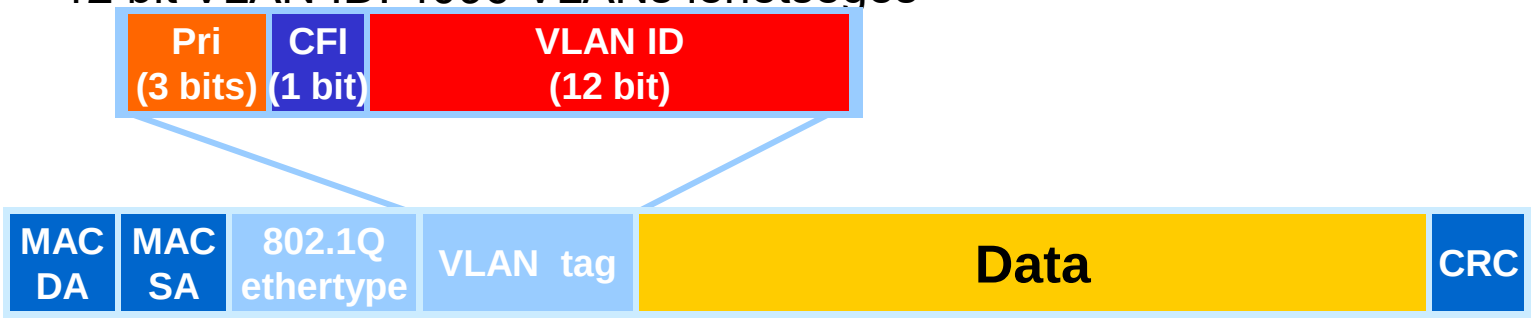
Ethernet alapú átvitel

Budapest University of Technology and Economics

Department of
Telecommunications and Media Informatics

IEEE 802.1Q - VLAN

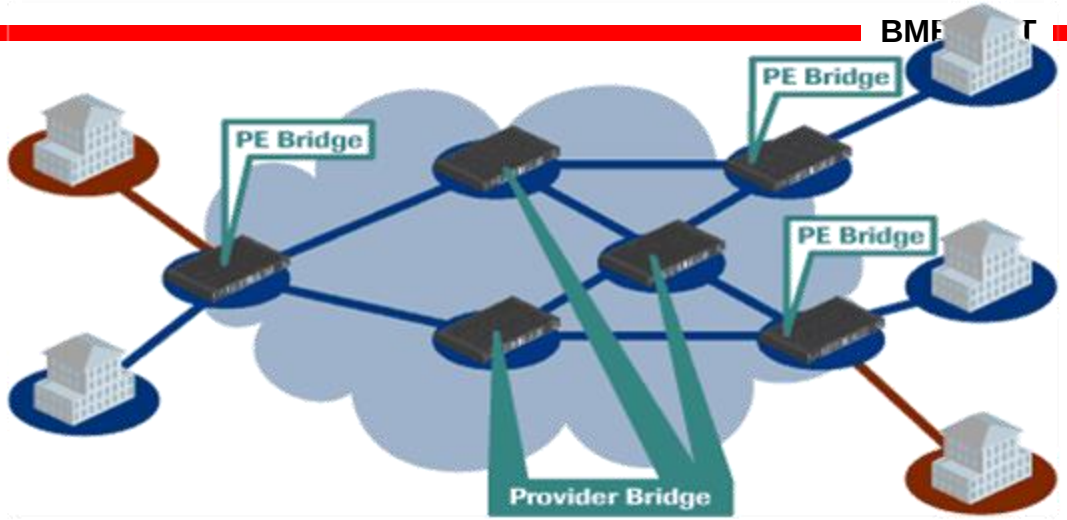
- VLAN tag
  - QoS: prioritás bitek
  - 12 bit VLAN ID: 4096 VLANs lehetséges



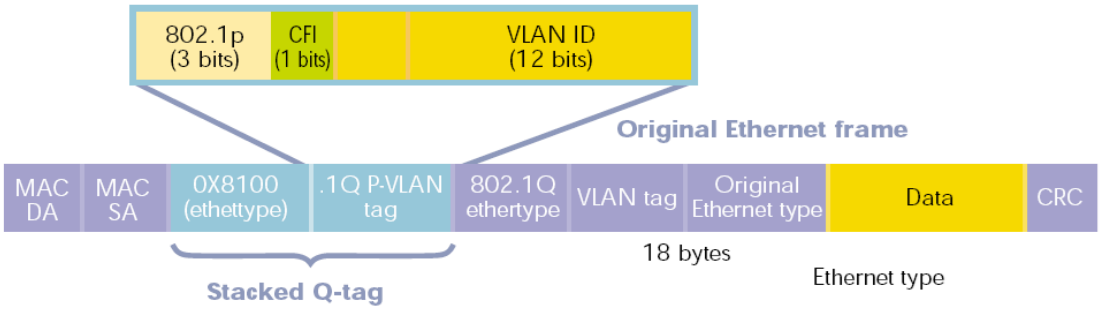
- Felhasználási módok:
  - Felhasználó azonosítás
  - Szolgáltatás azonosítás
- Mindkét esetben korlát a 4096 – szolgáltatói környezetben kevés!
- De: a legelterjedtebb UNI
  - Fel kell készülni hogy transzparensen át kell vinni a VLAN csomagot

Provider Bridges (IEEE 802.1ad)

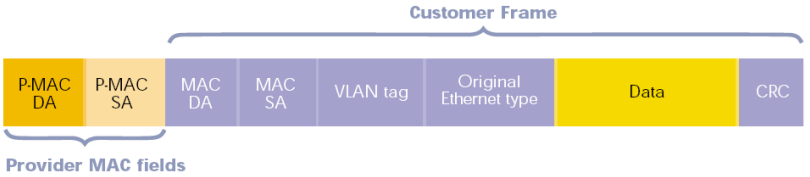
- Q-in-Q néven ismert
- Széles körben elterjedt



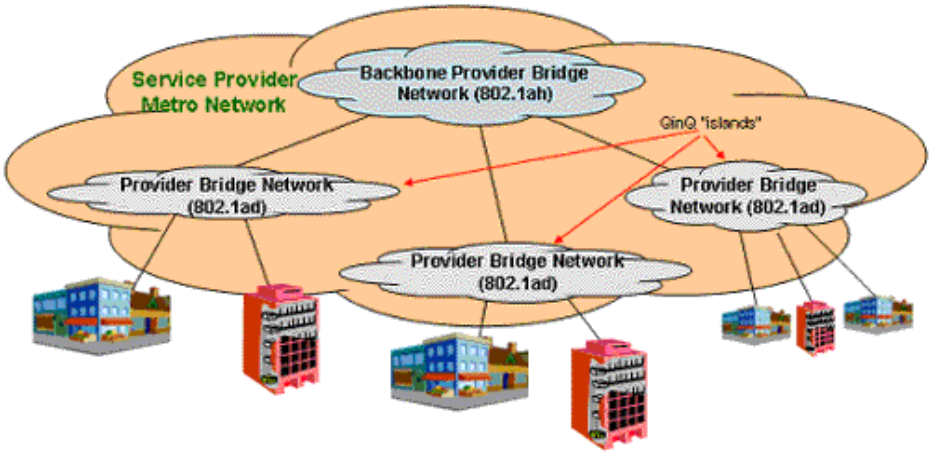
- A legelterjedtebb felhasználói interfész
- 4K Szolgáltatás (12-bits)
- Egyedi szolgáltatás ID
  - (S-VID)
- A csomagtovábbítás a megszokott L2 tanuló bridge alapú a MAC DA/SA alapján S-VID szinten és xSTP a hurkok elkerülésére
- Skálázhatóság
  - 4K szolgáltatás



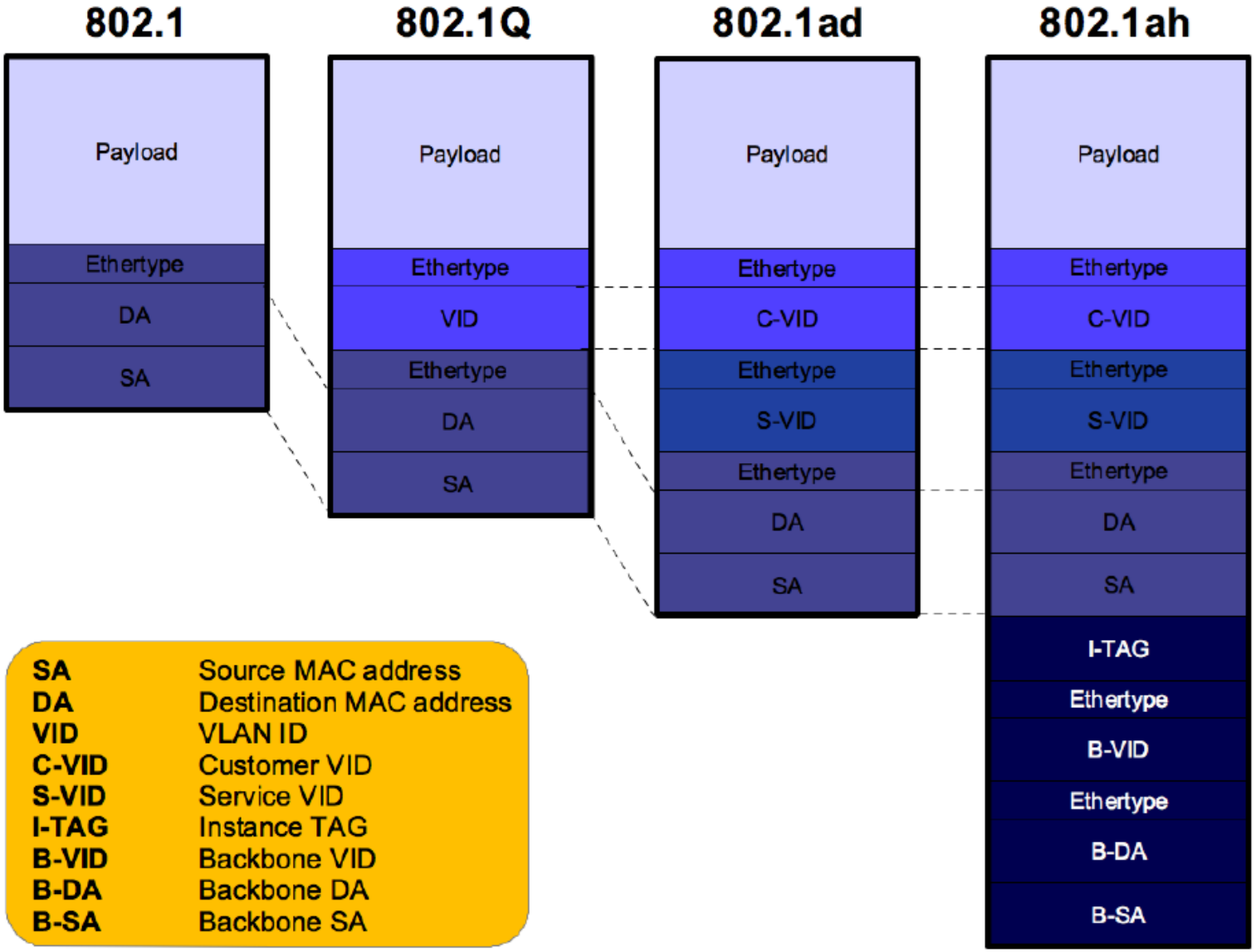
Provider Backbone Bridges



- 4K összekötött többesadásos hálózat
- Egyedi Szolgáltatás ID
  - (LAN = I-SID)
- A csomagtovábbítás a megszokott L2 tanuló bridge alapú a MAC DA/SA alapján B-VID szinten és xSTP a hurkok elkerülésére
- A szolgáltatások engedélyezése egyszerű mert az I-SID társítás hasonlít az S-VID beállításhoz
- Skálázhatóság
  - Maszív szolgáltatás skálázhatóság (24-bit)
  - Nincs szükség hogy minden csomópontban beállítsunk egy I-SID-et egy P2P mesh hálózat kialakításához
  - A C-MAC címeket megtanulja és B-VID/I-SID alapján társítja



Összehasonlítás – hozzáadott fejlécek



PB/PBB tények

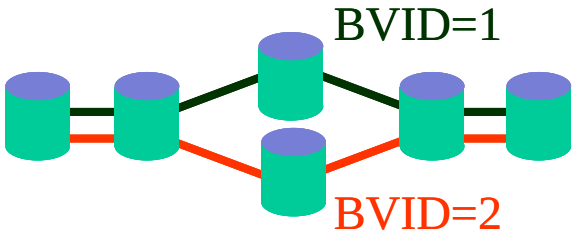
- Skálázhatóság megoldva ☑
- Marad az olcsó Ethernet kapcsolás ☑

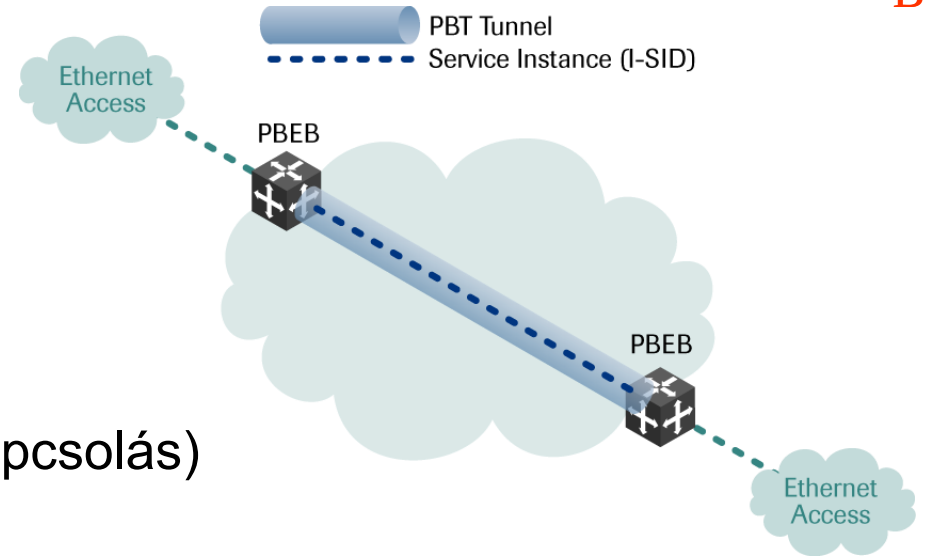
- Továbbra sincs Traffic Engineering ☒
- Védelem/helyreállás STP alapú ☒
- Nehézkes a menedzsment ☒
  - Több szintű VLAN-ok sokasága
  - Nincs hiba- és performancia menedzsment

- Még mindig nem megfelelő a maghálózatban…

PBT

- A cél:
  - marad az Ethernet csomagtovábbítási mechanizmus
  - Lecseréljük a vezérlési síkot (kikapcsoljuk az STPt és tanulást)
  - Az útvonalakat a hálózatban előre beállítjuk
    = Traffic Engineering - Ethernet

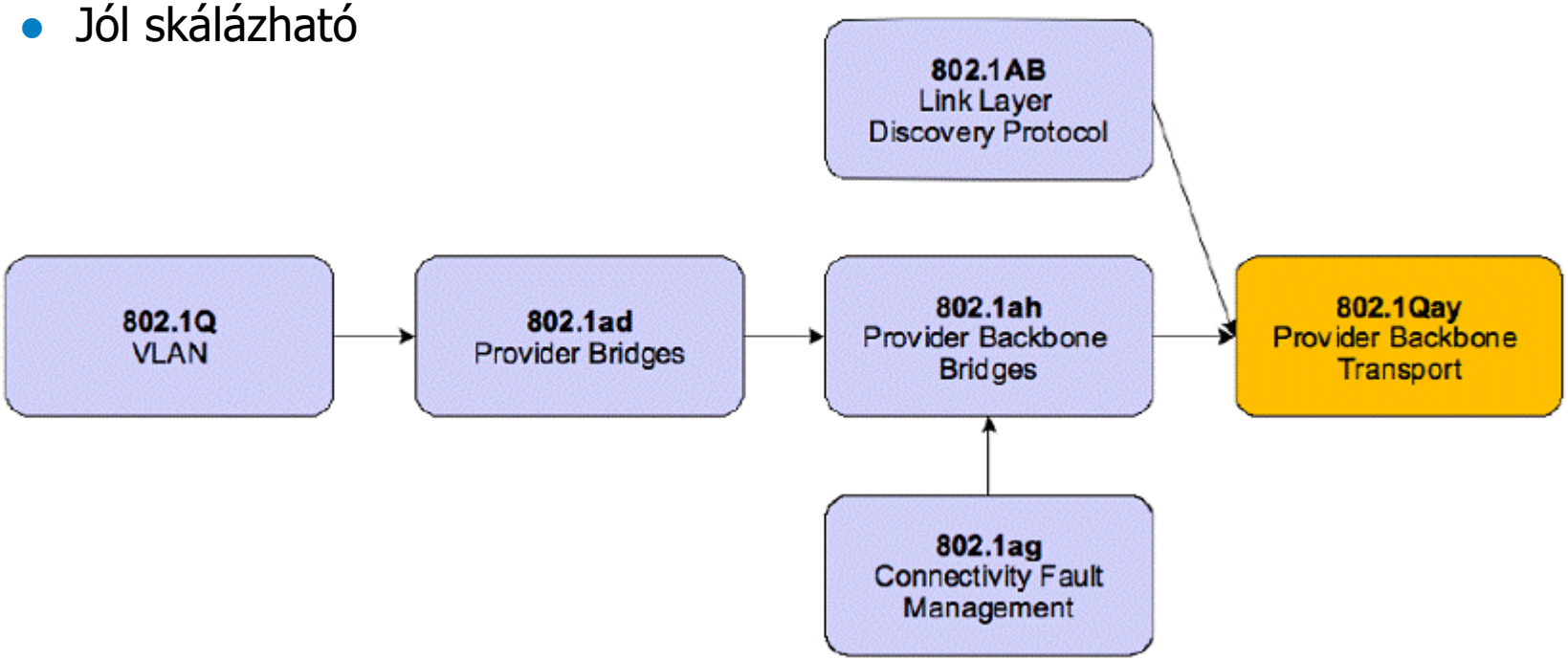




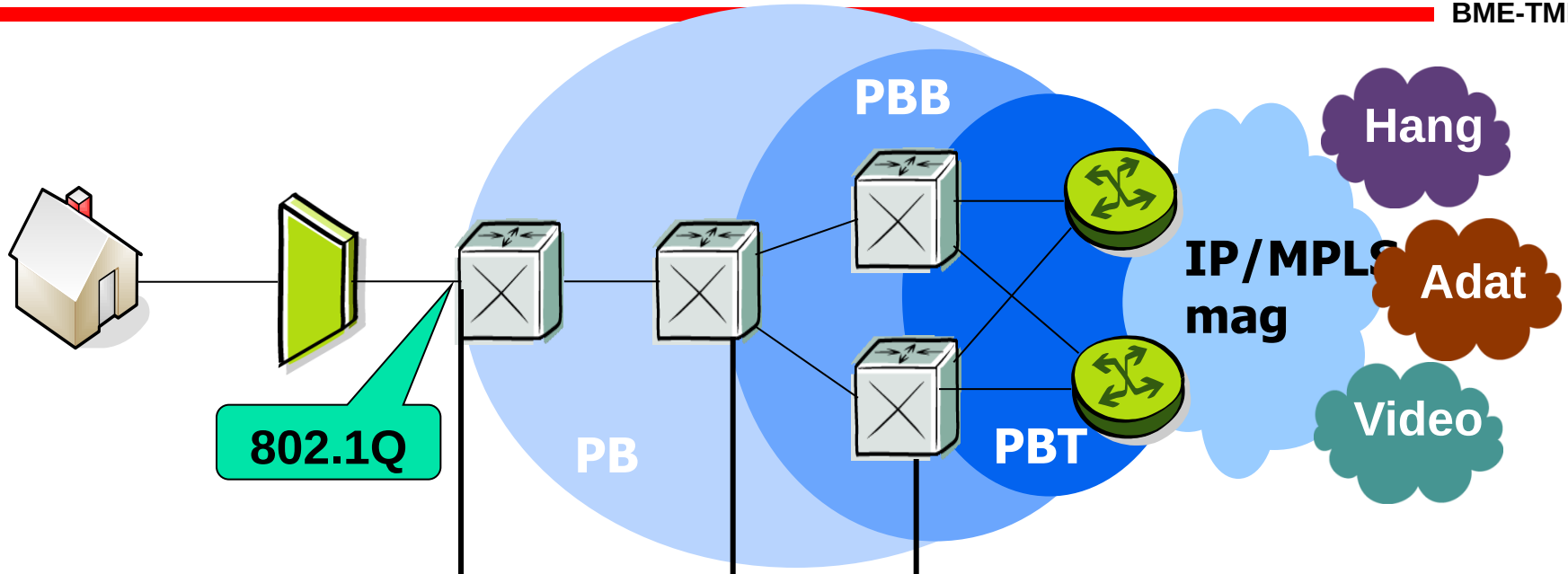
- Amit kapunk:
  - Pont-pont tunnelek
  - Traffic Engineering
  - Védelem (védelmi kapcsolás)

PBT

- Provider Backbone Transport – IEEE 802.1Qay
  - Nortel kezdeményezte
  - A PBB-re épül
- Újrahasznosítja a meglévő technológiákat
  - Determinisztikus QoS-t nyújtó szolgáltatás a cél
  - Jól skálázható



Ethernet Transzport technológiák alkalmazása



802.1Q: 4K felhasználóig

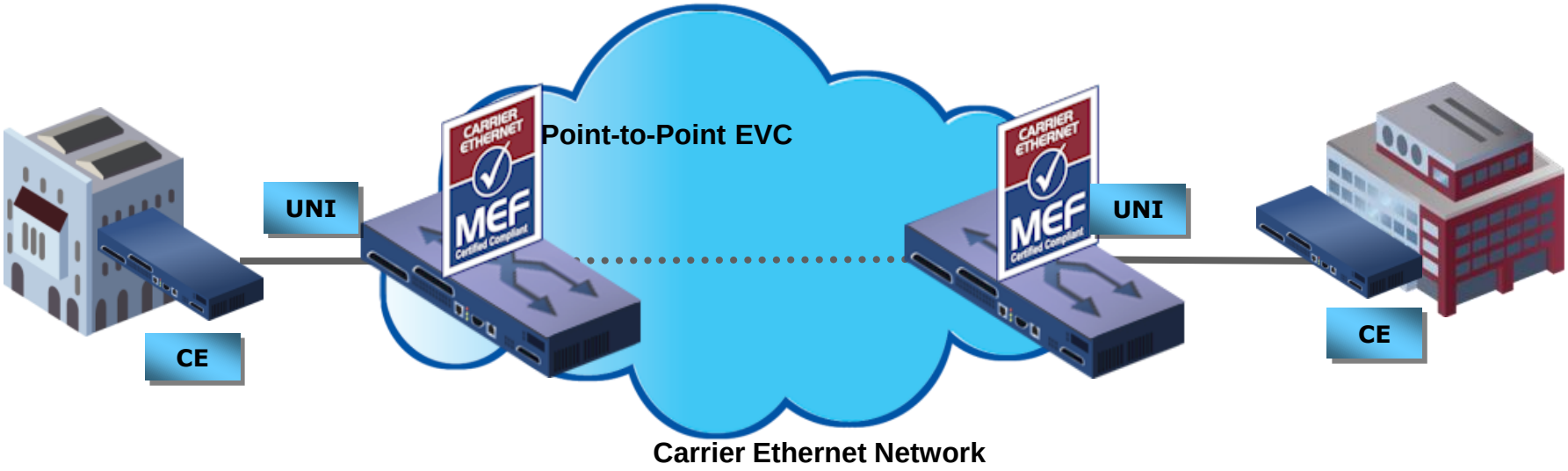
PB: 4K szolgáltatásig

PBB: jól skálázható

Hozzáadott érték: TE, OAM

PB – Q-in-Q – IEEE 802.1ad
PBB – Mac-in-Mac – IEEE 802.1ah
PBT – PBB-TE – IEEE 802.1Qay

Példa: L2 pseudowire



- Provider oldalon
  - VLAN beállítás: UNI-k között
- Customer oldalon
  - -

MPLS alapú átvitel

Budapest University of Technology and Economics

Department of
Telecommunications and Media Informatics

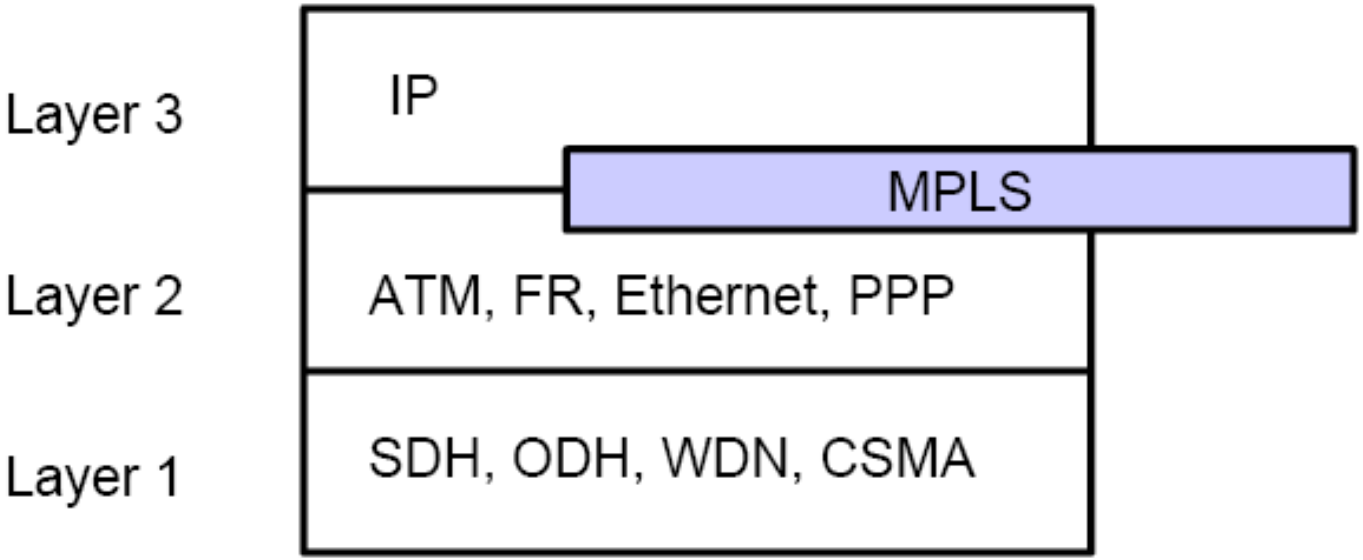
MPLS

- MPLS: MultiProtocol Label Switching
- Alapvető cél
  - A vezérlés és továbbítás szétválasztása
- „Label-switching” paradigma
  - Az L2 címkekapcsolás és az L3 routing összekrapcsolása

moldovan@tmit.bme.hu

Helye a Protocol Stack-ban

- MPLS az IP és Layer 2 között van
  - Az L2 protokollok széles körét támogatja
  - Támogatja a felsőbb szintű mechanizmusokat is



moldovan@tmit.bme.hu

Label – címke hordozása

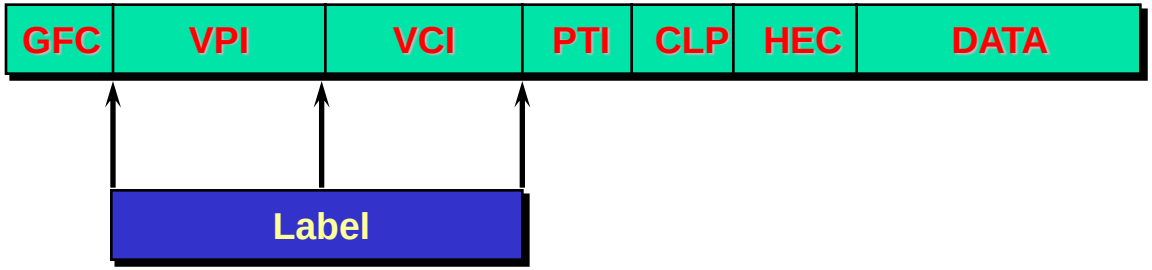
- Bizonyos L2 technológiák képesek a címkét a saját fejlécük részeként kezelni
  - **pl. VPI/VCI az ATM esetén, DLCI a FR esetén vagy MPLS címke PPP/Ethernet esetén**
- Azon L2 rétegek amelyek nem támogatják a címkéket egy külön „shim” fejlécben hordozzák

Link layer fejléc	“Shim” label fejléc	Network layer fejléc	Network layer fejléc

moldovan@tmit.bme.hu

Beágyazás

ATM Cella Fejléc



PPP Fejléc
(Packet over SONET/SDH)

LAN MAC Label Fejléc

moldovan@tmit.bme.hu

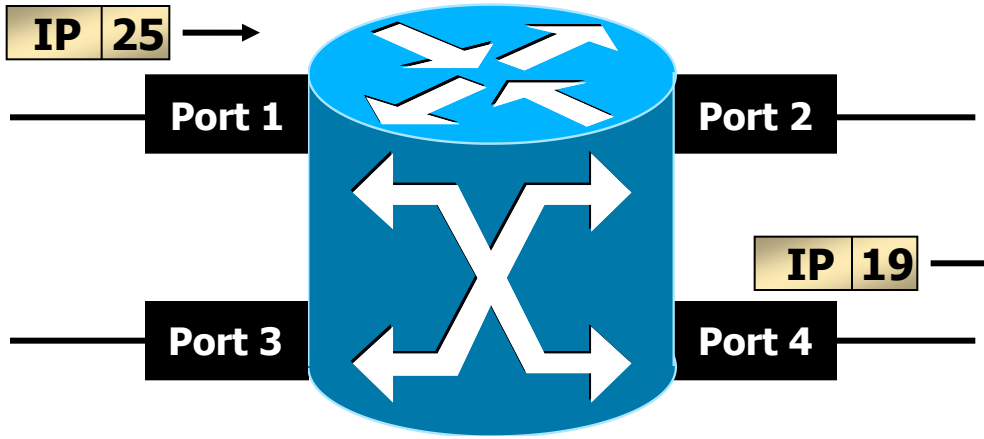
Az MPLS Shim Header

- A címke - Label (Shim Header) valójában egy is Label Stack Entry szekvencia, azaz egy vagy több bejegyzés
- Minden Label Stack Entry 4 byte (32 bit) hosszú
- 20 Bit fenntartva a címke azonosítónak (Label Identifier) – ez a „Label”, címke

Label : **Label value** (0 to 15 are reserved for special use)
Exp : **Experimental Use**
S : **Bottom of Stack** (set to 1 for the last entry in the label)
TTL : **Time To Live**

moldovan@tmit.bme.hu

Továbbítás - kapcsolás



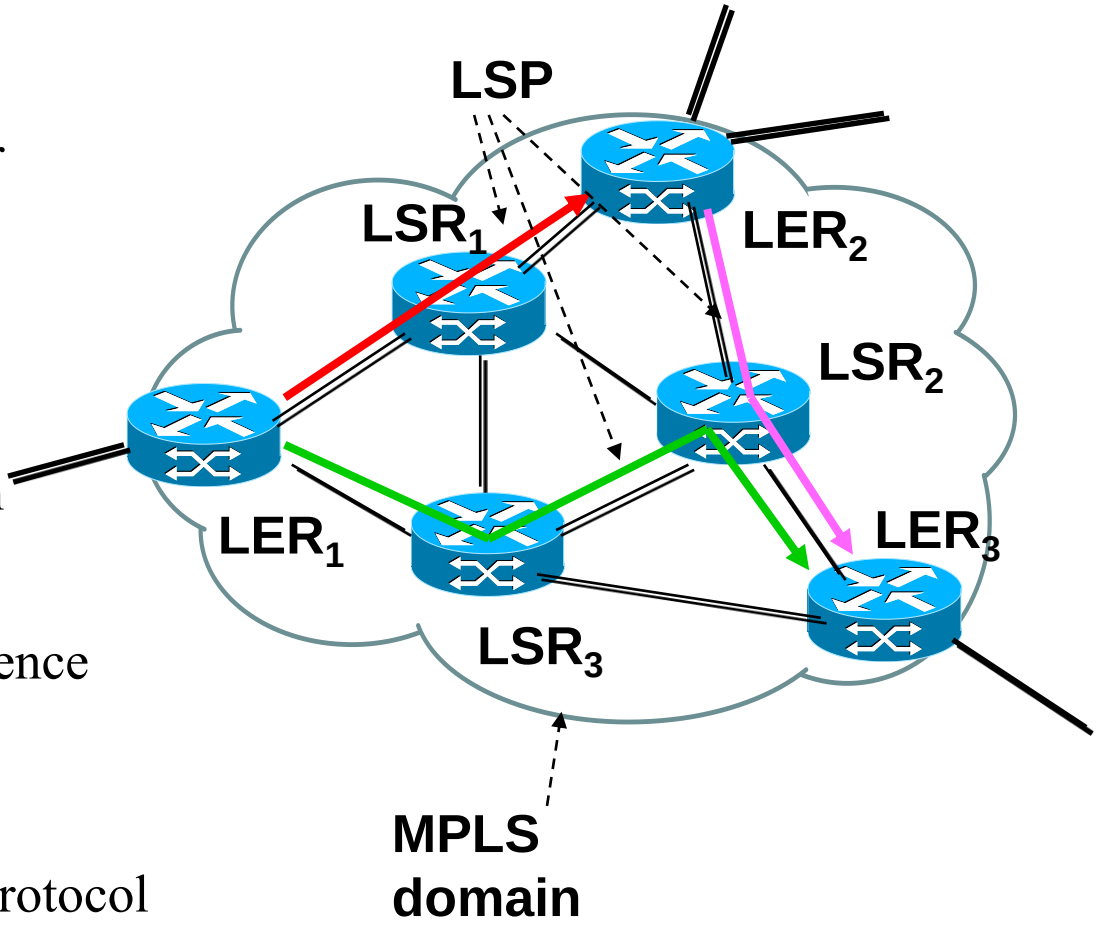
Connection Table

In (port, label)	Out (port, label)	Label Operation
(1, 22)	(2, 17)	Swap
(1, 24)	(3, 17)	Swap
(1, 25)	(4, 19)	Swap
(2, 23)	(3, 12)	Swap

- Label Swapping
  - A kapcsolat tábla tartalmazza a bejegyzéseket („Connection table”)
  - Exakt találat keresés (nem mint IP routing esetén)
  - Bemenet: Input (port, label) meghatározza:
    - Címke művelet
    - Kimenet - Output(port, label)
  - Hasonló továbbítást használ az ATM és Frame Relay is

MPLS Komponensek

- LSR
  - » Label Switch Router
- LER
  - » Label Edge Router
- LSP
  - » Label Switched Path
- FEC
  - » Forwarding Equivalence Class
- LDP
  - » Label Distribution Protocol



moldovan@tmit.bme.hu

MPLS célok

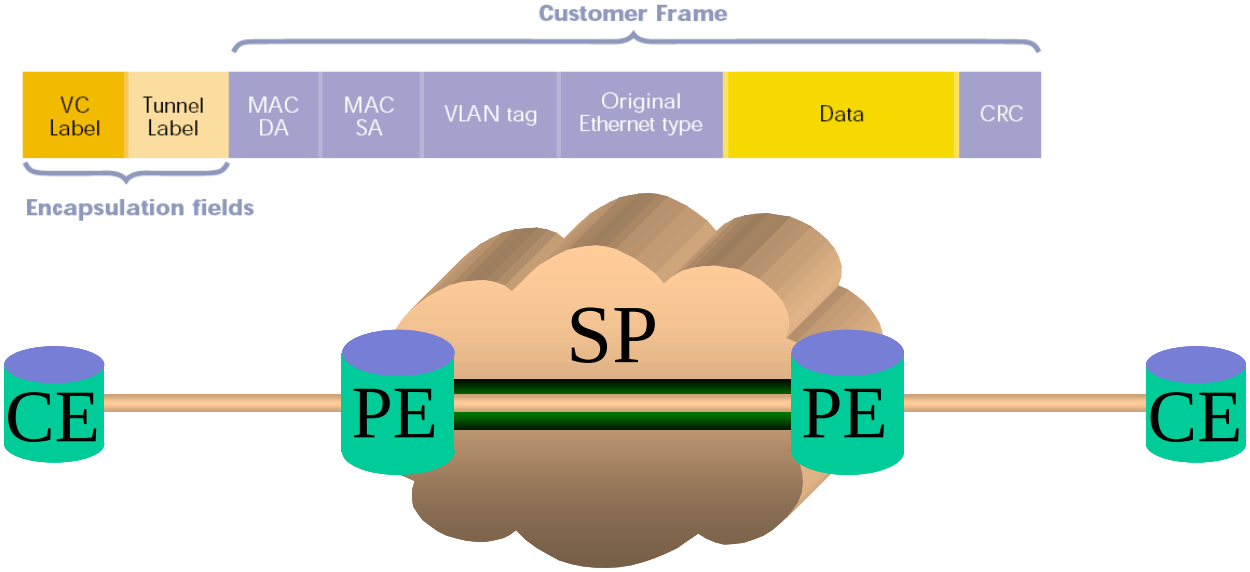
Az MPLS kiterjeszti a hagyományos IP-t a következő területeken::

- Egyszerűsített továbbítás
- Hatékony Explicit útvonalak
- Traffic Engineering
- QoS Routing
- A csomagok nem triviális módon történő útvonalakba rendezése
- Védelem

moldovan@tmit.bme.hu

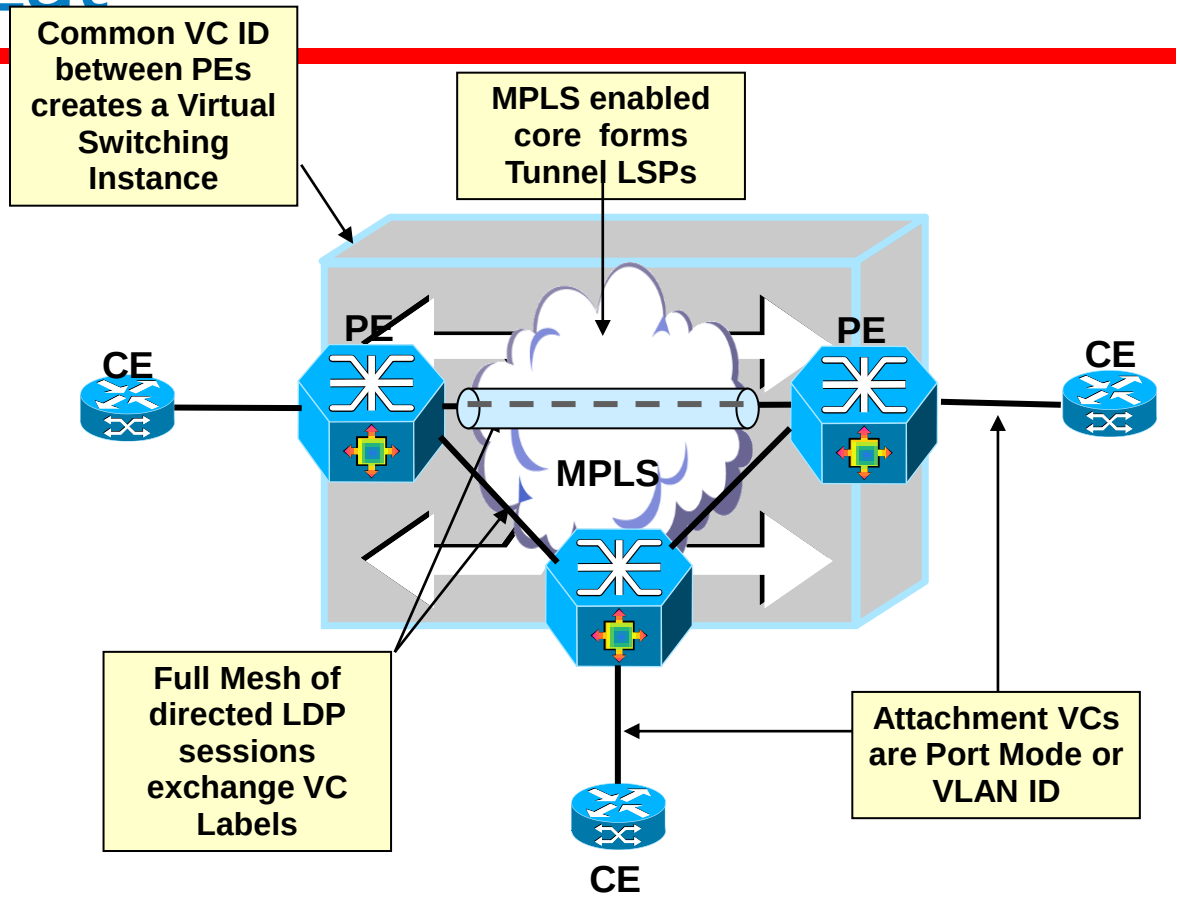
MPLS Pseudowire - VPWS

- Ethernet p2p kapcsolatot tesz lehetővé
  - Az IETF pwe3 csoport dolgozta ki, a draft neve alapján Martini – enkapszulációnak is nevezik
  - Az MPLS címke is beágyazott, egy UNI-n belül több virtuális kapcsolatot megkülönböztetve (VC)
  - A tunnel címke alapján továbbítódik a hálózatban



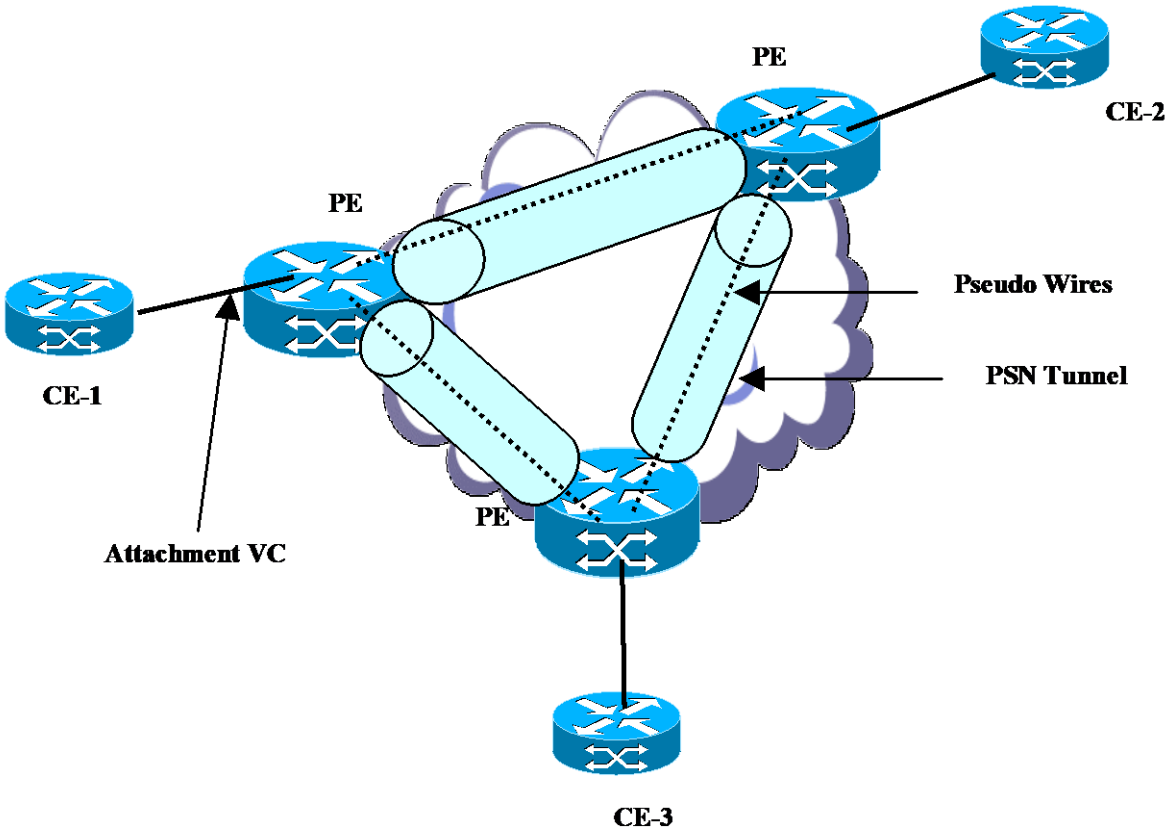
- A megoldás örökli az MPLS összes jó tulajdonságát:
  - Traffic Engineering, Védelem, OAM

VPLS hálózat



Customer Edges (CE): kliens oldali eszköz, tipikusan Etherneten csatlakozik
Provider Edges (PE): itt található a VPLS inteligencia, kezdő/végső pont
Core: csak a továbbításban vesz részt

VPLS rendszer példa



Full Mesh alagutak a PE-k között

- nem feltétlen fizikai, sőt!

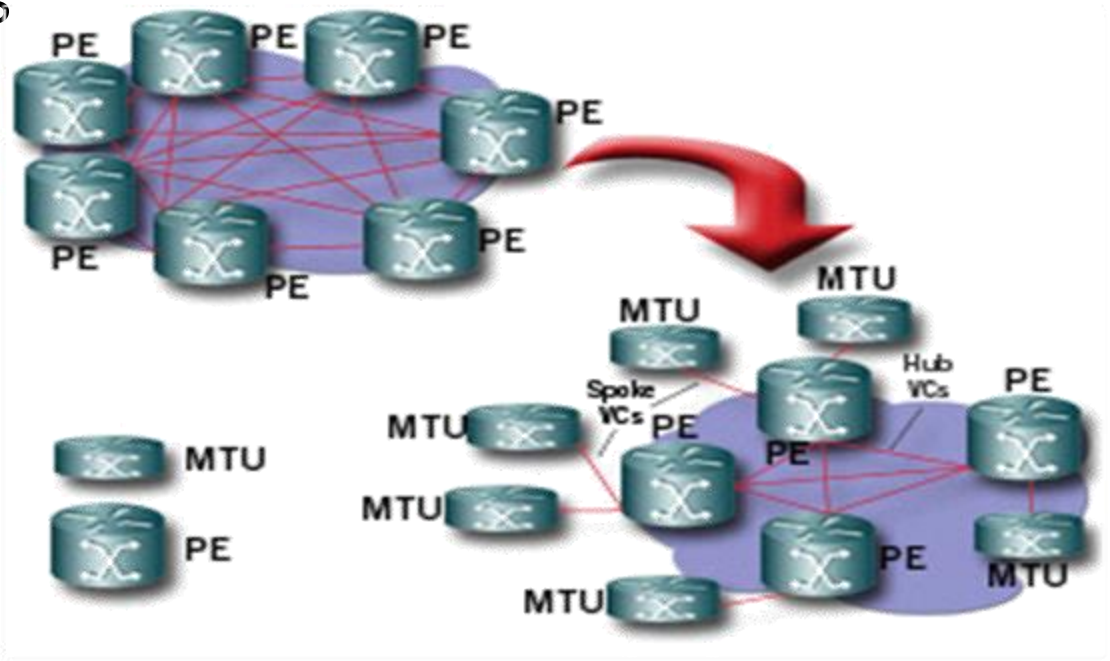
PE-k egy virtuális bridge-t mutatnak a CE-k felé

VPLS Működési elv

- VPLS instance : Service–identifier (Svc-id)
- Full mesh tunnelek kialakítása
  - Célzott LDP üzenetekkel
- Csomag továbbítás: tanuló bridge
  - Ismeretlen cél: broadcast az összes tunnelre
  - Split-horizon: soha nen továbbít oda, ahonnan érkezett – a hurkok ellen

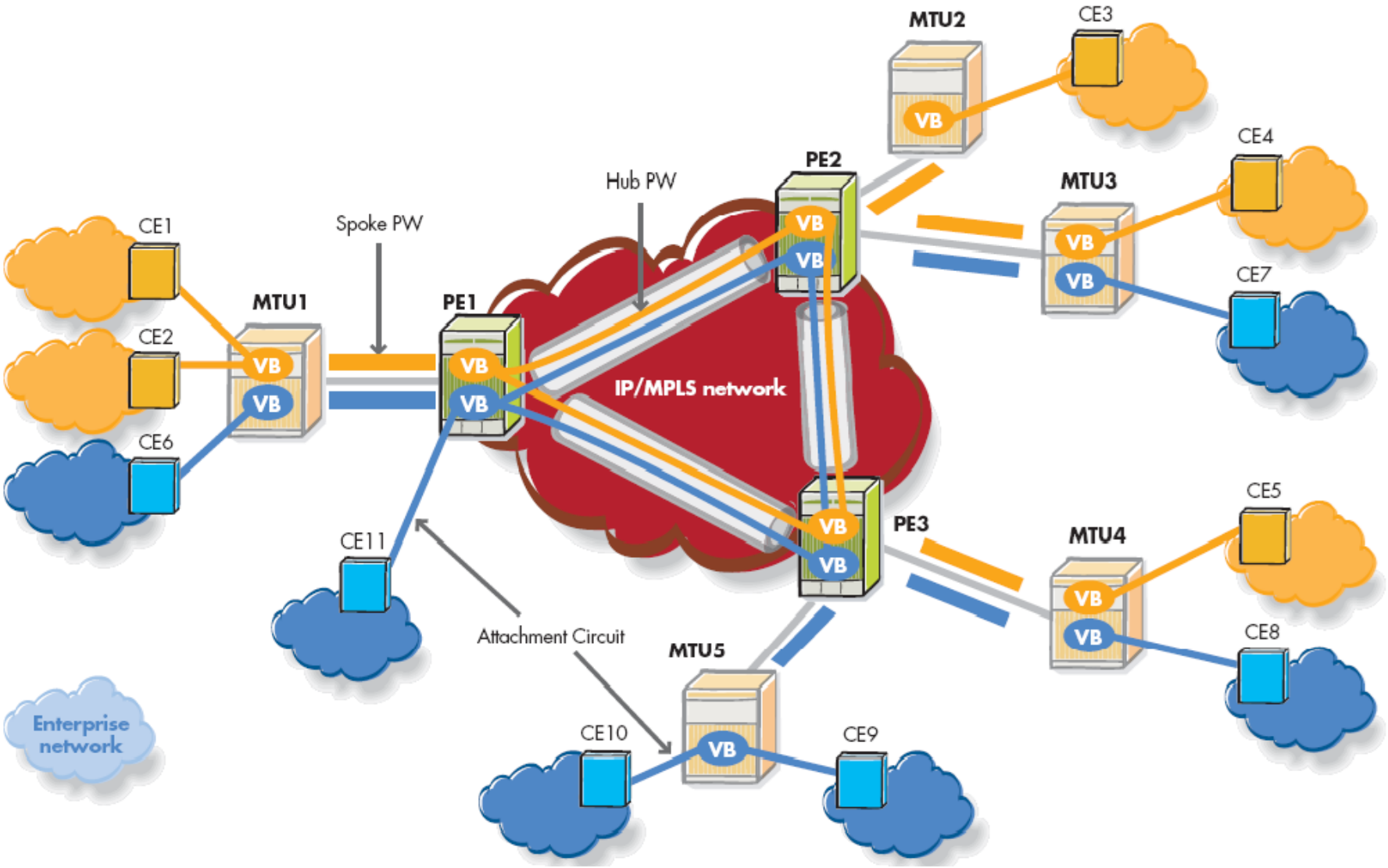
VPLS skálázhatóság - hierarchia

- MTU - Multi-Tenant Unit: több felhasználó által bérelt eszköz, bridge
- MTU-ig kiterjeszthető a VPLS
  - MAC/VLAN skálázhatóság megnő
  - Komplexebb MTU



- Hierarchikus VPLS
  - PE-k között „HUB” pseudowire-k (hub PW)
  - MTU-PE között „spoke” PW
    - Spoke PW lehet QiQ, MPLS, …

Hierarchikus VPLS



VPLS és H-VPLS skálázhatóság

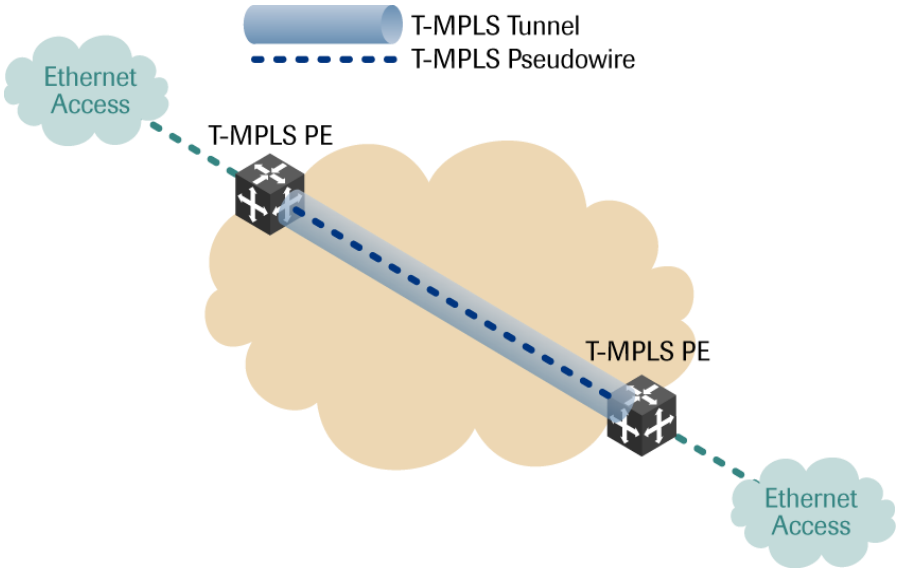
- PW kapcsolatok az MPLS vezérlő sík által kihúzva
- A Hub-and-Soke csökkenti a full-mesh PW igényét

- A szolgáltatások számának növekedésével a MAC tábla mérete és a PW-k száma közt egyensúlyt kell teremteni

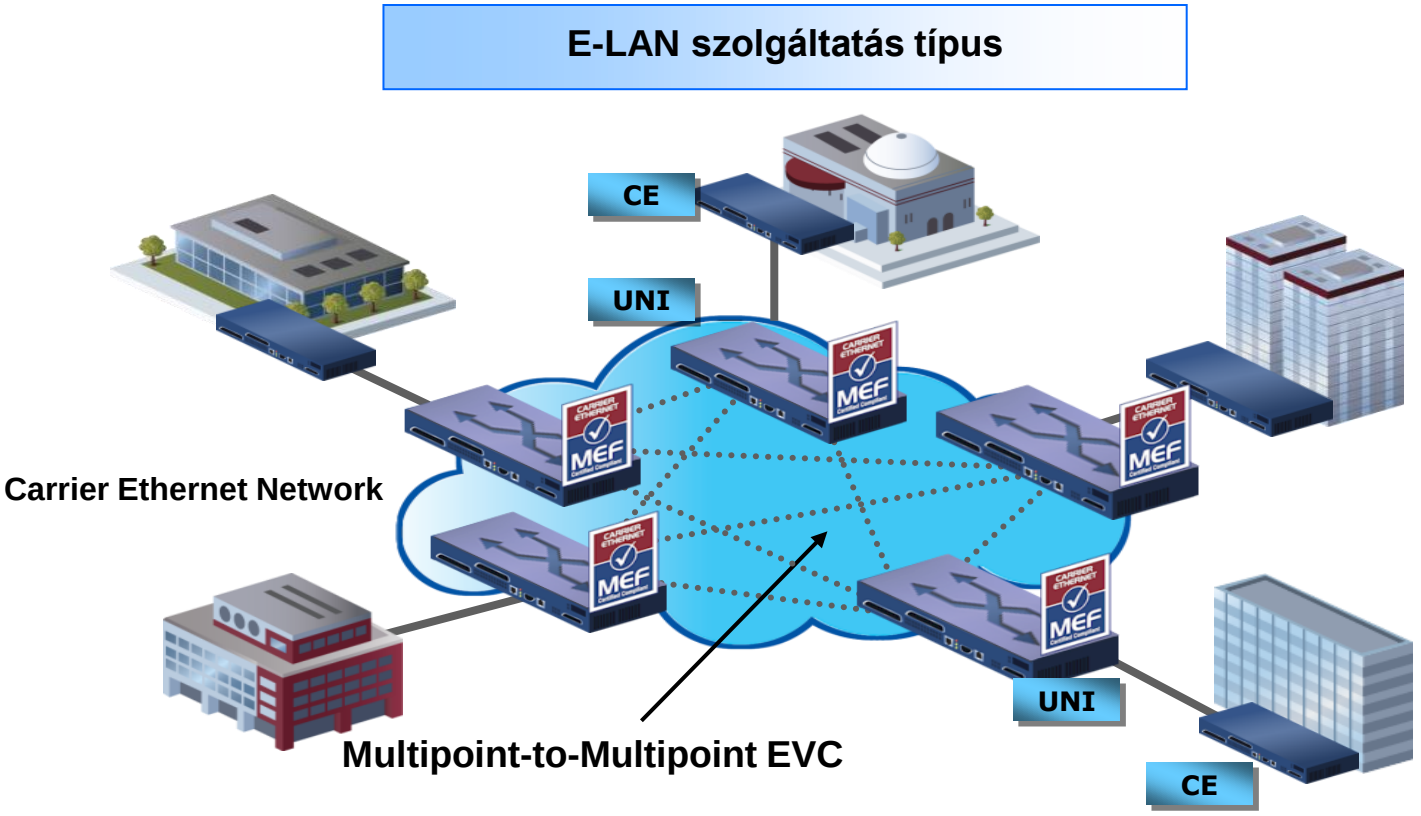
	Services	PEs	MTU-s	PW mesh	MACs (1K per service)
VPLS	512	64	-	1M	512K
H-VPLS	512	16	256	60K	512K
	8,192	16	256	1M	8M

Vissza az áramkör kapcsoláshoz: T-MPLS

- Transport-MPLS
- **Kimondottan kapcsolat orientált alcsoportja az MPLS-nek**
- Az ITU-T szabványosítja
  - Az MPLS egy része, amely a p2p kapcsolatok kezeléséhez szükséges
- arra helyezi a hangsúlyt, hogy az IP menedzsmentet eliminálva az MPLS megoldások menedzsmentjét leegyszerűsítse
- Fő szempontok
  - Védelem: 50ms
  - Traffic Engineering
  - Garantált SLA
  - OAM: hiba és performancia menedzsment



Példa: MPLS L2VPN



- Konfigurálás:
  - Tunnel mesh az UNI-k között

Layer 1 L2VPN - EoSDH

- Pont-Pont kapcsolat
- Generic Framing Procedure (GFP)
  - Szabvány az első és második rétegbeli protokollok Sonet/SDH keretezésére
- Virtual Concatenation (VCAT)
  - Az SDH sávszélesség felosztása virtuálisan
  - Link Capacity Adjustment Scheme (LCAS)
    - Elősegíti a dinamikus sávszélesség kiosztást a VCAT segítségével

Összefoglalás

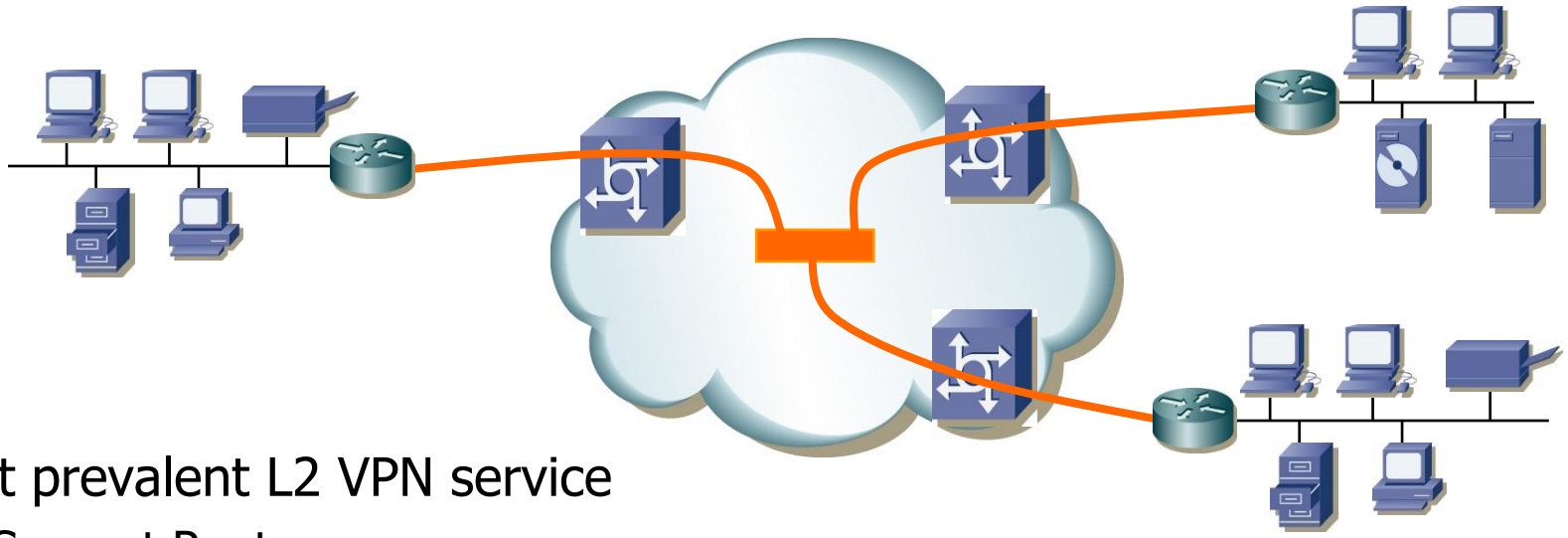
- Az Ethernet alapú szolgáltatások gyorsan fejlődnek
  - Szabványosítás
  - Alkalmazás
- Több, egymással versenyző technológia van az Ethernet szolgáltatások átvitelére
  - MPLS és Ethernet alapú megközelítések
  - Mindkettőnek megvan az előnye-hátránya
- A különböző technológiák arányát/határait a hálózatokban a szolgáltatók fogják eldönteni

Köszönöm a figyelmet

Budapest University of Technology and Economics

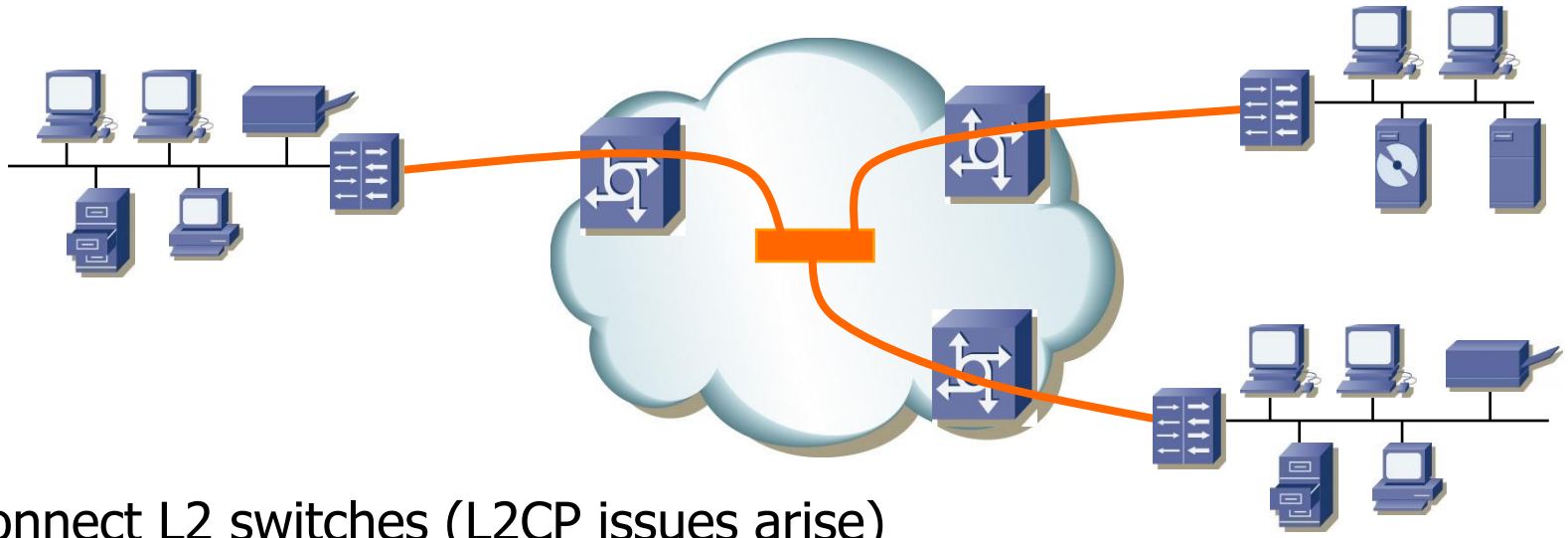
Department of
Telecommunications and Media Informatics

Router Inter-connect Characteristics



- Most prevalent L2 VPN service
  - Connect Routers
  - Routers provide clear demarcation
    - Possibility of unnecessary BC/MC eliminated
    - L2CP issues eliminated
    - One MAC address per site
- Most customers use routers to connect multiple sites together
  - Well-known design
  - Considerably reduces management overhead (single connection per site)

Switch Inter-connect Characteristics



- Connect L2 switches (L2CP issues arise)
- Multiple MAC address per site
  - Potential scalability issues
  - Malfunctioning L2 switches can also flood the provider network with BC/MC traffic
  - Requires controls of FIB size (# MAC per site) and BC/MC rate-limiting
- Should be sold as a premium service
  - Charge customers per site per block of MAC addresses