

# Ethernet2/L2VPN gyakorlat

Moldován István

[moldovan@tmit.bme.hu](mailto:moldovan@tmit.bme.hu)

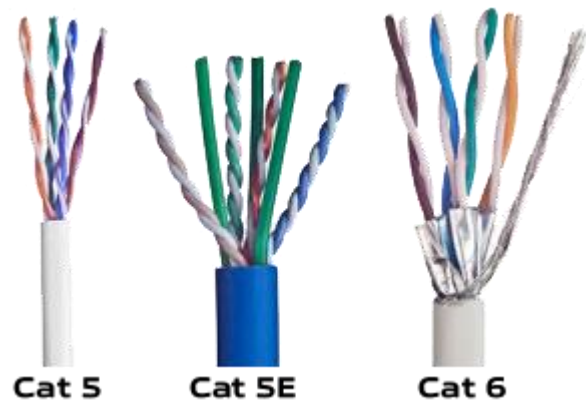


BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM  
TÁVKÖZLÉSI ÉS MÉDIAINFORMATIKAI TANSZÉK

# Interfészek



BME-TMIT

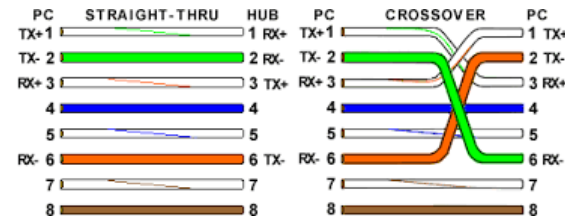
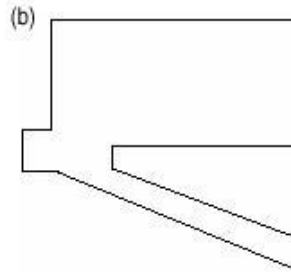
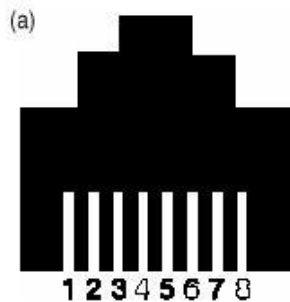


# UTP – Category 5, 6



BME-TMIT

- RJ-45 dugasz



## Láb kiosztás (10/100)

- |                       |                      |
|-----------------------|----------------------|
| 1 TD+ (Transmit Data) | 5 Nem használt       |
| 2 TD- (Transmit Data) | 6 RD- (Receive Data) |
| 3 RD+ (Receive Data)  | 7 Nem használt       |
| 4 Nem használt        | 8 Nem használt       |

## Láb kiosztás (>1000)

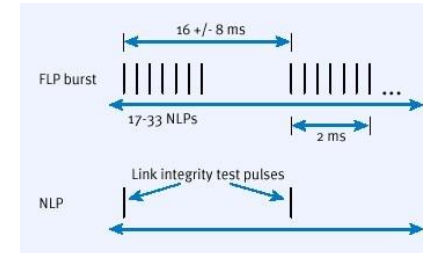
**mind a 8 szálát használja!**  
**Hibrid alapú működés: egyszerre ad/vesz**  
**mind a 4 érpáron**  
**Ugyanúgy 125MHz!**

# Auto negotiation



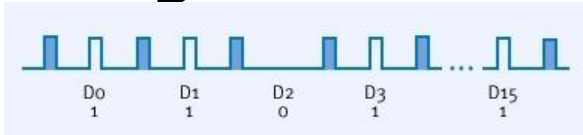
- 10/100/1000 interfészek – együttműködés?

- Auto negotiation




- Out of band: nem Ethernet csomagokban

- Link pulzus alapú
- Még nem tudjuk a közös sebességet
- Hasonló a link integritás ellenőrzéséhez



- Az eszközök megegyeznek a közös sebességben

- Transceiver:
  - Jellemzően SFP+ 
- Réz alapú átvitel
  - 10GBASE-T
  - Cat6a/Cat7 100m-ig.
- SFP+ direct attach cables (DAC)
- és active optical cables (AOC)
- Optikai transceiver típusok:

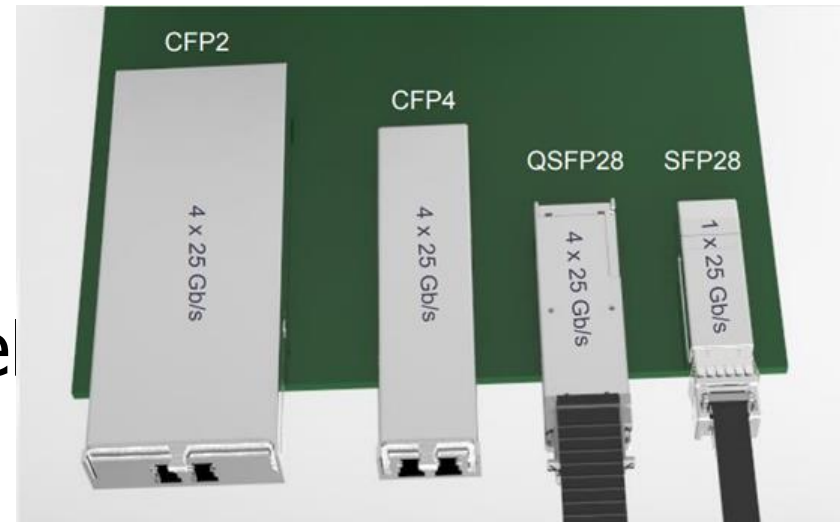


<b>STD</b>	<b>F.O. Type</b>	<b>Dst.</b>
<b>10GBase-USR</b>	<b>MM OM1,2,3</b>	<b>100mt</b>
<b>10GBase-SR</b>	<b>MM OM3</b>	<b>300mt</b>
<b>10GBase-LRM</b>	<b>MM OM1,2,3</b>	<b>220mt</b>
<b>10GBase-LR</b>	<b>SM</b>	<b>10Km</b>
<b>10GBase-ER</b>	<b>SM</b>	<b>40Km</b>
<b>10GBase-ZR</b>	<b>SM</b>	<b>80Km</b>
<b>10GBase-LX4</b>	<b>MM/SM</b>	

# 25G



- 25G – 1x RX és 1x TX
- Transceivererek: többféle
  - SFP28 – réz – 4m
  - AOC optikai patch kábelek



- Nagy távolság áthidalása

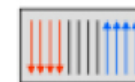
25GBASE-SR

50µm MMF / 70m

25GBASE-LR

9µm SMF / 10km

- 4x10G: 4 optikai szál vagy WDM
- Transceiver: QSFP+ a legelterjedtebb



Name	Cabling Type	Max Reach
40GBASE-CR4/10G DAC	Copper RJ45	7m
40GBASE-T	Copper RJ45	30m
40GBASE-SR4	OM3 MMF MTP/MPO	100m
	OM4 MMF MTP/MPO	150m
40GBASE-CSR4	OM4 MMF MTP/MPO	400m
40GBASE-SR	OM4 MMF LC duplex	150m
40GBASE-LR4	SMF LC Duplex	10km
40GBASE-ER4	SMF LC Duplex	40km
40GBASE-LX4	OM3/OM4 MMF	150m
	SMF	2km
40GBASE-PLR4	SMF MTP/MPO	10km
40GBASE-LR4L	SMF LC duplex	2km
40GBASE-PLRL4	SMF MTP/MPO	1.4km



# 100G



- Még nagyobb sűrűség elérése a cél
- Kétféle megvalósítás:
  - 10G – 40G - 100G
  - 25G – 100G



- Transceivererek:
  - CFP-100G: 10x10Gbps
    - 802.3ba
  - QSFP28: 4x 25Gbps WDM
    - 802.3bj



CFP



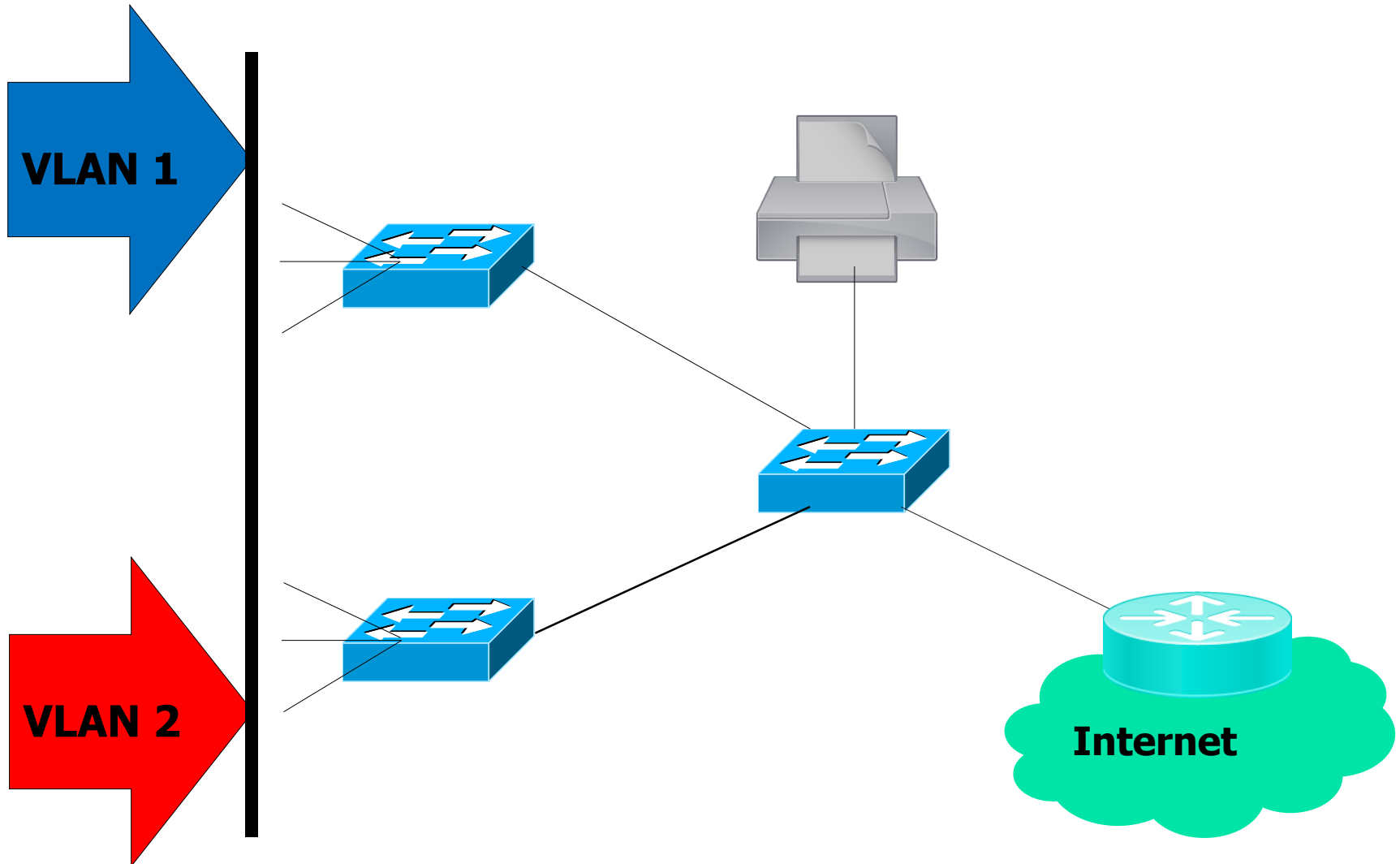
QSFP28





# VLAN-ok

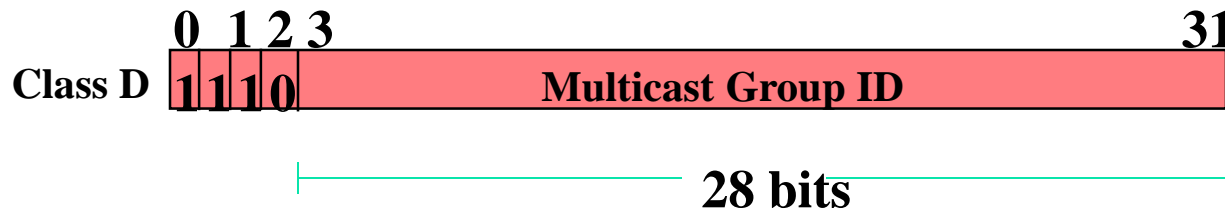
# VLAN





# Multicast és Ethernet

# Multicast címzés



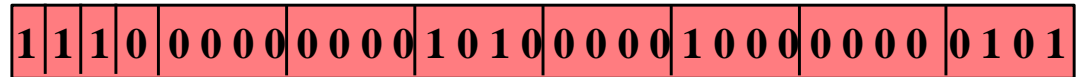
- Internet Assigned Numbers Authority (IANA)
- 224.0.0.1-224.0.0.255-->Reserved
- **224.0.1.0-238.255.255.255-->Multicast Group**
- 224.0.0.1: All multicast-capable hosts group
- 224.0.0.2: All multicast routers group
- 224.0.0.4: All DVMRP routers

# Address Mapping



**Class D Address 224 . 10 . 8 . 5**

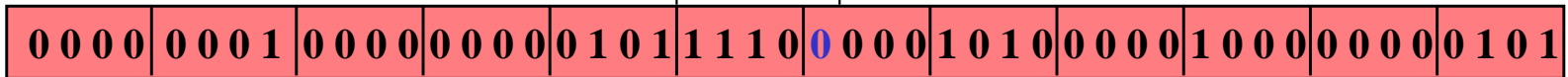
**E 0 0 A 0 8 0 5**



Not used

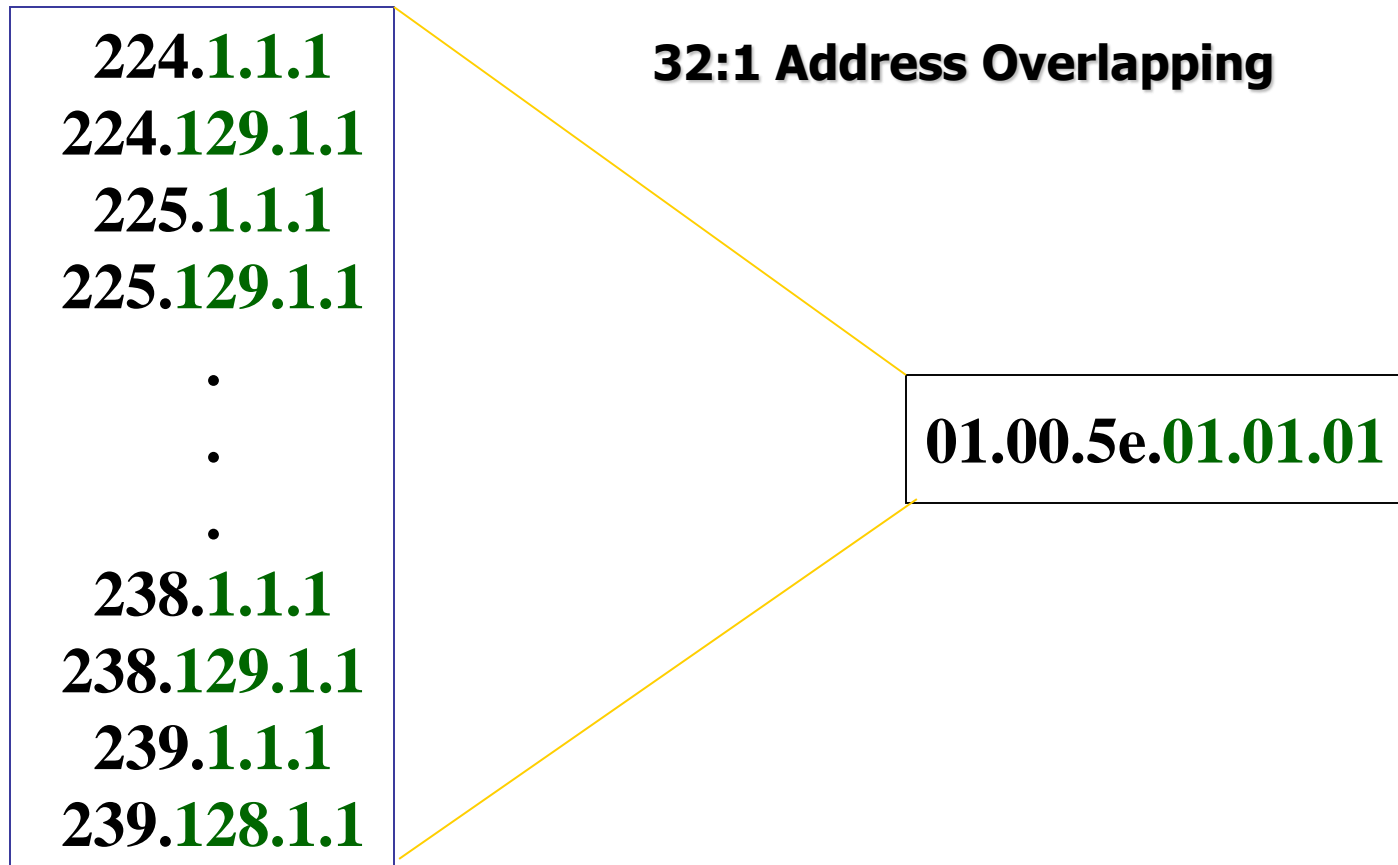
Low-ordered 23-bits mapped

**Ethernet Multicast Address**



**0 1 0 0 5 E 0 A 0 8 0 0 5**

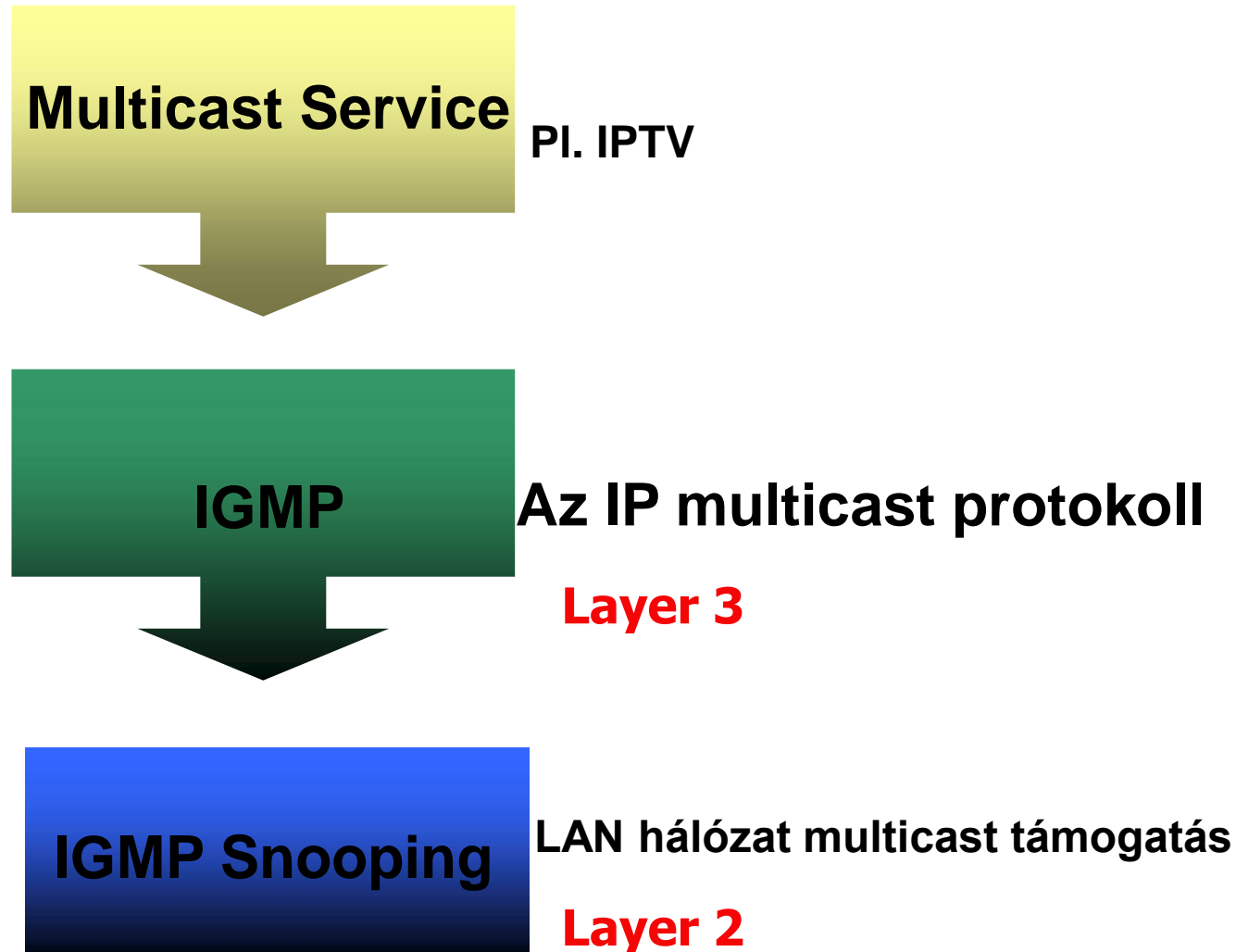
# Címek átlapolása



# Multicast Service



BME-TMIT

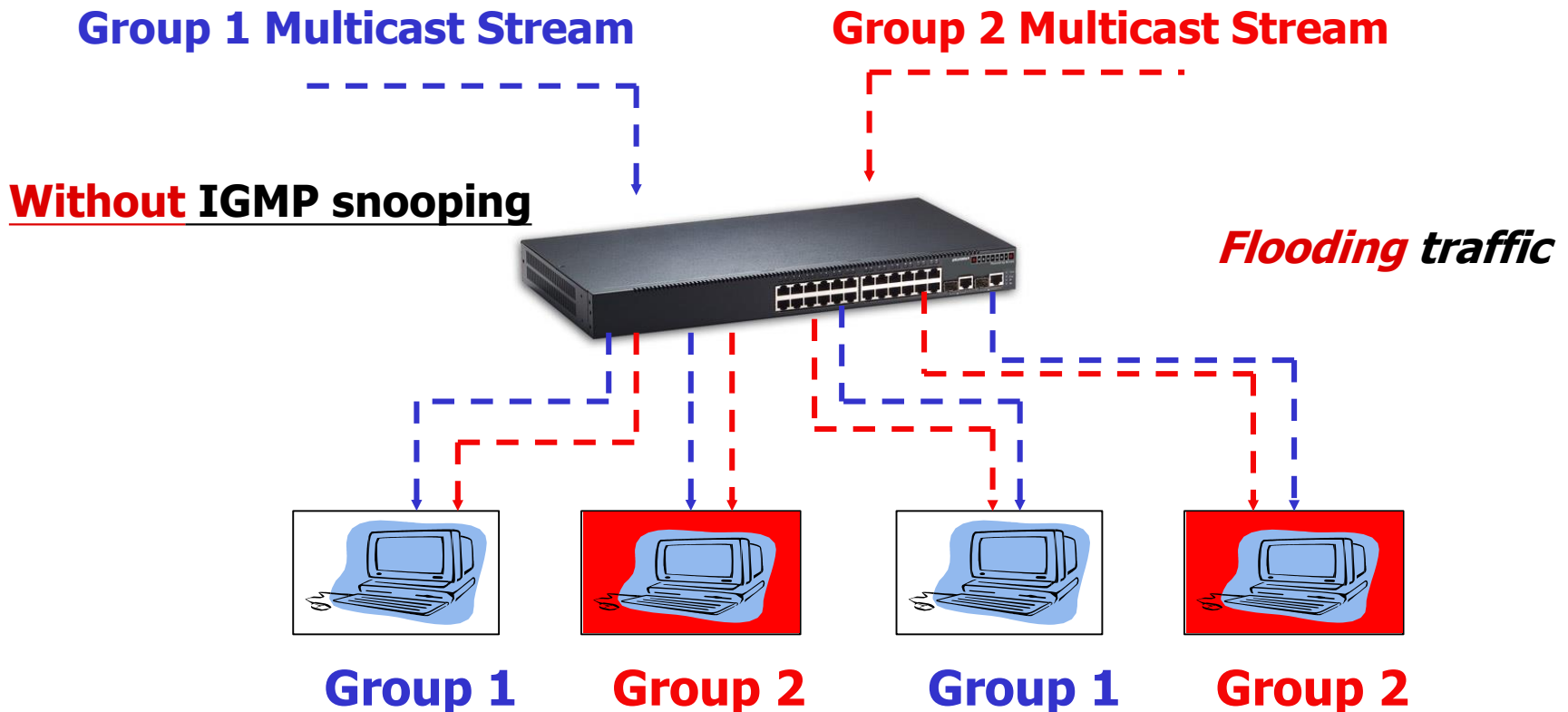


# Az IGMP Snooping



## ***IGMP Snooping - hatékony multicast Etherneten***

**All hosts need to handle the traffic whether they need it or not.**





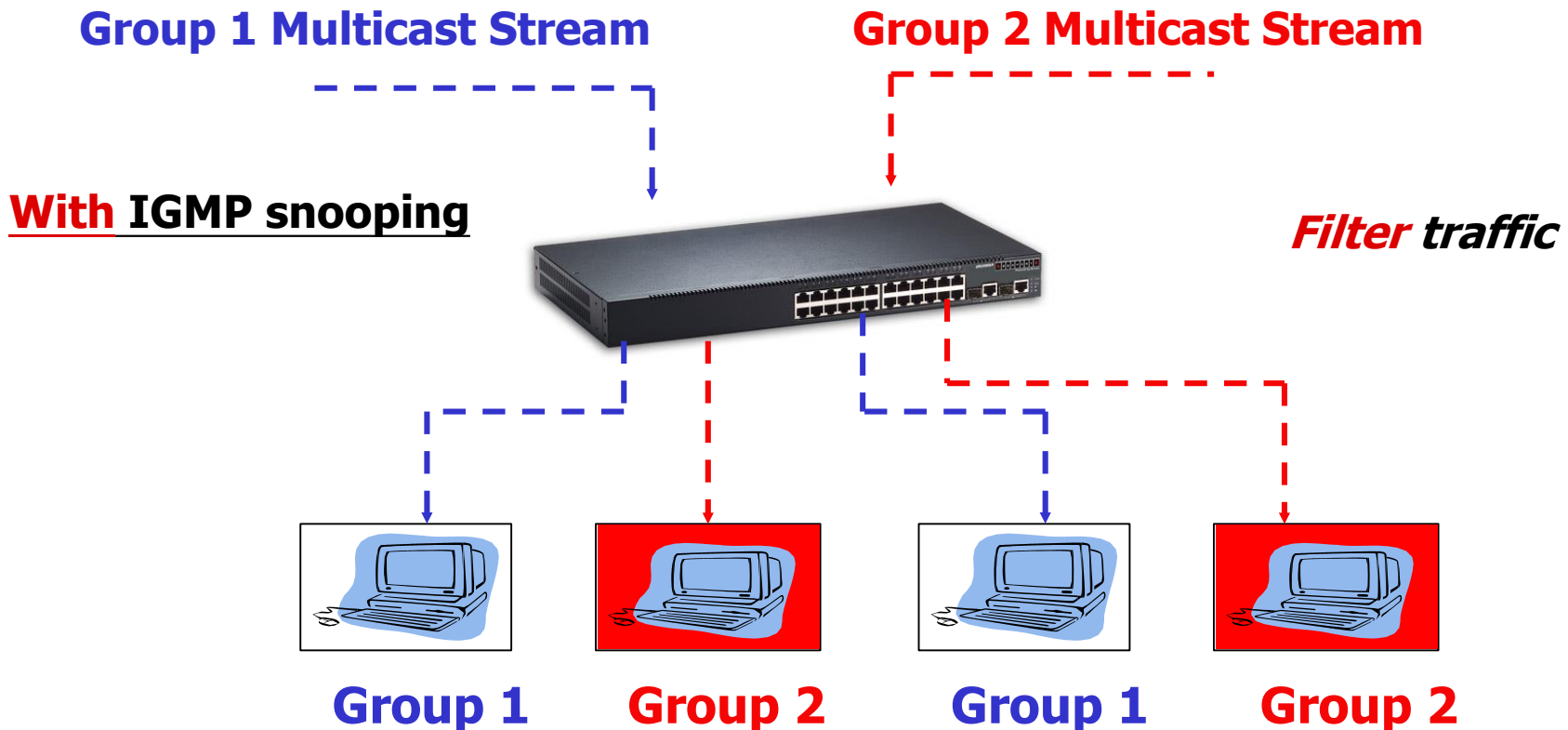
# Az IGMP Snooping



BME-TMIT

## ***IGMP Snooping - hatékony multicast Etherneten***

**Hosts only receive dedicated traffic belonging to the same group**



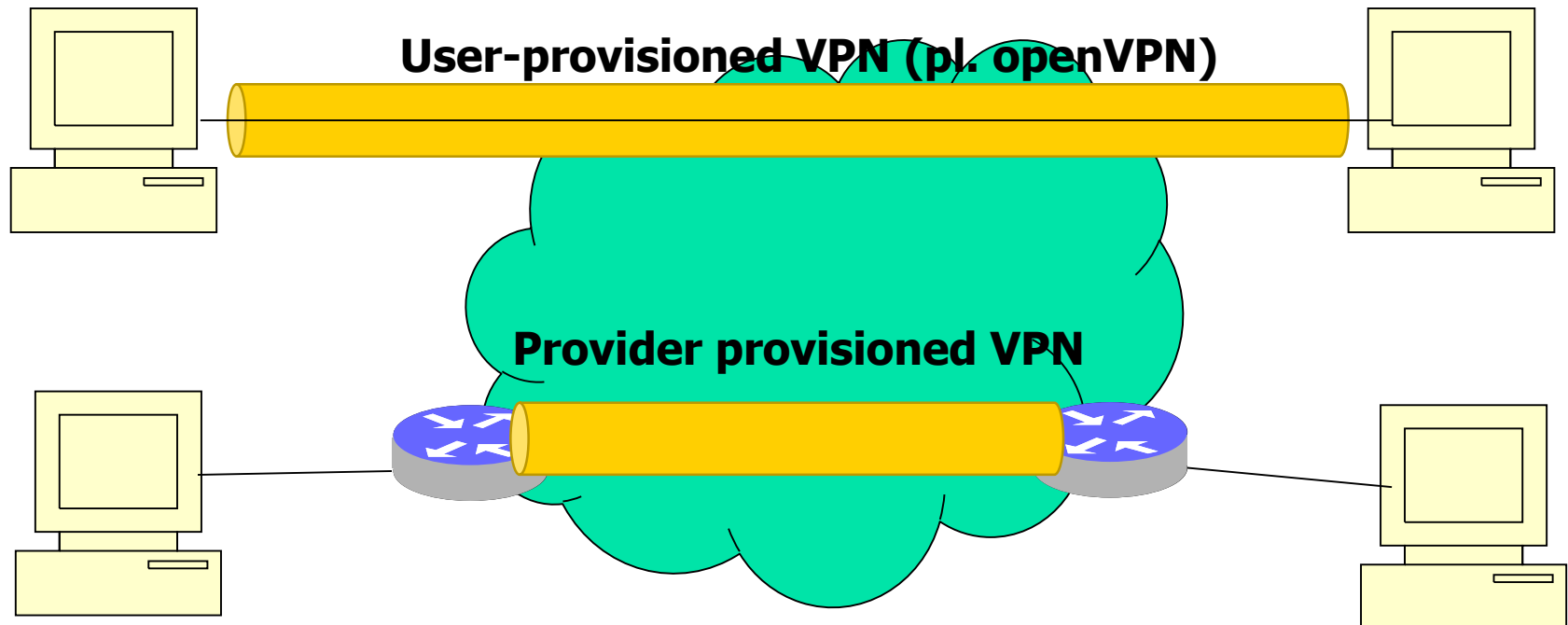
- Ethernet MAC szerint továbbít
  - MAC cím egyedi kell legyen
  - A bridge megtanulja a forrást – mi van ha 2 egyező cím van?
- Mac cím egyediség – nem garantálható
  - Ki lehet cserélni könnyen
- MAC „spoofing” – a MAC címek manipulálása
  - Forgalom eltérítés
  - MAC szűrő kikerülése
  - DOS támadás



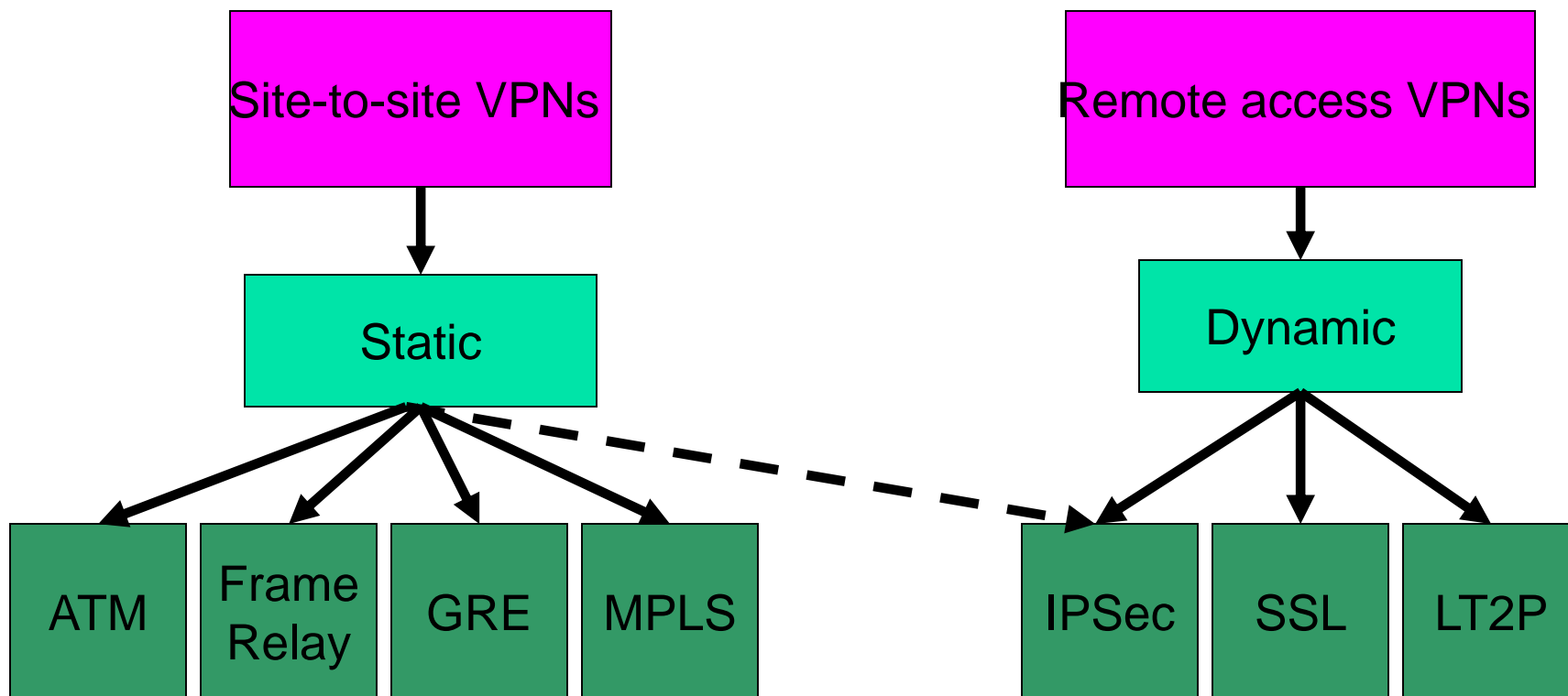
# VPN-ek

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

- L2 és L3 VPN példa



# VPN típusok

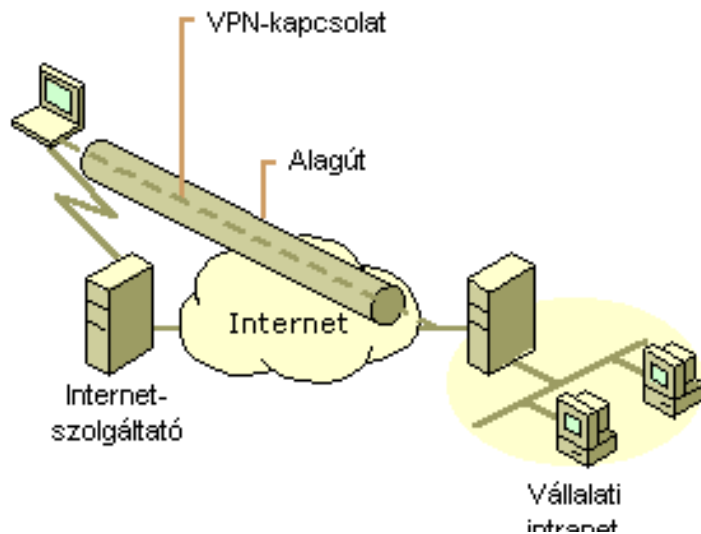


- Bérelt vonal – nem költséghatékony
- Internet – olcsó kommunikáció
  - Nem biztonságos!
- Megoldás: biztonságos kapcsolat kialakítása az Interneten kódolt alagutak használatával
  - Egy vagy több kliens használhat egy alagutat
  - A biztonságot a kódolás adja
  - Minőiségbiztosítás az Internet szolgáltatótól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

# VPN az ügyfél típusa szerint

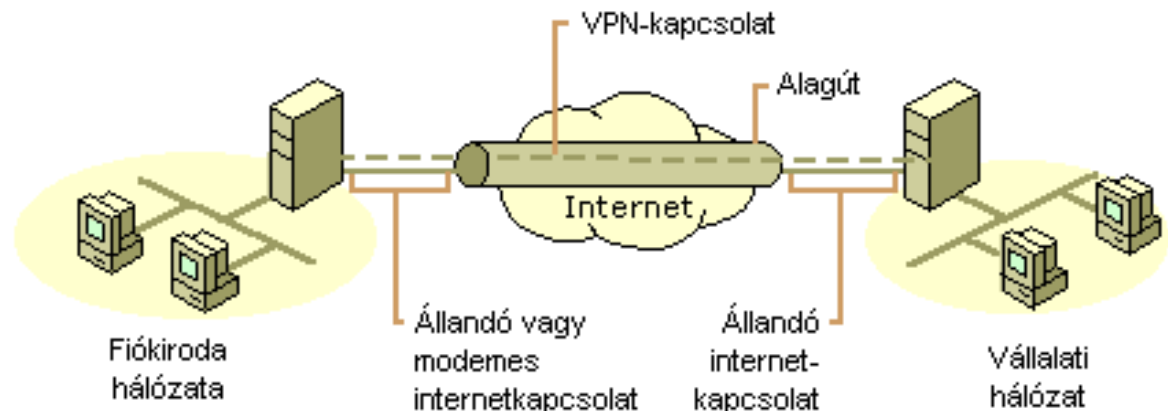


BME-TMIT



**Ügyfél-kiszolgáló  
(Client-2-Router)**

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

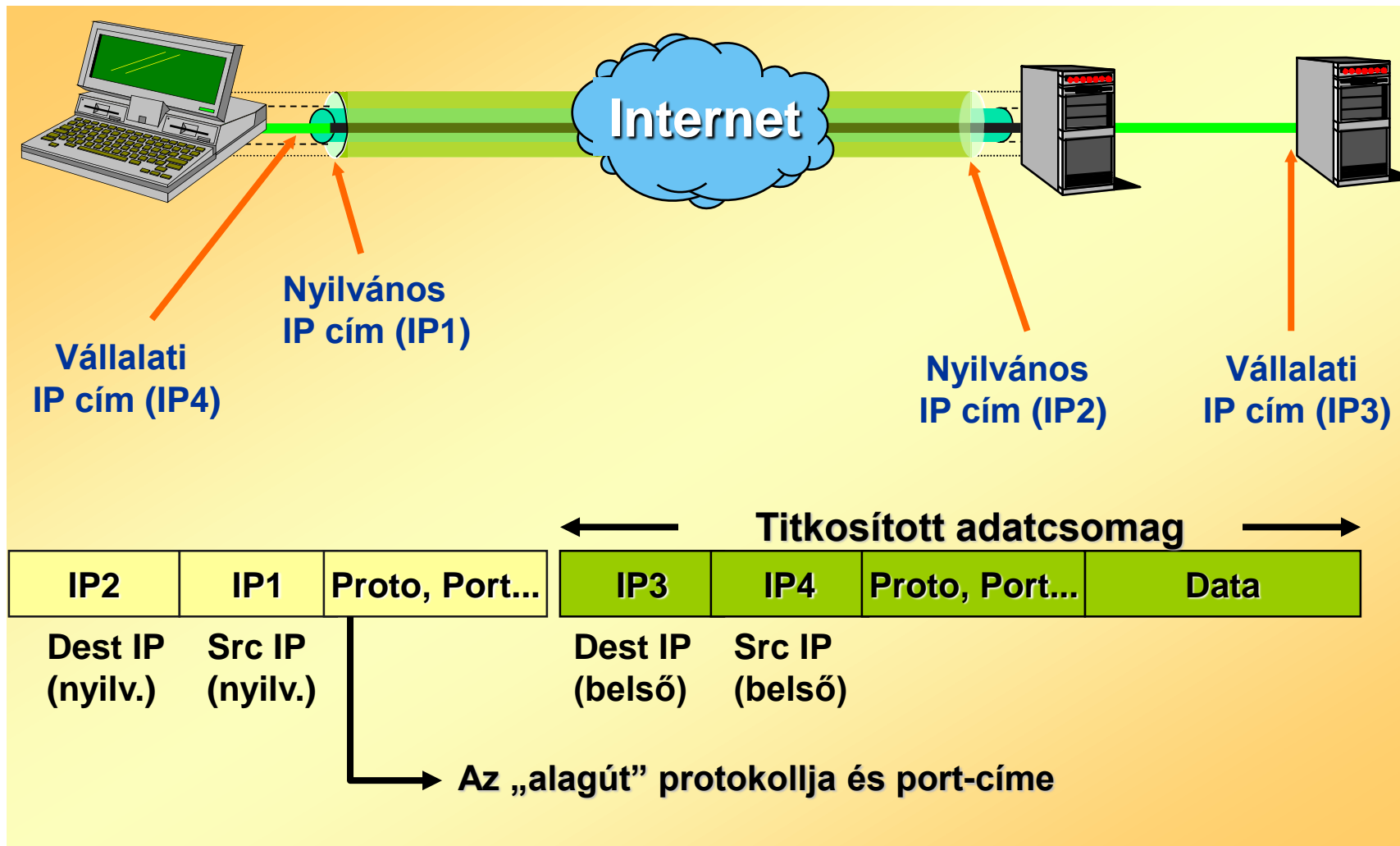




# Alagúthálózat



BME-TMIT



- 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



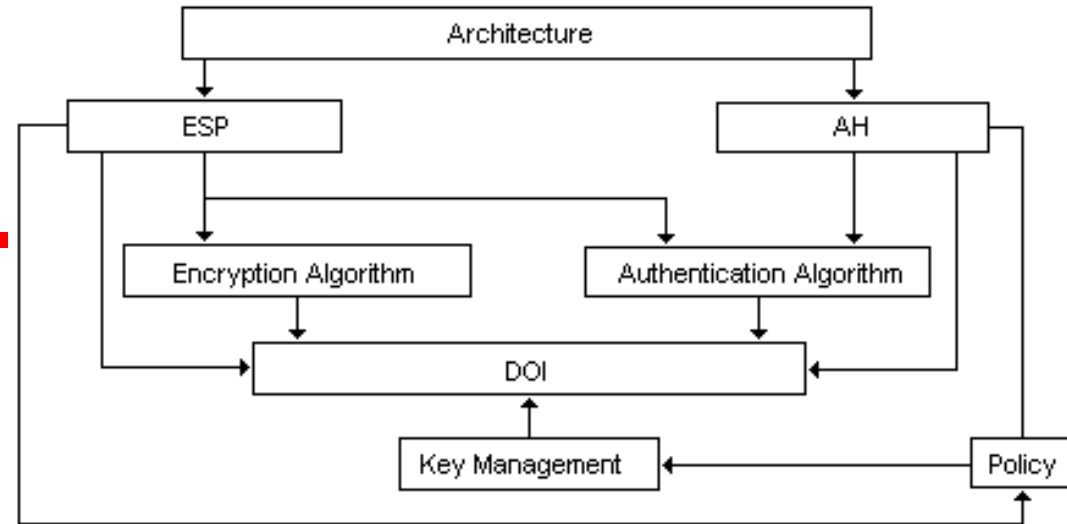
BME-TMIT

- 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:

- 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:
  - Internet 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



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

- 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.

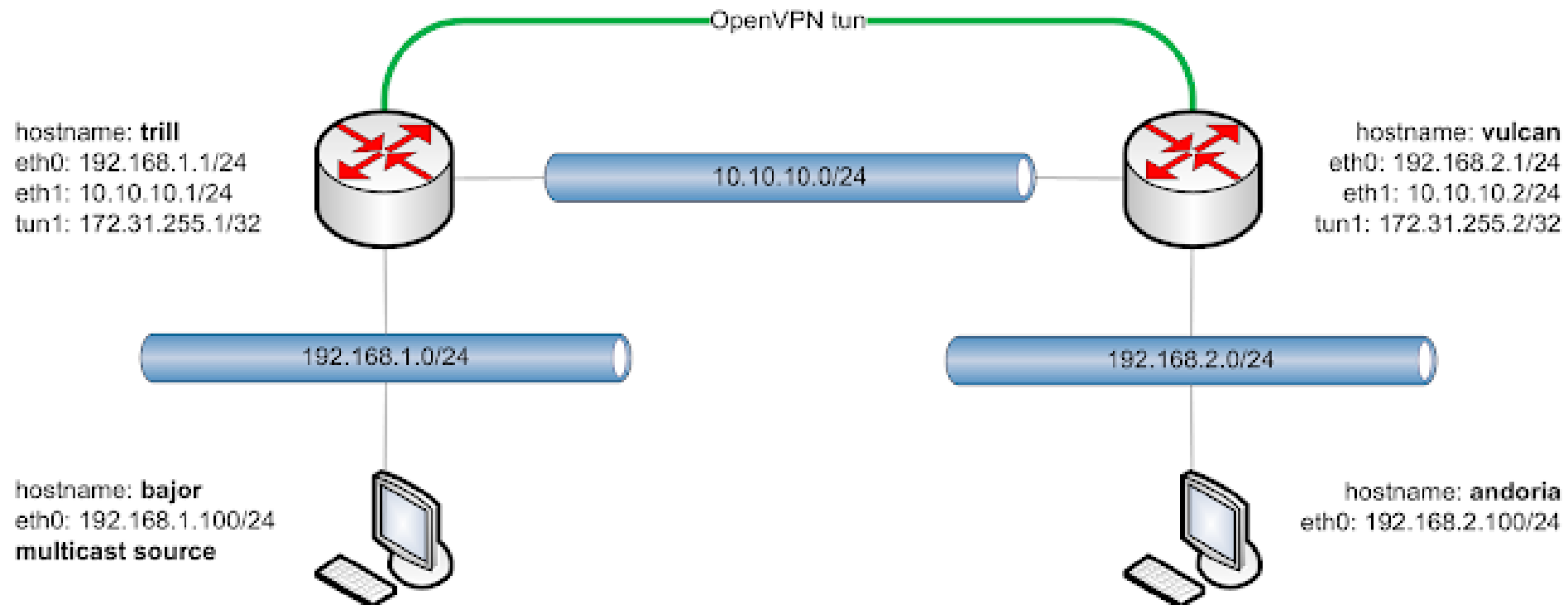
- Mikor SSL és mikor IPSec VPN?
- Az SSL VPN egyszerűbb
  - Felhasználó által menedzselhető
  - Egyszerűen konfigurálható
  - TCP – nem támogat QoS-t, UDP-t
- Az IPSec VPN komplexebb
  - Adminisztrátor állíthatja be (root jog)
  - IP szintű – QoS támogatás lehetséges
  - Transzparens a felhasználó felé



# Példa: OpenVPN



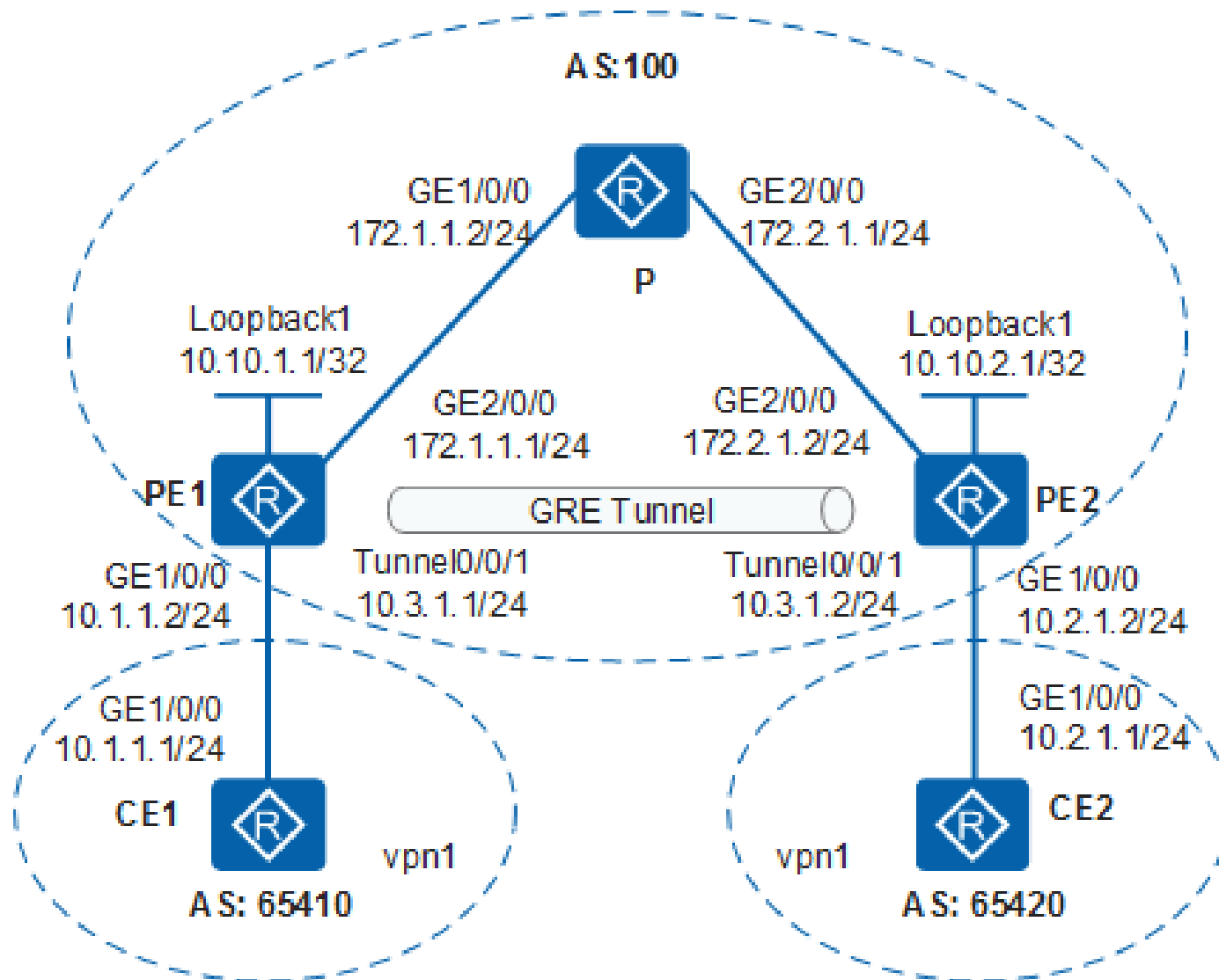
BME-TMIT





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

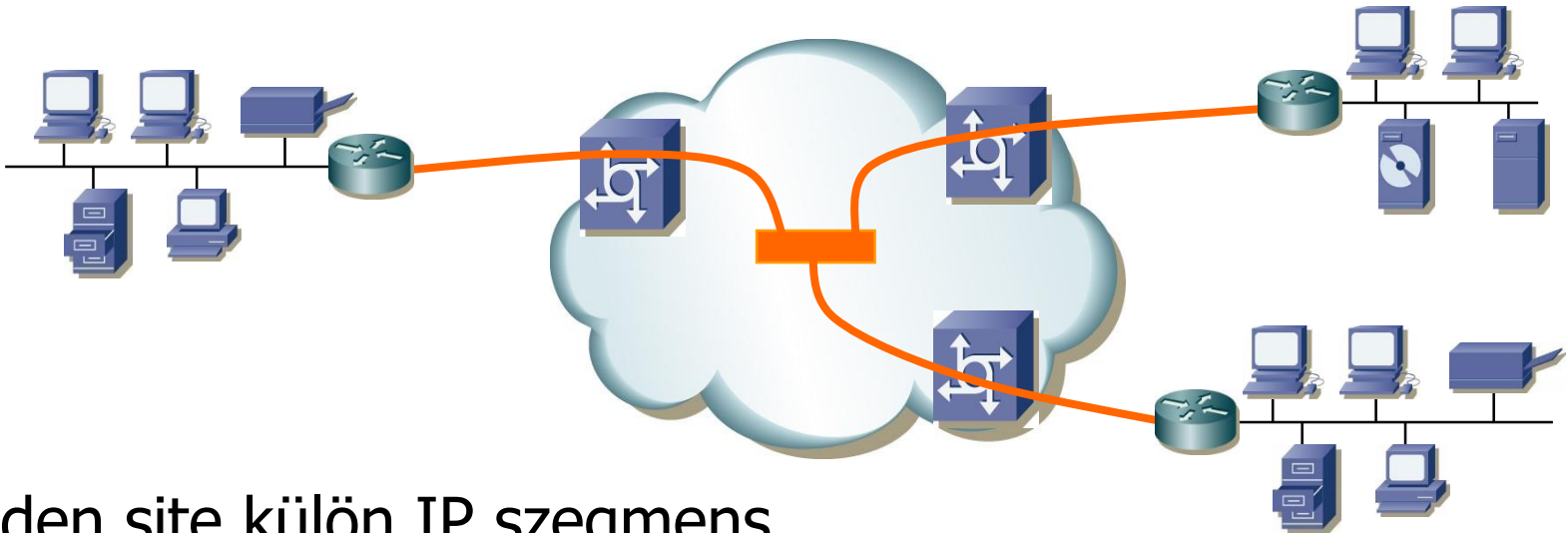
# Példa: L3 (IP) VPN



# Router Inter-connect



BME-TMIT

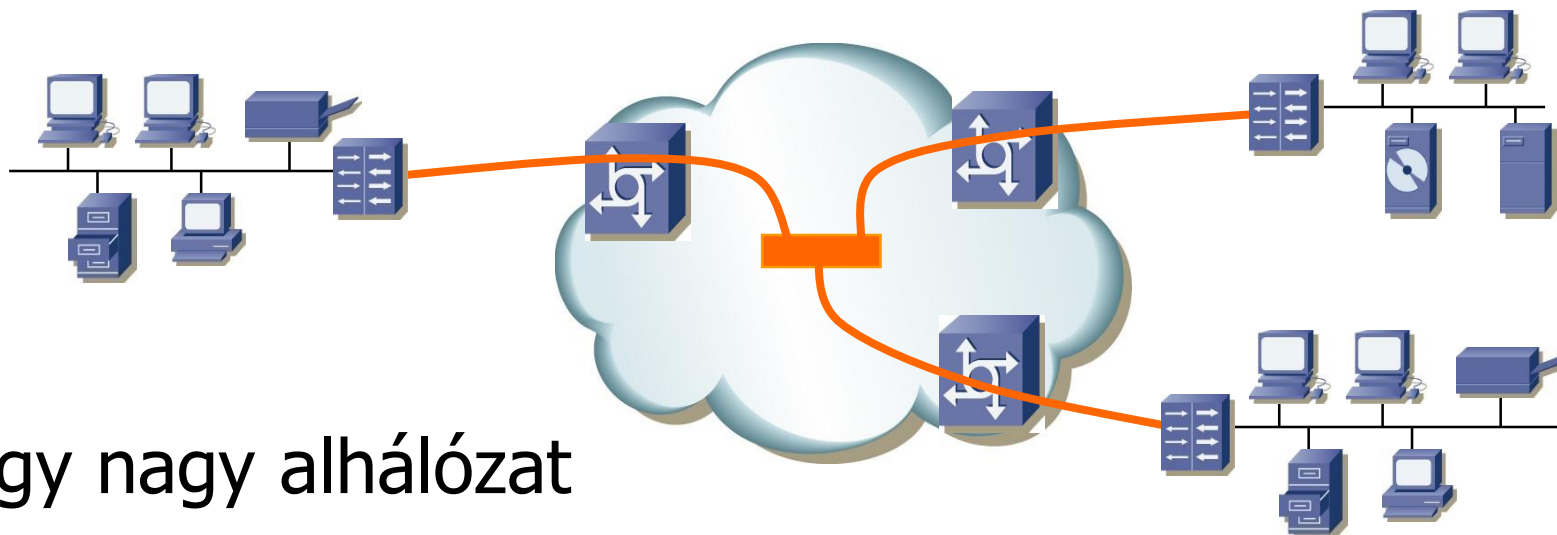


- Minden site külön IP szegmens
  - A routerek routolnak
- Beállítások
- Kliens:
  - routerek címzése – default GW/útvonal a többi site felé
- Szolgáltató:
  - UNI alap paraméterek (BW, QoS:delay, loss), site-ok

# Switch Inter-connect



BME-TMIT



- Egy nagy alhálózat
  - Közös címtartomány
- Beállítások
  - Kliens: -
  - Szolgáltató:
    - UNI alap paraméterek (BW, QoS:delay, loss), site-ok
    - MAC cím korlát/site, Broadcast/MC korlátok, L2CP kezelés

# LTE – Backhaul

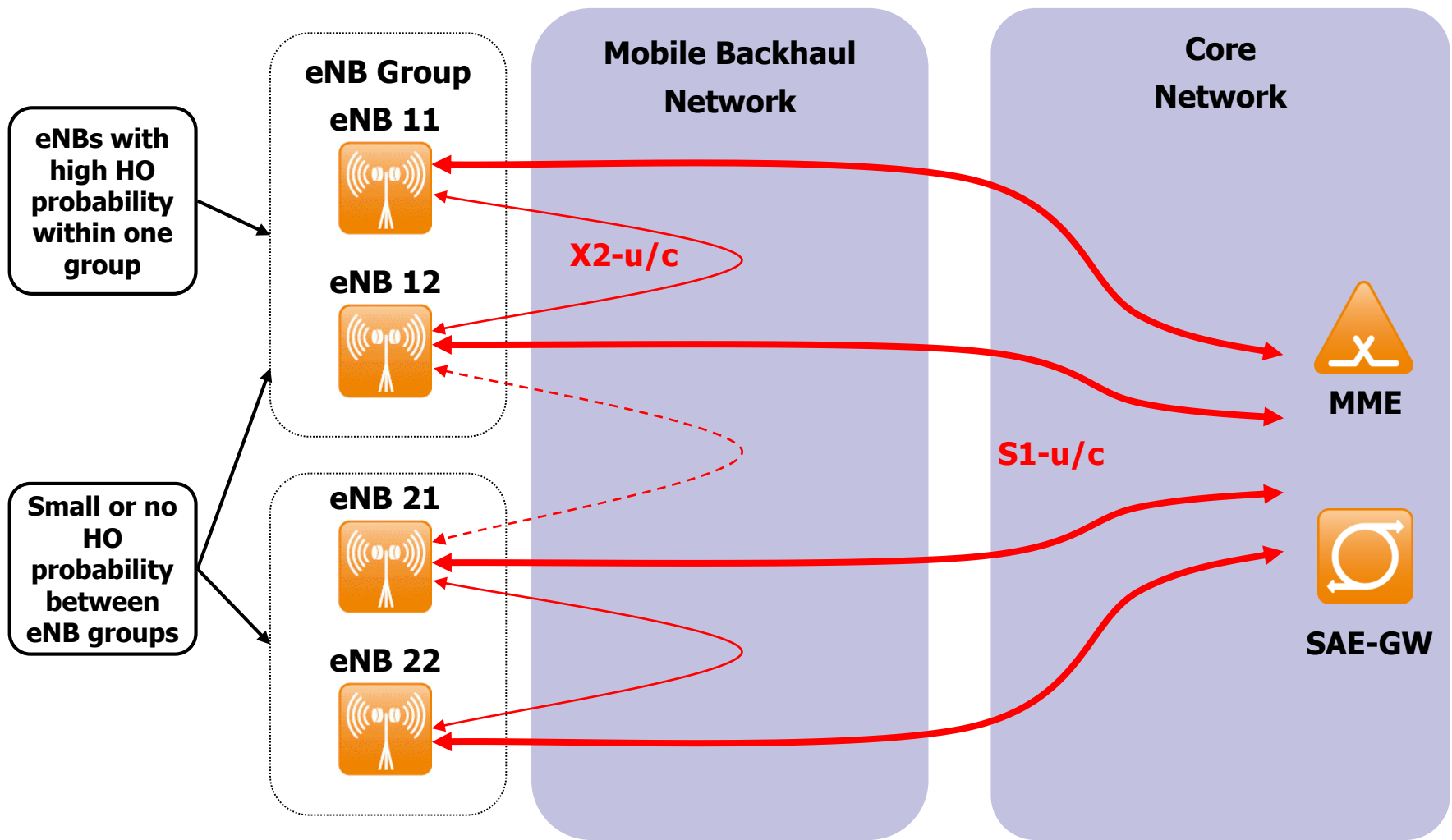
bérelt vonali és VPN  
szolgáltatások



M Ū E G Y E T E M 1 7 8 2

**BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM  
TÁVKÖZLÉSI ÉS MÉDIAINFORMATIKAI TANSZÉK**

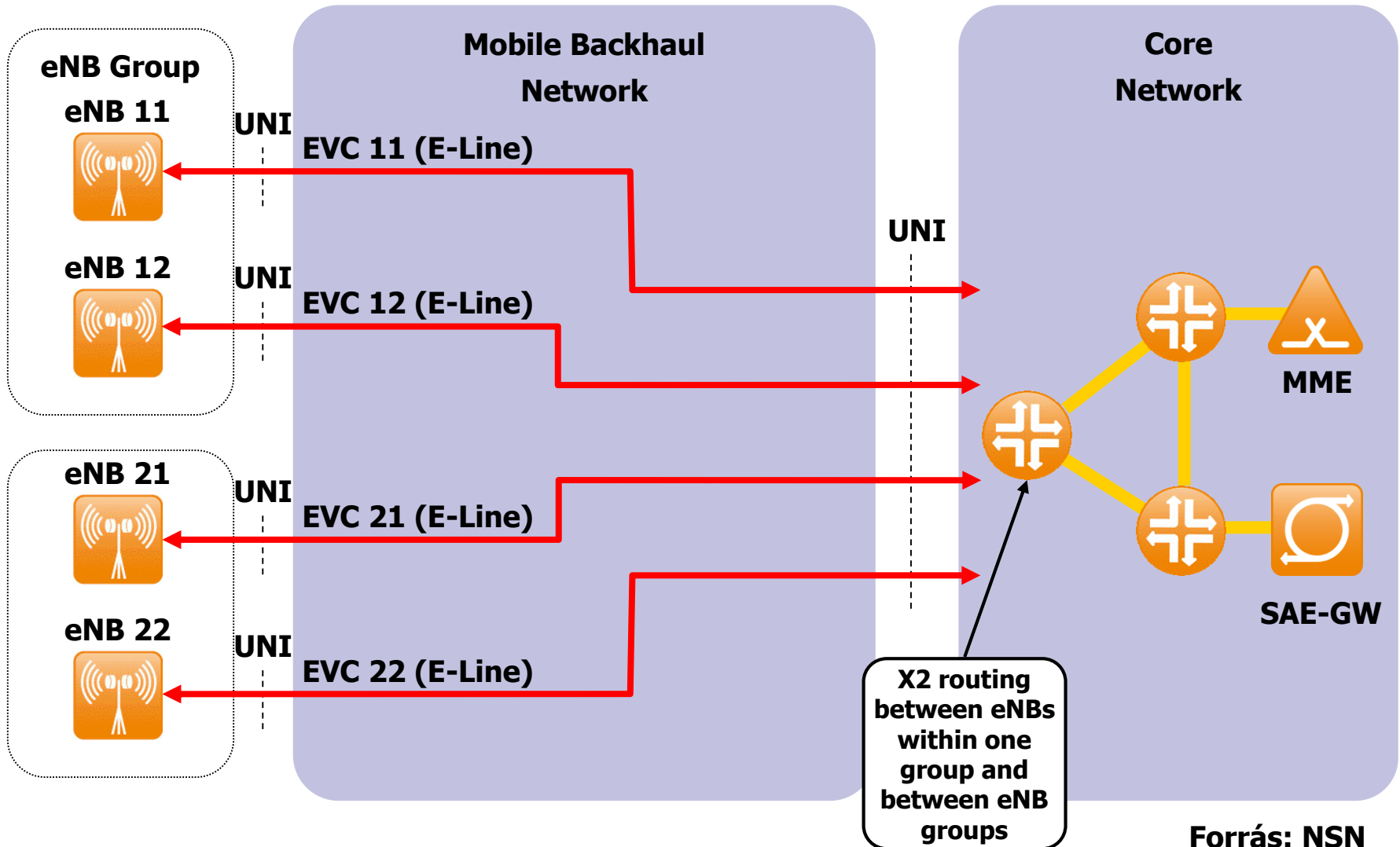
# LTE E2E Architecture and Connectivity



# L2 Mobile Backhaul - E-Line

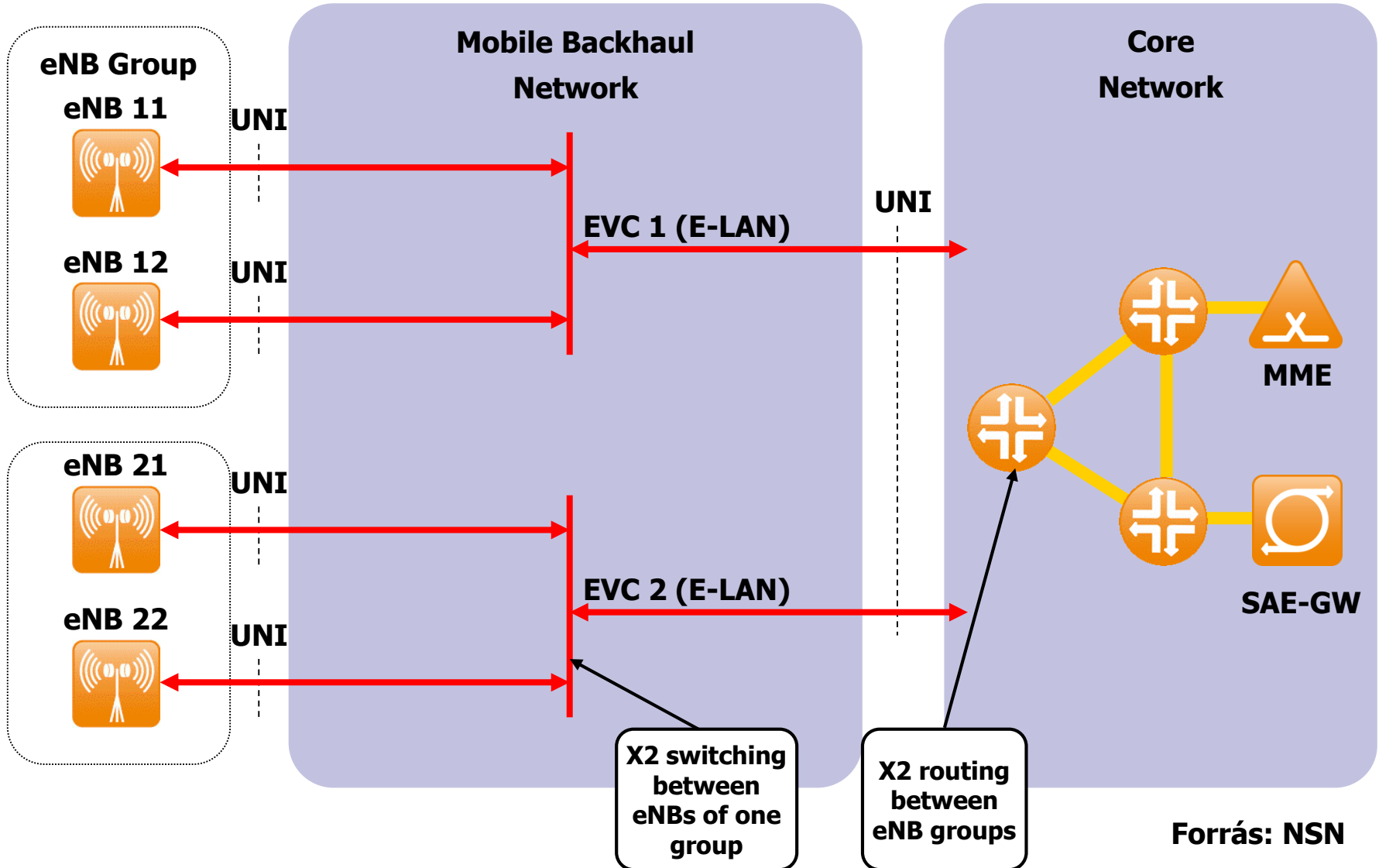


BME-TMIT





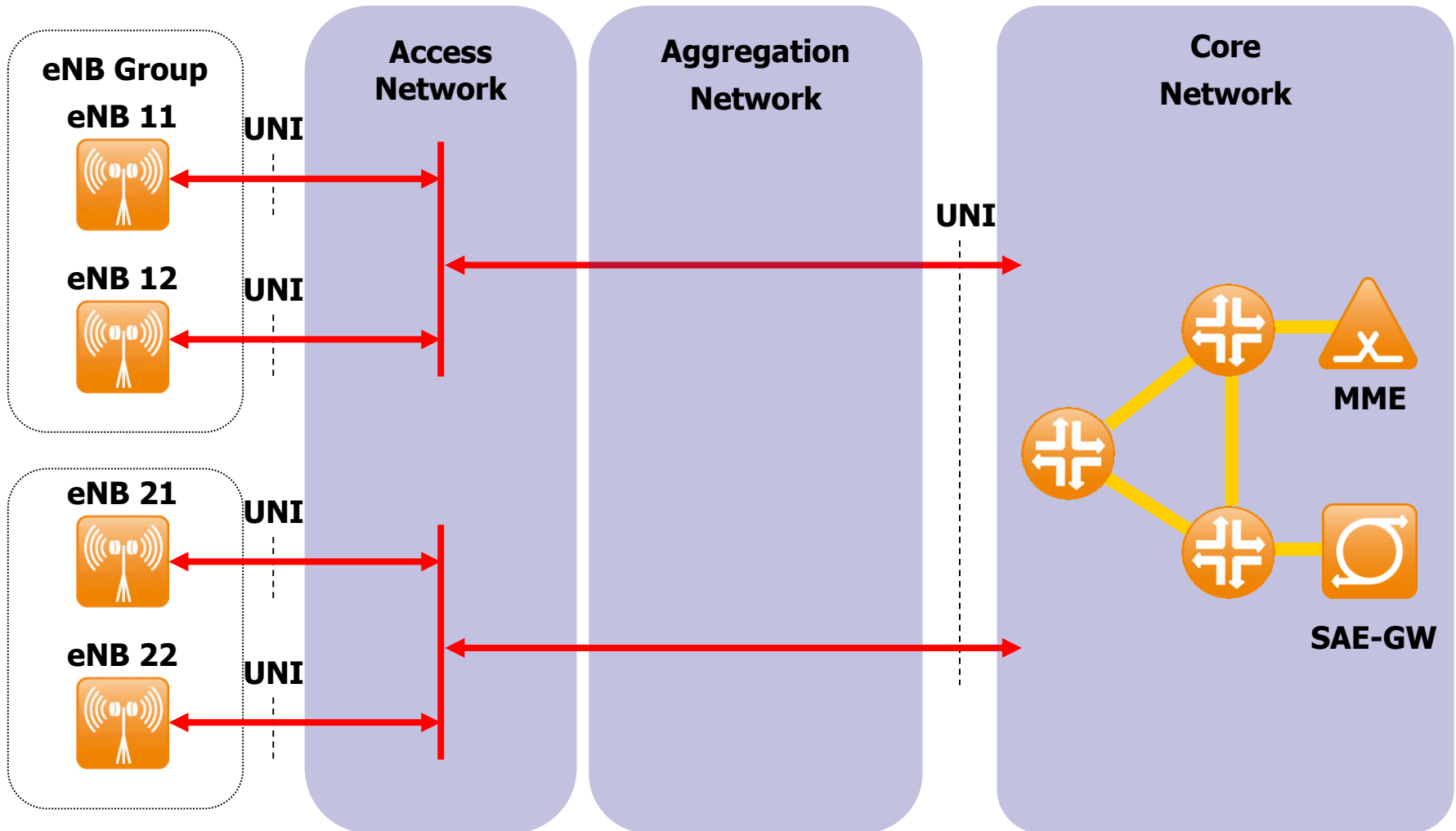
# L2 MBH - E-LAN



# L2 Access és Aggregációs hálózat – Logikai felépítés



BME-TMIT

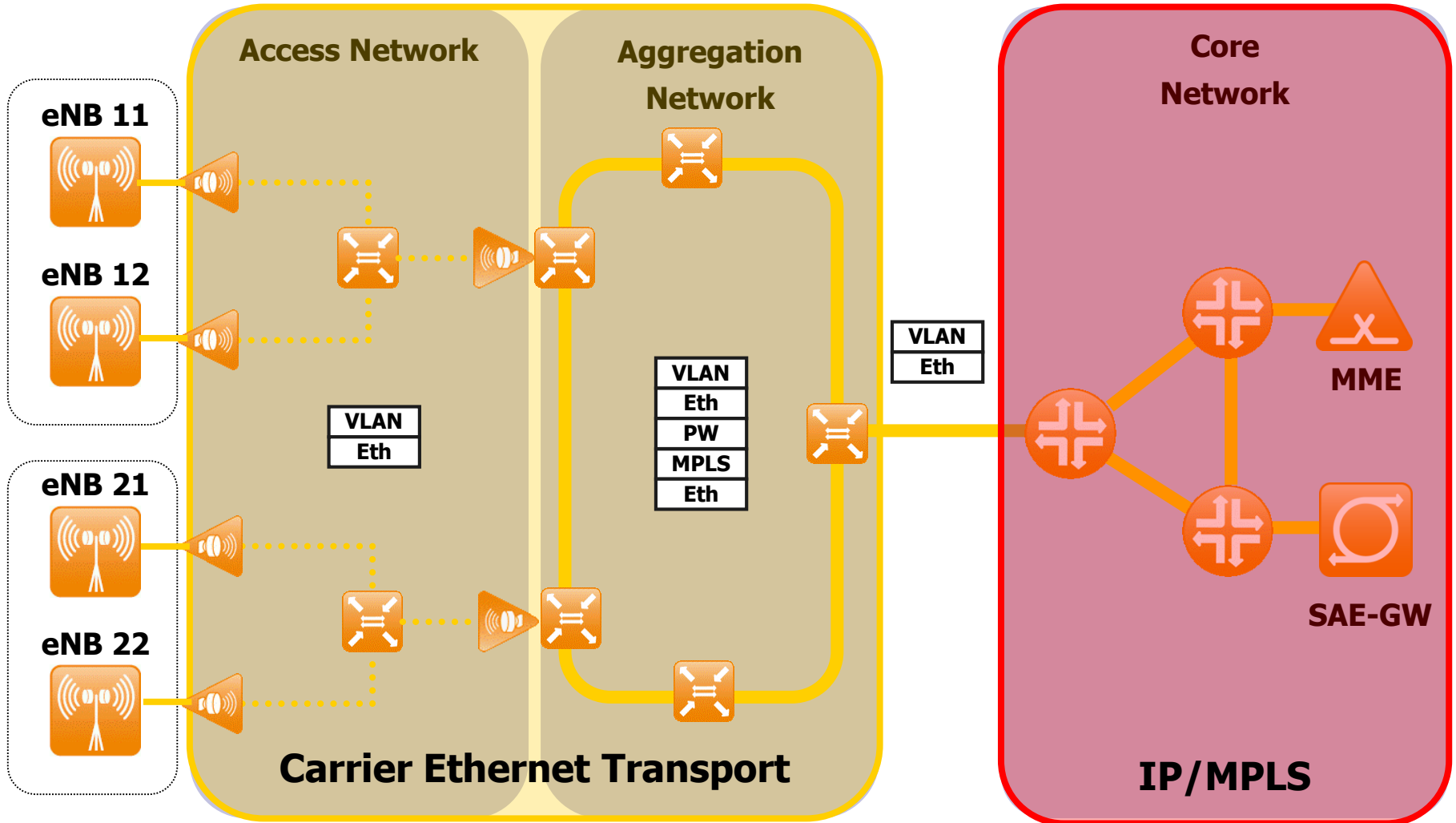


Forrás: NSN

# Carrier Ethernet Transport for Backhaul, IP/MPLS for Core



BME-TMIT



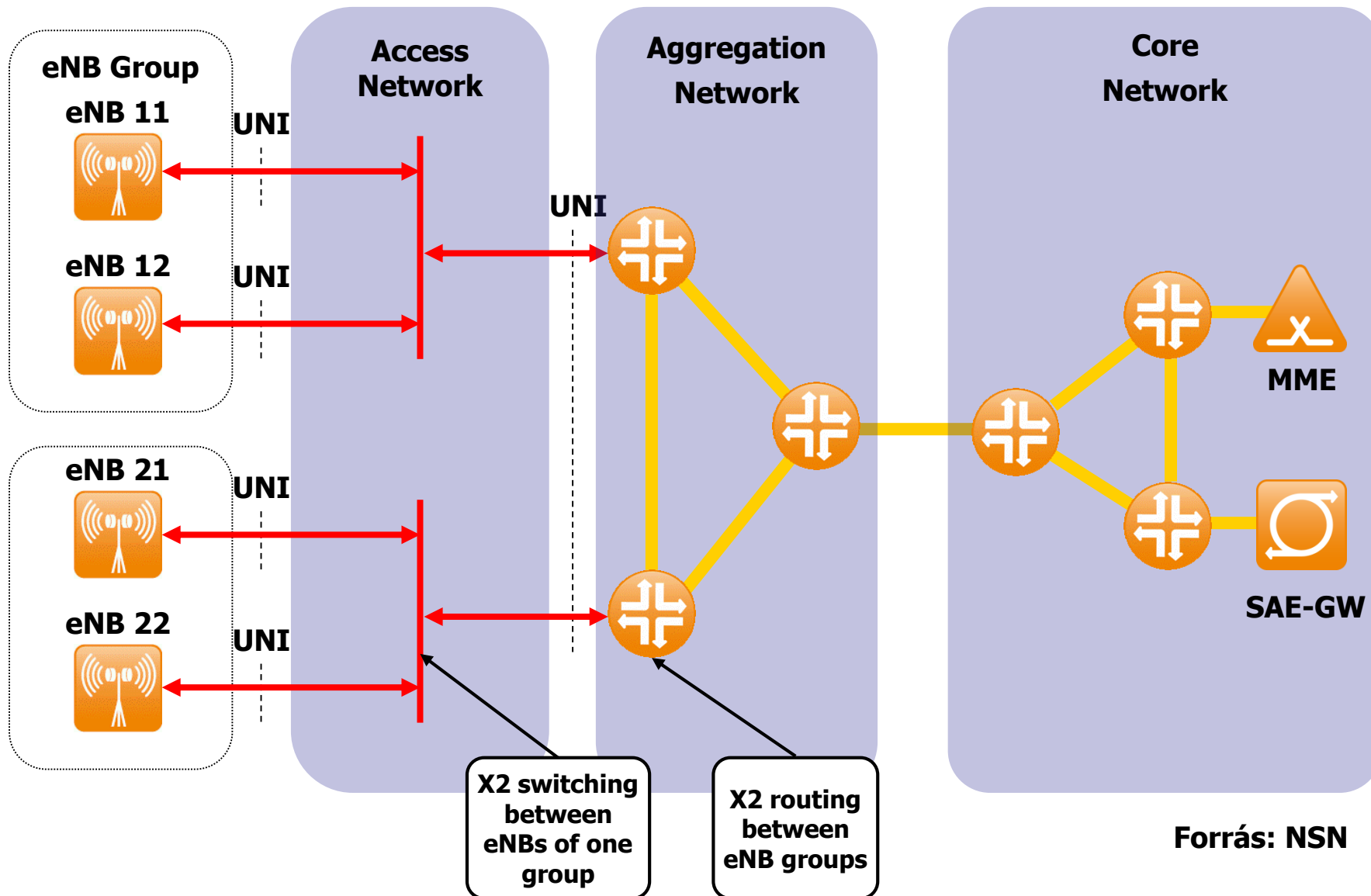
eNB / eNB group identification with VLAN

Forrás: NSN

# Alternatíva: L2 Access & L3 Hozzáférés



BME-TMIT





# Köszönöm a figyelmet!