IP címzés - gyakorlat

Moldován István

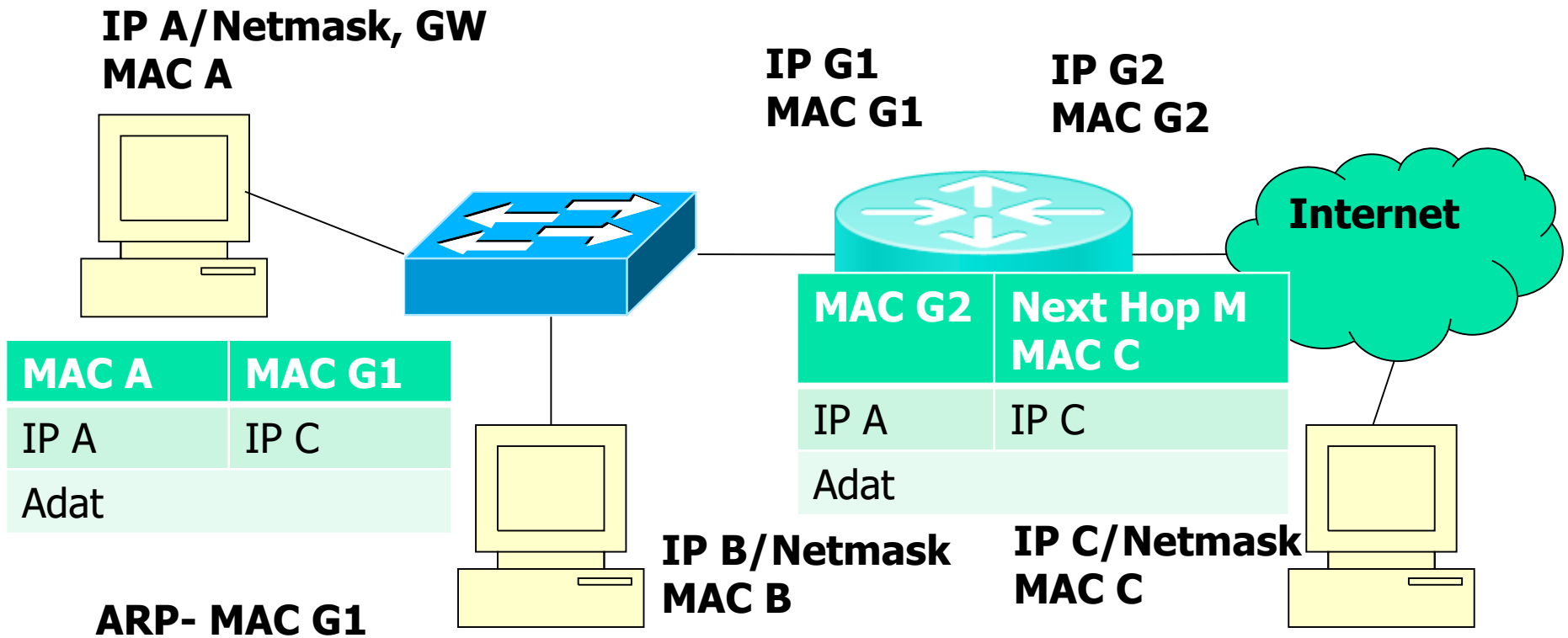
moldovan@tmit.bme.hu

BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
TÁVKÖZLÉSI ÉS MÉDIAINFORMATIKAI TANSZÉK

Áttekintés

- IP címzés (subnet)
  - 2 subnet 1 if?
  - Vlan interfesz routing
- L2 és L3 VPN
- QoS
  - Linux PC

IP+Ethernet működés - Címek



IP A, B, G1: ugyanaz a subnet
IP G2, C: más subnet

Egy alhálózat?

- IP A, NETMASK
- IP C

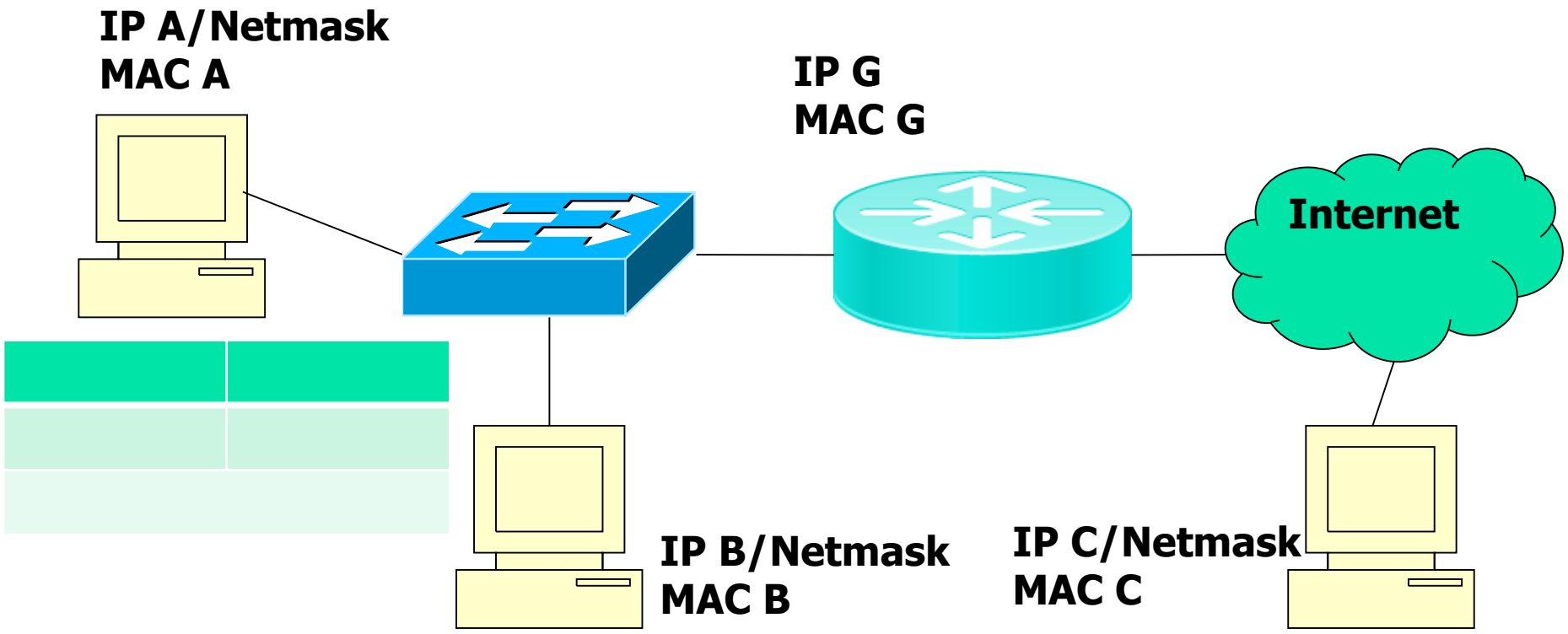
- A: 192.168.1.5, 255.255.255.0
- B: 192.168.1.17
- C: 192.168.2.5
- N 11111111.11111111.11111111.00000000
- A 11000000.10101000.00000001.00000101
- B 11000000.10101000.00000001.00010001
- C 11000000.10101000.00000010.00000101

/26 alhálózat példa

- A 192.168.1.15/26 255.255.255.192
- B 192.168.1.71

- N 11111111.11111111.11111111.11000000
- A 11000000.10101000.00000001.00001111
- B 11000000.10101000.00000001.01000111
- 00 – 0-63
- 01 – 64-127
- 10 – 128-191
- 11 – 192-255

IP+Ethernet működés

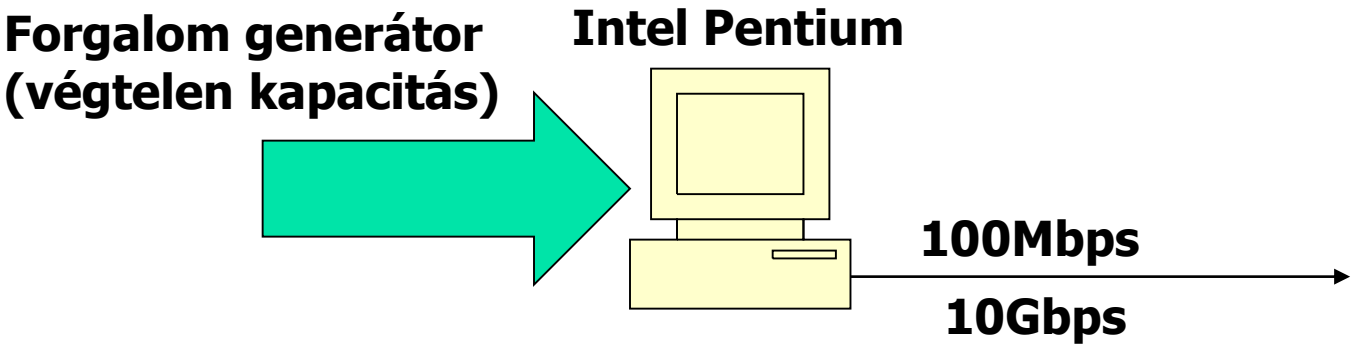


1. A->B – ugyanaz a subnet, cél MAC: B
2. A->C – nem lokális háló, GW-en keresztül
   - cél MAC: G

MAC cím feloldása: ARP

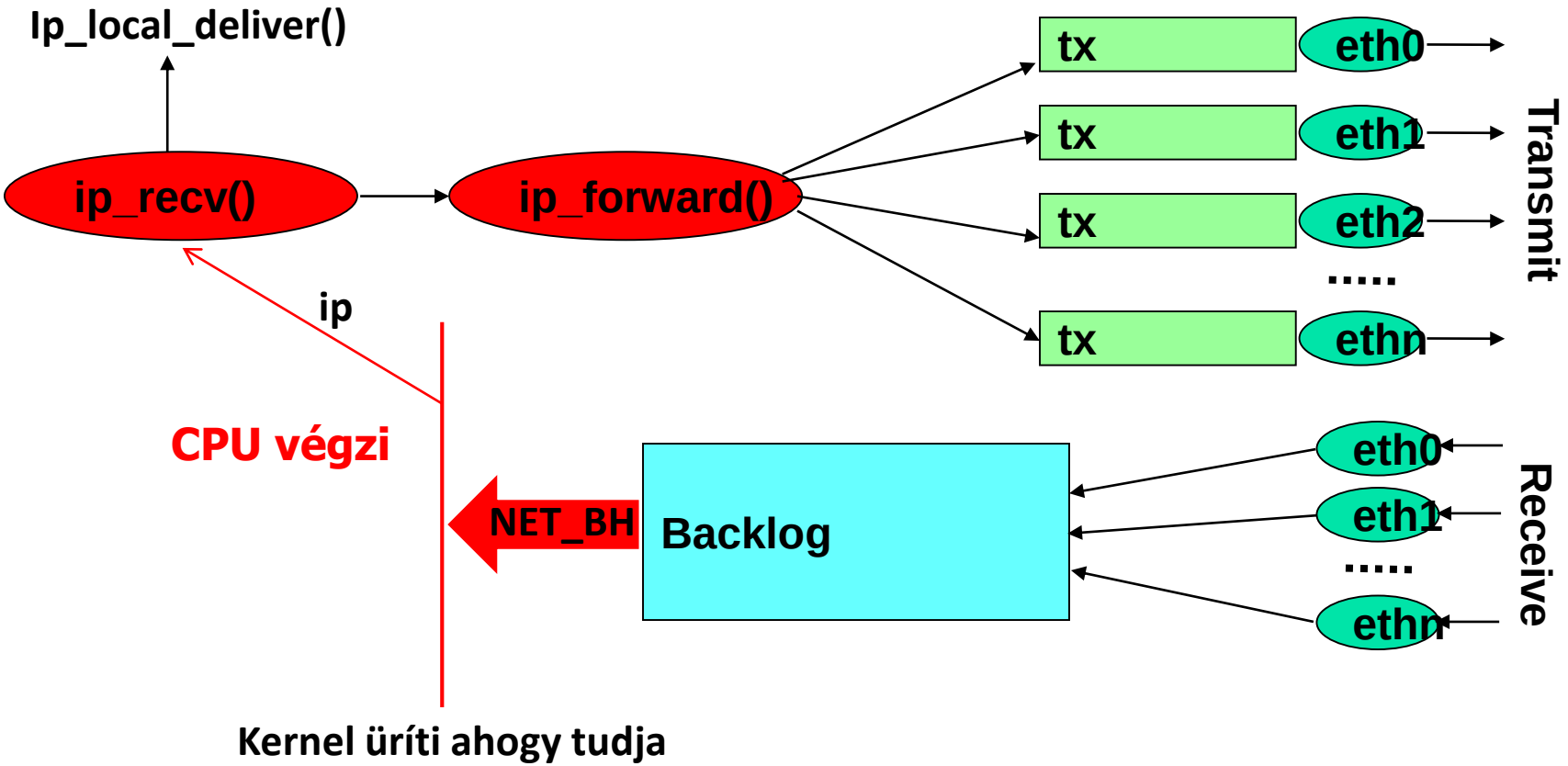
QoS példa

- Szűk keresztmetszet kialakulása
  - Ethernet interfész
  - Processzor



  - 100Mbps – a PC bírja, a korlát az interfész
  - > 10Gbps – a PC nem képes meghajtani az interfészt maximális sebességgel

Hol alakul ki szűk keresztmetszet - Linux

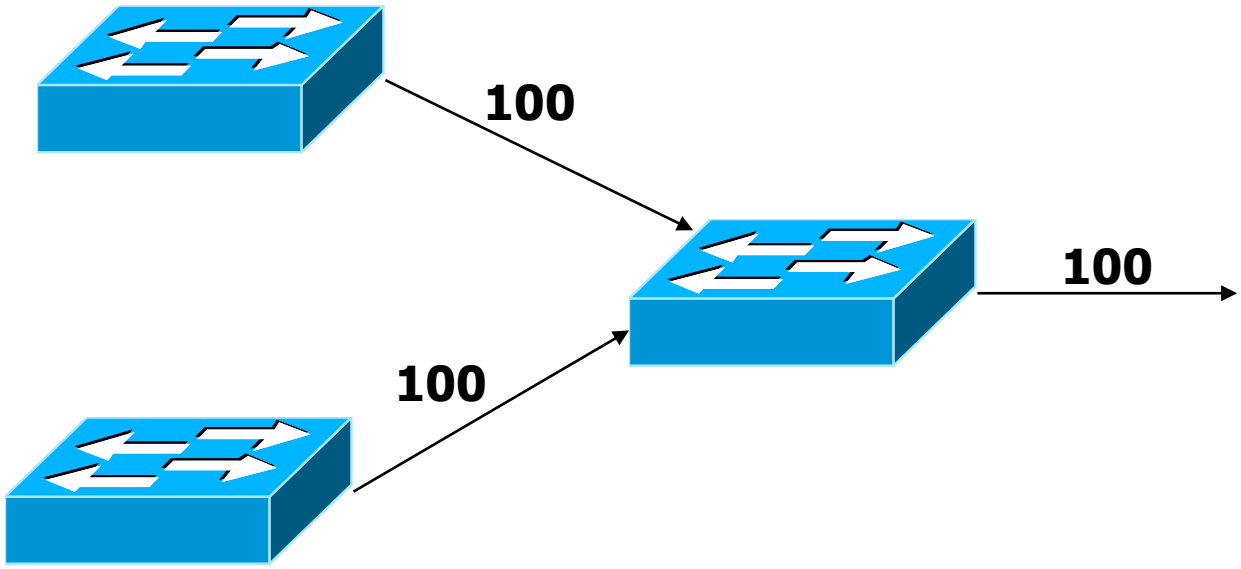


Szűk keresztmetszet:

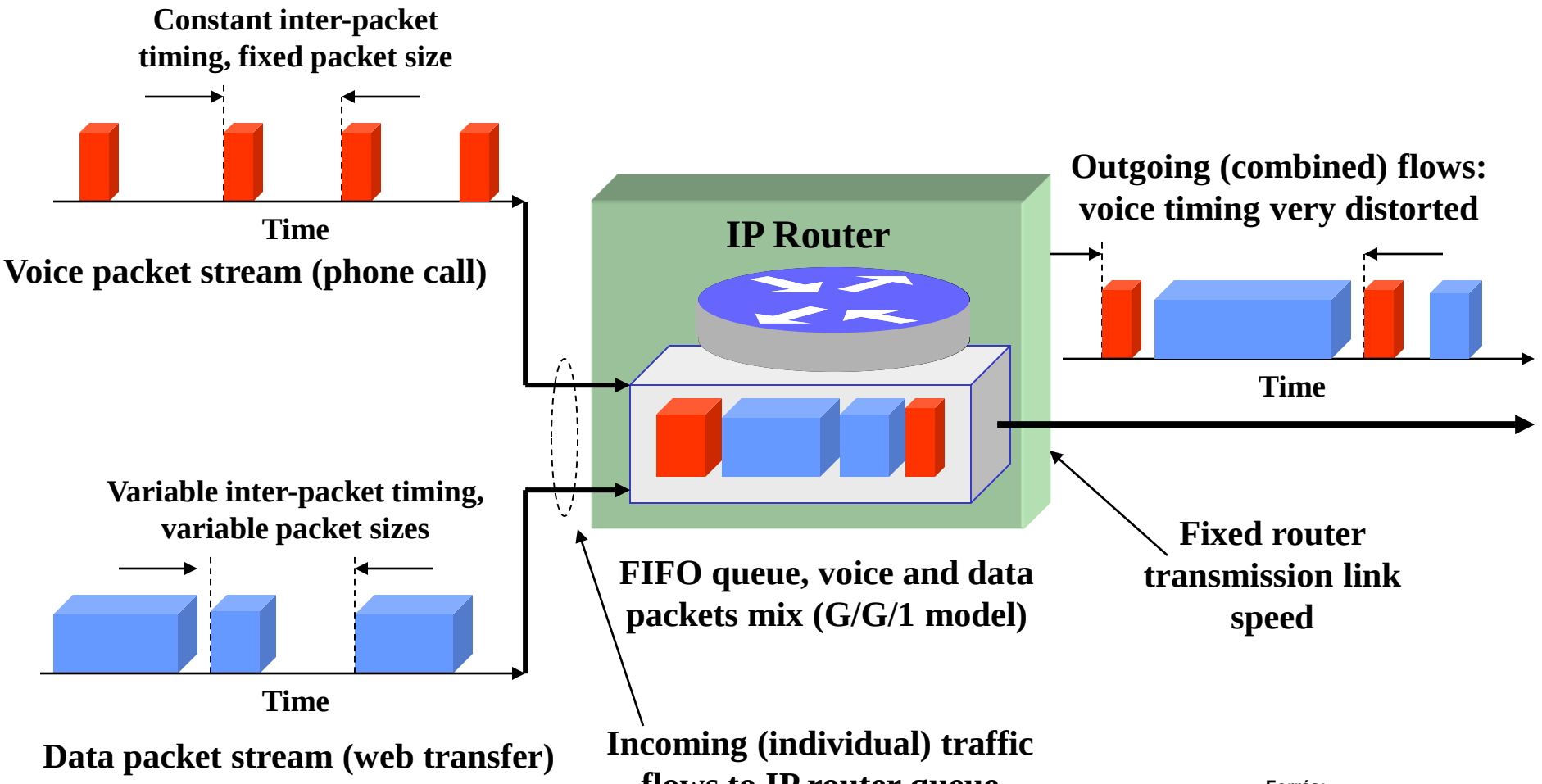
Interfésznél: tx sorok

CPU-nál: backog

Ethernet szűk kereszt



„Best Effort" - aggregációs mechanizmus



Forrás:
Next Generation Networking Group,
CCNY of CUNY

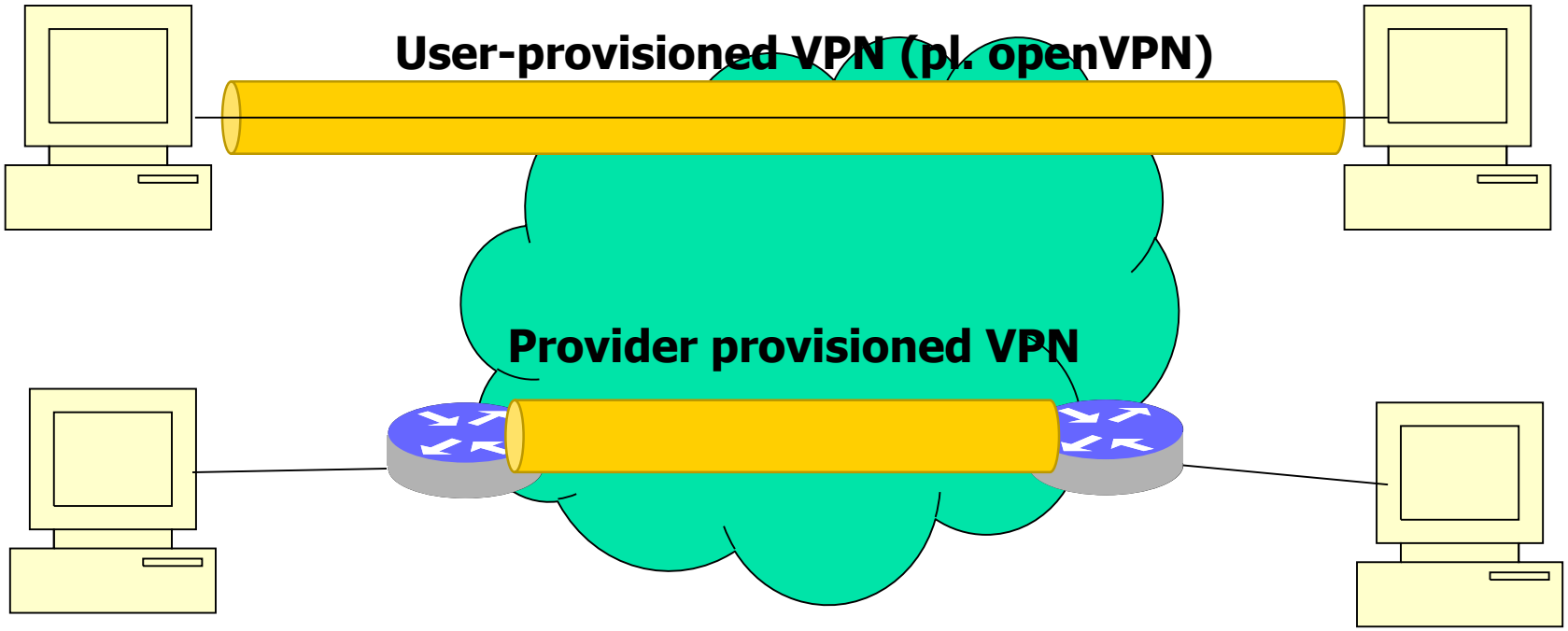
VPN-ek

Virtuális Magánhálózatok

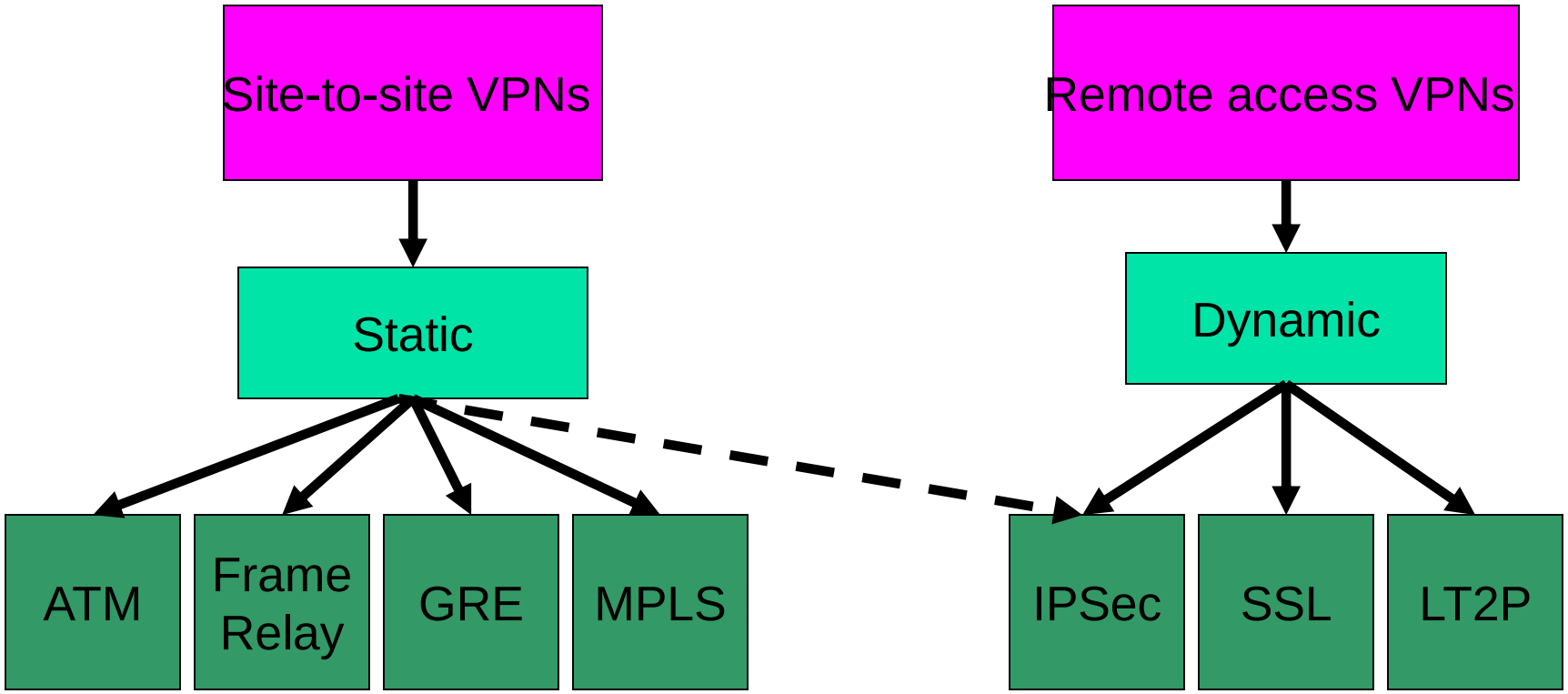
- Virtual Private Network (VPN)
- Két alapvető típus
  - User-space VPN
  - Provider Provisioned VPN (ppvpn)
    - L2VPN –Ethernet szolgáltatás
    - L3VPN – IP alapú
- Mindkettő a hálózat erőforrásainak költséghatékony kihasználását célozza

L3-L2 VPNs

- L2 és L3 VPN példa



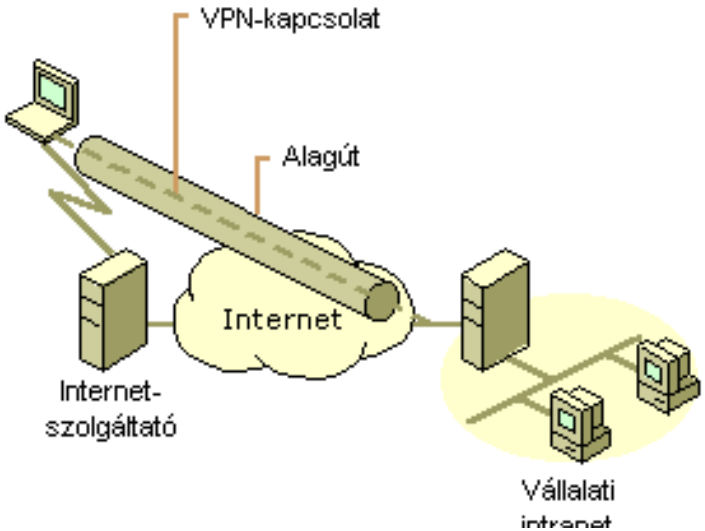
VPN típusok


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

Felhasználói VPN

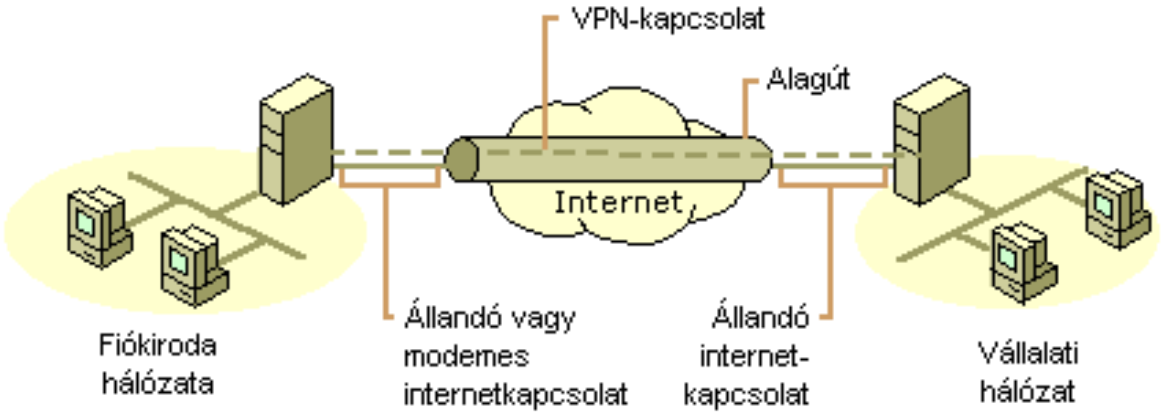
- Bérelt vonal – nem költséghatékony
- Internet – olcsó kommunikáció
  - Nem biztonságos!
- Megoldás: biztonságos kapcsolat kialakítása az Interneten kódolt alagutak használatával
  - Egy vagy több kliens használhat egy alagutat
  - A biztonságot a kódolás adja
  - Minőségbiztosítás az Internet szolgáltatótól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

VPN az ügyfél típusa szerint



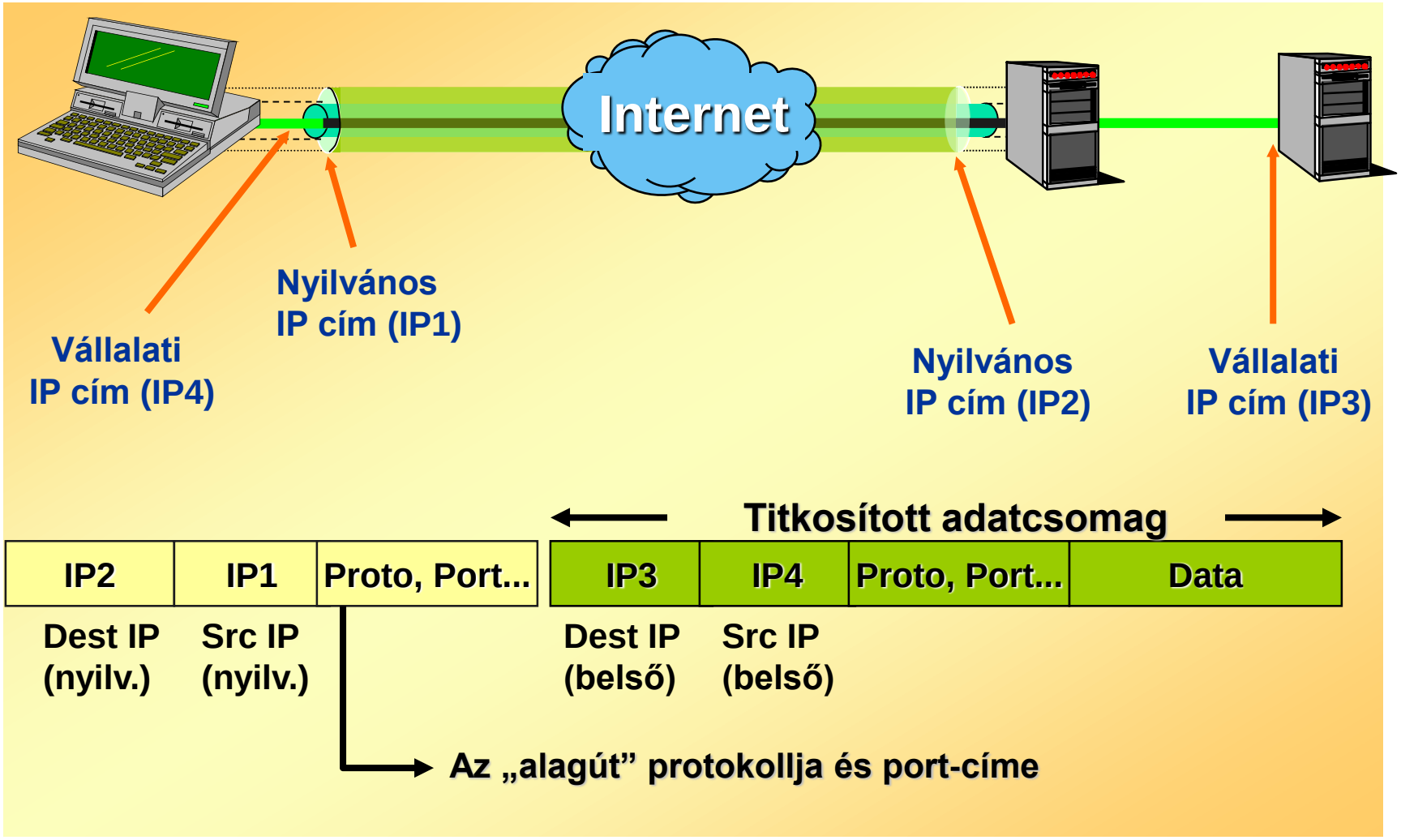
Ügyfél-kiszolgáló (Client-2-Router)

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

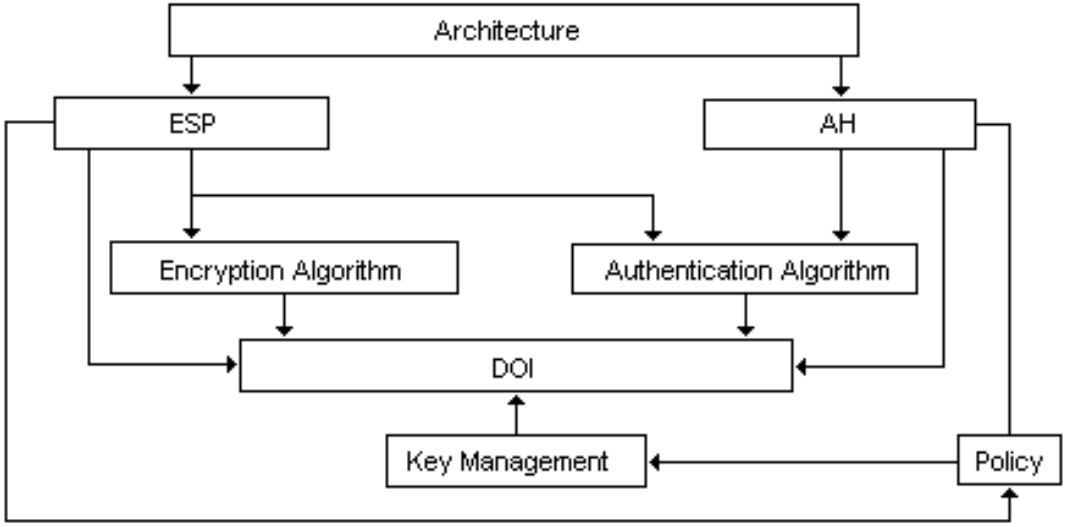
Alagútprotokollok: L2TP

- 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

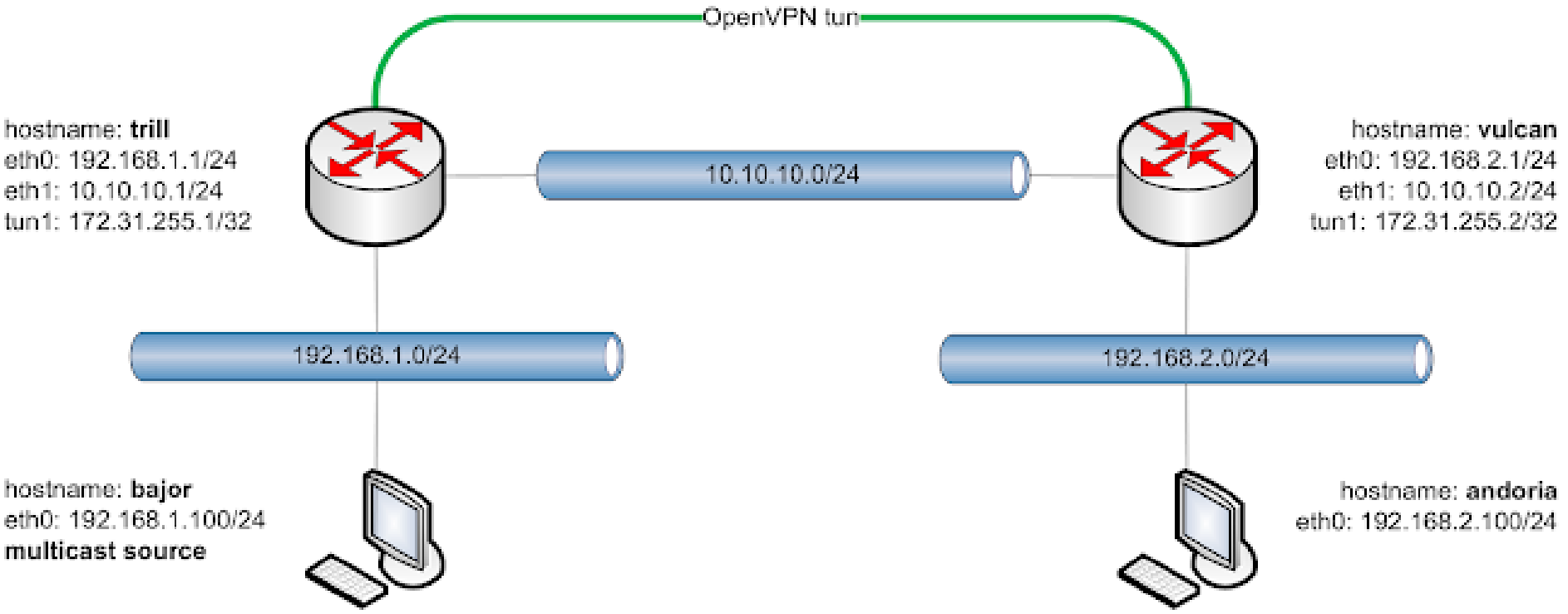
SSL VPN – működés

- 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

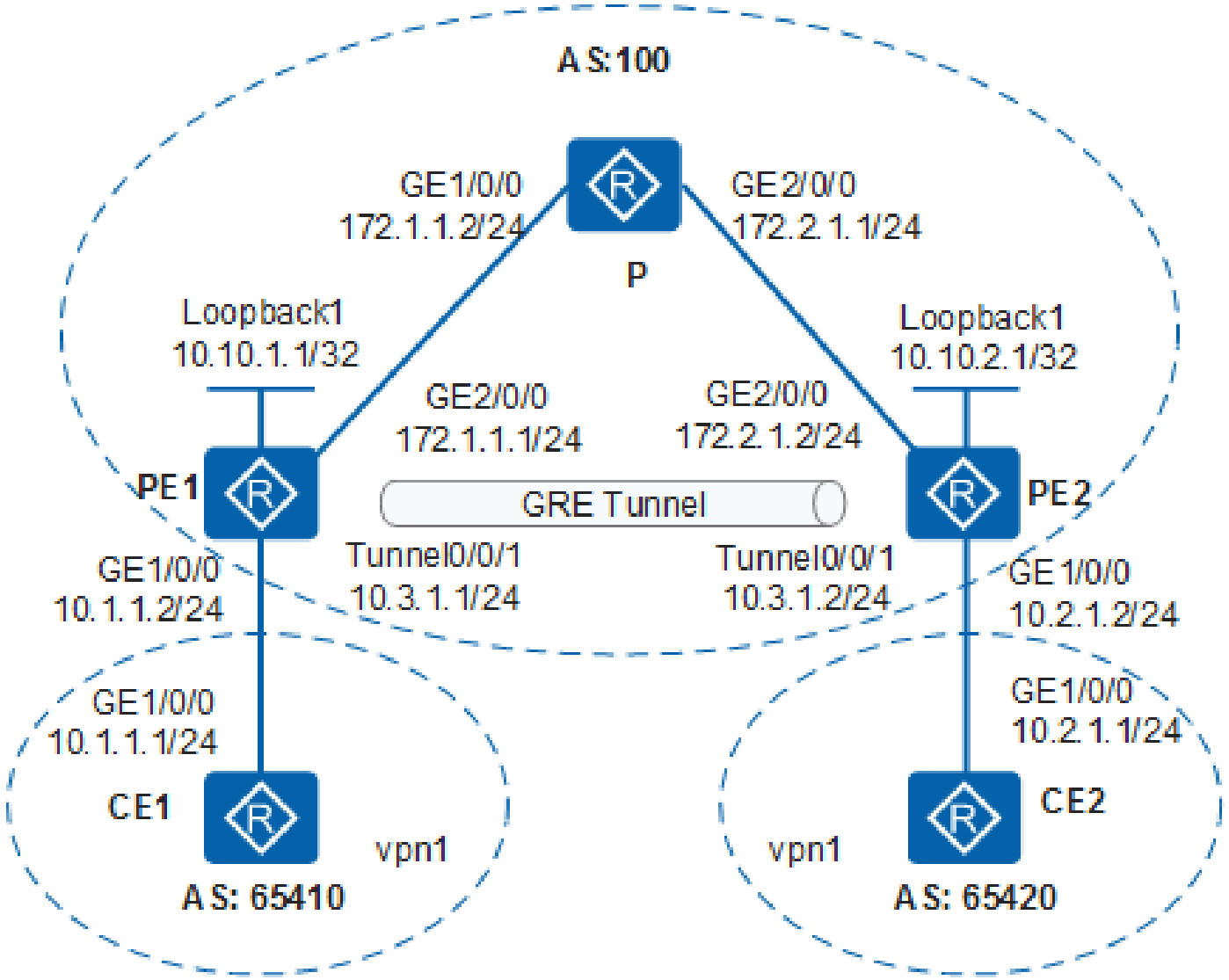
- Mikor SSL és mikor IPSec VPN?
- Az SSL VPN egyszerűbb
  - Felhasználó által menedzselhető
  - Egyszerűen konfigurálható
  - TCP – nem támogat QoS-t, UDP-t
- Az IPSec VPN komplexebb
  - Adminisztrátor állíthatja be (root jog)
  - IP szintű – QoS támogatás lehetséges
  - Transzparens a felhasználó felé

Példa: OpenVPN

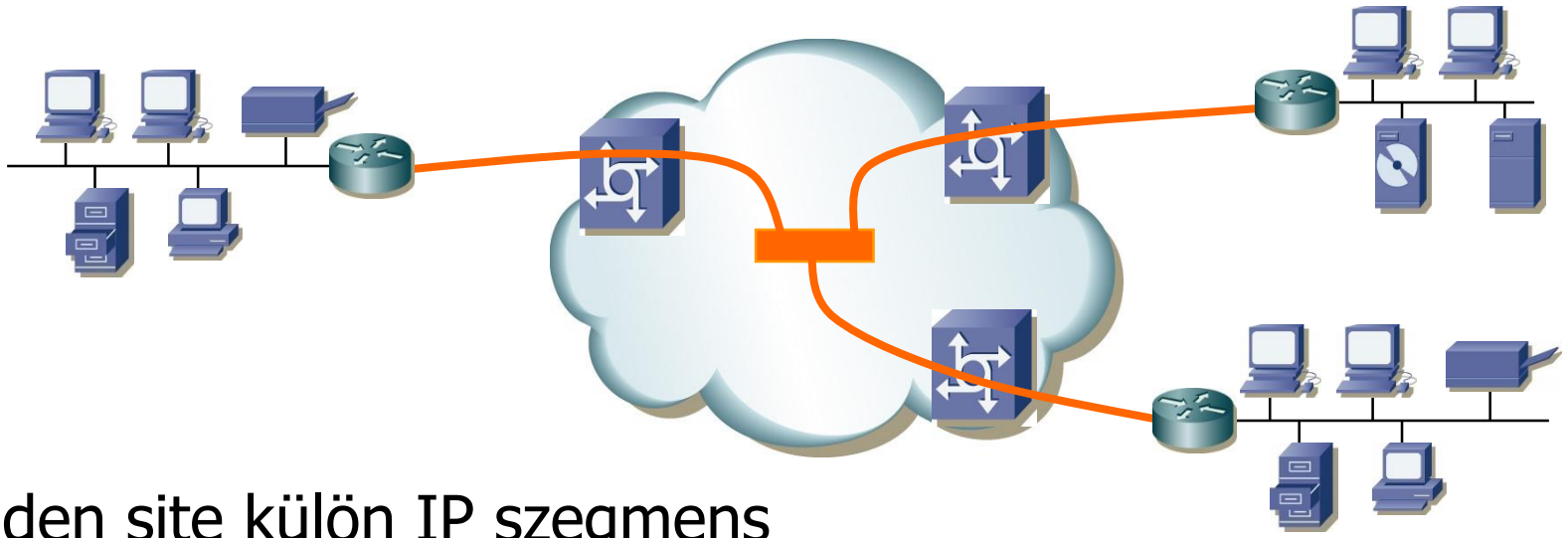


Szolgáltatói VPN-ek
Provider Provisioned VPN (PP-VPN)

Példa: L3 (IP) VPN

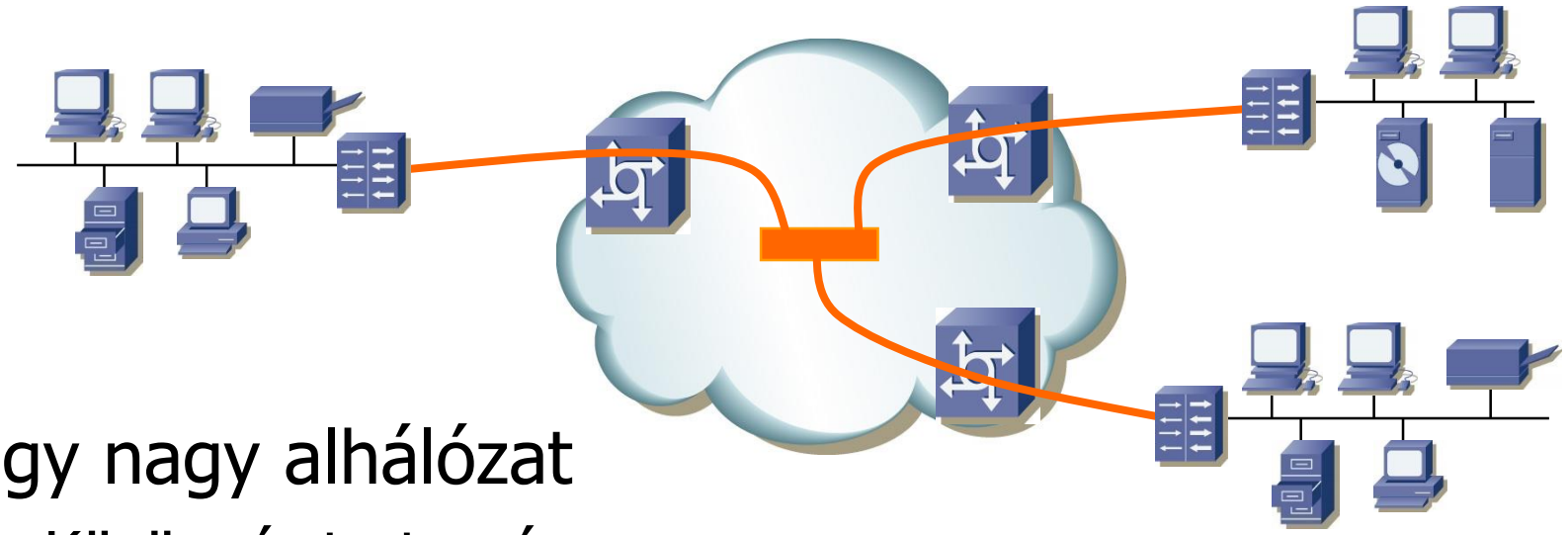


Router Inter-connect



- 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



- 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

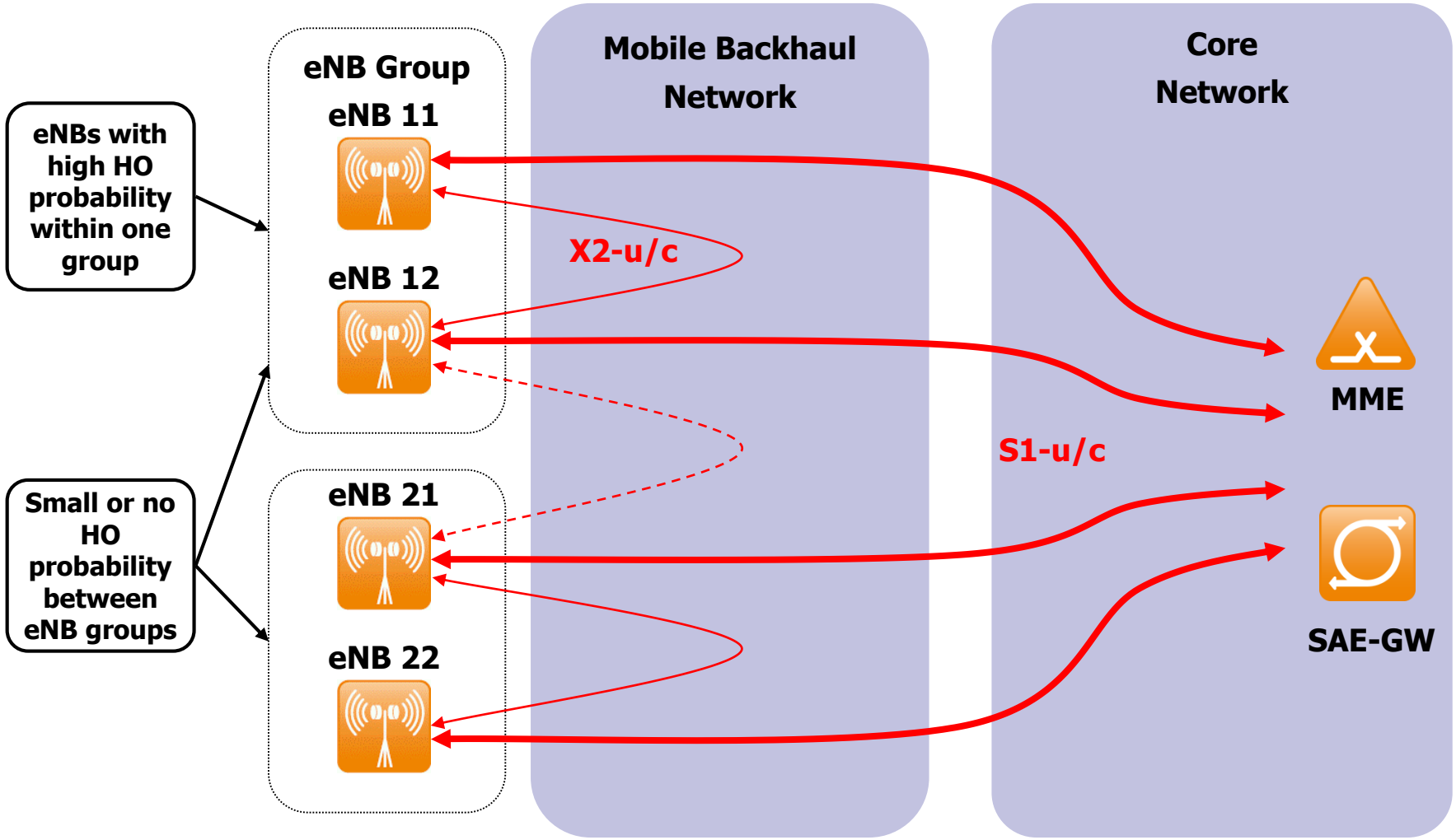
LTE – Backhaul

bérelt vonali és VPN szolgáltatások

BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
TÁVKÖZLÉSI ÉS MÉDIAINFORMATIKAI TANSZÉK

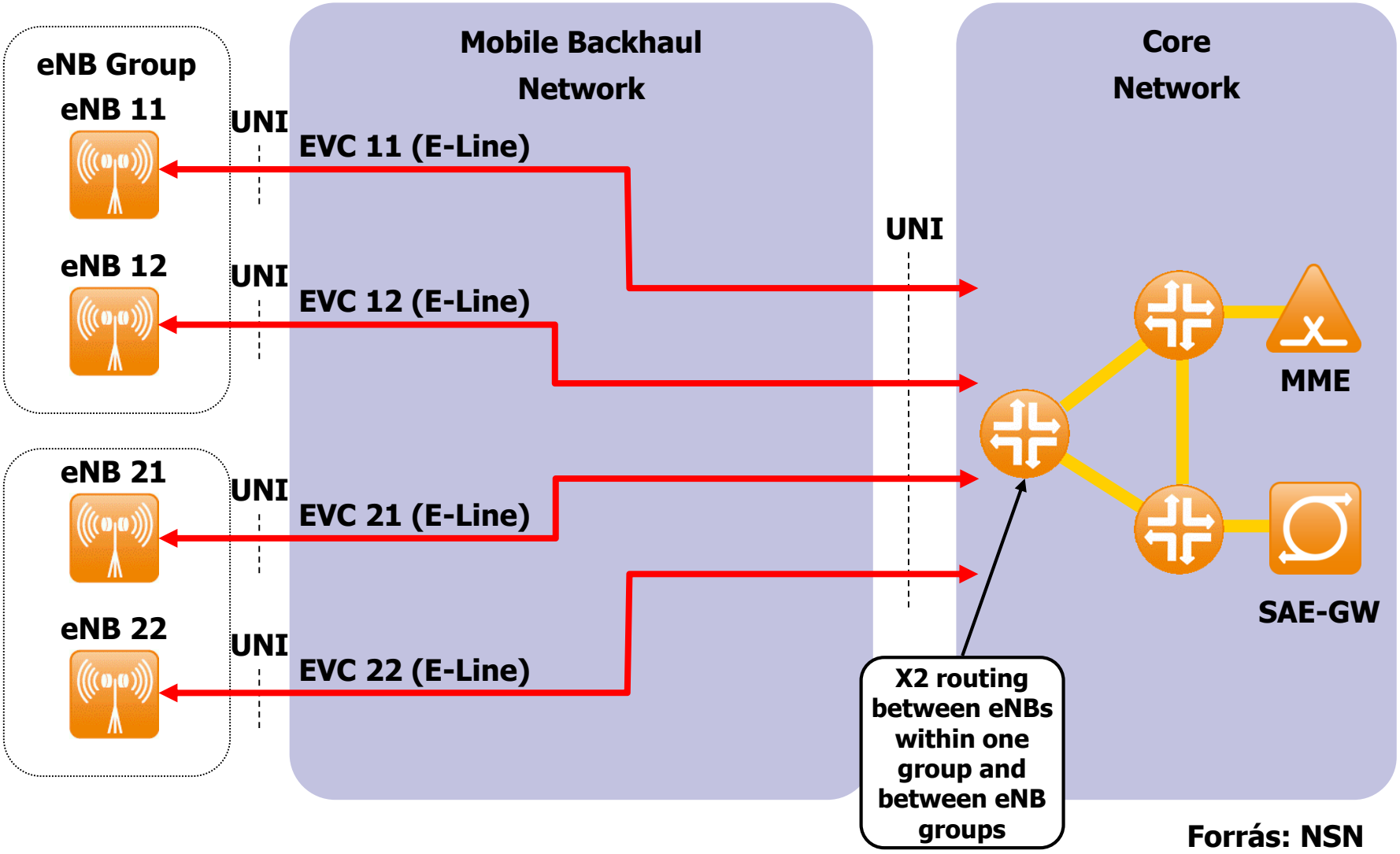
moldovan@tmit.bme.hu

LTE E2E Architecture and Connectivity



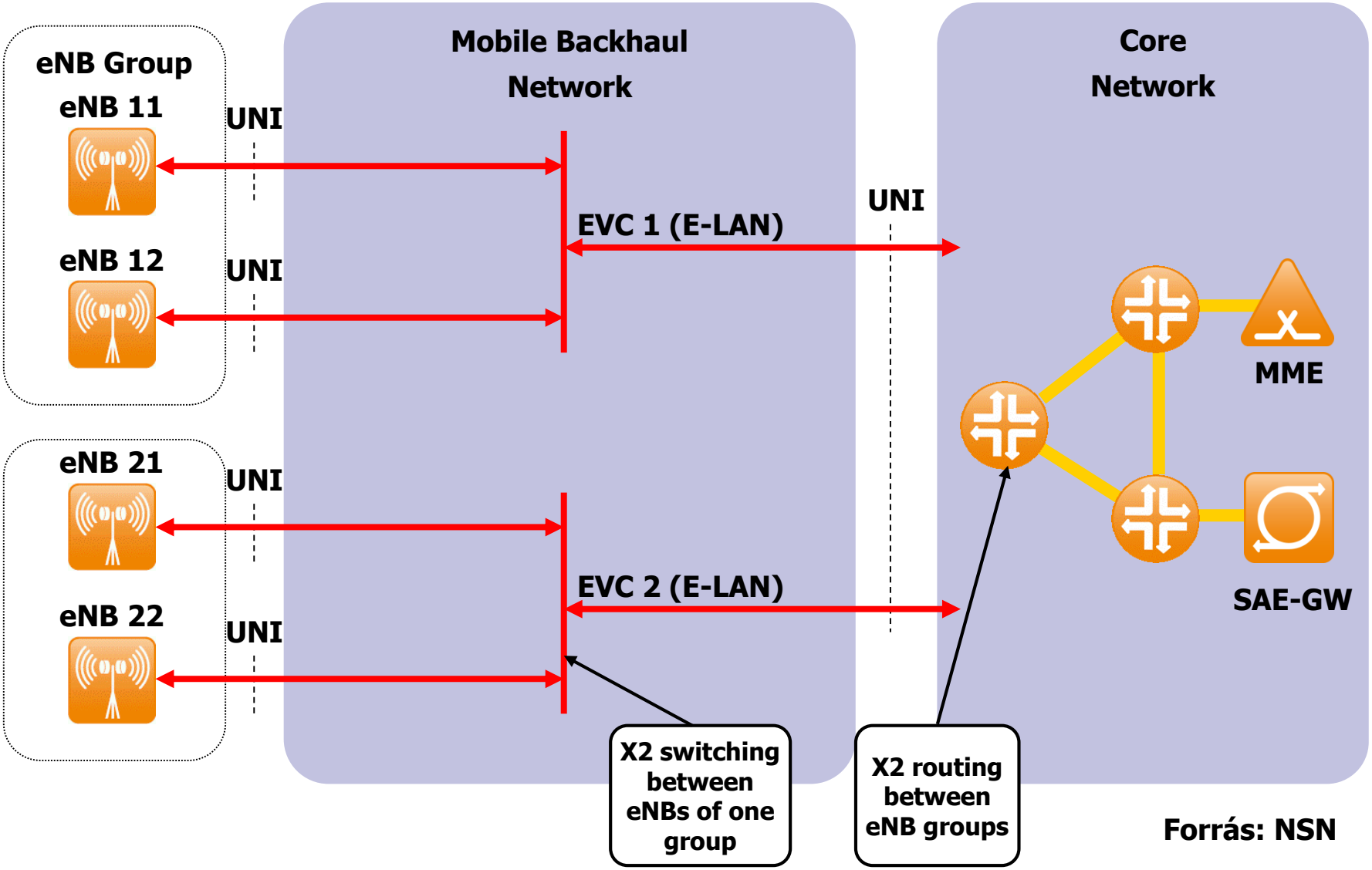
Forrás: NSN

L2 Mobile Backhaul - E-Line



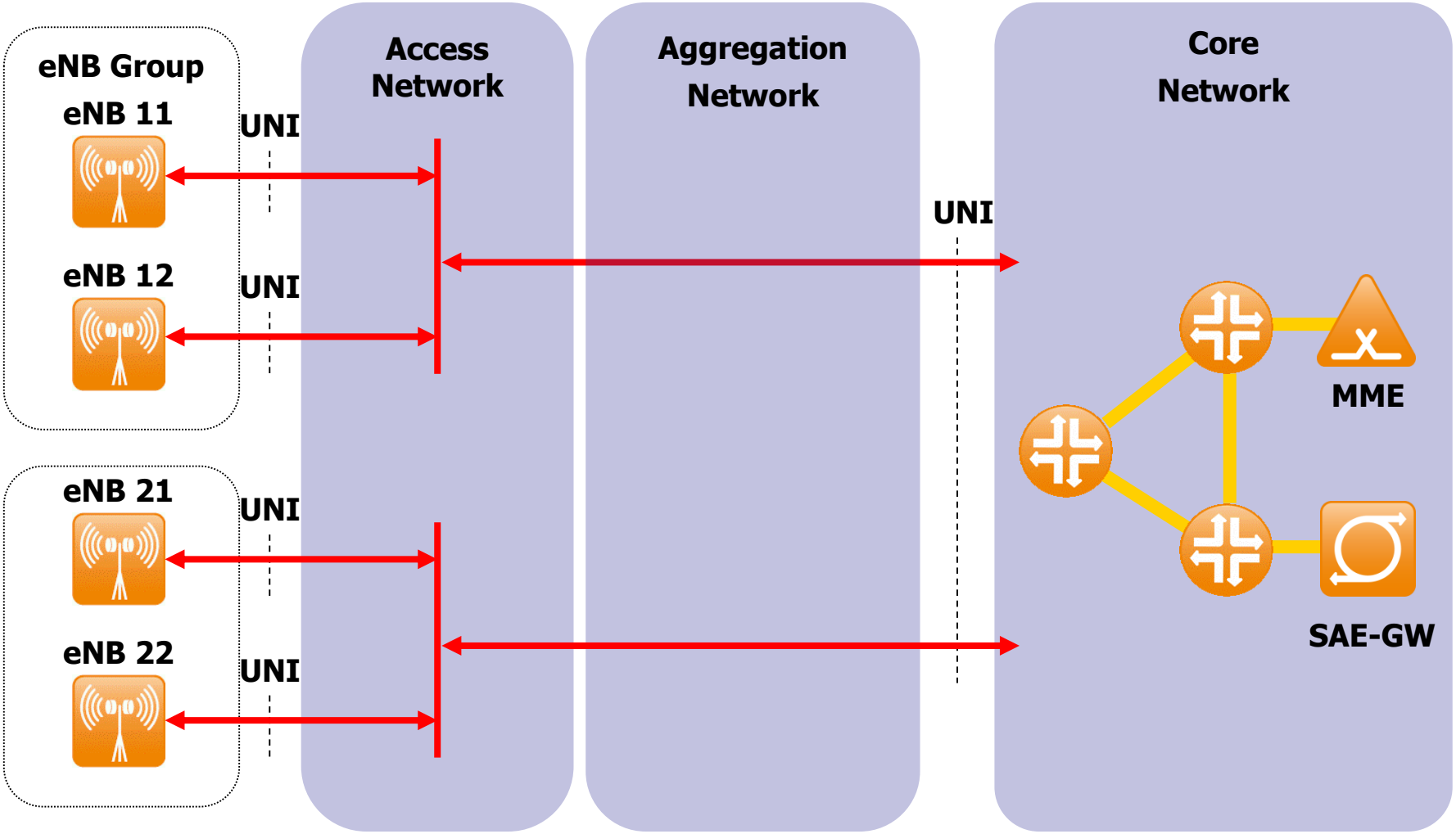
Forrás: NSN

L2 MBH - E-LAN



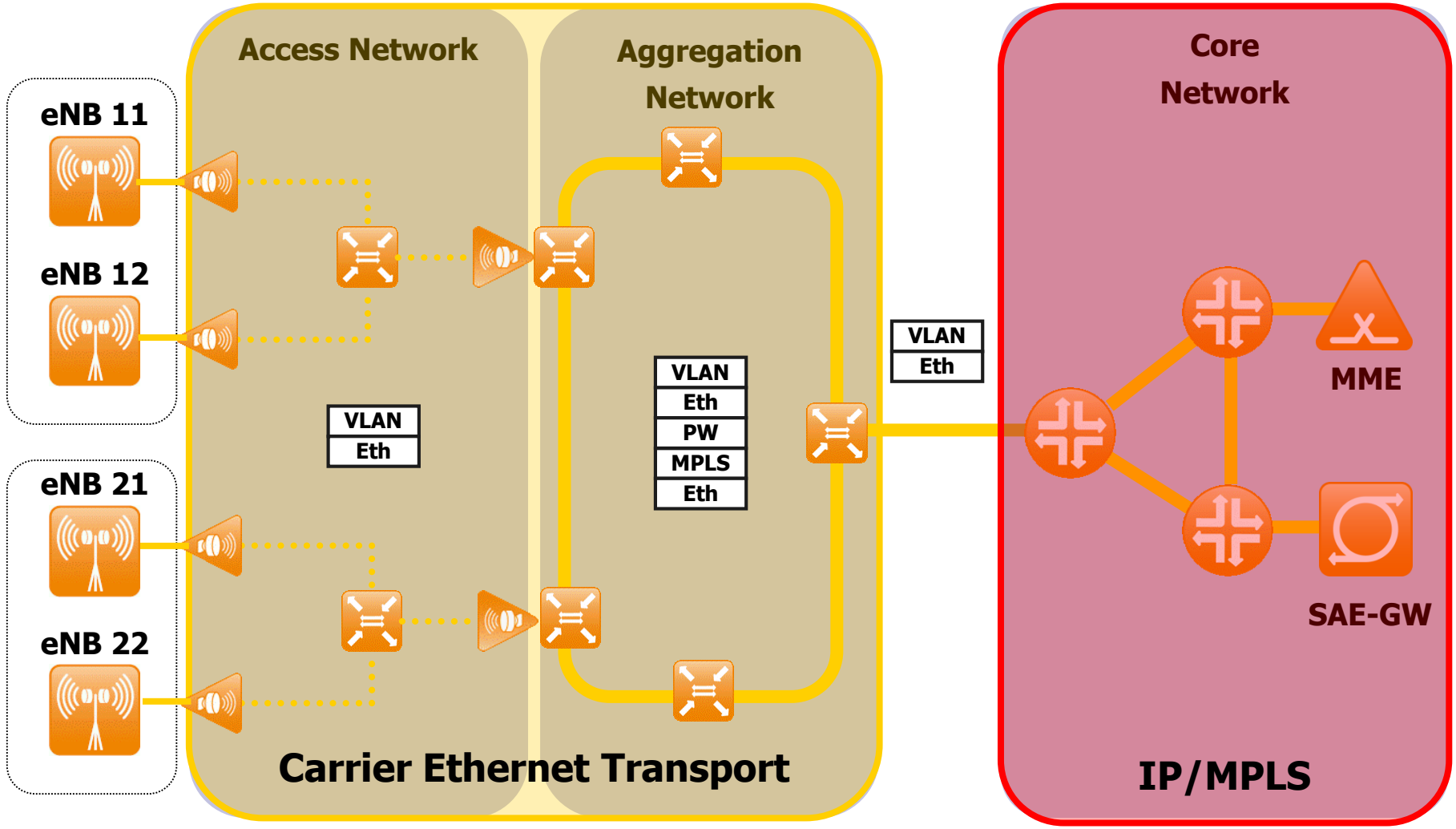
Forrás: NSN

L2 Access és Aggregációs hálózat – Logikai felépítés



Forrás: NSN

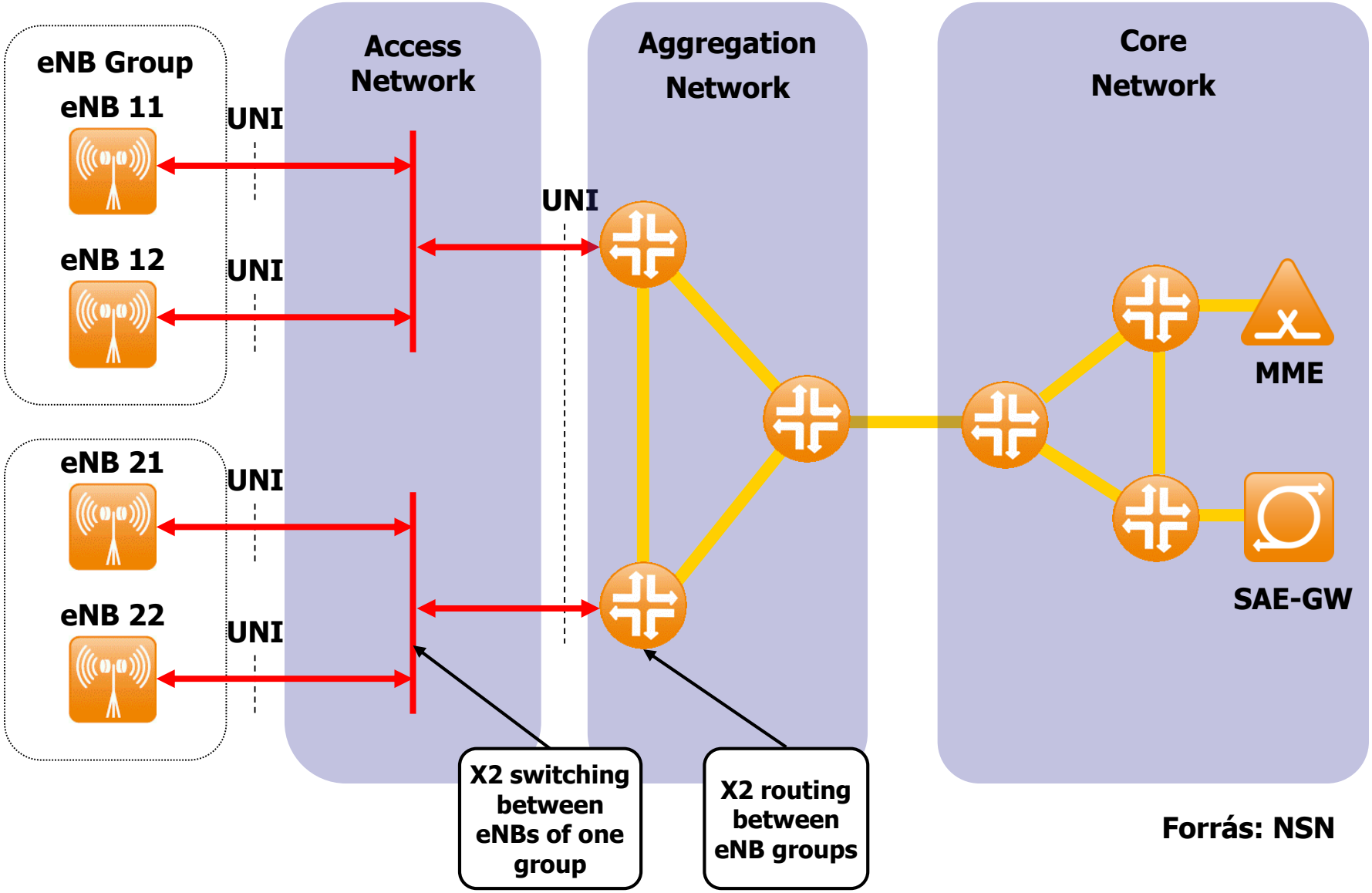
Carrier Ethernet Transport for Backhaul, IP/MPLS for Core



eNB / eNB group identification with VLAN

Forrás: NSN

Alternatíva: L2 Access & L3 Hozzáférés



Forrás: NSN

Köszönöm a figyelmet!