

Mobil és Vezetéknélküli Hálózatok  
Teljes kidolgozás

Matolcsy Balázs

2015. május 18.

# 1. Videóátviteli szolgáltatások

## 1.1. Csoportosítsa a videóátviteli szolgáltatásokat, jellemezze az egyes csoportokat!

A csoportosítási lehetőségek:

- hálózat üzemeltetője és a tartalom szolgáltatója szerint: azonos (T-Home videótár), különböző (YouTube, Online-TV)
- elérhetőség ideje szerint: lineáris (sima TV, műsorfolyamba bekapcsolódunk), on-demand: fogyasztó határozza meg mikor történik a lekérés
- a tartalom átvitele és fogyasztás egyszerre történik-e: Streaming vagy előre letöltött állományt nézünk meg később
- valós idejű átvitel: valós idejű (Skype, drónok irányítása, online gaming), kvázi valós idejű (IPTV, pár másodperces késleltetés)

## 1.2. Írja le a videóátvitel legfőbb jellemzőit, valamint különféle videóátviteli szolgáltatások minőségi követelményeit!

Egy videófolyam legfontosabb tulajdonságai a következők:

- a videó felbontása (480p, 720p, 1080p, 4K, 8K)
- színmélység (high color 16 bit/px, true color 24 bit/px)
- képkocka / másodperc (FPS)
- az átvitelhez szükséges adatsebességek (pl.: 720p 2-3 Mbps, 480p 1 Mbps stb.)

Minőségi jellemzők:

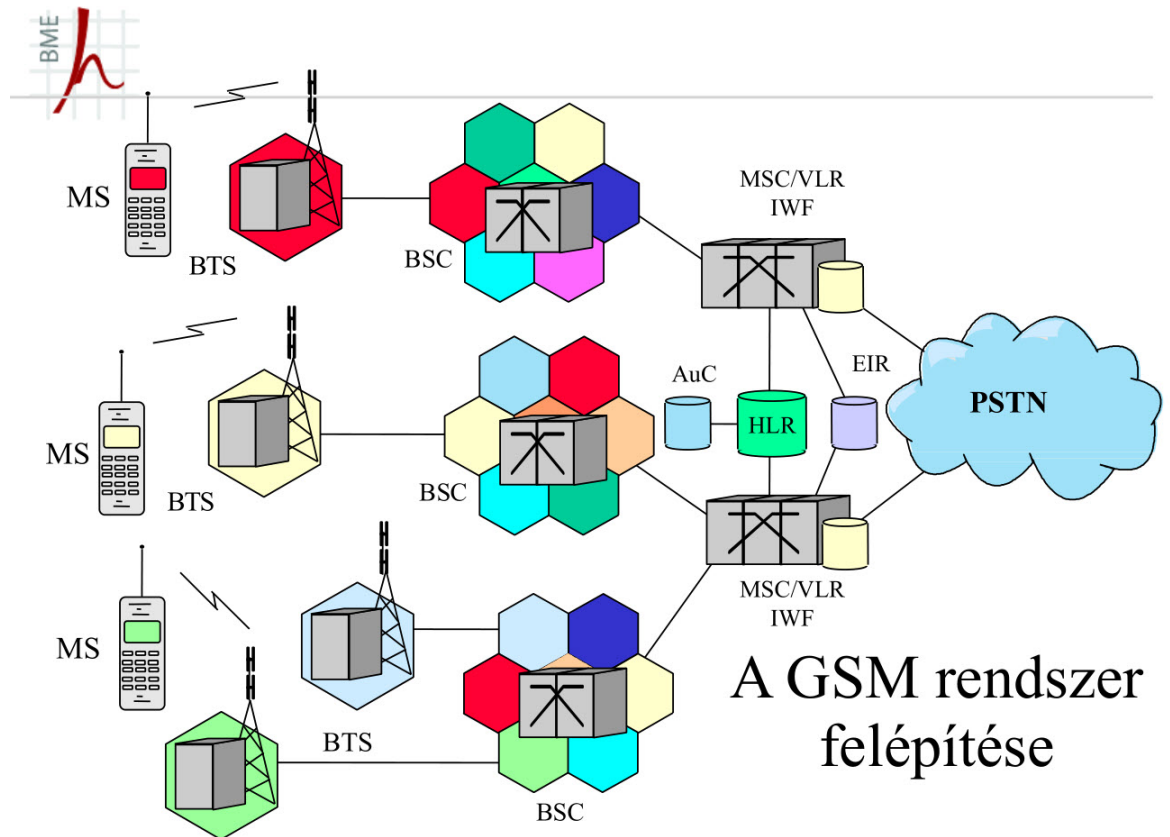
- QoE, QoS nem egyértelműen definiált, szubjektív
- késleltetés
- késleltetés ingadozás (jitter)

Szolgáltatásoknál megengedett határértékek jitter-re:

- videotelefonálás - max. 50 ms
- online gaming - 10-20 ms
- valós idejű vezérlés - 5-10 ms
- streaming video - több másodperc is lehet

## 2. GSM és 3G hálózatok

### 2.1. Ismertesse a GSM hálózatok felépítését, írja le a hálózat elemeinek fő funkcióit!



**BTS feladata:** a digitális beszédcsatornából előállítják a rádiós interfészen küldött fizikai jelet és vissza

**BSC feladata:** a rádiós erőforrás menedzselése, összekapcsoló funkció az NSS és a BSS között

**MSC feladata:** alapvető kapcsolás és irányítási funkciókért felel az NSS-en belül, NSS-ben lehet több MSC is, beszédflowmokat irányítja, egyéb szolgáltatásokat is támogat, amik szükségesek a GSM hálózatban (ettől eltekintve nem sokban különbözik egy hagyományos telefonközponttól)

**AuC feladata:** az előfizetők azonosítására szolgáló biztonsági adatokat tárolja, minden regisztráláskor bejelentkezünk rá, minden szolgáltatónak egy van!

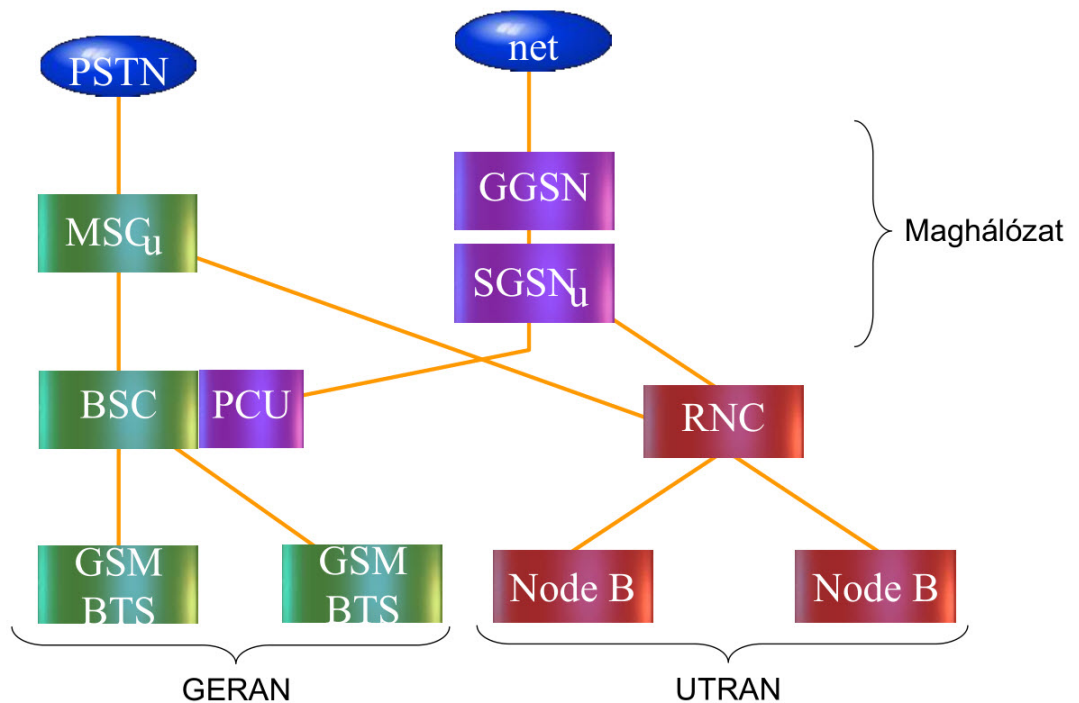
**EIR feladata:** Equipment Identity Register, adatbázis, amely a mobil készülékek főbb adatait tárolja, három listás rendszer IMEI alapján (fekete, szürke, fehér)

**HLR feladata:** Home Location Register, előfizető helyére és a neki nyújtható szolgáltatásokra vonatkozó információkat tárolja

**VLR feladata:** Visitor Location Register, MSC-vel együtt van és az adott MSC szolgáltatási területén tartózkodó készülékek pontos helyét tárolja (pontosabb a HLR-nél), roaming-nál is fontos!

**2.2. Ismertesse a 3G hálózatok felépítését, írja le a hálózat elemeinek fő funkcióit!**

 **GSM/EDGE/UMTS hálózat – ism.**



**GERAN:** GSM/GPRS-EDGE Radio Access Network, BSC mellé az adatátvitel miatt szükséges volt egy csomagszervező egység (Packet Control Unit), új BSC integráltan tartalmazzák.

**UTRAN:** UMTS Terrestrial Radio Access Network, rádiós hozzáférés biztosítása a maghálózat és a mobil készülékek közt

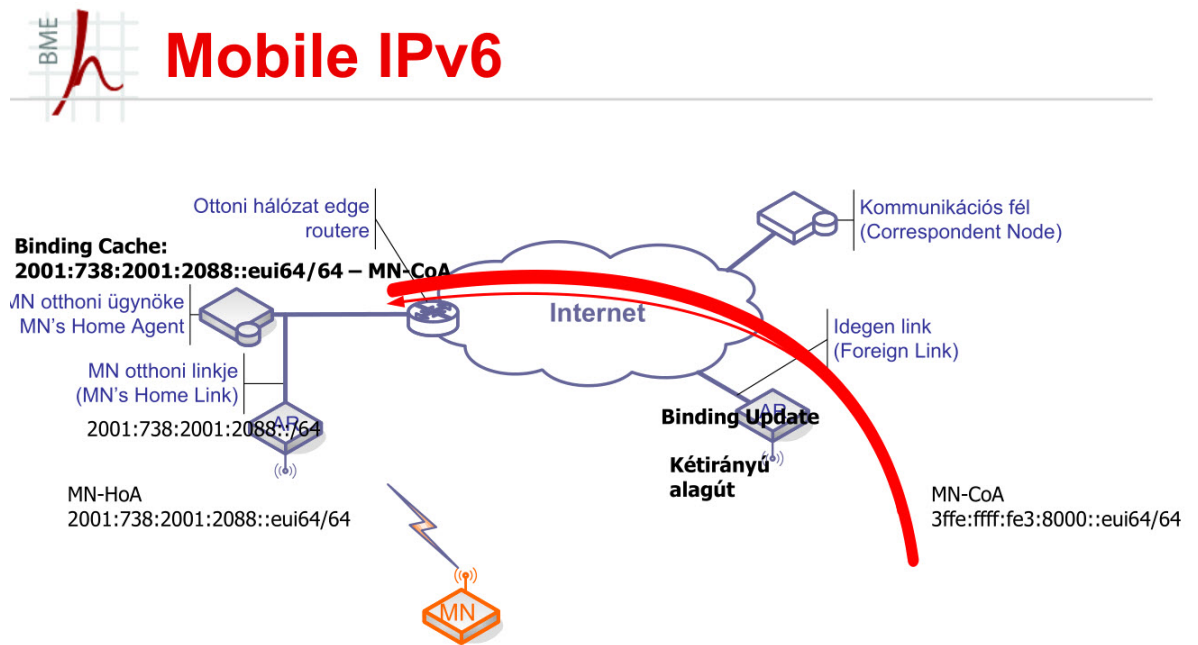
**Node B:** megfelel a GSM BTS-ének, !de! más moduláció, közeghozzáférés, sűrűbben kell elhelyezni, más frekvenciasávok, fizikai rétegbeli feladatokat lát el.

**RNC:** Radio Network Controller, hasonló a GSM BSC-hez, egy RNC a Node B-ket egy csoportját vezérli, kapcsoló funkciója van!

**SGSN:** Serving GPRS support node, csomagtovábbítás GSN és PCU-közt, csomagkapcsolt kommunikáció középpontja, mobilitás menedzsment (követés), számlázás, cellaváltás (handovering)  
**GGSN:** számlázás a kifelé irányuló hálózatok fele, átjáró az IP hálózatok felé, home agent funkció a mobil IP-ben

### 3. IP hálózatok

#### 3.1. Ismertesse az IPv6 mobilitás támogatását, ismertesse a NEMO (hálózati mobilitás) eljárást!



- Minden helyváltoztatást követően
  - A mobil terminál beregisztrálja a címét (helyét)
  - A kommunikációs fél az állandó címen (azonosítón) éri el a mobil terminált
  - Az otthoni ügynök (Home Agent) átirányítja a forgalmat

#### NEMO Basic Support protokoll:

- amíg a mozgó hálózat az otthoni hálózatban van - hagyományos útválasztás
- változik a hálózat helye a topológiában - beregisztrálja a helyét és a hálózati prefixét a HomeAgent-nél, majd a HomeAgent az összes ide érkező csomagot tunnelezi a Mobil router felé.

- minden új helyen - új ideiglenes cím a Mobil Router állandó címéhez, mozgó hálózat többi csomópontjának címe változatlan, transzparens mozgás

### 3.2. Ismertesse a HIP és az SCTP protokollokat!

**HIP:** Host Identity Protocol, új névtér, új protokoll réteg bevezetése, ez a hálózati és a transzport réteg között helyezkedik el. A HIP réteg végzi el a HIP-IP cím összerendelést. HIP réteg alatt az IP cím az azonosító (kb. csak a helymeghatározó. A felső rétegek kapcsolatai nem szakadnak meg, ha IP cím változás történik. Erre jó a HIP.

**SCTP:** Stream Control Transmission Protocol, transzport rétegben TCP és UDP-hez hasonló, nem általánosan támogatott (de az LTE-ben már szabványos interfész), megbízható(hibamentes, duplikáció mentes), több folyam egyetlen kapcsolaton belül, Multihoming, Torlódáskezelés, Slow Start. Ezek a tulajdonságok kellenek a VoIP telefonáláshoz, illetve egyéb multimédiás szolgáltatásokhoz.

### 3.3. Ismertesse a SIP protokollt, hol, mire használják, milyen funkciókat lát el?

Alkalmazási rétegbeli protokoll a SIP. Ez egy jelzési és vezérlő protokoll multimédia alkalmazásokhoz. A SIP alapvető funkciói:

- Helymeghatározás - hol van a végpontunk
- Végpont képességei - milyen médiát, milyen paraméterekkel lehet szállítani
- Végpont elérhetősége - távoli végpont hajlandó-e a kommunikációra
- Hívás indítás - csörgetés
- Hívás kezelés - hívás konfigurálás, befejezés

Gyakorlatban alkalmazzák: VoIP, PSTN, Átirányítás, Csevegés, Konferencia hívások, Médiafolyam szabályzás

## 4. Backhaul, Fronthaul

### 4.1. Ismertesse a hagyományos és az elosztott bázisállomás architektúrákat, definiálja a backhaul és a fronthaul hálózat fogalmát!

**Hagyományos bázisállomás struktúra:** Tipikusan makro bázis állomásoknál, teljes DSP a torony alján levő szekrényben. Nincs aktív elem a tornyon, RF jel coax-szal felvezetve az antennáig, de ennek van vesztesége (3-5 dB)! MIMO esetben sok kábel kell.

**Elosztott architektúra:** pl. CPRI, elektronikus vagy optikai jelátvitel, nagyon nagy sebességre van szükség (614 MBps többszöröse), ezt a CPRI-t az

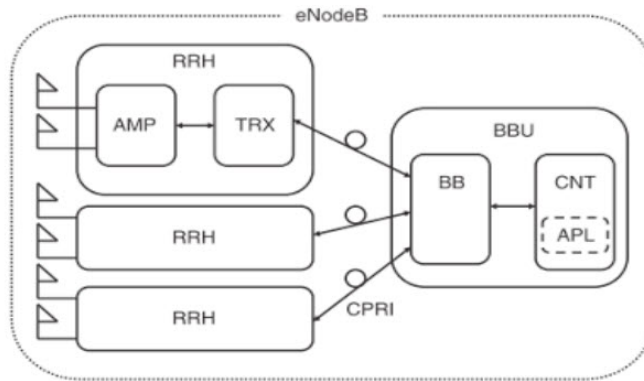
enodeB-n belül használjuk, hogy összekössük a BBU-t és az RRH-kat.

**Backhaul:**

- hagyományos architektúra: BS-től a hálózat többi része felé
- Backhaul link: összeköttetések
- backhaul hálózat: több BS bekötése a hálózatba
- elosztott architektúra: a Backhaul a BBU-t köti a hálózatba

**Fronthaul:** A BBU és az RRH közti részt nevezzük így. Fronthaul hálózat: nincs akadálya, hogy egyetlen BBU-hoz több RRH-t kapcsoljunk.

**4.2. Ismertesse az eNodeB logikai elem felépítését! Továbbá ismertesse az egyes rész egységek feladatait!**



Az enodeB egy logikai elem, amely két fő funkcionális elemből áll. Ezek a BBU (Baseband Unit) és a RRH (Remote Radio Head). köztük optikai kábeles csatlakozás van.

**A BBU feladatai:**

- A maghálózatból jövő S1 kapcsolat itt végződik
- Az X2 interfész is itt végződik (eNode B-k közti kapcsolat)
- Az alapsávi digitális jelfeldolgozásért felel
- Az RRH-kból jövő digitális jeleket demodulálja, illetve az IP hálózati csomagok modulációja is itt történik (RRH felé)

**Az RRH feladatai:**

- RF jelek küldése vétele
- alapsávi jelek RF jellé alakítása
- az UE-től vett RF jeleket digitális alapsávi jellé alakítja, és továbbítja a BBU-nak.

### 4.3. Ismertesse a WLAN hálózatok EPC-hez kapcsolásának lehetőségeit (megbízható, nem megbízható kapcsolat esetén)!

EPC: Evolved Packet Core, Az ilyen EPC-khez lehetséges csatlakozni, mind a 3GPP által szabványosított hálózaton (UMTS, GSM, LTE), és a nem általuk szabványosítottan is (WLAN, WiMax). A nem szabványosított hozzáférési hálózaton keresztül történő kapcsolódás történhet megbízható, vagy nem megbízható kapcsolaton keresztül. Például a WLAN hálózatot kapcsolhatjuk össze az LTE-vel úgy, hogy a felhasználónak észrevétlen legyen az átmenet a kettő közt. (ezzel tehermentesíthetjük a hálózatot)

**Nem megbízható kapcsolat esetén:**

- WLAN hálózattal a kapcsolat ePDG-n keresztül jön létre, majd ez kapcsolódik a PDN GW-hez
- Az ePDG SWn interfészen kapcsolódik a WLAN-hoz
- Az ePDG SWa interfészen kapcsolódik a 3GPP által biztosított Authentication, Authorization, Accounting szerverhez (AAA)
- UE-t (felhasználó) azonosítani kell az AAA szerverrel
- IPSec csatorna az UE és ePDG között (így lesz biztonságos)
- ePDG lekéri az AAA-tól SWm interfészen az Authentikációs információt, UE és ePDG közt Internet Key Exchange v2 jelzésátvitel történik és kiépül az IPSec-kel védett csatorna UE-től az EPC-ig

**Megbízható kapcsolat esetén:** Itt nincs ePDG, ezért a WLAN közvetlenül kommunikál az EPC-vel, nem is kell IPSec csatorna. Az AAA szerverhez STA interfészen keresztül kapcsolódunk. Mindkét esetben az autentikáció független a WLAN-tól. (uSIM alapján történik HSS segítségével)

### 4.4. Mit értünk a heterogén hálózat (HetNet) alatt, mik a tulajdonságai? Sorolja fel a Heterogén hálózatok előnyeit és hátrányait!

A Heterogén Hálózat (HetNet) elnevezés alatt többféle hozzáférési hálózat kombinációját értjük, ahol a különböző rádiós technológiák, különböző adóteljesítménnyel rendelkező bázisállomások mellett, az elképzelés szerint a felhasználó számára észrevehetetlenül biztosít átjárást az egyes hozzáférési rendszerek között.

**A HetNet hálózat előnyei:**

- közelebb viszi a bázisállomást a felhasználóhoz
- jobb lefedettséget és nagyobb kapacitást biztosít



- skálázhatóság, makrocella terheltsége csökkenthető

#### A HetNet hálózat hátrányai:

- Interferencia forrás (a makrocellához kapcsolódó felhasználóknál interferenciát okoznak pl. a femtocellák)
- Femtocellákat a felhasználók telepítik/üzemeltetik, függetlenül üzemelnek a mobil szolgáltatótól.
- ezt mindenképpen kézben kell tartani a szolgáltató oldalán

#### 4.5. Mi a relé node (Relay node - RN)? Ismertesse a relé node típusokat, csoportosításukat és mutassa be a lehetséges alkalmazásukat! Mi(k) a különbség(ek) a femtocellák és a relé node-ok között?

**Relay Node:** a bázisállomástól vett jelet demodulálja, dekódolja, elvégzi a hibajavítást, majd új jelet állít elő és továbbítja a relék kisteljesítményű bázisállomások, melyek egy donor BS-hez kapcsolódnak (DeNB), előnye, hogy a cellahatáron jobb lefedettséget biztosít. Hátránya, hogy az önininterferencia megnő, és a Donor eNode-B erőforrásai megoszlanak a Relay-k között.

#### Csoportosítási lehetőségek:

- hely szerint - külső, belső, thru-wall
- továbbítási mód szerint - half-duplex, full-duplex
- frekvenciatartomány szerint - inband, outband

#### Típusok:

- Type 1 LTE Relay - van saját cella ID, ált. half duplex inband
- Type 2 LTE Relay - nincs saját cella ID, ugyanolyan mint egy donor cella (úgy viselkedik)

**Lehetséges alkalmazások:** előnyök közül bármelyik lehet, femtocellák (épületeken belül, felhasználó üzemelteti), relék (épületeken belül, vagy kívül is telepíthető, szolgáltató üzemelteti)

#### 4.6. Milyen interferencia típusok fordulhatnak elő Small cellás rendszerek használata esetén? Az LTE és LTE-Advanced rendszerekben milyen interferenciacsökkentő eljárásokat ismer?

Az előforduló interferencia típusok:

- Cross-tier interference (rétegek közötti interferencia)
- Intra-tier interference (rétegen belüli interferencia)

**Interferenciacsökkentő eljárások:**

- Cell Range Expansion (CRE) - makrocella tehermentesítése a forgalom small cellákra való terelésével, ezt a cella RSRP értékének egy ofszettel való "meghamisításával" éri el, ennek hatására megnő a small cella által lefedett terület, több UE forgalmat visz el, kevesebb HO és jobb erőforrás kihasználtság
- Inter-Cell Interference Coordination (ICIC) - Célja, hogy a makró eNB-k esetén a cellahatáron lévő UE-nek a szomszéd makró eNB ne okozzon interferenciát. eNB-k az X2 interfészen kommunikálva az interferencia mértékétől függően csökkentik az adóteljesítményt az adott PRB-ken
- eICIC - makró eNB ne okozzon interferenciát a small cella határán lévő UE számára. Almost Blank Subframes (ABS) alkalmazása, ezekben a keretekben csak vezérlő és referencia jelek mennek. (felhasználói adat nem, időtartományi megoldás)
- FeICIC - eICIC és eICIC alkeretek használata, eICIC kereteket csak small cellák használhatnak, nem eICIC kereteket small és makro cellák is. Reduced Power Almost Blank Subframes (RP-ABS), nem teljesen üres, de csökkentett teljesítményű keret (makró eNB közepén nagyobb teljesítménnyel ad a RP-ABS alkereteken is, míg a cella határon továbbra is csak a kontroll csatornák jelét adja)

**4.7. Ismertesse a Small cellás rendszerekben alkalmazott szinkronizációs megoldásokat!**

LTE-ben a DL OFDMA, míg az UL SC-FDMA alapú, így biztosítani kell az alvivők közti ortogonalitást. Az eNB és UE oszcillátorai közötti szinkronitást biztosítani kell, ellenkező esetben inter-carrier interference (ICI) és handover fail lehet.

Lehetőségek:

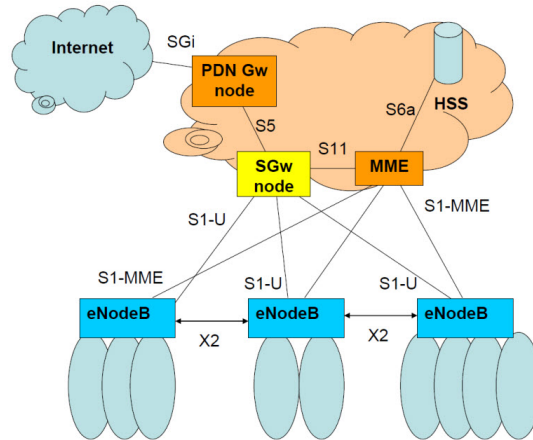
- Backhaul-on keresztül történő szinkronizáció (Precision Time Protocol (PTP), Network Time Protocol (NTP), Synchronous Ethernet (SyncE))
- Backhaul-t nem igénylő szinkronizáció (Global Navigation Satellite Systems (GNSS), Cellular Network Listening)
- Hibrid megoldások (1. és 2. pontok kombinálva)

#### 4.8. SAE EPC architektúra (rajz) és az egyes entitások funkciói



### SAE – EPC 3.

- Funkcionális entitások az EPC-ben:
  - Mobilitás kezelő egység, Mobility Management Entity, MME
  - Kiszolgáló átjáró egység, Serving Gateway, SGW
  - Adathálózati átjáró egység, Packet Data Network Gateway, PDN Gw

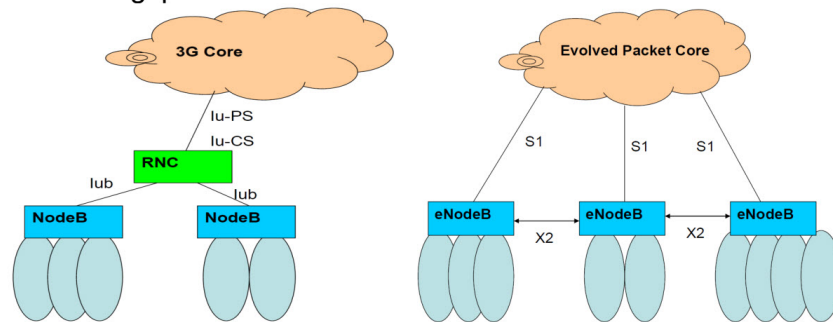


#### 4.9. SAE E-UTRAN architektúra - változások az UMTS-hez képest



### SAE – E-UTRAN 2.

- E-UTRAN architektúra változások:
  - A központi (RNC) egység eltűnt
  - RNC funkciók átkerültek az eNodeB-be:
    - 3G NodeB is létezik (virtuális RNC)
    - HSPA+ szabványok definiálják
  - Biztonsági problémák



#### 4.10. LTE-Advanced motivációk és a small cellák koncepciója

Az LTE-A-val szembe állított általános követelményei a következők:

- Magasabb spektrális hatékonyság
- Magasabb arányú frekvencia újrahasználát (freq. reuse factor)
- Magasabb QoS: magasabb adatsebesség (DL 3Gbps, UL 1.5Gbps), alacsonyabb késleltetés, gyorsabb kapcsolatfelépítés

Trendek:

- felhasználói forgalom más hálózatokra terhelése
- kisebb cellaméreték (femto, pico-cellák)
- alacsonyabb adóteljesítmény

A Small cellák koncepciója annyi, hogy rengeteg piko és femtocellát telepítünk le. Az ilyen Small celláknak kicsi rádiós lefedettsége van (30 m). Pikocellák telepítésének nagy előnye, hogy egyszerű őket telepíteni, és olcsó is, és jobb jelerősséget is biztosítanak. Hátrányai közt a legfontosabb, hogy ezek mind interferencia források, illetve, hogy a mobilitás nehezen megoldható.

#### 4.11. LTE RRC protokoll funkciói

RRC: Radio Resource Control, rendszerinformációk broadcastolása (szomszéd cella paraméterek, adatok UE-k számára)

- RRC kapcsolatvezérlés (paging, kapcsolat felépítés/bontás, QoS vezérlés, jelzésinformációk kezelése)
- mérési konfigurálás és jelentés

#### 4.12. Hívásátadás típusai, handovering

A hívásátadás fogalma: észrevehetetlen, gyors, zökkenőmentes átkapcsolás két bázisállomás közt. Ennek a típusai:

- kemény (break before make) - rövid szakadás van a kapcsolatban (csomagvesztés)
- puha (make before break) - rövid ideig több BS-hez kapcsolódunk
- veszteséges és veszteségmentes
- bázisállomások száma szerint
- kezdeményező fél szerint - UE vagy a mobil terminál
- horizontális - ugyanazon rendszer két cellája közt
- vertikális - két rendszer cellája közt pl. WLAN-LTE, LTE-HSPA

Probléma akkor keletkezik, ha sokszor lépünk át cellahatárt, ekkor szükségtelesen sokszor váltunk cellát és ez erőforrás igényes, ráadásul csökkenti a QoS-t.

**4.13. Feladat: Számítsa ki egy LTE cella lefedettségi sugarát méterben, ha a környékét síknak tekintjük, a terjedés csillapítás a távolság  $x$  hatványával arányos és a bázisállomás adóteljesítménye  $y$  W és a cellahatárt  $z$  dBm! (paraméterezhető pl.:  $x = 3$  v.  $4$ ,  $x = 10-30$  W,  $z = -70 -120$  dBm)**

$$P_{transmit1} = 10 W \quad (1)$$

$$P_{transmit2} = 30 W \quad (2)$$

$$L_{attenuation1} = d^{-4} \quad (3)$$

$$L_{attenuation2} = d^{-3} \quad (4)$$

$$P_{cellborder1} = -70 dBm \quad (5)$$

$$P_{cellborder2} = -120 dBm \quad (6)$$

Tudjuk, hogy  $-70\text{ dBm}$  érték  $10^{-7}\text{ mW}$  teljesítménynek felel meg, a másik esetben ez  $10^{-12}\text{ mW}$ . Ki kell számolnunk a szakaszcsillapítást  $\rightarrow P_{\text{transmit}} - P_{\text{cellborder}}$ . Ennek egyenlőnek kell lennie a következővel:

$$10 \log(L_{\text{attenuation}}) = P_{\text{transmit}} - P_{\text{cellborder}} \quad (7)$$

...ahol  $P_{\text{transmit}}$  és  $P_{\text{cellborder}}$  dB skálán értelmezendő. Ebből megkaphatjuk a  $d$  értékét, visszahelyettesítéssel.

#### 4.14. Ismertesse a vezeték nélküli lokális hálózatok különféle típusait, röviden jellemezze azokat!

Vezeték nélküli kis kiterjedésű lokális hálózatok: épületen, irodán belüli lefedettséget biztosít (10 cm - 100 m).

Adatátviteli távolság szerint:

- Nagyvárosi vezeték nélküli hálózatok (Wireless Metropolitan Area Networks – WMAN), Nagyváros különböző pontjai közötti vezeték nélküli kommunikáció biztosítása
- Helyi vezeték nélküli hálózatok (Wireless Local Area Networks – WLAN) pl: IEEE 802.11 Wi-Fi, Irodán, épületen belüli összeköttetés biztosítása
- Vezeték nélküli személyes hálózatok (Wireless Personal Area Networks – WPAN) pl: IEEE 802.15.1 BlueTooth és 802.15.4 ZigBee, Általában perifériák összeköttetését biztosítja

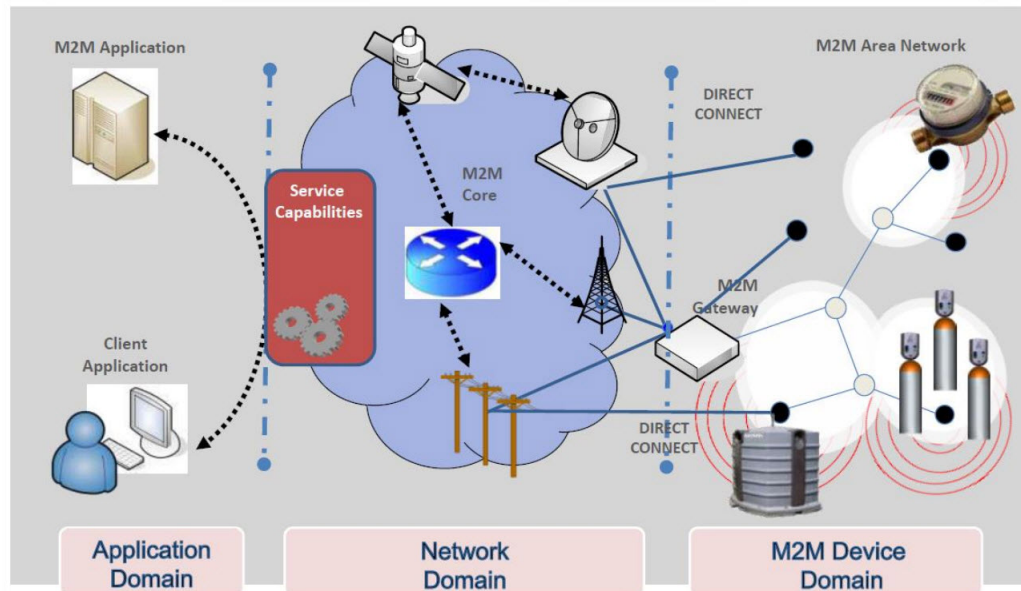
#### 4.15. Mutassa be a Machine-to-Machine kommunikáció megvalósításának kihívásait, valamint az ilyen típusú hálózati architektúra különbségeit a hagyományos hálózati architektúrákkal szemben!

Machine-to-Machine (M2M) kommunikáció: Eszközök közötti kommunikáció, mely nem (vagy csak minimálisan) igényel emberi beavatkozást. A hálózatra kapcsolható eszközök száma rohamosan növekszik (Internet-of-Things, IoT), minden eszköznek egyedi IPv6 címe lesz. Az ehhez kapcsolódó kihívások:

- azonosítás, címzés, energiahatékonyság, biztonság
- komoly méretű jelzésforgalom (kisméretű adatból sok, pl szenzoradatok, gyakori hozzáférés-nagy jelzésforgalom)
- nagyméretű adatok folyamatos stream-elése (pl. CCTV, ritka de folyamatos hozzáférés)
- szabványosítás kísérletek (sokféle technológia és felhasználási terület, együttműködési problémák)

Az M2M architektúra az ETSI ajánlás szerint:

## M2M architektúra (ETSI ajánlás)



### 4.16. Vázolja fel a M2M kommunikáció megvalósításához szükséges 3GPP hálózati architektúra kiegészítéseket, valamint ismertesse az elemek funkcióit!

A 3GPP core hálózat az alábbi kihívásoknak kell megfeleljen az MTC (Machine type communication) realizációja során: kommunikáció megvalósítása az MTC szerverrel mobil irányú és a mobil által kezdeményezett kommunikáció támogatása (egyedi azonosítás) biztonsági mechanizmusok (biztonságos kommunikáció PLMN (Public Land Mobile Network) és az MTC szerver között). ???

### 4.17. Mutassa be a ZigBee szabvány által definiált eszköz típusokat, valamint a lehetséges topológiákat!

Szenzorhálózatok kialakításához terveztek: alacsony fogyasztás, hosszú akkumulátor élettartam, gyors kapcsolatfelépítés, nagyszámú node, titkos adatkapcsolat.

- ZigBee Coordinator Node (ZCN): A hálózat gyökere, más hálózatokat köt össze, egy hálózatban csak egy darab lehet. Hálózati információkat és

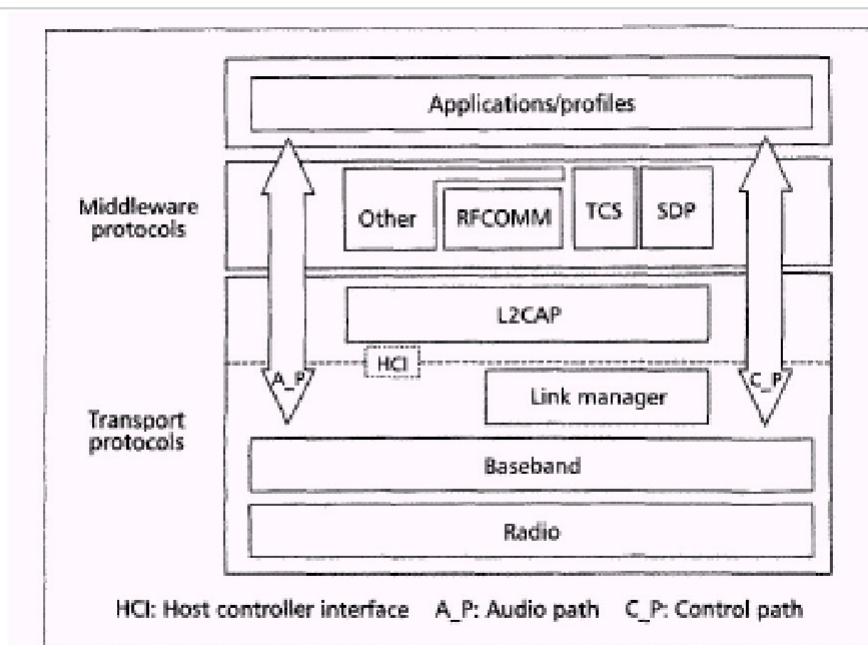
biztonsági kulcsokat tárolhat.

- ZigBee Full Function Device: Közbülső eszközök, melyek az adattovábbítást végzik, kisebb a memóriaigény, mint a ZCN-nek. Alacsonyabb gyártási költség, működhet koordinátorként is.
- ZigBee Reduced Function Device: Végkészülék, nem képes más eszközök adatait továbbítani. Legkevesebb memóriaigény, alacsonyabb gyártási költség és csak a koordinátorral kommunikál.

Definiált topológiák: csillag, fa, mesh

#### 4.18. Mutassa be a Bluetooth protokoll szerkezetét és röviden ismertesse az egyes részek fő feladatait!

## BME Bluetooth protokoll szerkezet

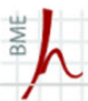


- **Transport:** speciális Bt protokollok, minden kommunikációban részt vesznek
- **Middleware:** spec. Bt és adoptált protokollok. ezek teszik lehetővé a spec. és hagyományos alkalmazások kommunikációját Bt hálózaton
- **Radio:** fizikai réteg, modulált



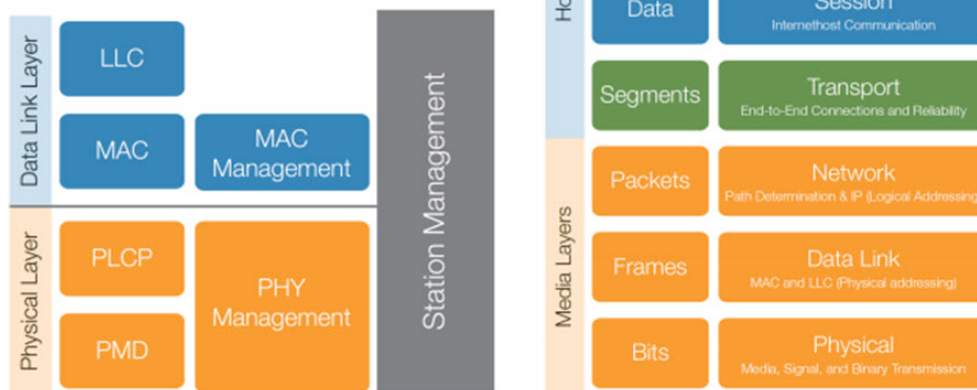
- **Baseband:** kb. felső fizikai és MAC és : a Bt kommunikáció, hálózat szervezés, kapcsolatok felépítése
- **HCI Host controller interface:** nem protokoll, hanem if., kapcsolódási pont a baseband protokollhoz
- **Link Manager:** LMP protokollal kommunikálnak, kapcsolatok menedzselése, titkosítási, hitelesítési információk
- **L2CAP:** Logical Link Control és Adaptation Protocol, Bt specialitások eltakarása, if. a felső rétegek felé
- **SDP Service Discovery Protocol,** az egyes eszközök ezzel derítik ki az igénybe vehető szolgáltatásokat
- **RFCOMM:** RS232 soros port protokoll emulációja, olyan alkalmazások számára, amik RS232 vezetéken kommunikálnának
- **TCS Telephony Control Signaling + egyéb:** számos protokoll, RFCOMM fölött megvalósítva

- 4.19. Ismertesse az IEEE 802.11 szabvány és az OSI modell közötti kapcsolatot, valamint mutassa be a 802.11 szabványban definiált rétegek és alrétegek fő feladatait!



## A 802.11 és az OSI modell kapcsolata

- A 802.11 szabványok az OSI modell két alsó rétegét, a fizikai és az adatkapcsolati (más néven közeghozzáférési) rétegeit definiálják



Az egyes **MAC alrétegek** feladatai:

- MAC alréteg: közeghozzáférési megoldások
- MAC Management alréteg: teljesítmény menedzsment, roaming, szinkronizálás, biztonsági szolgáltatások

A **PHY** alrétegek feladatai:

- Physical Layer Convergence Protocol (PLCP): illesztési feladatokat lát el, vagyis a MAC kereteket fizikai csomagokká alakítja, különféle PHY-k számára megfelelő csomagokat állít elő
- Physical Medium Dependent (PMD) alréteg: moduláció és kódolás,
- PHY Layer Management: management funkciók ellátása
- Station Management: MAC és PHY rétegek közti együttműködését koordinálja

#### 4.20. Mutassa be a PCF működést!

A Point Coordination Function működése:

- A Point Coordinator (az AP) vezérli ezt a működést (PointCoordinator)
- A versengés elkerülése végett a PC lekérdezi azon STA-kat, aki képes a PCF működésre, hogy akar-e adni, vagy sem – polling
- STA válasza SIFS idő múlva
- Polling lista készítése és frissítése – kiosztják, ki, melyik idősrben adhat
- A DCF mellett működik ez a mód
- Contention Free Period (CFP) – versengésmentes időszak
- CFPMaxDuration határozza meg a versengésmentes időszak maximális hosszát
- Periodikus beacon üzenet tartalmazza a CFP hosszát
- A DCF-ben részt vevő STA-k a CFP alatt nem figyelik a csatornát – NAV (Network Allocation Vector) értékét a CFP idejére állítják
- A CFP ideje alatt a kereteket SIFS időközönként adják, ezáltal a DCF működésben részt vevő terminálok nem tudnak a csatornához férni, valamint a backoff idejük sem csökken

#### 4.21. Ismertesse a CSMA/CA és a CSMA/CD működését, valamint definiálja a felhasználási területeiket (melyik milyen környezetben használható)!

CSMA: Carrier Sense Multiple Access, CD (Collision Detection)

Ennél a módszernél, mielőtt az állomás elkezdene adni, behallgat a csatornába, hogy megtudja van-e éppen olyan állomás, aki lefoglalja a csatornát. Ha nincs akkor elküldi az üzenetét, ha van akkor egy adott időtartamig várakozik. Az állomás által küldött üzenet eljut minden címre és aszerint, hogy ki ismer magára címzettként feldolgozza vagy eldobja az adott adatot. Amennyiben a csatornán ütközés lép fel, az állomás véletlen ideig várakozik, majd újra próbálkozik (behallgat a csatornába). Az ilyen protokoll szerint működő állomások 3 állapotot vehetnek fel: versengő, átviteli, tétlen. Ezt a fajta protokollt az Ethernet használja.

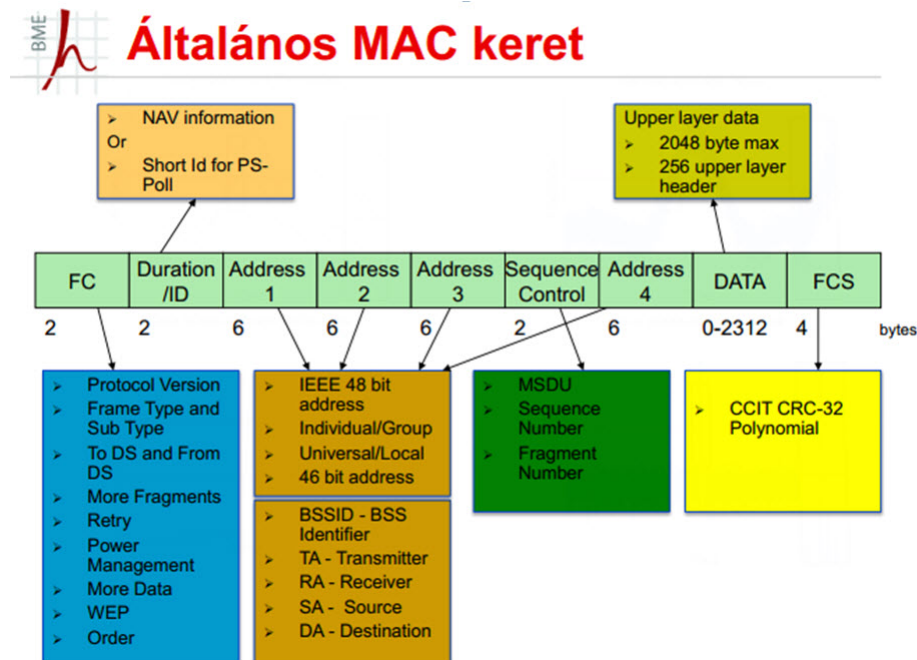
CSMA: Carrier Sense Multiple Access, CA (Collision Detection)

Az előzőekhez hasonlóan működik azzal a különbséggel, hogy itt minden állomás adást figyelve “behallgat” a csatornába. Az adás befejezése után minden állomás egy adott ideig vár, amit egy logikai listában elfoglalt helyük határoz meg. Ha ez alatt az idő alatt más állomás nem kezd adni, akkor elkezd az adást. Így biztosan nem lesz ütközés emiatt. (nem csak detektálni tudjuk az ütközést, hanem elkerülni is!)

**4.22. Mutassa be a 802.11 szabványban definiált kerettípusokat, valamint definiálja az általános MAC keret felépítését!**

A MAC keret felépítése:

- Adat keret: adatátviteli célra
- Vezérlő keret: közeghozzáférési célra, RTS, CTS, ACK
- Menedzsmet keret: menedzsmet információk kerülnek továbbításra, pl. probe request és authentication



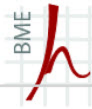
**4.23. Röviden mutassa be a 802.11n szabványt, különös tekintettel a nagysebességű adatátvitel megvalósításának lehetőségeire!**

A moduláció típusa Orthogonal Frequency-Division Multiplexing (OFDM, 56 segédvívvel 20 MHz, 114 segédvív 40 MHz). Működési frekvencia: 2,4 GHz és opcionálisan 5 GHz. Hagyományos 20 MHz sáv szélesség mellett a szélesebb 40 MHz-es sáv szélesség is használható (channel bonding, 2 db 20 MHz vív).

- MIMO alkalmazása
- PHY és MAC rétegbeli javítások

- PHY: hatékony jelfeldolgozás, fejlett modulációs technikák, többes antenák használata
- MAC: protokoll kiegészítések a sávszélesség hatékony kihasználása szempontjából
- Az eredeti 802.11 –hez képest nagyobb méretű keretek, illetve több keret együttes küldése
- Előbbi módosításoknak (High Throughput (HT) javítások) köszönhetően a sebesség elérheti a 600 Mbits/s értéket

4.24. Mutassa be a Two Way Time of Arrival ranging működési módot!



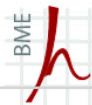
## Two Way Time of Arrival (TW-TOA)

- Alap TOA
  - A cél node jelzi a forrás által küldött jel beérkezési idejét
  - A beérkezési idő alapján forrás node képes kiszámítani a TOF-ot
  - Elengedhetetlen a két node szinkronizációja
- TW-TOA
  - Szinkronizáció nem szükséges a működéséhez
  - Lépései:
    1. A cél node ranging kérést ( $RFRAME_{req}$ ) küld a forrás node-nak és feljegyzi a küldés időpontját ( $T_1$ )
    2. A forrás node ranging válasz ( $RFRAME_{rep}$ ) üzenettel felel a kérésre
    3. A cél node feljegyzi a válasz beérkezésének időpontját ( $T_2$ )  
A cél node kiszámolja a körülfordulási időt ( $T_r$ ):  

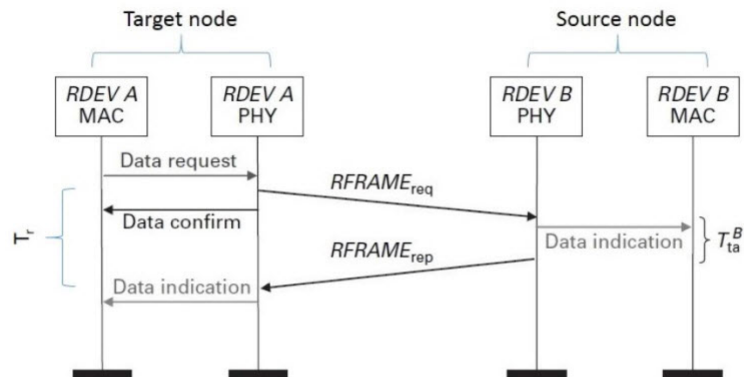
$$T_r = T_2 - T_1$$
  - Ez alapján a TOF a két node között:  

$$T_{TW} = T_r / 2$$
  - A két node közötti távolság pedig:  

$$d = c \cdot T_{TW}$$



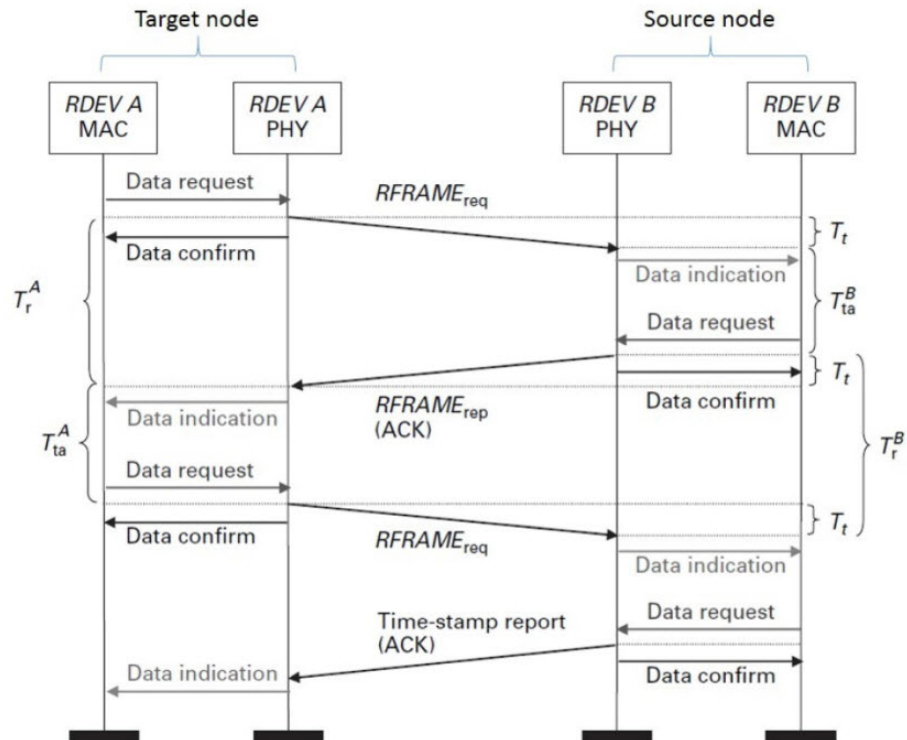
## Alap TW-TOA



- 3 forrás node pozíciója és tőlük mért 3 távolság alapján a cél node pozíciója pontosan kiszámítható (idealizált esetben)
- A valóságban azonban a forrás node-nál van némi késleltetés az  $RFRAME_{req}$  üzenet vétele és az  $RFRAME_{rep}$  üzenet elküldése között ( $T_{ta}^B$ )
- $T_{ta}^B$  a nanoszekundumos tartományban van, ami nagyságrendileg tíz centiméteres távolságbecslési hibát eredményez  $\rightarrow$   $T_{ta}^B$  nagyon pontos becslése szükséges a pontos pozicionáláshoz

4.25. Röviden ismertesse az SDS TW-TOA és az alap TW-TOA megvalósítások közötti különbségeket!

**SDS TW-TOA**



A TW-TOA becslése során hibák keletkezhetnek, az eszközökben működő órák eltolódása stb. Az SDS protokoll célja ezen offset hiba kiküszöbölése. Mindkét Node becsli a  $T_r$  és a  $T_{ta}$  időket. Végül a forrás node elküld egy időbélyeget, mely tartalmazza az általa mért  $T_r$  és  $T_{ta}$  időket. Sokkal pontosabban lehet megmérni az időket.

4.26. Foglalja össze a szélessávú és a keskenysávú jelek közötti különbségeket!

A szélessávú jelek alapvetően abban különböznek a keskenysávú jelektől, hogy a szélessávú jelek időtartományban nagyon keskenyek és frekvenciatartományban nagyon szélesek (impulzus-szerű jelek). Jól használható, kis távolságokon belül pozíció követésre és adatátvitelre. UWB jeleknek nevezzük azokat a jeleket, amelyeknek az elfoglalt frekvenciasávja 500 MHz-től 5 GHz-ig terjed. (1 - 10.6

GHz frekvenciáig) Az adó oldalon időben nagyon keskeny impulzusokat adunk, a vevők pedig nagyon pontosan tudják detektálni a vett impulzus hosszát és időpontját. (alkalmas lehet távolság mérésére és nagy sebességű adatátvitelre) A sávszélesség növelésével, az adatátviteli sebesség lineárisan, míg az SNR növelésével ugyanez csak logaritmikusan növekszik. (megéri sávszélességet növelni, SNR helyett)

$$C = B \log\left(1 + \frac{S}{N}\right) \quad (8)$$

#### 4.27. Ismertesse a 802.15.4 szabvány fő paramétereit, funkcióit!

- Különböző adatsebességek: 250, 40, 20 kbps
- Különböző frekvenciasávok támogatása: 16 csatorna 2,4 GHz-en, 10 csatorna 915 MHz-en, 1 csatorna 868 MHz-en
- Két működési mód: csillag vagy P2P
- CSMA/CA közeghozzáférés
- Dinamikus eszközcímzés
- Teljes kézfogás protokoll az átvitel megbízhatósága miatt
- Alacsony késleltetésű eszközök támogatása, alacsony fogyasztás

#### 4.28. Részelt ALOHA teljesítőképessége, throughputja, random hozzáférés általános jellemzése ez alapján (számpélda is lehet).

A részelt ALOHA alapötlete, hogy a csatornán  $T$  hosszúságú időréseink vannak. A felhasználók csatornahasználata véletlenszerű, és alacsony valószínűségű. Egy csomag leadása pont  $T$  idő alatt végbemegy. Az egy időrésben küldeni kívánt csomagok száma így Poisson eloszlásúnak tekinthető. A **Throughput** az egy időrés alatt a csatornán átjutott hibátlan csomagok száma, részelt ALOHA esetében ez 1. A **Load** megmutatja, hogy a felhasználók átlagosan időrésenként hány csomagot akarnak küldeni. Ezt nevezzük a csomag érkezési intenzitásnak jele  $G$ . A sikeres csomag küldés valószínűsége  $P_{sikeres}$  nem más, mint az az eset, amikor pont egyetlen csomagot akar küldeni egyetlen felhasználó (az adott időrésben). Így a következő összefüggésre jutunk ( $S$  a várható érték):

$$P_{sikeres} = G e^{-G} = S \quad (9)$$

$$S = \frac{1}{e} \quad (10)$$

Az utóbbi összefüggés pontosan akkor érvényes, ha  $G = 1$ . Pontosán ekkor van maximuma a  $P_{sikeres}$  valószínűségnek.



## 5. QoS paraméterek

A szolgáltatás minőségét alapvetően meghatározó elemeket soroljuk ide:

- Késleltetés - terjedési, kapcsolási, kiszolgálási, szegmentálási
- Jitter (késleltetés ingadozás) - a fentiek ingadozása
- Csomagvesztés - torlódás, fizikai rétegben, hálózati elem hibája stb.
- Throughput - link, osztály, út kapacitás... mérés: átlagos adatsebesség egy időszakra
- Rendelkezésre állás -  $Availability = \frac{T_{workingtime}}{T_{totaltime}}$
- Tapasztalt minőség - QoE, főleg videó és hangátvitelnél, esetleg online gaming esetén

## 6. Várható érték, szórás, relatív szórás

A valószínűségszámításból ismert alapfogalmak itt is érvényesek. Legyen  $X$  véletlen valószínűségi változó, és  $E(X)$   $X$  várható értéke.  $X$  ingadozása  $E(X)$  körül pedig szemléletesen a szórás. Tehát az  $X$  változó várható értékétől való **eltérés** várható értéke (szórás), és az ebből származtatott szórásnégyzet:

$$S(X) = E((X - E(X))) \quad (11)$$

$$S^2(X) = E(X^2) - E(X)^2 \quad (12)$$

A normalizált ingadozás a várható érték körül (relatív szórásnégyzet):

$$CV(X) = \frac{S(X)^2}{E(X)^2} \quad (13)$$

**Független** események várható értékei összeadódnak, szórásnégyzetei négyzetesen adódnak össze:

$$E(X + Y) = E(X) + E(Y) \quad (14)$$

$$S(X + Y)^2 = S(X)^2 + S(Y)^2 \quad (15)$$

## 7. Korreláció

$X$  és  $Y$  egymástól függő változók és kérdés, hogy mennyire korreláltak egymással. Ez a korreláció:

$$Corr(X, Y) = \frac{E(XY) - E(X)E(Y)}{S(X)S(Y)} \quad (16)$$

Ennek maximuma, ha a minták teljesen hasonlóak:

$$Corr(X, Y)_{max} = 1 \quad (17)$$

Speciális esete az auto-korreláció, ami az  $n$  mintával későbbi minták korrelációját jelenti, vagy  $d$  idővel távolabb levő minták korrelációját. (egyetlen valószínűségi változó mellett)

## 8. Aggregálás hatása

Tudjuk, hogy **független** véletlen események aggregálása csökkenti a relatív szórást. Ha ez megtörténik, az adott erőforrás kihasználtsága nő, kisebb erőforrás is elégséges, de a redundancia csökken, így a sebezhetőség nő.

## 9. Forgalmi méretezés definíciók

### 9.1. Erlang forgalom

Erlang forgalom a következőt jelenti:

- egész értékű véletlen folyamat
- heti, napi periodicitás
- szolgáltatási célkitűzés ennek optimalizálása
- forgalmas óra

A **véletlen** forgalom:

- igények egyensúlyi eloszlása: Poisson eloszlás
- kapcsolódó Poisson/Exponenciális modell
- Markov láncos leírás

## 10. Forgalmi tervezés különböző sáv szélesség igényekkel

Ide tartozik az Erlang B féle veszteségi formula, amely megenged egy bizonyos szintű blokkolást és ennek segítségével tervezhető a felajánlott forgalom.

- egyesével ugráló
- egész értékű
- véletlen igényfolyamatok esetén csonkolt Poisson eloszlás

## 10.1. Kaufmann-Roberts Formula

- nem csak egyesével ugráló
- egész értékű
- véletlen igényfolyamatok esetén rekurzív kifejezés

Nem jó közelítés mindig az exponenciális eloszlás (Poisson folyamat)

## 10.2. Önhasonló forgalom

Az önhasonló forgalom, más néven fraktál-jellegű forgalom szerencsétlen modellezés ismét, mivel az autokorrelációja nagyon lassan csökken az idő függvényében (pontosan ez jelenti azt, hogy önhasonló a folyamat). Exponenciálisnál lassabban cseng le az autokorrelációs függvénye.

## 10.3. Nehézfarkú eloszlás

Itt a problémánk az, hogy a folyamatunk szórása elméletileg végtelen, így nehezíti az előre tervezést.  $S(X) \rightarrow \infty$

## 11. Forgalmi osztályok és jellemzőik

Amikhez az adott forgalmi osztályoknak alkalmazkodniuk kell azok a következők:

- Igény érkezési intenzitás [a]
- Átlagos igény tartási idő (foglalás) [b]
- Sáv szélesség (több állapot is lehetséges) [c]
- Minimum és Maximum sáv szélesség [d]
- Átvitt adatmennyiség [e]

Ezeknek a tulajdonságoknak felelnek meg részlegesen az egyes forgalmi osztályok:

- CBR (Constant Bit Rate) - [a, b, c]
- VBR (Variable Bit Rate) - [a, b, c]
- Adaptív - [a, b, d]
- Elasztikus - [a, d, e]
- Best Effort - "ami a csövön kifér" elv

## 12. Erőforrás-menedzselési módszerek

Ennek lényege, hogy a rendelkezésre álló erőforrásokat maximálisan kihasználjuk, illetve, hogy az elvárt szolgáltatási minőséget tudjuk biztosítani. Ehhez kell erőforrás allokáció és erőforrás megosztás. Ezek módjai a következők lehetnek:

- Prioritásos kiszolgálás a közös erőforráson
- Súlyozott erőforrás kiszolgálás
- vagy a fentiek valamilyen kombinációja...

A súlyozott erőforrás kiszolgálás lehetséges bit-szinten, illetve csomag szinten. A csomag szintű implementációk a következők:

- Weighted Round Robin - csomagmérettől függő súlyozás Round-Robin mellett
- Weighted Fair Queueing - csomagmérettől függően súlyozva áll rendelkezésre az erőforrás az egyes folyamatoknak (FIFO FQ)
- Deficit Round Robin - mindenki azonos ideig kap erőforrást és nincs súlyozás, viszont egyszerű implementálni

## 13. Mobil backhaul követelmények

### 13.1. Milyen alapvető szempontok alapján határozhatók meg a mobil backhaul-lal szemben támasztott követelmények?

- Mit kell kiszolgálni? - pl. beszéd, SMS, Internet, Mobil hálózati szolg., RAN működési jelzések
- Hogyan kell kiszolgálni? - alkalmazásforgalmak minőségi követelményei
- Milyen környezetben kell kiszolgálni? - mindent IP felett (NGN), hálózati infrastruktúra (vez/mobil), gazdaságosan és hatékonyan, menedzselte hálózat és szolgáltatások figyelembe vételével
- Mik a kiszolgálás főbb jellemzői? - távolságok, kapacitások, üzemeltetés, fejlesztés, topológia, hibatűrés, költségek stb.

### 13.2. Hogyan befolyásolja a backhaulban alkalmazható technológiákkal szemben támasztott követelményeket a kiszolgált mobil technológia? (Adjon példákat is!)

???

A backhaul felépítése képes kell legyen arra, hogy a mobil szolgáltatás előírt jellemzőit teljesítse. Például: szolgáltatás rendelkezésre állása, blokkolás maximális valószínűsége, csomagvesztés, késleltetés és jitter előírások stb.

???

### 13.3. Hogyan befolyásolja a meglévő vezetékes hálózati környezet a mobil backhaul megvalósítását?

Értelemszerűen olyan mobil backhaul rendszert szeretnénk felépíteni, amely minél kevesebb módosítással kialakítható a meglévő vezetékes hálózati rendszerből. Ilyen párosítások például a következők:

- GSM - SDH
- 3G - SDH / Ethernet - IP/MPLS
- 4G - Ethernet és IP/MPLS
- Heterogén hálózatok esetén külön van mikro-,makro-,femto-cellákhoz (általában Ethernet vagy IP/MPLS)

**13.4. Hogyan befolyásolják a backhaul megoldások a mobil hálózatok üzemeltetésének és a mobil hálózat szolgáltatásainak minőségét?**

???

... talán inkább a harmadik kérdésre adott válasz illik ide ...

???

**13.5. Jellemezze és hasonlítsa össze a mobil backhaul kialakításakor alkalmazott topológiai megoldásokat! (A topológiák jellemzése, értékelése során vegye figyelembe az összekapcsolandó mobil hálózati funkciókat és az az összekapcsolásuk során nyújtandó hálózati szolgáltatásokat!)**

- fa topológia - jól aggregál, de sebezhető (nem redundáns)
- gyűrű topológia - egyszerű védelem (redundancia), rossz skálázódás, homogén szerkezet
- szövevényes (mesh) - rugalmasan alakítható, több redundancia, komplexebb berendezés (hátrány!), heterogén szerkezetű is lehet
- összetett - ezek valamilyen kombinációja, előnyök egyesítése, hierarchikus vagy lapos kombinációk

## 14. SDH topológia és hálózat

### 14.1. Tipikusan milyen mobil hálózatelemek között, milyen célra, milyen követelmények alapján alkalmaznak SDH technológiát a mobil backhaulban?

A mobil hálózati elemek, amelyeket SDH hálózattal kapcsolnak össze:

- BTS-BSC közti kapcsolat
- BSC-MSB közti kapcsolat
- MSC-MSB közti kapcsolat
- MSC-PSTN közti kapcsolat

Alapvetően jelzéseket, adatokat és szinkronizációs információkat visznek át rajta. Ezen keresztül osztják szét a Master órajelet is. Fizikailag lehet optikai szálal összeköttetés, vagy mikrohullámú link.

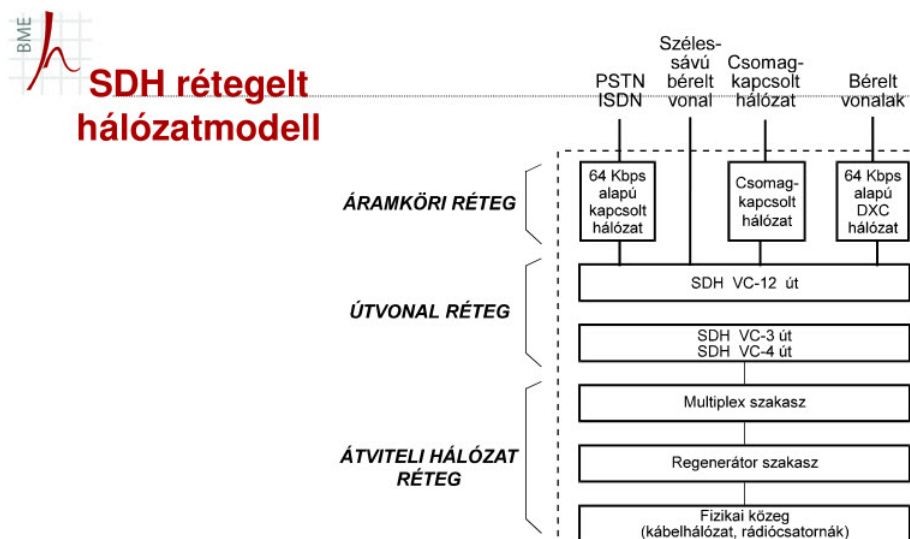
### 14.2. Jellemezze röviden az SDH technológiát (hálózati szolgáltatások, (hálózati és csomóponti funkciók, hálózat-szervezési alapelvek), és kapcsolja ezeket a jellemzőket a GSM hálózat backhauljával kapcsolatos követelményekhez!

Az SDH technológia alapvető hálózati szolgáltatásai a következők:

- fix átviteli kapacitások
- többfajta kliens kiszolgálása (ezért lehet sok helyen alkalmazni)
- alapvető hálózati funkciók
  - útképzés
  - védelem és hibadetektálás
  - menedzselhetőség
- alapvető csomóponti funkciók
  - jelalakformálás (erősítés, regenerálás)
  - illesztés, multiplexálás
  - kapcsolás

Az SDH hordozója legtöbbször mikrohullámú link, de lehet üvegszál is.

14.3. Hogyan épül fel az SDH hálózat rétegszerkezete, melyik SDH hálózati réteg milyen szerepet játszik a mobil backhaulban szükséges funkciók megvalósításához?



- adaptálás (beillesztés, keretezés, rétegspecifikus információk hozzáadása)
- terminálás (rétegspecifikus információk eltávolítása, feldolgozása)
- önállóan menedzselhető rétegek, rétegfunkciók, rétegszolgáltatások

14.4. Milyen logikai (hálózati) topológiai megoldásokat támogat az SDH technológia, hogyan szolgálják ezek a topológiák a mobil backhaul kialakítását?

Az egyes hálózati elemek között más-más topológiát használunk:

- BTS-BSC közti kapcsolat esetén
  - pont-pont topológia (sebezhető)
  - felfűzéses topológia (TM-ADM-...-ADM-DXC)
  - gyűrű topológia (ADM-ADM-ADM...ADM-ADM vagy DXC), redundáns, tipikusan a legmegfelelőbb
  - szövevényes topológia - többszörös összefüggőség, komplex védelem viszont nagyon összetett és költséges



- BSC-MSC közti kapcsolat esetén
  - pont-pont topológia
  - felfűzéses topológia
  - gyűrű topológia
  - szövevényes topológia
- MSC-MSC és MSC-PSTN közti kapcsolat
  - szövevényes hálózat kell mindenképpen a redundancia miatt, nagyon fontos a védelem ezen a szinten

#### **14.5. Miért szükségesek hálózatvédelmi megoldások (védett hálózati szolgáltatások) a mobil backhaul kialakításához? Adjon példát SDH védelmi megoldásra!**

Az egyre növekvő forgalom és kapacitásigény miatt erősen megnőtt az adatfolyamok koncentráltsága. Ez azt jelenti, hogy ha valamelyik linken hiba történik akkor arányosan sokkal nagyobb veszteség keletkezik a nagy adatsűrűség miatt. Illetve a szolgáltatók a szolgáltatás minőségével, megbízhatóságával akarják eladni a termékeiket, így számukra is kritikus, hogy a fellépő hibákat minél gyorsabban orvosolják. A mobil backhaulban ez kifejezetten fontos és az SDH nyújt is ilyen védelmi megoldásokat. Hálózati szinten ez a következőkből áll:

- végponttól végpontig több független út
- kapcsolódási pontok hibái elleni védelem
- hálózat méretezési problémák
- nyálábrendezés (DXC vagy STM-1 szinten)

### **15. Szolgáltatói kategóriájú Ethernet**

#### **15.1. Tipikusan milyen mobil hálózatelemek között, milyen célra, milyen követelmények alapján alkalmaznak Ethernet technológiát a mobil backhaulban?**

A mobil adatszolgáltatások megjelenésével előtérbe került a backhaulban megvalósított adattranszport. Szolgáltatói szintű Ethernet kapcsolatot használnak a következő helyeken:

- PCU-SGSN között
- RNC-SGSN között
- SGSN-GGSN között

- GGSN-PDN között

Ezt a kapcsolatot használják jelzés és adatátvitelre, illetve szinkronizációra. Követelmény, hogy jól menedzselhető legyen a hálózat, illetve legyenek hálózati védelmek beépítve.

### **15.2. Jellemezze röviden a Ethernet technológiát, miért, hogyan változott a LAN-os Ethernet a nyilvános hálózati MAN és WAN megoldások kiszolgálására?**

Az Ethernet technológia elterjedésével igény lett arra, hogy az addig kisebb helyi hálózatokban használt (Local Area Network) Ethernet rendszert képessé tegyék nagyobb léptékű város/település (WAN, MAN) méretű hálózatok ellátására. Technológiailag át kellett tudni térni a koaxiális kábeles, UTP-s, illetve optikai szál as átviteli közegre, mindemellett többféle átviteli sebességet is ki kellett alakítani, és ehhez persze hálózati eszközöket is be kellett szerezni. Elvárások a nagy léptékű Ethernet-tel szemben:

- alacsony bevezetési költség (egyszerű, olcsó eszközök és működés)
- hálózatok összekapcsolása és aggregált forgalmak kezelése
- gerinchálózatra alkalmasság tétel, nagyobb sebesség pl. 1G, 10G, 100G Ethernet (optikai szálon is)

### **15.3. Az Ethernet protokoll milyen módosításai szolgálják a nagy méretű (felhasználószám, hálózatelemek száma) szolgáltatói Ethernet hálózatok hatékony megvalósítását?**

A szolgáltatói Ethernet kiegészült a következő szolgáltatásokkal a szabványos Ethernet-hez képest:

- Szabványos szolgáltatások: E-LINE, E-LAN, E-TREE, áramkörkapcsol emulációs szolgáltatások: SDH szolgáltatás Ethernet felett
- skálázhatóság: 1G, és 10G Ethernet
- rendelkezésre állás: hálózati támogatás és architektúrális változatok a hibadetektáláshoz (nem szakad meg a szolgáltatás közben!)
- QoS opciók támogatása :)
- Szolgáltatás menedzsment: központi felügyelet
- Flow Controlling: gyorsabb link elárastja a lassabbakat!
- Hardveres redundancia: több kapcsoló, több ventilátor stb.
- Menezsment funkciók: fejlett hibajelzések, hibabehatárolás

#### 15.4. Milyen támogatást nyújt a szolgáltatói Ethernet technológia a különböző forgalmi osztályok, különböző minőségű szolgáltatások megvalósításához? Miért szükségesek ezek a mobil backhaul kiszolgálása során?

A szolgáltatói Ethernet támogatja a QoS-t és ezt a mobil backhaul esetén is elvárjuk, így itt is szükséges. 8 szolgáltatási osztály van és ezek alapján a prioritások.



#### Szolgáltatások, megoldandó problémák: Szolgáltatási osztályok (QoS) támogatása

- 8 szolgáltatási osztály (3 bit) a DiffServ Assured Forwarding Code Point-oknak megfelelően (IP QoS Differentiated Services architektúra)

S-Tag	Priority	CFI	S-VLAN ID	Type/Length
	3b	1b	12b	16b
	<b>Priority</b>	<b>Class</b>		
	7	Strict Priority		
	6	AF1		
	5	AF2		
	4	AF3		
	3	AF4		
	2	AF5		
	1	AF6		
	0	Best Effort		

#### 15.5. Milyen redundanciák, milyen védelmi megoldások vannak az Ethernet hálózatelemekben és hálózatokban? Miért szükségesek hálózatvédelmi megoldások (védett hálózati szolgáltatások) a mobil backhaul kialakításához?

Layer-1, Layer-2 és Layer-3 szinten is van redundancia. Layer-1 esetén értelemszerűen több eszköz, szünetmentes táp, védett memória, hot-swappable alkatrészek. Layer-2 szinten gyűrűs topológia, többszörös összeköttetések, STP stb. Layer-3 szinten Routing és VLAN aggregáció. Továbbiak: port duplikálás, Ethernet Protection Switching (VLAN alapokon), logikai részhálózatok közti átkapcsolás.

## 16. IP és IP/MPLS

### 16.1. Hogyan támogatja az IGP (pl. OSPF) a hálózati szolgáltatások fenntartását hálózati hibák (pl. linkhiba) esetén? Miért szükségesek hálózatvédelmi megoldások (hibatűrő hálózati szolgáltatások) a mobil backhaul kialakításához?

A kapcsolatállapot alapú IGP esetén minden egyes linkben tárolódik a hálózat szerkezetére vonatkozó információhalmaz (melyik link merre van és milyen távol). A hálózat állapotának változásakor a változás ténye tovaterjed a teljes hálózaton, és mindenki átállítja az állapotát ennek megfelelően. (Link State Database) LSD hö :) OSPF esetén: több másolatban létező elosztott adatbázis modell (minden routeren pontosan ugyanaz!), a terjedés elárasztásos modellel működik (flooding), ezek alapján minden végpont-hoz megtalálható a legrövidebb út (Dijkstra algoritmus). Amennyiben link szakadás történik, rögtön újra tudjuk számolni a legrövidebb utat, mert mindenkihez eljut a rossz link címe és helye. Frissül az útadatbázis minden routeren, és így képes útválasztásra ismét.

### 16.2. Ismertesse röviden az SRLG (Shared Risk Link Group) fogalmát, és szerepét a hibatűrő szolgáltatások kialakításában? Miért szükségesek hálózatvédelmi megoldások (hibatűrő hálózati szolgáltatások) a mobil backhaul kialakításához?

Shared Risk Link Group: azon linkek csoportja, amelyek ugyanazon fizikai hiba hatására esnek ki, L2 és L1 hibák, esetleg tágabb értelemben L3 hibák is. Ezért függetleníteni kell a linkeket, és minél több redundanciát szervezni a hálózatba (backup tunnelek).?? A szerepe, hogy segítségével felderíthetők a hálózat "gyenge" pontjai. ??

### 16.3. Az IP/MPLS milyen szolgáltatási képességei meghatározóak a mobil backhaul kialakítása során?

IP/MPLS tulajdonságai:

- címke alapú továbbítás a Core hálózatban
- nagy mennyiségű és nagy aggregátságú forgalom
- fejlett címkekezelés (megállapítás, fenntartás, visszavonás)
- menedzselt szelektív védelmi funkciók
- on-line mérés és vezérlés (QoS-t nem bántjuk)

- komplex SW, on-line mérések, kiértékelés, tervezési és konfigurációs akciók

#### **16.4. Miért nem kézenfekvő a garantált minőségű szolgáltatások megvalósítása az IP és IP/MPLS hálózatokban? Miért szükségesek garantált minőségű szolgáltatások a mobil backhaul kiszolgálása során?**

Az alapproblémánk az, hogy az IP réteg felett csomag/keret alapú az adattovábbítás, ezek a forgalmak a közös erőforrásokért versengenek. A forgalom nem kontrollált, éppen ezért időnként előfordul erőforrás szűkösség, ilyenkor megnő a késleltetés, jitter stb. romlik a QoS. A gond az, hogy alapvetően ez egy **Best Effort** típusú szolgáltatás.

#### **16.5. Ismertesse, hogy milyen architektúrális megoldások szolgálnak a garantált minőségű szolgáltatások megvalósítására? Miért szükségesek garantált minőségű szolgáltatások a mobil backhaul kiszolgálása során?**

Az architektúrális megoldások közül legfontosabb az IntServ, ez a következőkből áll:

- Routerenként menedzselt erőforrás állapotok
- Session felépítés: egy új adatfolyamnak le kell foglalnia a szükséges erőforrásokat routerenként
- Léteznek forgalmi osztályok: (Best Effort, Controlled Load, Guaranteed Service)
- IntServ jellemzők összefoglalása: flow alapú, routerenkénti CAC, komplex, jól skálázható

### **17. Nagysebességű vezetékös hozzáférés**

#### **17.1. Milyen szerepet játszanak a rézalapú és a fényvezető alapú hozzáférési technológiák a mobil backhaul kialakításában?**

✓

## 17.2. Mik a főbb jellemzői ezeknek a hozzáférési technikáknak? Hogyan illeszkednek ezek a hálózati képességek a mobil backhaulban betölthető szerepükhöz?

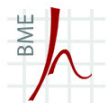
A DOCSIS rendszerekben fontos, hogy ezek támogatják a QoS-t így ez a tulajdonság a mobil backhaul-ban is jól használható:

- DOCSIS 1.1 és 2.0 Service Flow: egyirányú adatfolyam készletetés, jitter, sávszélesség, stb. paraméterekkel
- csomagok rendezése, forgalom osztály alapú kiszolgálás: prioritás, IP paraméterek, MAC cím stb.
- 5 féle upstream QoS szolgáltatás

✓

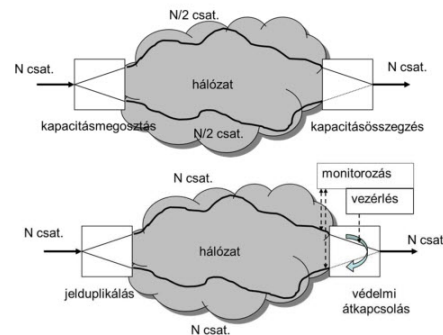
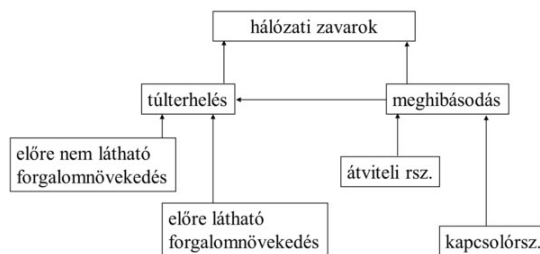
## 18. Integrált hálózati kép

### 18.1. SDH-GSM

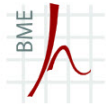


### Mobil hálózatok vezetékes backhaul technológiái Szolgáltatásminőségi és rendelkezésreállási vonatkozások rövid áttekintése: **1. TDM alapú backhaul**

- TDM (GSM –SDH)
  - beszédszolgáltatás, GSM jelzések
  - beszédszolgáltatás minősége
    - érthetőség (rádiós lefedettség, az SDH backhaul gyakorlatilag nem befolyásolja)
    - blokkolás (rádiós kapacitás, GSM SW és backhaul hibatűrés)
      - méretezések névleges feltételekre (becsült forgalom, hibamentes erőforrások)
      - gyakorlati esetben a SDH backhaul hibái befolyásolhatják (pl. BTS – BSC – MSC összeköttetés degradálódása: BTS-BSC osztott utas elvezetés egyik ága kábelhiba miatt kiesik)
      - ha öngyógyító az SDH hálózat (automatikus védelmi átkapcsolások), akkor a védett hibáknak nincs hatása, ha a védelmi erőforrások függetlenül hibásodnak meg

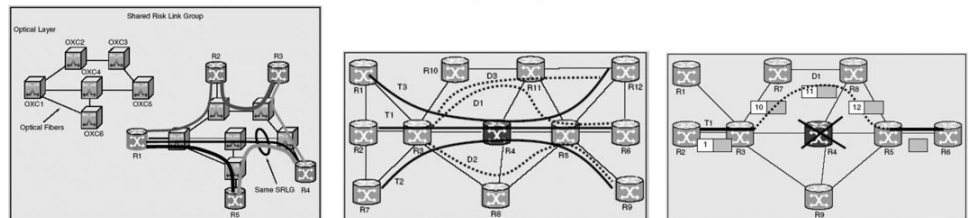


## 18.2. LTE-IP



### Mobil hálózatok vezetékes backhaul technológiái Szolgáltatásminőségi és rendelkezésreállási vonatkozások rövid áttekintése: **2. csomag alapú backhaul**

- Csomag/keret alapú (LTE - IP és szolgáltatói Ethernet)
  - adatszolgáltatás, LTE jelzések (csomag/keret alapú emuláció - CES- TDM szolgáltatást is szállíthat)
  - adatszolgáltatás minősége
    - BER (rádiós lefedettség, a backhaul gyakorlatilag nem befolyásolja)
    - QoS: csomagvesztés, késleltetés, késleltetés-ingadozás (rádiós kapacitás, IP és Ethernet szolgáltatás, külső aggregációban esetleg hordozó MAC pl. PON dinamikus sáv szélesség kiosztás)
      - méretezések névleges feltételekre (becsült forgalom, hibamentes erőforrások)
      - ha IP alatt kapcsolt Ethernet, akkor az L3 és L2 QoS architektúrákat össze kell hangolni (pl. DiffServ AF CP és Ethernet 802.1Q prioritás), IP/MPLS TE védelmek hatása ennél kézben tarthatóbb (explicit utak)
      - gyakorlati esetben a backhaul hibái befolyásolhatják: IP IGP adaptáció, Ethernet STP adaptáció megváltoztatja a hibamentes terhelési viszonyokat
      - ha az IP-t, Ethernetet szállító WDM hálózat öngyógyító (automatikus védelmi átkapcsolások), akkor a védett hibáknak nincs hatása, ha a védelmi erőforrások függetlenül hibásodnak meg (SRLG)



## 18.3. Circuit Emulation Services

A szolgáltatói szintű Ethernet extra szolgáltatása, hogy képesek vagyunk az áramkörkapcsolt hálózat emulációjára Ethernet réteg felett. Így például az SDH hálózatot is képes emulálni. (TDM Access Line Service)

## 18.4. Szinkronizálás

A szolgáltatói Ethernet rétege fölött visszük át a rendszerek közti órajelet, amelyet szinkronizálásra is használunk.

L<sup>A</sup>T<sub>E</sub>X