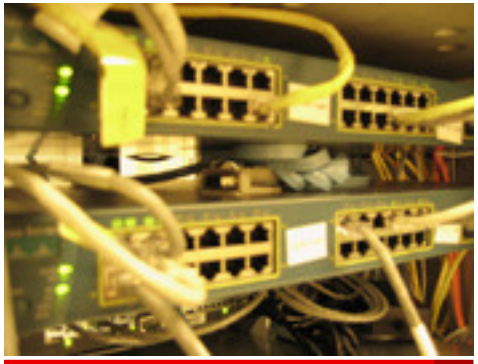


INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK

Authentication, Authorization, Accounting (AAA)

Dr. Imre Sándor
Szabó Sándor
BME Híradástechnikai Tanszék
szabos@hit.bme.hu

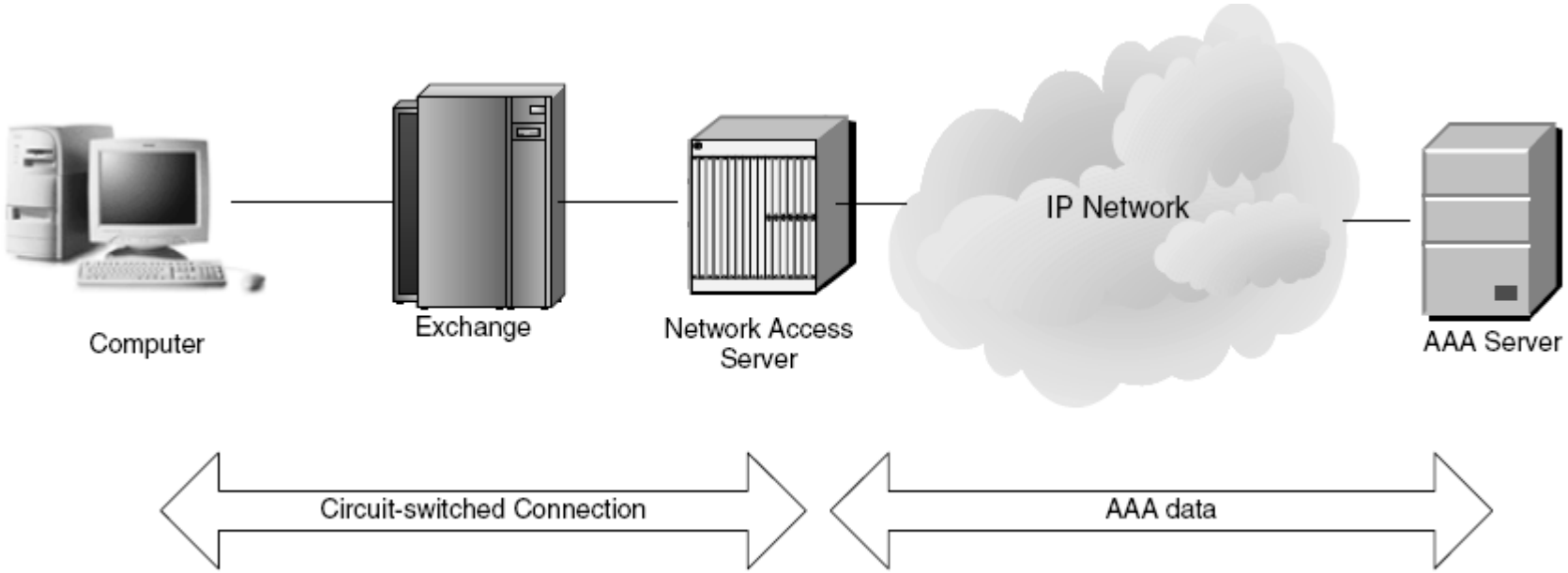
2011. március 4.,
Budapest

Authentication, Authorization, Accounting (Hitelesítés, Engedélyezés, Számlázás)

- Végfelhasználó számára láthatatlanul működő funkciók, melyek révén a szolgáltató hozzáférés ellenőrzést, monitorozást és számlázást valósíthat meg.
- Authentication: Az entitás beazonosításának folyamata.
- Authorization: Az egyes entitások jogosultságainak meghatározása (pl.: hálózat elérése, használható sávszélesség mértéke, stb.)
- Accounting: Információgyűjtés az erőforrások használatáról a tervezés, auditálás, számlázás, és költségvetés készítés érdekében.

AAA az interneten

- 1997-ben az IETF definiálja a RADIUS-t (Remote Authentication Dial In User Service protocol)

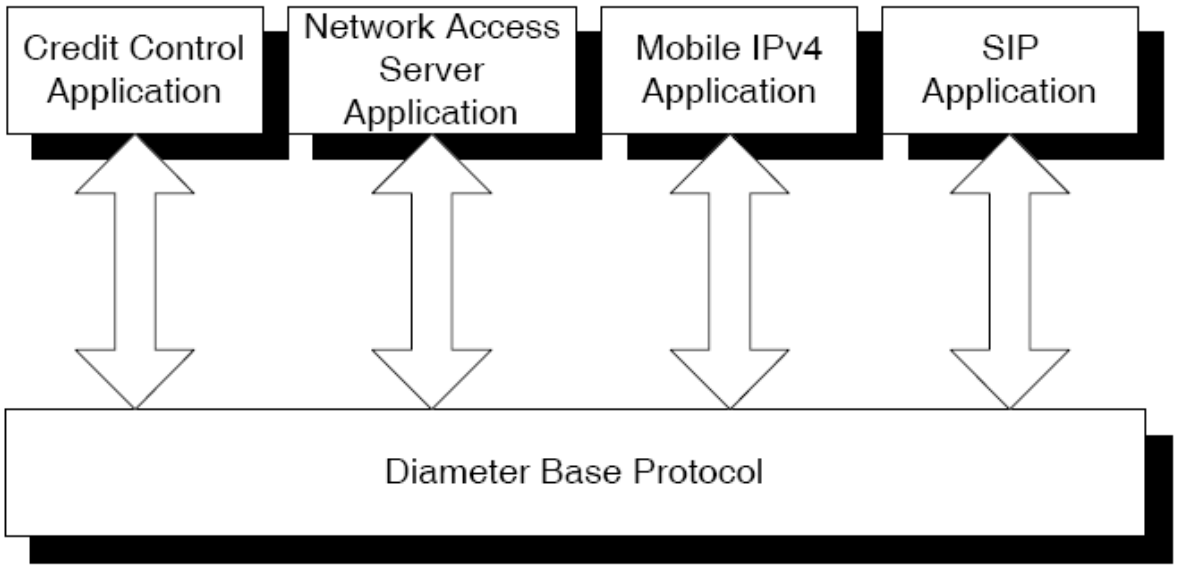


AAA az interneten

- A felhasználó betárcsáz a Network Access Serverhez (NAS), és vonalkapcsolt összeköttetést épít ki vele.
- Mivel minden felhasználóról adatokat tárolni túl körülményes lenne minden NAS-ban, ezért az azonosítást és jogosultságellenőrzést egy AAA szerver végzi AAA protokollon keresztül (pl.: RADIUS)
- A RADIUS protokoll elég jól működik kisebb hálózatokban. Mivel UDP felett működik, nem tartalmaz torlódásvezérlést.
- Hiányoznak belőle bizonyos felhasználói és hálózati funkciók, mint például a kérés nélküli üzenet küldése a hozzáférési szervernek.
- Ezek miatt az IETF kifejlesztette a RADIUS újabb változatát, a DIAMETER-t, melyet az IMS AAA funkciókat ellátó protokolljának választottak.

Diameter

- A DIAMETER egy alap protokoll és a hozzá tartozó kiegészítő alkalmazások együtteseként specifikált protokoll.
- A protokoll minden csomópontban implementálva van az alkalmazásoktól függetlenül.
- Az alkalmazások kiegészítik a protokoll alap funkcióit, amiket a DIAMETER protokoll egy bizonyos felhasználására készítettek, meghatározott környezetekben.



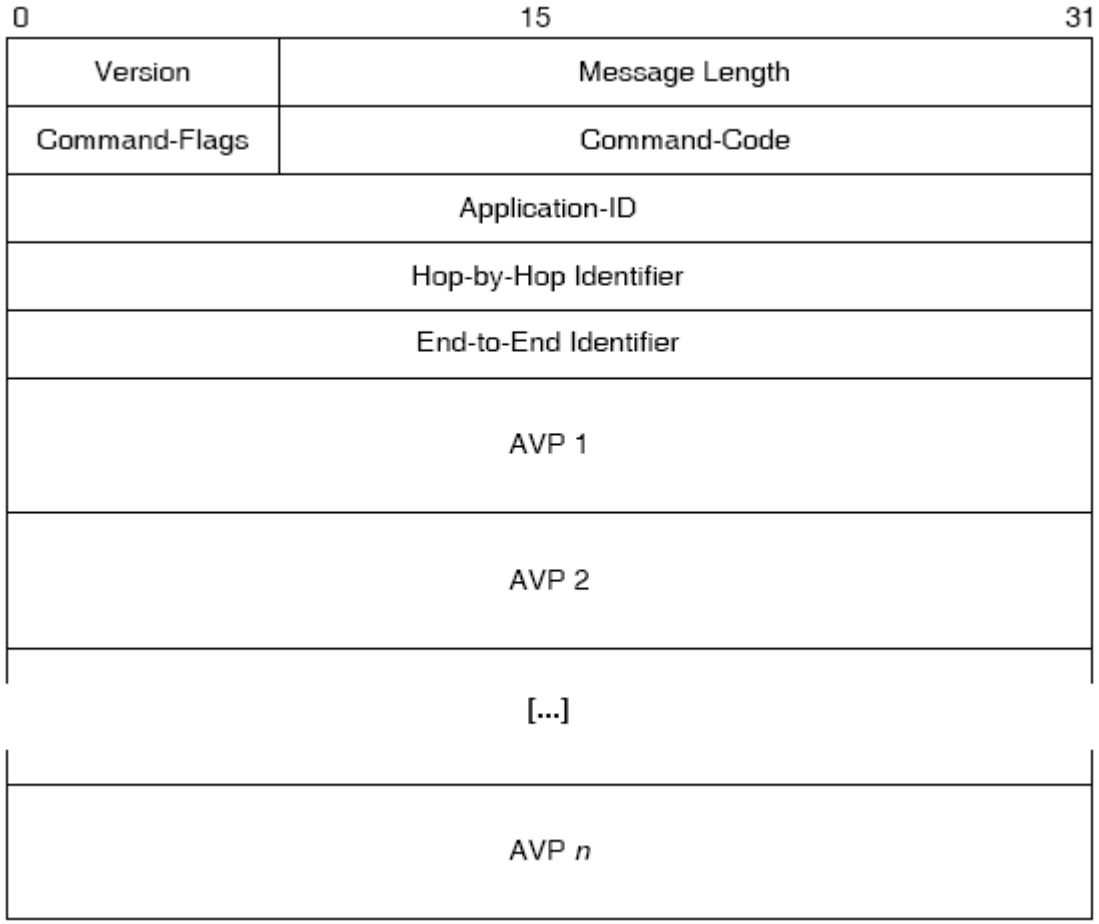
Diameter

- A Diameter base protokoll különböző funkcionális entitásai:
  - Diameter client: hálózati végpontban található, access controll feladatokat lát el. Pl.: NAS, Foreign Agents.
  - Diameter server: AAA feladatok ellátása.
  - Proxy: üzenetközvetítő szerep, policy döntéseket is hozhat az erőforrás kihasználtság, beléptetés és felügyelet kapcsán.
  - Relay: üzenetközvetítő szerep az útválasztás függvényében. Általában transzparens, csak útválasztással kapcsolatos adatmódosításokat végezhet az üzeneten.
  - Redirect agent: kliens és szerver közti közvetlen kapcsolatot teszi lehetővé.
  - Translation agent: protokoll fordítás pl.: Daimeter és RADIUS között.
  - Diameter node: funkcionális entitás, amiben implementálva van a Diameter protokoll.

Diameter

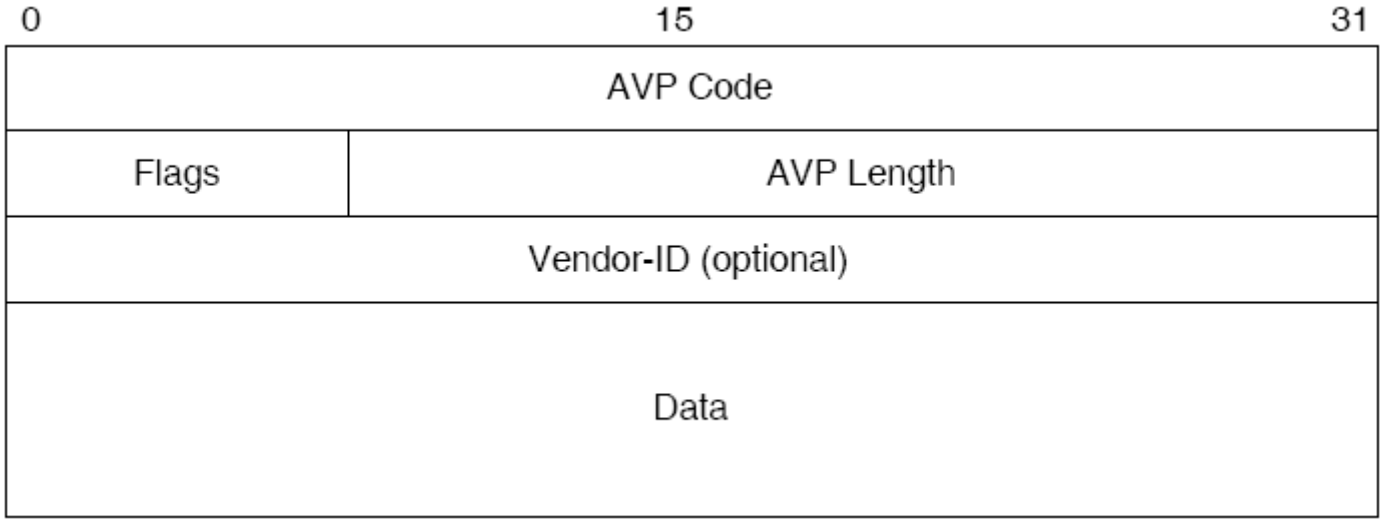
- Peer-to-peer protokoll (nem kliens/szerver)
- Bármely peer aszinkron küldhet kérést bármely másiknak.
- Nem hagyományos kliens, szerver funkciók, mindkettő küldhet kérést is és választ is. Kliens access controll-ért, szerver AAA-ért felel.

Diameter üzenetformátum



Diameter üzenetformátum

- Egy Diameter üzenet fix, 20 oktett hosszú fejlécből és néhány AVP-ből (Attribute Value Pairs) áll.
- Az AVP-k száma az aktuális Diameter üzenetektől függ.
- Az AVP az adathordozó, AAA adatokat tartalmaz.
- AVP felépítése:



Diameter protokoll alap üzenetei

- Minden üzenet kérés, vagy válasz lehet.
- Az üzeneteket a fejlécben utasítás kódok azonosítják.
- Egy kérésnek és a hozzá tartozó válasznak ugyanaz a kódja, egy flag dönti el, hogy melyikről van szó.

Diameter base commands

Command-Name	Abbreviation	*Command-Code*
Abort-Session-Request	ASR	274
Abort-Session-Answer	ASA	274
Accounting-Request	ACR	271
Accounting-Answer	ACA	271
Capabilities-Exchange-Request	CER	275
Capabilities-Exchange-Answer	CEA	275
Device-Watchdog-Request	DWR	280
Device-Watchdog-Answer	DWA	280
Disconnect-Peer-Request	DPR	282
Disconnect-Peer-Answer	DPA	282
Re-Auth-Request	RAR	258
Re-Auth-Answer	RAA	258
Session-Termination-Request	STR	275
Session-Termination-Answer	STA	275

Diameter protokoll alap üzenetei

- Abort Session Request/Answer (ASR, ASA)
  - Szerver részéről szolgáltatás megszakítás, pl.: credit elfogyása, biztonsági okok vagy egyszerűen adminisztrációs utasítás hatására. ASR-t a szerver, míg az ASA-t a kliens küldi.

- Accounting Request/Answer (ACR, ACA)
  - Diameter node küldi a számlázási beszámolót a szervernek. Tartalmazza pl.: szolgáltatás kezdetét, végét.

- Capabilities Exchange Request/Answer (CER, CEA)
  - Az első üzenetpár a kapcsolat felépítése után. Tartalma: node azonosítója, képességei (protokoll verzió, támogatott Diameter alkalmazások és biztonsági mechanizmus, stb.).

Diameter protokoll alap üzenetei

- Device Watchdog Request/Answer (DWR, DWA)
  - Alapvető fontosságú, hogy a Diameter észlelni tudja a szállítási- és felhasználói-rétegben bekövetkezett hibákat amilyen gyorsan csak lehet. A watchdog a felhasználói rétegben működik és figyeli, hogy a 2 node közötti kérésre időben érkezik-e válasz. Mivel általános forgalom hiányában ily módon nem lehetséges a detektálás, ezt a Diameter a DWR és DWA üzenetek küldésével helyettesíti.

- Session Termination Request/Answer (STR, STA)
  - Kliens küldi a szervernek, ha már nem akarja tovább igénybe venni az adott szolgáltatást. STR üzenetküldés történik akkor is, ha a kapcsolat valamiért megszakad.

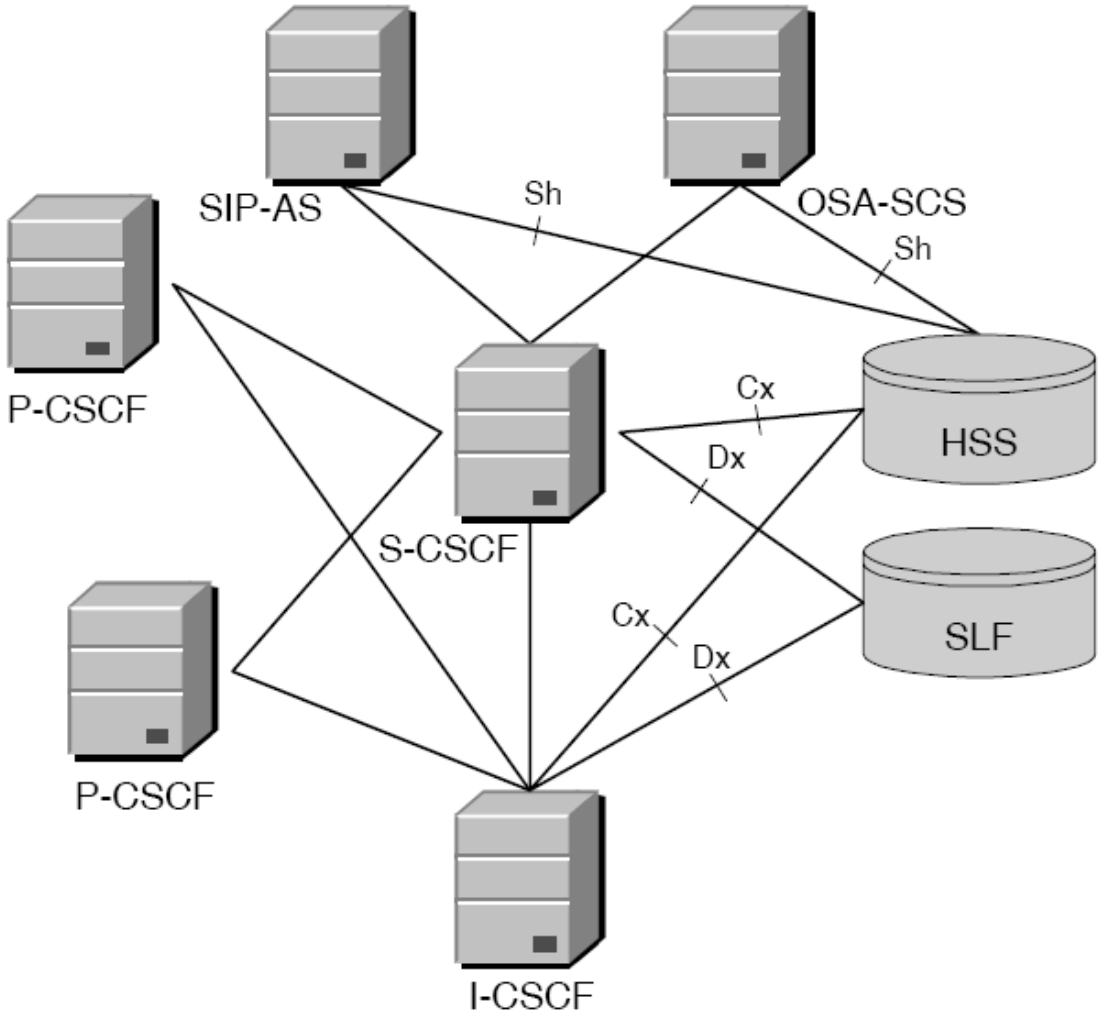
Diameter protokoll alap üzenetei

- Disconnect Peer Request/Answer (DPR, DPA)
  - Kapcsolat megszakítása.
- Re-Authentication Request/Answer (RAR, RAA)
  - Általában hosszú ideje fennálló session-nél küldi a szerver biztonsági okokból.

AAA az IMS-ben

- Az IMS-ben a hitelesítés és jogosultság kezelés általában szervesen összekapcsolódik.
- A számlázás egy elszeparált funkció, melyet különböző node-ok végeznek.
- Három interfész van, amin keresztül az autentikáció és az autorizáció történik: Cx, Dx, Sh
- Cx: I-CSCF és a HSS között, valamint az S-CSCF és a HSS között található.
- Dx: Ha szükség van SLF-re, akkor az I-CSCF-et és az S-CSCF-et köti össze az SLF-fel.
- Sh: Az alkalmazás szervert és a HSS-t köti össze.

AAA az IMS-ben



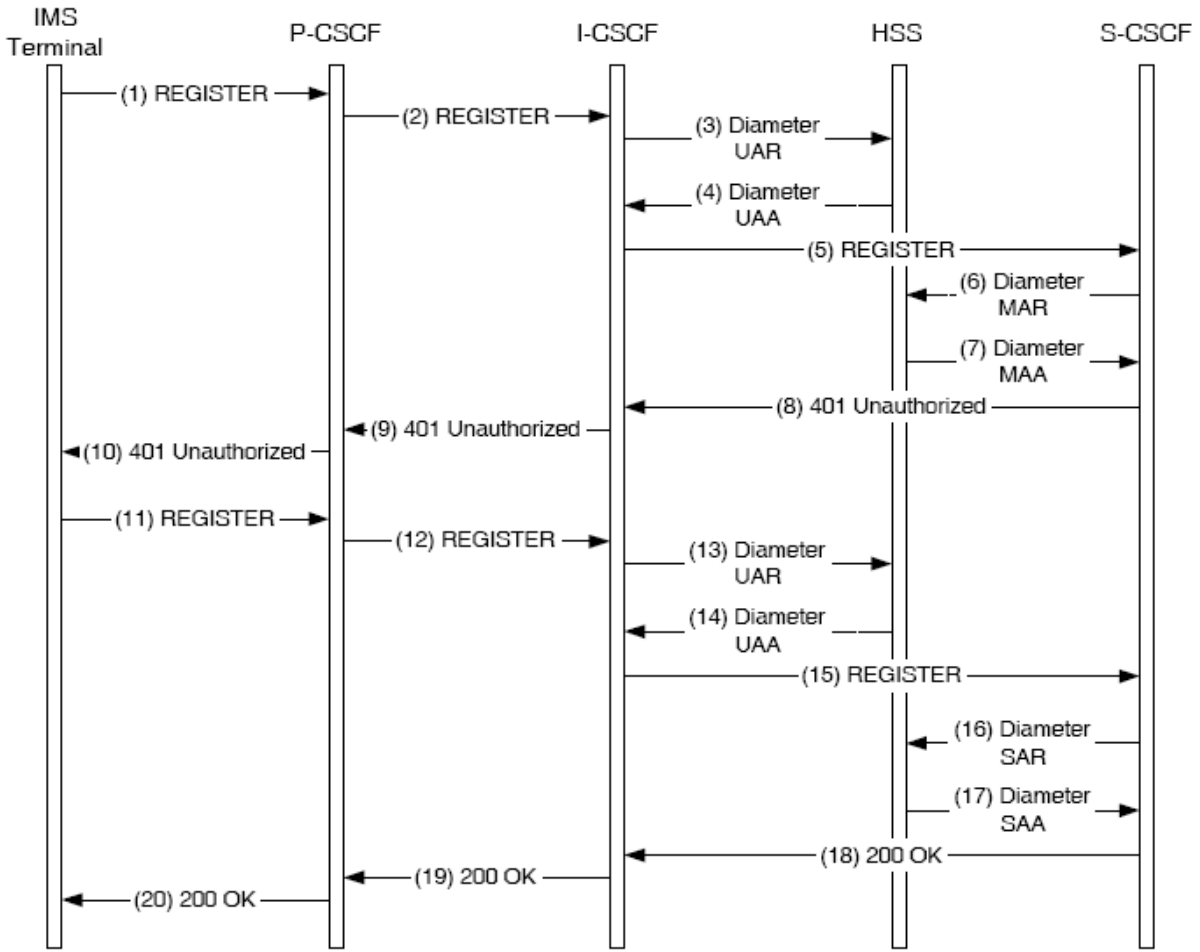
Cx és Dx interfész

- Az I-CSCF és S-CSCF a Cx és Dx interfészeket használja a következő funkciók megvalósítására:
  - Felhasználóhoz rendeli a már lefoglalt S-CSCF-et.
  - Letölti a felhasználóra vonatkozó hitelesítési vektorokat (HSS-ben vannak tárolva).
  - Feljogosítja a felhasználót roaming használatára látogatott hálózatban.
  - Feljegyzi a HSS-ben a felhasználóhoz rendelt S-CSCF címét.
  - Tájékoztatja a HSS-t a felhasználó regisztrálásának állapotáról.
  - User profile letöltése a HSS-től.
  - Ha a user profile változik, a HSS tájékoztatja az S-CSCF-et.
  - Ellátja az I-CSCF-et az S-CSCF választásához szükséges információkkal.

A Cx interfész üzenetei

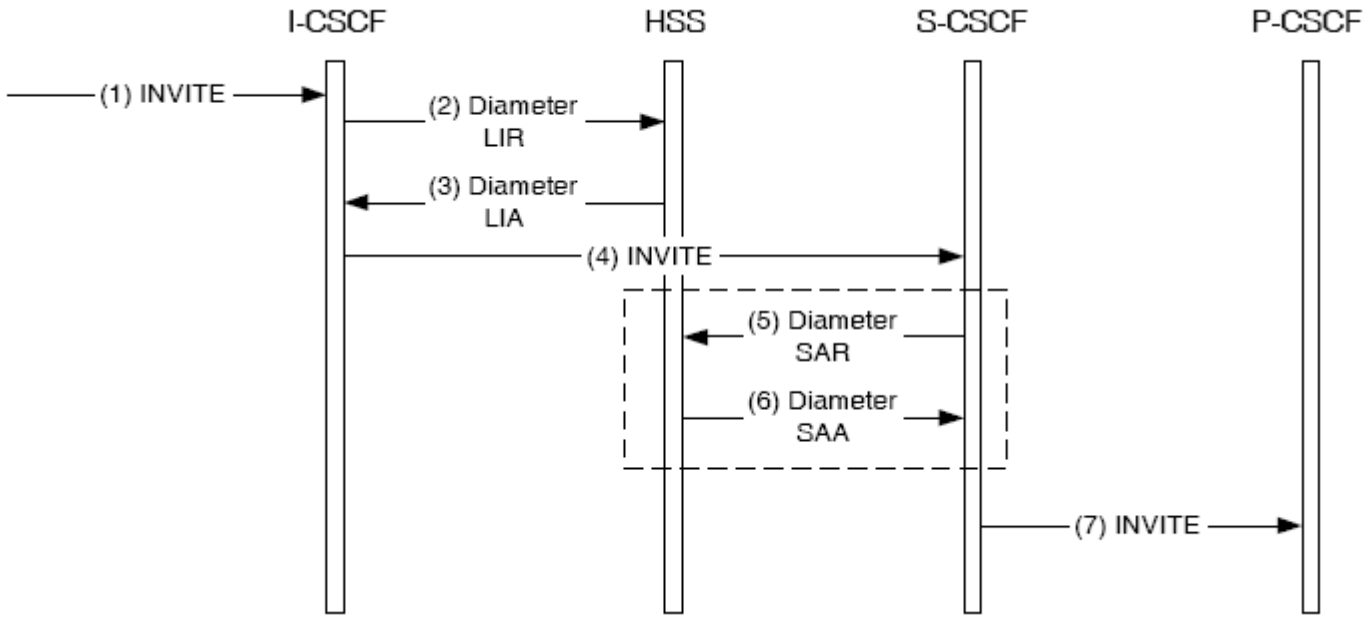
Command-Name	Abbreviation	*Command-Code*
User-Authorization-Request	UAR	300
User-Authorization-Answer	UAA	300
Server-Assignment-Request	SAR	301
Server-Assignment-Answer	SAA	301
Location-Info-Request	LIR	302
Location-Info-Answer	LIA	302
Multimedia-Auth-Request	MAR	303
Multimedia-Auth-Answer	MAA	303
Registration-Termination-Request	RTR	304
Registration-Termination-Answer	RTA	304
Push-Profile-Request	PPR	305
Push-Profile-Answer	PPA	305

Diameter üzenetek regisztrációkor



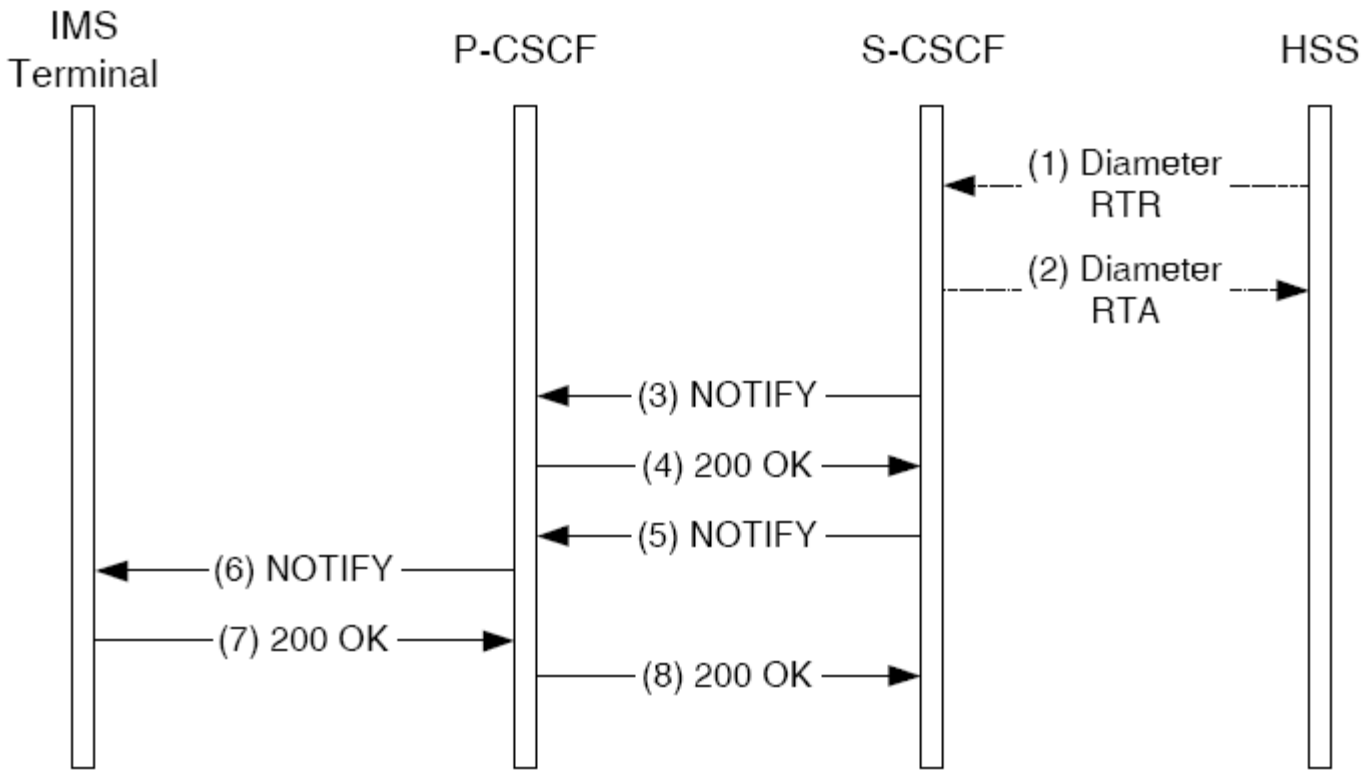
LIR/LIA üzenetpár

- Ha az I-CSCF olyan SIP kérést kap, mely nem tartalmaz a következő (felhasználóhoz tartozó) SIP hop-ra (S-CSCF-re) vonatkozó címet:



RTR/RTA üzenetpár

- Adminisztratív okokból szükség lehet egy felhasználóhoz tartozó, már regisztrált Public User Identity törlésére. Itt a HSS küldi a kérést az S-CSCF-nek, ahova a user regisztrálva van.



Felhasználói profil

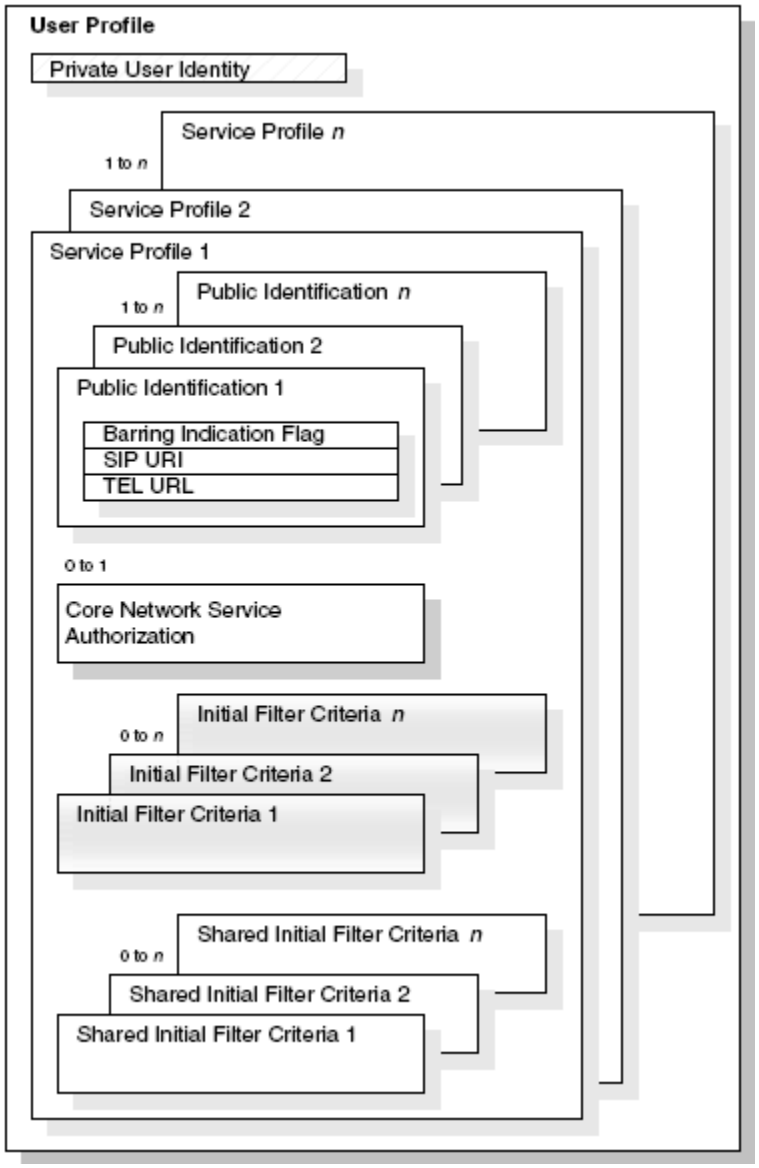
- A felhasználói profilokat a HSS tárolja, és információkat tartalmaz a felhasználókról.

- Az S-CSCF letölti a profilt a HSS-től, mikor a felhasználó először regisztrál.
- Ha változik a felhasználói profil, a HSS ezt egy PPR üzenetben tudatja az S-CSCF-fel.

- A felhasználói profil egy Private User Identity-hez van kötve, és több Public User Identity-hez, amik hozzá vannak rendelve a Private User Identity-hez.

- Számos service profile-t tartalmaz, ami definiálja a trigger eseményeket, amik alkalmazhatóak a Public User Identityk-nél.

Felhasználói profil felépítése



Az Sh interfész

- Az Sh interfész az alkalmazás szerverek és a HSS között található.
- Le- /feltöltést valósít meg AS és HSS között.
- Észlelési feladatokat is ellát: adatváltozás esetén HSS figyelmezteti az AS-t
- Megjelenik a „user data” kifejezés az eltérő adattípusokra utalva. Ezek a következők:
  - Repository data: Az AS transzparens adatok tárolására használja a HSS-t.
  - Public Identifiers: A felhasználók által lefoglalt Public User Identity-k listája.
  - IMS User State: A felhasználók regisztrációs állapota:
    - Registered
    - Unregistered
    - Pending
  - S-CSCF name: Felhasználó által lefoglalt S-CSCF címe

Sh interfész

- Initial Filter Criteria: Szolgáltatáshoz szükséges információk
- Location Information: Felhasználó helye
- User State: Felhasználó állapota
- Charging Information: számlázó egységek címe

- Az Sh interfész 8db új Diameter üzenetet definiál:

Command-Name	Abbreviation	*Command-Code*
User-Data-Request	UDR	306
User-Data-Answer	UDA	306
Profile-Update-Request	PUR	307
Profile-Update-Answer	PUA	307
Subscribe-Notifications-Request	SNR	308
Subscribe-Notifications-Answer	SNA	308
Push-Notifications-Request	PNR	309
Push-Notifications-Answer	PNA	309

Számlázás

Számlázás

- Hívások/szolgáltatások árának meghatrározása
- Számlák előállítása és nyomtatása
- Pénz beszedése, elmaradások kezelése
- Technológia, marketing és szolgáltatás orientált
- Folyamatos változás
- Egyedi megoldások

Számlázás fajtái

- **Online számlázás** során a beérkezett hívásadatok alapján rögtön megállapítjuk a hívás árát, és levonjuk/hozzáadjuk a felhasználó számlájáról/számlájához. A valós idejűségi követelmény miatt socket alapú kommunikáció.

- **Offline számlázás** esetén nincs valós idejűségi követelmény, a szolgáltatás árát elég később(akár hó végén) megállapítani. Az információk file-ként jutnak el a számlázóközpontba. Egy file-ban több számlázási rekord is szerepel. A formátumot **CDR**-nek (Call Detail Record vagy Charging Data Record) hívják.

  Mindkettő lényege, hogy a hálózati elemek által nyújtott szolgáltatásokat regisztrálja, kiszámítsa a szolgáltatás pontos árát, elkészítse a számlaképet és nyomon kövesse a befizetések élettörténetét.

A számlázás feladatai

- **Mediation**
  - különböző HW elemektől érkező adatok egységes formátumra hozása:
    - a különböző gyártók különböző üzeneteket küldenek (Ericsson, Siemens, Nokia, Nortel)
    - más formátumban jön számlázási információ a honos hálózatból, és más roaming során.
  - felesleges rekordok eldobása

A számlázás feladatai

- **Rating**
  - a felhasználó által igényelt szolgáltatás árának előállítása (transzformáció) a következők függvényében:
    - a felhasználó által előfizetett szolgáltatások
    - a felhasználó által megrendelt kedvezmények
    - az igényelt szolgáltatás paraméterei
    - a felhasználó paraméterei, beállításai
    - a felhasználó eddigi viselkedése

A számlázás feladatai

- **Billing**
  - a havi adatokból a számlainformációk előállítása
    - igényelt szolgáltatások
    - Kedvezmények
  - a számla megformálása
  - a nyomtatandó / elküldendo file eloállítása
  - adatok az A/R-nak

A számlázás feladatai

- **Accounts/Receivable (A/R)**
  - pénzügyek kezelése
  - számlabefizetések (banki tranzakciók)
  - pre-paid kártyák (top-up) kezelése
  - figyelmeztetések, felszólítások
  - forgalomfelügyelet (credit limit check)
  - pénzügyi kimutatások készítésa

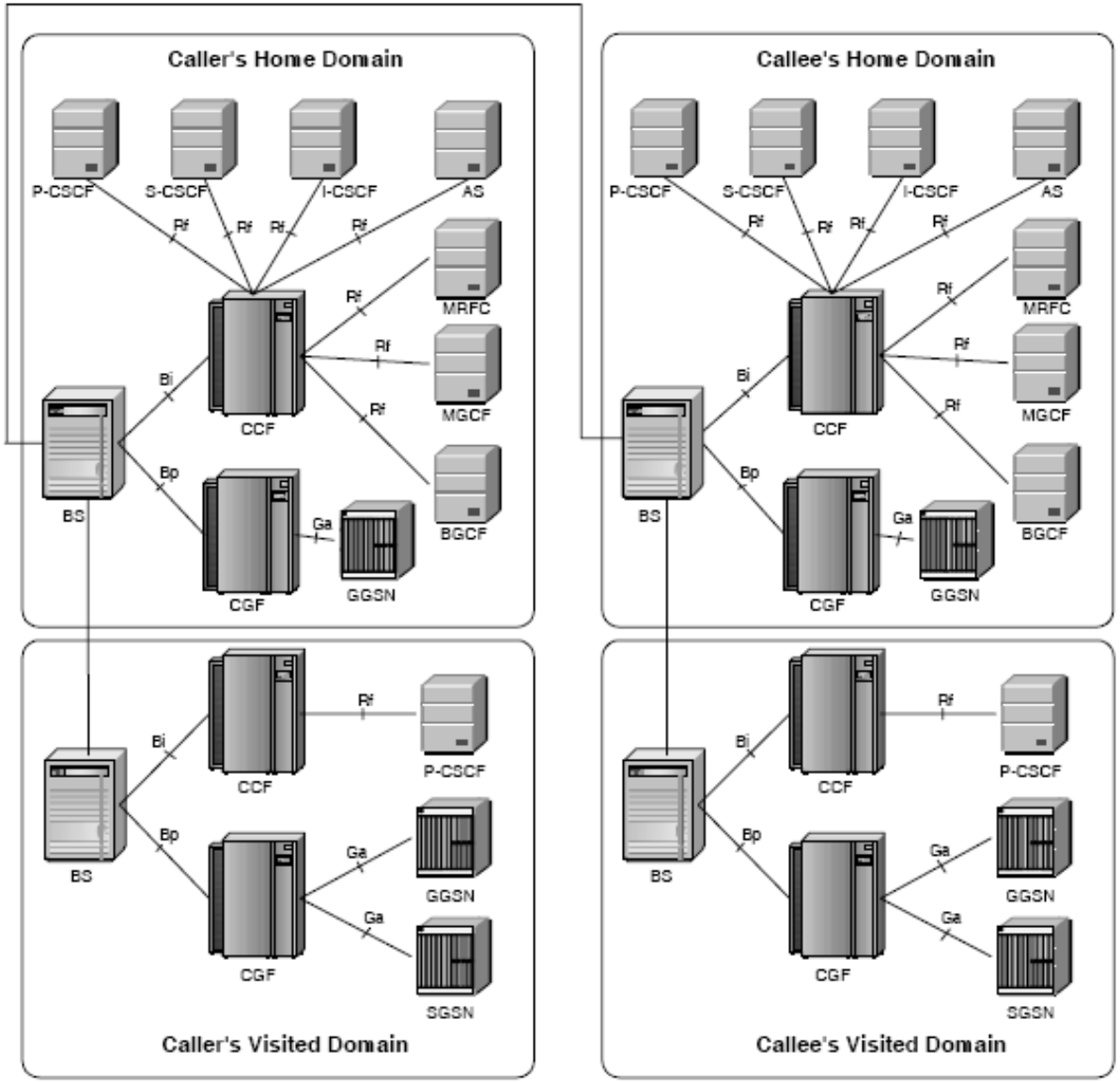
A számlázás feladatai

- **Customer Relationship Management (CRM)**
  - előfizetők definiálása, információk tárolása
  - szolgáltatások definiálása, eladása, paraméterek tárolása
  - készülékek eladása (részletfizetés)
  - különböző egyéb akciók

IMS számlázás

- Az IMS a Dimeter protokollt használja a számlázási információk továbbításához.
- A CSCF-ek továbbítják a felhasználól által indított session-ök típusát és hosszát, a routerek (pl. GGSN) pedig a „*media activity-t”* a számlázó rendszernek.
- A számlázó rendszer minden session-höz egyedi azonosítót rendel, így tudja, hogy a különböző entitásoktól érkező számlázási információk (pl. CSCF és GGSN) egy session-höz tartozik-e, vagy nem.
- A rendszer felhasználónként összegyűjti ezeket az információkat, és kiszámlázza őket.

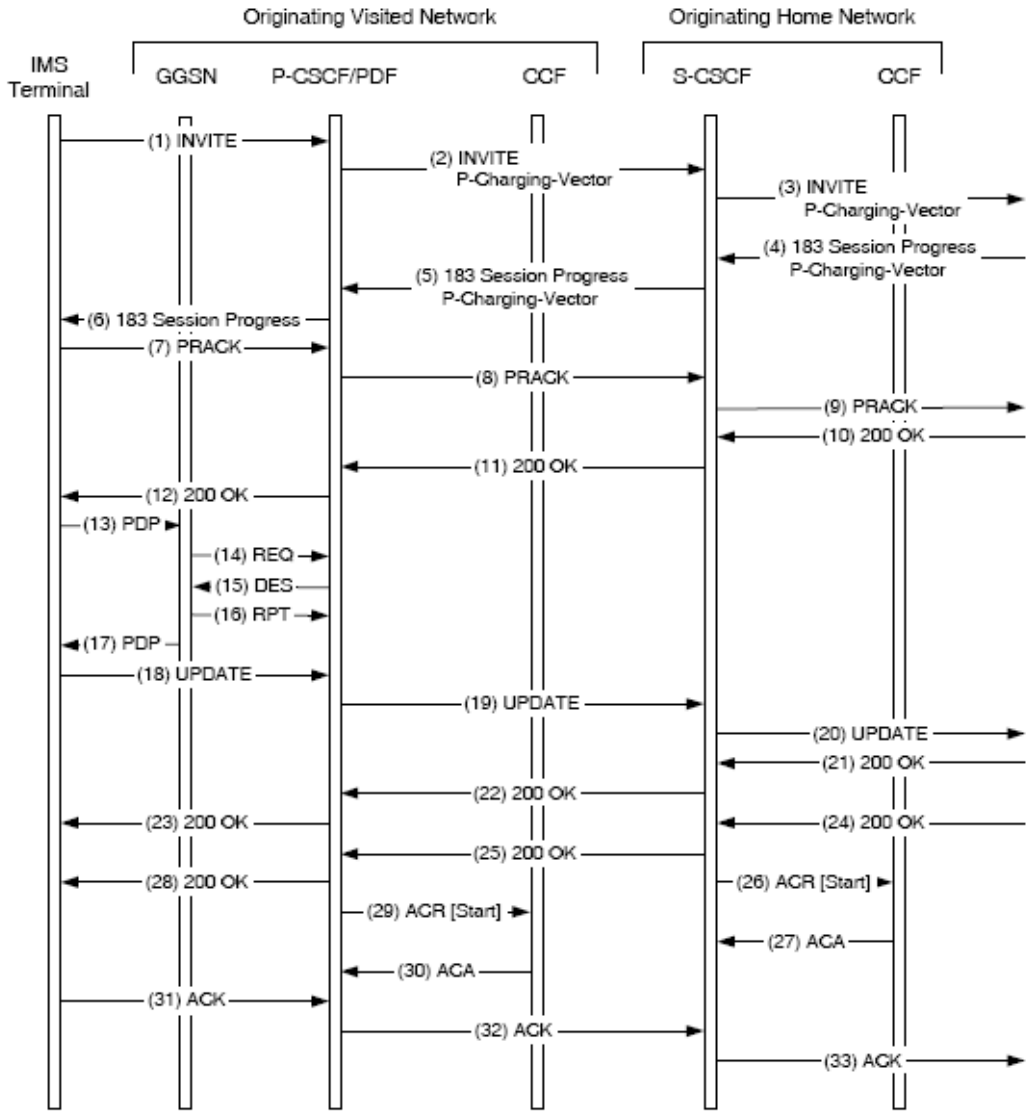
Offline számlázási architektúra



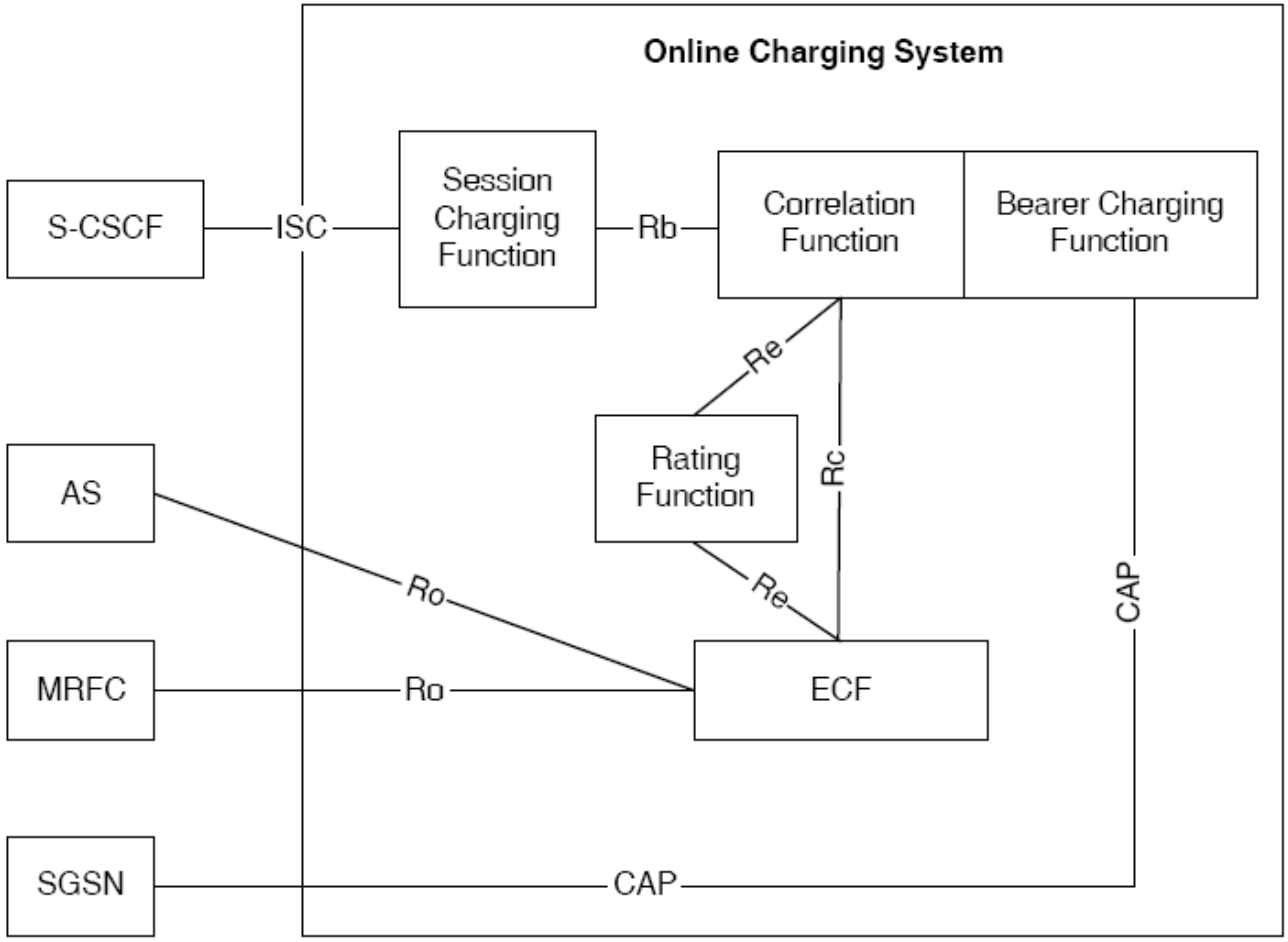
Offline számlázás

- A csomópontok az Rf interfészen küldik a számlázási információkat a CCF-nek. (Charging Collection Function)
- A CCF a kapott információkból CDR-eket generál, és elküldi a BS-nek (Billing System) a Bi interfészen.
- GPRS kapcsolatnál a CDR-ek a CGF-en (Charging Gateway Function) keresztül jutnak el a BS-hez.
- Az Rf interész a Diameter protokollon alapul, a Bi és a Bp interfész pedig FTP protokollon.
- Release 6-tól CCF-et CDF-nek (Charging Data Function)

Offline számlázás



Online számlázási architektúra



Online számlázás

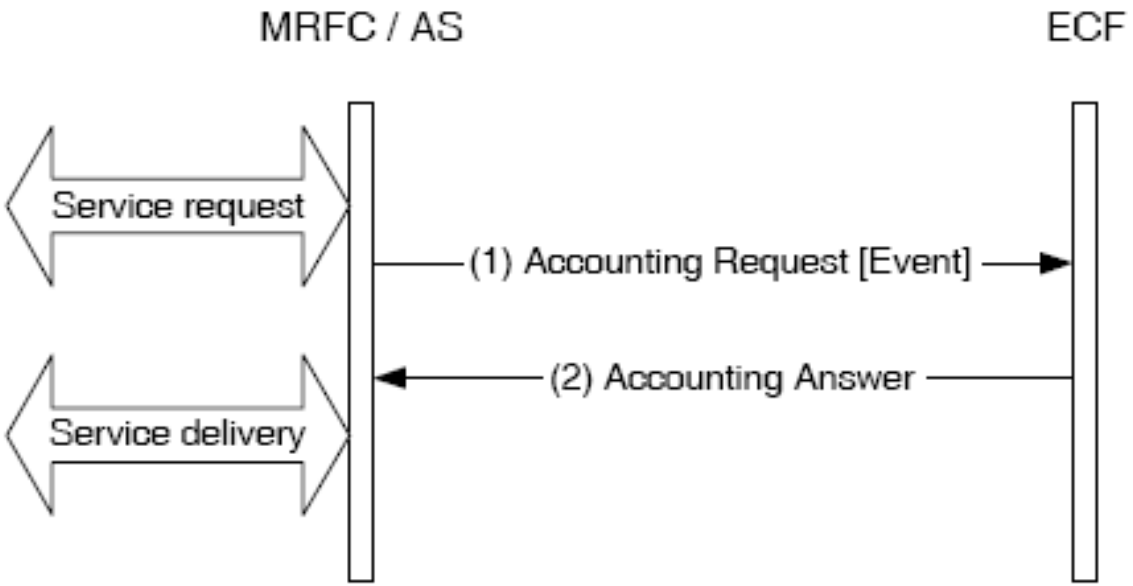
- Az S-CSCF az ISC interfészt használja, ami SIP alapú.
- Az AS és az MRFC az Ro interfészt használja, ami Diameter alapú.
- Az operátor a user profile-beli filter criteria definiálásával határozza meg a session-ökre vonatkozó számlázási módszereket.
- A filter criteria továbbküldi a SIP kéréseket az AS-nek, mely SCF-ként (Session Charging Function) működik.
- Az SCF az Rb interfészen látja el a CF-et (Correlation Function) számlázási információkkal.
- Ha a felhasználónak elfogy a kreditje, értesíti az SCF-et, mely megszakítja a kapcsolatot B2BUA-ként és egy-egy BYE üzenetet küld a terminálóknak.

Online számlázás

- Az AS-ek vagy MRFC és az ECF között Ro interfész található.
- Az AS vagy MRFC az S-CSCF-től kapja az ECF címét a SIP üzenet P-Charging-Function-Address fejlécmezőn keresztül.
- Az Online számlázás kredit-egység alapú, azaz a felhasználó addig élvezheti a szolgáltatást, amíg van elég kredit a számláján.
- Az Online számlázásnak 2 típusa van:
  - Immediate Event Charging (IEC)
  - Event Charging with Unit Reservation (ECUR)

Immediate Event Charging

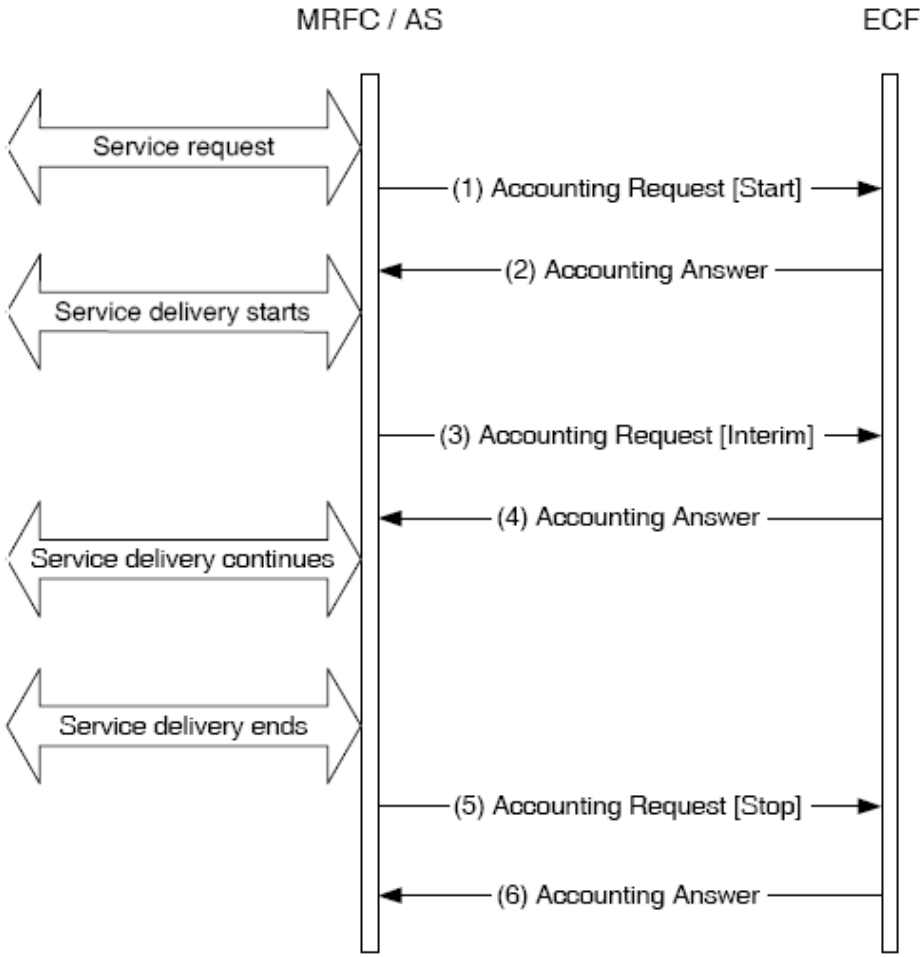
- ECF levonja a krediteket a számláról és utána engedélyezi az MRFC-nek vagy AS-nek a szolgáltatás biztosítását.



Event Charging with Unit Reservation

- Először csak lefoglalja, majd szolgáltatás végén vonja le a krediteket. Ha a lefoglaltat túllépi, újabb lefoglalás következik be.

- Mikor a szolgáltatásnak vége, az AS vagy az MRFC jelenti a felhasznált kreditek mennyiségét az ECF-nek. A lefoglalt, de fel nem használt kreditek az ECF felszabadítja.



Kérdések?

KÖSZÖNÖM A FIGYELMET!

Híradástechnikai Tanszék

Dr. Imre Sándor
Szabó Sándor
BME Híradástechnikai Tanszék
szabos@hit.bme.hu