Infokommunikációs szolgáltatások és alkalmazások

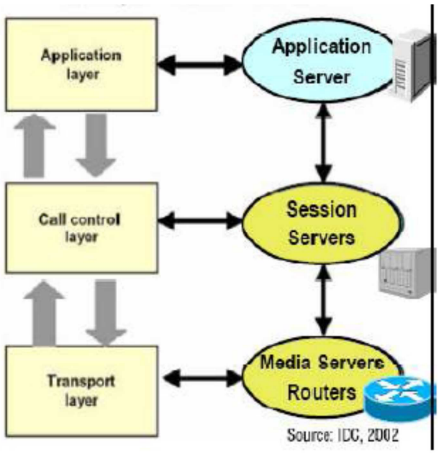
Tételkidolgozás 2010/2011 tavaszi félév

1. NGN hálózati koncepció, NGN ALL-IP architektúra, NGN átmenet, az IMS szerepe. Konvergencia folyamatok, FMS, FMC, IMS alkalmazások.

NGN hálózati koncepció:

Egységes, csomagalapú szolgáltatás platform

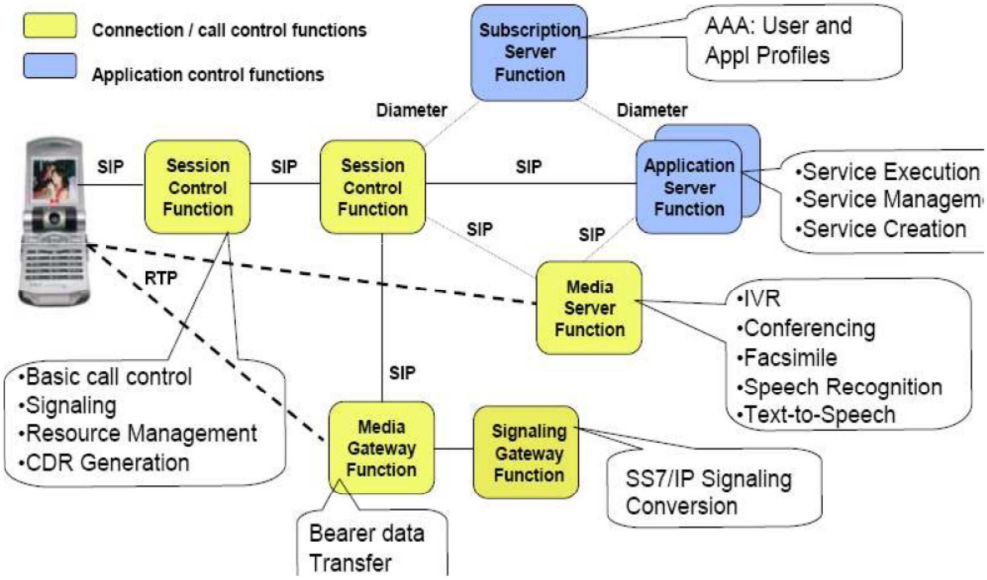
- A külön kezeli a menedzsment feladatokat:
  - Mobilitás kezelés, biztonság, azonosítás, hitelesítés, számlázás (AAA)
- A különböző hozzáférési hálózatok egységesen kezelhetőek, függetlenül attól, hogy:
  - Az alkalmazott technológia vezetékes, vagy vezeték nélküli
  - A szolgáltató saját hálózatáról, vagy egy független hálózatról van szó
- Egységes architektúra, szolgáltatások, szabványos interfészek
- Rugalmas, gazdaságos, gyors alkalmazásfejlesztés



3 szintű architektúra:

- **Application szerverek**: független szolgáltatási réteg
- **Session szerverek**: hívásvezérlés, soft switchek, SIP protokoll
- Routerek: a jelzésüzenetek és a tartalom (média) szállítása
- **Media gateway**, Media szerverek: a call szerverek irányításával adatfeldolgozás, konvertálás

NGN ALL-IP architektúra:

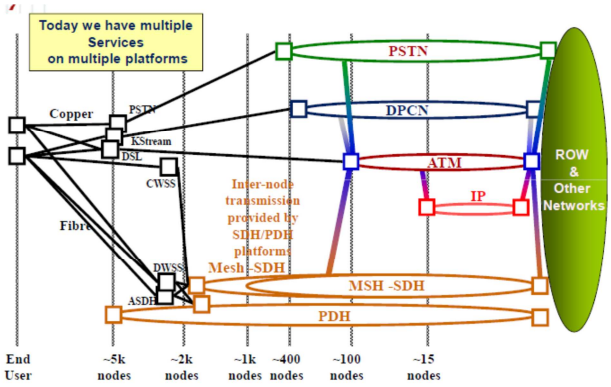


NGN átmenet:

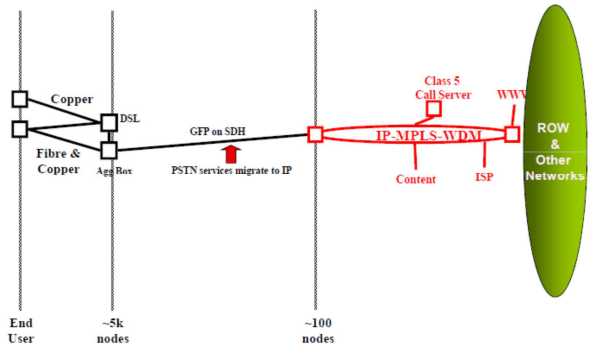
- Jelenleg hat „csatornán” bonyolódik a világ távközlése, ezek: a PSTN, a DPCN (Data Packet Core Network), az ATM + az IP, az MSH-SDH (Mesh – Synchron Digital Hierarchy) és a PDH.
- Először a DPCN fog eltűnni, majd az ATM és az IP közös IP csatornába megy át egy Call Server felügyelete alatt.

- Ezt követően eltűnik a PDH, majd az MSH-SDH és végül a PSTN eltűnésével kialakul a konszolidált állapot, amikor mindenfajta forgalom integráltan egy IP-MPLS-WDM „csatornán” fog bonyolódni egy „Class 5 Call Server” felügyelete alatt.
- Az egységes világhálózat intelligens vezérlő rétegének alapját az IMS technológia (IPbased Multimedia Services) fogja képezni

Ebből:



Ez lesz:



IMS:

- IMS =IP Multimedia Subsystem (Packet Switched domain)
- Multimédia hívások vezérlése csomagkapcsolt hálózaton
- Az IMS bevezeti az IP alapú szolgáltatásokat a mobil világba
  - egyszeri login (authentication)
  - access charging, service charging és content charging
  - multimédiás kapcsolatok felépítése, kezelése és bontása
- Az IMS bevezet új, fejlett hálózati szolgáltatásokat
  - Presence, Conferencing, Push, Chat, Push-to-talk, …
  - lehetőség biztosítása, hogy harmadik fél a hálózatot használva szolgáltatást nyújthasson a felhasználóknak
- Az IMS egy újabb lépés az IETF Internet világa felé
  - Az IMS több mint az IETF SIP: nem csak protokollok, hanem egy architektúra

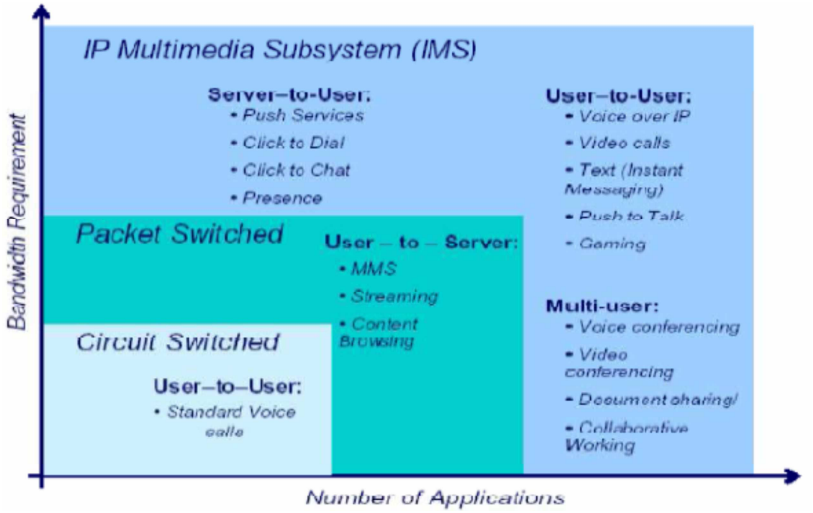
- Az IMS a 3G architektúra kulcs eleme: Internet szolgáltatások elérése mobil és fix hálózatokról
- Miért szükséges az IMS, ha az Interneten a szolgáltatások nagy része ma is elérhető?
  - QoS
  - Számlázás
  - Szolgáltatás integrálás
  - Fix mobil konvergencia
  - Internet alkalmazás fejlesztési elv bevezetése

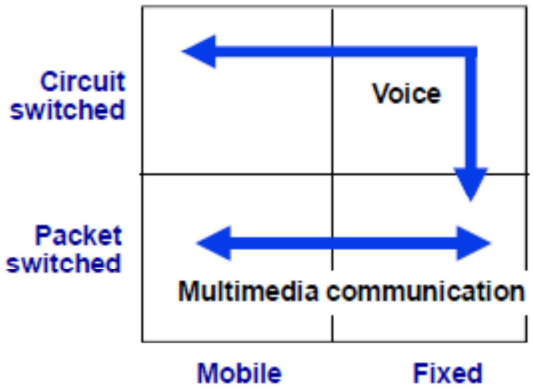
- IMS előnyei:
  - Egyszerű szolgáltatásfejlesztés, egységes megjelenés, látványos szolgáltatások
  - Fejlett QoS és számlázás támogatás
  - Közös IP mag
  - Session felépítés, vezérlés, roaming támogatás
  - Új szolgáltatás képességek

Konvergencia:

- A hagyományos beszédszolgáltatások piaca szűkül
- Új szolgáltatások szükségesek a kieső bevételek pótlására
- Piaci jellemzők:
    - Új IP multimédia szolgáltatások a fix és mobil hálózatokon
    - Voice over IP (VoIP) terjedése a fix hálózatokon
    - Fix-mobil helyettesítés (FMS) – a hangforgalom a mobil hálózatokra tevődik át
- A kommunikáció súlypontja a nyílt, IP alapú hálózatok felé mozdul el
- Az IP alapú maghálózat új szolgáltatásokat tesz lehetővé, elősegíti az FMC-t
- Az IP Multimedia Subsystem (IMS) a szolgáltató hálózatában a kulcsfontosságú elem
- Fókusz a szolgáltatásokon a hálózatok helyett:
    - Transzparenssé válnak a fizikai hálózatok
    - A belépési korlát eltűnik az új szolgáltatások számára
    - Az értéklánc horizontálisan szétválik
    - Bevétel csökkenés
    - A felhasználók „tulajdonlása” elveszik
    - A mobil értéklánc kikerül a szolgáltató kezéből

IMS alkalmazások:





FMS – Fix-mobil helyettesítés
FMC – Fix-mobil konvergencia

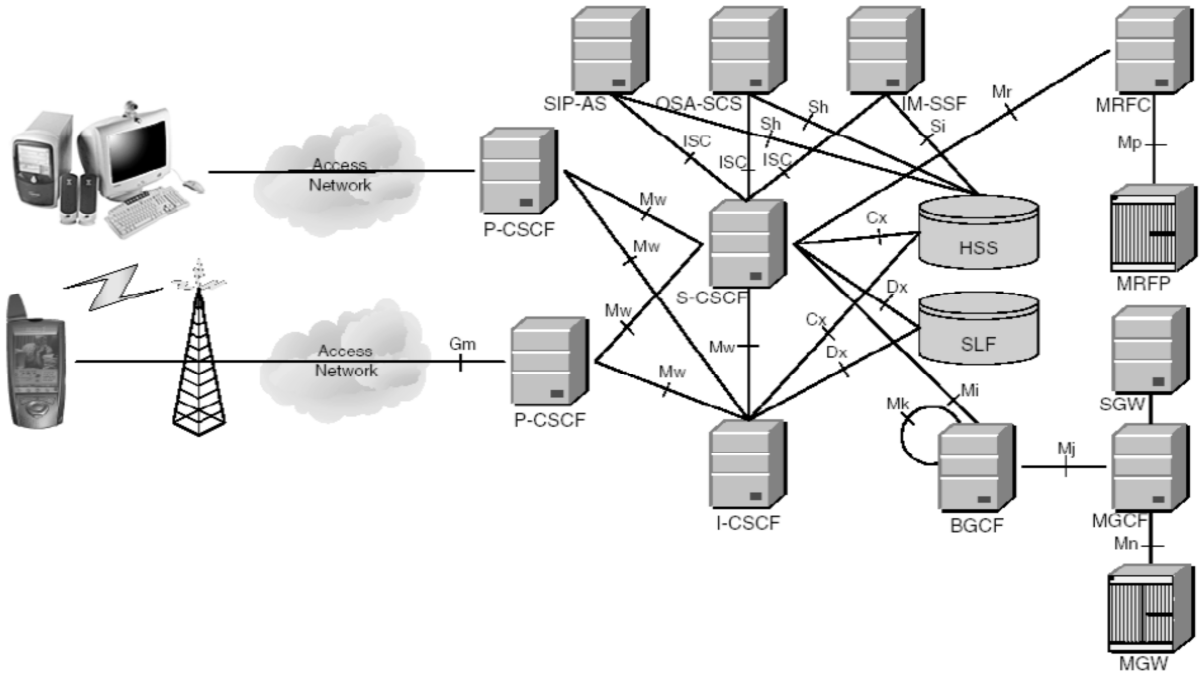
2. IMS architektúra, az egyes elemek szerepe. Az UMTS architektúra fejlődése, az IMS megjelenése.

IMS architektúra alapelvek:

- IMS nem definiál konkrét szolgáltatásokat, csak „enabler”-eket
- „Beépített” támogatást nyújt multimédia over IP, VoIP, IM, presence
- Szolgáltatásokhoz
- Flexibilis multimédia átvitel támogatás IP felett
- Horizontális architektúra
- Meglévő IETF szabványokat alkalmaz
- Moduláris felépítés, nyílt interfészek

Az IMS nem node-okat, hanem funkciókat standardizál, azaz az IMS architektúra funkciókat csoportosít melyek standardizált interfészekkel vannak összekötve. Több funkció kombinációja is lehet egy különálló node (pl.: egy doboz), de egy funkció szét is lehet bontva.
Az IP Multimedia Core Network Subsystem tartalma:

- Egy vagy több HSS (Home Subscriber Servers) és SLF (Subscriber Location Functions).
- Egy vagy több SIP szerver (Call/Session Control Functions)
- Egy vagy több AS (Application Servers)
- Egy vagy több MRF (Media Resource Functions)
- Egy vagy több BGCF (Breakout Gateway Control Functions)
- Egy vagy több PSTN gateway, szétbontva: SGW (Signaling Gateway), MGCF (Media Gateway Controller Function), és MGW (Media Gateway)



Home Subscriber Servers – HSS:

A GSM rendszerekben található HLR továbbfejlesztése.
A HSS a hálózat legfontosabb adatbázisa, tárolja az **előfizetőkkel kapcsolatos adatokat**:

- Felhasználói profilok
- Jogosultságok
- Előfizetett szolgáltatások
- Felhasználó helye
- Authentikációs és authorizációs információk
- Felhasználókhoz rendelt S-CSCF

Subscriber Locator Function (SLF):

Egy hálózatban lehet több HSS is, ha az előfizetők száma túl sok, és már egy HSS nem képes kezelni.
Több HSS esetén szükség van SLF-re, **ami megmondja, hogy melyik HSS-ben találhatóak meg egy adott felhasználó** adatai.
A HSS és az SLF is DIAMETER protokollon keresztül kommunikál a többi hálózati elemmel.

Call/Session Control Function (CSCF):

A rendszer elsődleges **feladata a hívások kezelése**. Ezt a CSCF-ek kezelik. A híváskezelés szét van osztva, hogy a hálózat hatékonyabb és skálázhatóbb legyen. A CSCF-ek dolgozzák fel a SIP jelzésüzeneteket. Három fajta CSCF felelős a hálózat működéséért:

- Proxy Call Session Control Function (P-CSCF)
- Interrogating Call Session Function (I-CSCF)
- Serving Call Session Control Function (S-CSCF)

P-CSCF

A P-CSCF **az első kapcsolódási pont egy IMS terminál és az IMS rendszer között** a jelzési síkon.
Csak jelzésforgalom megy rajta keresztül, más adatforgalom nem.
Úgy viselkedik, mint egy SIP proxy, minden üzenet, amit az IMS terminál kezdeményez, vagy azon végződik, keresztülmegy rajta, így biztosítja az adatintegritást, a biztonságért pedig az IPSec protokoll (IP Security) felel a terminál és a P-CSCF között.
A **felhasználók hitelesítését a P-CSCF végzi**, így az IMS többi csomópontjainál nem kell újra regisztrálni.
Ellenőrzi a SIP üzeneteket, hogy megfelelő formában vannak-e előállítva.
A SigComp (Signal Compression) segítségével képes a készülék és a hálózat között menő SIP üzenetek tömörítésére, ezzel jelentősen csökkentve a forgalmat a rádiós interfészen.
Kezeli a számlázási információkat, CDR-eket (Charging Data Record) készít és tart fenn, ami a CGF-ben (Chargign Gateway Function) kerül feldolgozásra.
QoS kezelésért is felelős lehet, ha a PDF (Policy Decision Function) és a PCSCF együtt van megvalósítva.
Egy IMS hálózatban általában több P-CSCF is található a skálázhatóság, és a redundancia miatt.
Megtalálható a helyi, és a látogatott hálózatban is, GPRS esetében mindig egy hálózatban van a GGSN-nel. (Gateway GPRS Support Node)

I-CSCF:

Az I-CSCF **egy SIP proxy az adminisztratív terület határán**.
Feladata **más IMS hálózatokkal való együttműködés** kezelése, a **külső hálózatból érkező üzenetek** továbbítása.
Vannak interfészei az SLF és HSS felé, ami a Diameter protokollon alapul. Ezeken az interfészeken keresztül szerzi meg a felhasználók információit, így tudja, merre kell továbbítania az üzeneteket.
Egy opcionális lehetőség, hogy képes a SIP üzenetek titkosítására. Ezt a lehetőséget THIG-nek (Topology Hiding Inter-network Gateway) hívják.
Az I-CSCF általában a helyi hálózatban van, néhány speciális esetben, mint pl. a THIG, a látogatott hálózatban is megtalálható.

S-CSCF:

Az S-CSCF a **központi rész a jelzésüzenet továbbításban**.
Alapvetően egy SIP proxy, **de sessionvezérlési feladatokat** is ellát.
SIP registrarként is működik, ami azt jelenti, hogy összerendeléseket tart fenn a felhasználó helye (pl.: IP-címe) és SIP címe között.
Összeköttetésben van a HSS-sel:

- Letölti a csatlakozó felhasználókhoz tartozó autentikációs vektorokat.
- Letölti a felhasználókhoz tartozó user profile-t, csak olyan szolgáltatásokat enged elérni a felhasználónak, amire elő lettek fizetve.
- Visszajelzi, hogy az adott S-CSCF le lett foglalva a felhasználónak a regisztrálás idejére.

Minden SIP üzenet, amit az IMS terminál küld és fogad, átmegy az S-CSCF-en.
Egyik fő feladata a routing.
Eldönti, hogy melyik alkalmazás szerverhez (Application Server, AS) kell továbbítani a SIP üzenetet, hogy a kért szolgáltatást igénybe vehesse a felhasználó.
Ha a felhasználó telefonszámot tárcsáz, és nem a SIP URI-t (Uniform Resource Identifier) használja, az S-CSCF DNS alapú fordítást végez.
Az S-CSCF mindig a helyi hálózatban található.

Application Server (AS):

Az IMS szolgáltatásai az alkalmazás szerverekben vannak implementálva.
Szolgáltatástól függően az alkalmazás szerverek különböző módokban képesek működni:
• SIP Proxy
• SIP UA (User Agent)
• SIP B2BUA (Back-to-Back User Agent): két SIP UA összekapcsolva egy applikáció specifikus logikával.
Az AS lehet a helyi hálózatban, vagy egy harmadik fél hálózatában, szolgáltatási szerződés alapján.
AS fajtái:
• SIP AS (Application Server): SIP alapú IP multimedia szolgáltatások futtatása a feladata.
• OSA-SCS (Open Service Access - Service Capability Server): SIP alkalmazás szerver az egyik oldalról, és interfész az OSA alkalmazás szerverhez és OSA API-hoz (Application Programming Interface) a másik oldalról.
• IM-SSF (IP Multimedia Service Switching Function): Ez a speciális alkalmazás szerver lehetővé teszi a CAMEL (Customized Applications for Mobile network Enhanced Logic) alkalmazások újrafelhasználását, ezeket a IMS-ben a GSMhez fejlesztettek ki.
• A gsmSCF (GSM Service Control Function) az IM-SSF-en keresztül kontrollálja az IMS session-öket.
• Az IM-SFF egyrészről alkalmazás szerverként működik, másrészről SFF-ként (Service Switching Function), interfész a gsmSCF felé a CAP (CAMEL Application Part) protokollon keresztül.

Media Resource Function (MRF):

Az MRF a **multimédia szolgáltatások forrása** a helyi hálózatban. Megvalósít minden médiával kapcsolatos funkciót, mint pl. a lejátszás, mixelés, transzkódolás különböző kodekek között.
Az MRF két részre van osztva:
• A jelzési síkon található a Media Resource Function Controller (MRFC), SIP User Agent-ként mőködik, van egy SIP interfésze az S-CSCF felé, kontrollálja az MRFP erőforrásait H.248 protokollon keresztül.
• A média síkon a Media Resource Function Processor (MRFP) található, felelős az összes médiával kapcsolatos funkcióért, mint pl. lejátszás, média mixelés.
Az MRF mindig a helyi hálózatban található.

Breakout Gateway Control Functions (BGCF):

A BGCF egy olyan SIP szerver, amely a **telefonszám alapú útvonalválasztásért felelős**. Csak azon hívások felépítésében vesz részt, amelyek IMS tartományból indítanak a PSTN vagy PLMN hálózatba.
A fő feladata a BGCF-nek:
• Kiválasztja azt a hálózatot, amelyik az áramkörkapcsolt hálózattal kapcsolatba lép,
• Vagy kiválasztja a megfelelő PSTN/CS gateway-t, ha az együttműködés az áramkörkapcsolt hálózattal ugyanabban a domain-ben törénik, ahol a BGCF is van.

IMS Application Layer Gateway (IMS-ALG):

Az IMS támogatja az **IPv4-et és az IPv6**-ot is.
Előfordulhat, hogy kommunikáció közben szükség van a két verzió **közötti együttműködésre**.
Ezt az IMS IMS-ALG és a TrGW (Transition Gateway) valósítja meg.
Az IMS-ALG a jelzésforgalom feldolgozásáért felelıs (SIP, SDP üzenetek). SÍP B2BUA-ként működik, két független lába van, egy a helyi hálózat felé, egy pedig a másik hálózat felé. A két lábon különböző verziójú IP protokoll működik. Az

üzenetekben átírja az IP címet és a portot a TrGW IP címére és portjára, így a felhasználó által generált forgalom átmegy a TrGW-n. Van egy interfésze az I-CSCF felé a bejövı forgalom, és egy másik a S-CSCF felé a kimenő forgalom kezelésére.

Transition Gateway (TrGW):

A TrGW a **felhasználók forgalmát dolgozza** fel (RTP, RTCP üzenetek.)
Az IPv4 és IPv6-os üzenetek átalakításáért felelıs a média síkon.
NAT-PT/NAPT-PT-ként (Network Address Port Translator–Protocol Translator) működik. Be van konfigurálva egy IPv4-es pool, amiből dinamikusan allokálja a címeket a session-ökhöz.

PSTN/CS Gateway:

A PSTN/CS Gateway az **interfész az áramkörkapcsolt hálózat** felé, így az IMS terminálok indíthatnak és fogadhatnak hívást a PSTN hálózatból.
A PSTN/CS Gateway részei:

- Signaling Gateway (SGW): Interfész a hagyományos telefonhálózat jelzési rétegéhez.
- Alacsony szintő protokoll konverzió a feladata: kicseréli az MTP (Message Transfer Part) forgalmat IP feletti SCTP (Stream Control Transmission Protocol) protokollra. Tehát kicseréli az MTP feletti ISUP* (ISDN User Part)

vagy BICC* (Bearer Independent Call Control) IP feletti ISUP vagy BICC üzenetekre.
*Az ISUP és BICC hívásvezérlı protokollok az áramkörkapcsolt hálózatokban.

Az UMTS architektúra fejlődése, az IMS megjelenése:

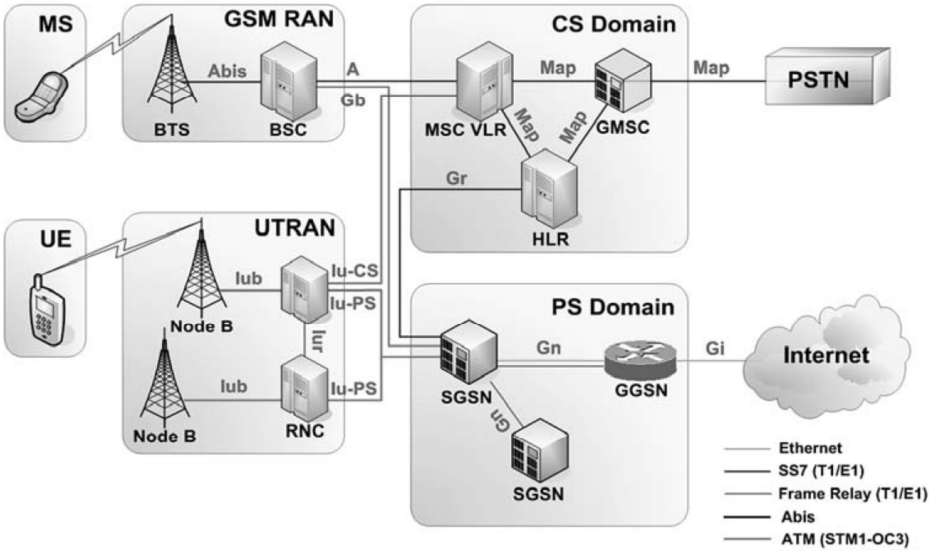
Az UMTS hálózatok egymást követő kiadások (release) alapján valósíthatóak meg.

- Release '99
  - Frozen: 1999 december
  - UTRA és más kezdeti funkciók definiálása
  - A korai 3G telepítések alapja
- Release 4
  - Frozen: 2001 március
  - Továbbfejlesztések az R99-hez képest, valamint a control és az user réteg szétválasztása a maghálózatban
  - Első lépések az IP alapú működés felé
  - TD-SCDMA
- Release 5
  - Frozen: 2002 március/június
  - Az R5 legjelentısebb újdonságai:
  - IMS - IP-based Multimedia Services
  - HSDPA - High Speed Downlink Packet Access
- Release 6
  - Frozen: 2004 szeptember/december
  - IMS második fázis,
  - HSUPA
  - Presence
  - Instant Messaging
  - Hozzáférési hálózat-függetlenség
  - DRM (Digital Rights Management)
  - További funkcionális fejlesztések a felhasználói élmény fokozása érdekében.
  - WLAN–3G együttműködés megjelenése.
- Release 6 elsődleges célja:

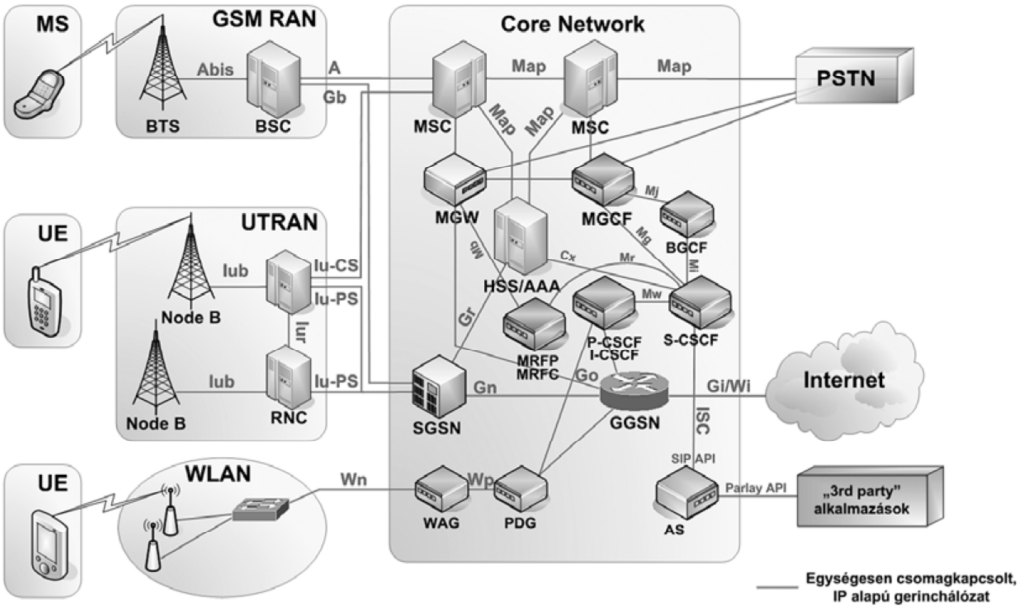
- Kapacitás növelés
- QoS támogatásra és valósidejű multimédiás csomagkapcsolt alapú szolgáltatások
- Teljes IP (all-IP) hálózat
- Technológiák integrációja: 2G, 3G, WLAN, stb
- Együttműködés kialakítása az UMTS rendszerrel
  - számlázás, biztonság, felhasználó azonosítása
- Azonos session control layer (IMS) használata minden szolgáltatás számára

- Release 7
  - Stage 1: 2005 december; Stage 2: 2006; Stage 3: 2007
  - Uplink fejlesztések
  - MIMO, spektrumkiterjesztés
  - Advanced Global Navigation Satellite System koncepció,
  - IMS vészhívás, e-call, stb.
- Release 8
- Release 9

R99:



Az R6 IMS-sel:



3. Kapcsolatvezérlési protokollok, soroljon fel néhány protokollt. Ismertesse a H.323 protokollt, hasonlítsa össze a SIP protokollal. A SIP architektúra elemei, SIP azonosítás

A legfontosabb kapcsolatvezérlési protokollok:

- H.323
- BICC (Bearer Independent Call Control)
- MGCP/Megaco/H.248
- **SIP (Session Initiation Protocol)**

H.323

- ITU protokoll család tagja
- Széles körben használják VoIP és videókonferencia-rendszerekben
- Audió, videó és adat küldésére is alkalmas
- Pont-pont és pont-multipont kapcsolatok létrehozása is lehetséges vele
- Egy tipikus H.323 hálózat a világháló segítségével összekötött zónákból áll
- Minden zónához tartozik egy Gatekeeper, bizonyos számú terminál, bizonyos számú Gateway és bizonyos számú Multipoint Control Unit egy lokális hálózaton belül
- A zóna állhat több LAN-ból is, egyedüli feltétel, hogy minden zóna csak egy darab Gatekeeper-t tartalmazhat

H.323 Terminál:

- Valós idejű, kétirányú multimédia kommunikációra alkalmas végpont
- Kommunikálhat egy hasonló terminállal, Gateway-jel, vagy MCU-val
- A két terminál közötti kommunikáció vezérlési, jelzési, audió, videó és adat típusú lehet
- Egy terminál egy másik terminállal két féleképpen kommunikálhat:
    - Közvetlenül
    - Közvetve (Gatekeeper segítségével)

Gateway:

- Különböző hálózatok közötti együttműködést teszi lehetővé
- Eltérő típusú hálózatok között fordítóként működik, ezekben az esetekben ők építik fel a kapcsolatot két terminál között
- A fordításhoz ismernie kell a használt audió/videó kódoló típusokat
- Az adat és jelzésátviteli formátumok között is elvégzi a szükséges átalakításokat

Gatekeeper:

- Opcionális, de ha van, akkor ı a központi „intelligencia”
- Ha a hálózat több zónából áll, akkor a zónák a Gatekeeper segítségével kommunikálnak
- Feladatai: címzés, hívásbeengedés szabályozása, hitelesítés, sávszélesség menedzselés, számlázás és hívásátirányítás
- Ha a hálózat tartalmaz Gatekeeper-t, akkor a többi elemnek regisztráltatnia kell magát vele, majd az elemek menedzselését a Gatekeeper végzi

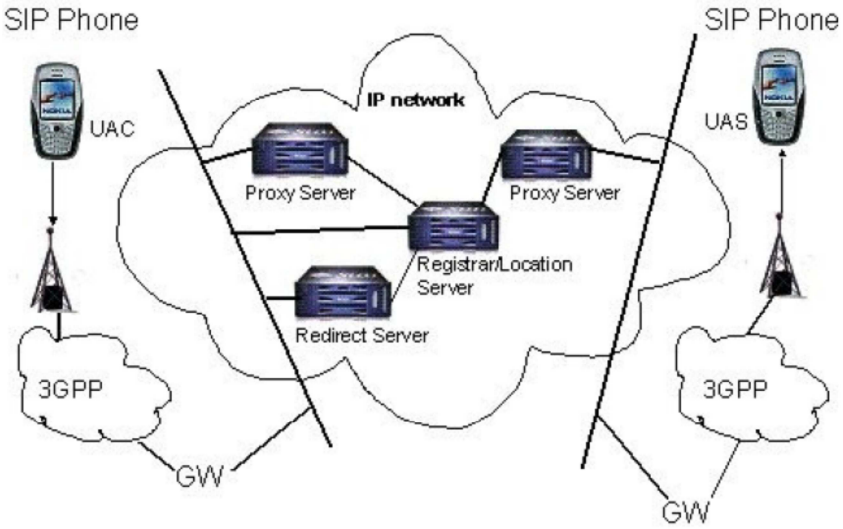
Multipoint Control Unit (MCU):

- Három vagy több terminál közötti konferenciahívást tesz lehetıvé
- A konferenciában résztvevı végpontok között fenntartja az audió/videó/adatfolyamot
- Külön is állhat, de általában a Gateway-be, vagy a Gatekeeper-be integrálják
- Két részegységbıl áll:
    - Multipoint Controller (MC): kezeli a terminálok közötti jelzéseket, meghatározza, hogy mely hang és kép jelfolyamot használja a rendszer
    - Multipoint Processor (MP): kapcsolja és feldolgozza a jelfolyamokat

Session Initiation Protocol (SIP):

- Az IMS fő protokollja
- Alkalmazás rétegbeli protokoll
- Legfontosabb feladata: multimédia session-ök létrehozása, módosítása és megszakítása
- Támogatja a képességegyeztetést és a mobilitást
- A jól ismert kliens-szerver modellt követi
- Az SMTP és a HTTP protokollokból fejlesztették ki
- Szöveg alapú protokoll

SIP architektúra:



User Agent:

- Azok a Internet végpontok, amelyek a SIP protokollt használják arra, hogy megtalálják egymást, illetve hogy egyeztessék a session beállításokat
- Általában a felhasználó számítógépén alkalmazás formájában van jelen, de lehet például PDA vagy SIP telefon is
- Lehet UAS (User Agent Server) vagy UAC (User Agent Client)
- UAS-ként viselkedik, ha az UAC-tól kéréseket fogad, majd azokra választ küld vissza
- UAC-ként viselkedik, ha az UAS-nak kéréseket küld, és az azokra érkezett válaszokat dolgozza fel

Proxy szerver:

- A SIP infrastruktúra legfontosabb eleme
- A user agent által küldött kéréseket és válaszokat továbbítja egy másik user agent, vagy egy másik proxy szerver felé
- Elvégzi a session felépítéshez szükséges útvonal választási feladatokat a hívott fél helyzetétől függően
- A hívó féltől érkező session hívást minél gyorsabban el kell juttatnia a hívó félhez
- Gyakori, hogy a hívó féltől érkező session hívás több proxy szerveren keresztül jut el a hívott félhez
- Két típusát különböztetjük meg:
    - Stateless:
        - Egyszerű és gyors üzenettovábbítás
        - A tranzakciókat nem ismeri
        - Nem képes az üzenetek újraküldésére
        - Felhasználás: például load balancing
    - Stateful:
        - Elágaztatás (forking)
        - Újraküldések kezelése
        - További funkciók: például számlázás

Registrar/Location szerver

- Speciális SIP entitás
- A felhasználók regisztrációs kéréseit fogadja, melyek tartalmazzák az adott előfizető pillanatnyi tartózkodási helyét (IP cím, port szám, felhasználónév)
- Tárolja a felhasználók helyzetére vonatkozó információkat a location databaseben
- Gyakran csak egy logikai entitás, melyet a proxy szerverrel együtt helyeznek el

Redirect szerver:

- Kéréseket fogad, amelyekre válaszként elküldi a kívánt felhasználó tartózkodási helyét
- A szükséges információkat a registrar által létrehozott location database-ből kapja meg
- SIP üzeneteket nem dolgoz fel és hívásokat sem fogad

A felhasználók azonosítása a SIP segítségével:

Bármely hálózathoz hasonlóan az IMS-ben is szükség van a felhasználók azonosítására
A felhasználói azonosítók csoportosítása:

- Nyilvános felhasználói azonosítók
    - SIP URI (SIP Uniform Resource Identifier)
    - Tel URI (Telephone Uniform Resource Identifier)
- Privát felhasználói azonosítók

Nyilvános azonosítók:
A szolgáltatók minden egyes felhasználóhoz legalább egy SIP URI-t és egy Tel URI-t rendelnek
SIP üzenetek irányításához szükségesek
SIP URI:
• Alakja: sip:Alice.Smith@domain.com
• Telefonszámot is tartalmazhat, ekkor a formája:
sip:+1-212-555-0293@domain.com;user=phone
• A regisztrálandó azonosító csak SIP URI lehet, Tel URI nem
• A felhasználók TLS-sel (Transport Layer Security) titkosíthatják is, ekkor alakja:
sips:Alice.Smith@domain.com
Tel URI:
• Nemzetközi formátuma: tel:+1-212-555-0293
• IMS és PSTN közötti átjárhatóság miatt van rá szükség
Privát azonosítók:
Minden falhasználó pontosan egy privát felhasználói azonosítóval rendelkezik
Az előfizetők azonosításához és hitelesítéséhez használják
Formátuma a SIP URI és a Tel URI helyett NAI (Network Access Identifier): Alice.Smith@domain.com
A felhasználónak nem kell ismernie, mivel a szolgáltató által kiadott chipkártyán tárolható

4. SIP protokollüzenetek. Az üzenet részei, kérés-válasz modell, a legfontosabb SIP kérések és válaszok. A legfontosabb fejléc mezők (pl. record-route). Az SDP.

SIP protokoll szabvány ismertetése:

- Egy SIP kommunikáció kérésekből és a kérésekre adott válaszokból áll.
- A kéréseket a hívást kezdeményező fél küldi.
- A felhasználói készülékektől érkező kéréseket a SIP metódusok azonosítják.
- A kommunikáció létrejöttét az adott kérésekre adott megfelelő válaszok segítik.

SIP üzenet részei

Start/status line:

• Kérésnél start line, válasznál status line van

• A start line a SIP kérés első sora, mely tartalmaz egy címhivatkozást, valamint a SIP protokoll verzióját és a SIP üzenetek típusát

• A status line a válaszok első sora, ami a SIP protokoll verziója mellett a kérés állapotát jelzi

Message headers:

• A start/status line-t követik

• Minden egyes fejléc olyan paramétereket tartalmaz, melyek további részleteket biztosítanak a kérésről, vagy a válaszról

• Az utolsó fejléc (Content-Length) az üzenettörzs (message body) hosszát határozza meg

Message body:

• Opcionális, két fél közötti kapcsolat létrehozásához nem, csak a hang és képátvitelhez szükséges

• Tartalmát a Content-Type fejléc írja le, leggyakoribb az SDP (Session Description Protocol)

• Tehát az üzenet más protokollt i tartalmazhat, ami újabb részleteket nyújt az éppen folyamatban lévő session-ről

A legfontosabb SIP metódusok:

REGISTER

• Leggyakrabban ez az üzenet az első, amit egy eszköz kezdeményez a bekapcsolás után

• Célja, hogy értesítse a hálózatot az eszköz helyzetéről és IP címéről, mivel ez alapján tudja a hálózat, hogyan kell továbbítani az üzeneteket az eszköz felé

INVITE

• Leggyakrabban használt üzenettípus

• Session-ök létrehozására használják

• Ennek elküldésével kér fel egy felhasználó egy másikat beszélgetésre vagy azonnali üzenetküldésre

ACK

• Utolsó üzenetet, ami szükséges a kapcsolat létrejöttéhez és a session megkezdésének engedélyezéséhez

• Kezdeményező fél küldi miután az INVITE üzenetre megkapta a szükséges válaszokat a címzettől

CANCEL

• A kezdeményező küldi, ha szeretné visszavonni az INVITE-ot, mielőtt az megérkezne a címzetthez

• Ha az INVITE megérkezése után kapja a CANCEL-t a címzett, akkor figyelmen kívül hagyja

BYE

• A session bármely végpontja küldheti, ha meg szeretné szakítani az összeköttetést

SUBSCRIBE

• A felhasználók profiljában történı esetleges változás lekérésére használják az alkalmazás szerverek

NOTIFY

• Értesítő üzenet, hogy a felhasználó megváltoztatta a regisztrációját (pl.: új szolgáltatásra fizetett elő)

• Tartalmazza az új regisztráció során végbement változásokat

A legfontosabb SIP válaszok:

Számos típusa létezik a válaszoknak, melyek mindegyike beleesik a hat féle besorolás egyikébe, melyek a következők:

- 1xx: Előzetes válaszok (pl.: 100 Trying)
- 2xx: Pozitív válaszok (pl.: 200 OK)
- 3xx: Átirányító válaszok (pl.: 300 Multiple Choises)
- 4xx: Kliens hibára utaló válaszok (pl.: 403 Forbidden)
- 5xx: Szerver hibára utaló válaszok (pl.: 503 Server Unavailable)
- 6xx: Globális hibára utaló válaszok (pl.: 600 Busy Everywhere)

A válaszokat az előttük álló háromjegyű számok azonosítják

Az első számjegy a válasz osztályát, míg a következő két számjegy a specifikus választ azonosítja

100 Trying

- Jelzi, hogy a hálózat megkísérli elérni a címzettet
- Proxy küldi, hogy megelızze az INVITE üzenet újraküldését

180 Ringing

- A címzett ezzel tudatja, hogy megkapta az INVITE üzenetet, illetve hogy az eszköz csöngeti az előfizetőt

200 OK

- A vevő elfogadta a kérést, így megkezdődhet a tényleges kommunikáció a két fél között

401 Unauthorized

- A hálózat küldi a kliensnek, miután az elküldte az első REGISTER üzenetet
- Hatására a kliens egy második REGISTER üzenetet fog küldeni

403 Forbidden

- Akkor használják, ha a hívás még a párbeszéd felépítése előtt el lett utasítva

407 Proxy Authentication Required

- Proxy küldi az előfizetői eszköznek, ha annak hitelesítésre van szüksége

A legfontosabb fejléc mezők:

Via

- Útvonalfeljegyzéshez szükséges
- Kérés tartalmazza, ennek segítségével éri el a hívott felet, majd ezután minden válasz ezt az útvonalat fogja követni
- Válasz küldése esetén a proxy-k a következő csomópont meghatározására használják

From

- A kérés kezdeményezőjét azonosítja a kijelzett név, a SIP URI vagy a Tel URI alapján
- A felhasználók számára találták ki, nem használják útvonal irányításra

To

- A kérést küldő végpontot, vagy a hívás során ezt módosító proxy-t azonosítja
- A From fejléchez hasonlóan nem használják útvonal irányításra

Contact

- Az előfizetőről biztosít további, a címmel kapcsolatos információkat
- Olyan címeket azonosít, amelyre a kérés még akkor is elküldhető, ha az első címre küldött kérésben hiba volt

Call-ID

- Egyedi azonosító a session-ökhöz, így a proxy-k a válaszokat hozzá tudják rendelni a kérésekhez

CSeq

- A párbeszéd alatt megfelelő sorszámmal látja el a tranzakciókat
- A végpontok használják a kérések és a hozzájuk tartozó válaszok azonosítására

Max Forwards

- Függetlenül attól, hogy kérés vagy válasz, kap egy értéket az üzenet elküldése előtt
- Ha az üzenet keresztül megy egy proxy-n, akkor a mező értéke eggyel csökken

• Ha egy proxy olyan üzenetet kap, amiben a Max Forwards értéke 0, akkor eldobja az üzenetet

Content-Type

• A message body-ban található tartalom típusát azonosítja (pl.: SDP)

Content-Length

• A message body hosszát tartalmazza oktettekben

Route és Record-Route

• Szigorú útvonal irányításnál használják ıket együtt

• A kérésekben a Route fejléc, a válaszokban a Record-Route fejléc a felelős az üzenetek irányításáért

• Ha egy kérés a hálózat több csomópontján keresztül halad a címzettig, akkor a közbülső proxy-k mindegyike beleteszi a Route fejlécet a kérésbe, természetesen a saját címeikkel együtt

• Ha a kérés eljut a címzettig, akkor a Route fejléc helyett a Record-Route fejlécet használja a válasz elküldéséhez, méghozzá úgy, hogy a Record-Route fejlécbe kerül a Route fejléc tartalma, így a válasz ugyan azon az útvonalon jut vissza a kezdeményezőhöz, mint amelyiken a címzetthez érkezett

Authorization

• A WWW-Authenticate fejlécet követő üzenetben kell lennie

• Az előfizető hitelesítéséhez szükséges információkat tartalmazza

• Legfontosabb tartalma a hitelesítési felhasználónév és a response, mely egy titkosítási algoritmussal számolt hitelesítéshez szükséges számsort tartalmaz

WWW-Authenticate

• A proxy-k ezzel a fejléccel szólítja fel az előfizetői klienset, hogy hitelesítse magát

• Erre a felhívásra indított SIP metódus tartalmazza az Authorization fejlécet

Session Description Protocol (SDP):

- A session leírók tulajdonképpen a session leírását tartalmazzák, ami szükséges ahhoz, hogy fel lehessen építeni egy multimédia kapcsolatot
- Elegendő információt biztosítanak a felhasználóknak, hogy csatlakozni tudjanak egy session-höz
- Multimédiás session-ök esetén ezen információk közé tartozik az IP cím és a port szám, ahova a médiát és a kodekeket kell küldeni, utóbbi a résztvevők hang és videó kódolásához szükséges
- A session leírókat szabványos formátumot használva hozzák létre, melyek közül a leggyakoribb a Session Description Protocol (SDP) – RFC 2327
- Fontos megjegyezni, hogy habár a „P” betű az SDP-ben a protokollt jeleneti, az SDP egyszerű szöveges formátumú

Ez egy Alice által Bobnak küldött SDP üzenet (Az SDP üzenet természetesen SIP üzenetbe van beágyazva (pl.: Invite)):

```
v=0
o=Alice 2790844676 2867892807 IN IP4 192.0.0.1
s=Let's talk about swimming techniques
c=IN IP4 192.0.0.1
t=0 0
m=audio 20000 RTP/AVP 0
a=sendrecv
m=video 20002 RTP/AVP 31
a=sendrecv
```

Többek között a következőket tartalmazza:

• Beszélgetés tárgya (Swimming techniques)

• Alice IP címe (192.0.0.1)

• Port szám, amin Alice a hangot szeretné fogadni (20000)

• Port szám, amin Alice a videót szeretné fogadni (20002)

• Audió és videó kodekek, amit Alice támogat:

- 0, ami a G.711-es audió kodeknek felel meg
- 31, ami a H.261-es videó kodeknek felel meg

Alapvetően két részre osztható egy SDP
- Session szintű információk
- Média szintű információk

SDP – A kérés/válasz modell:

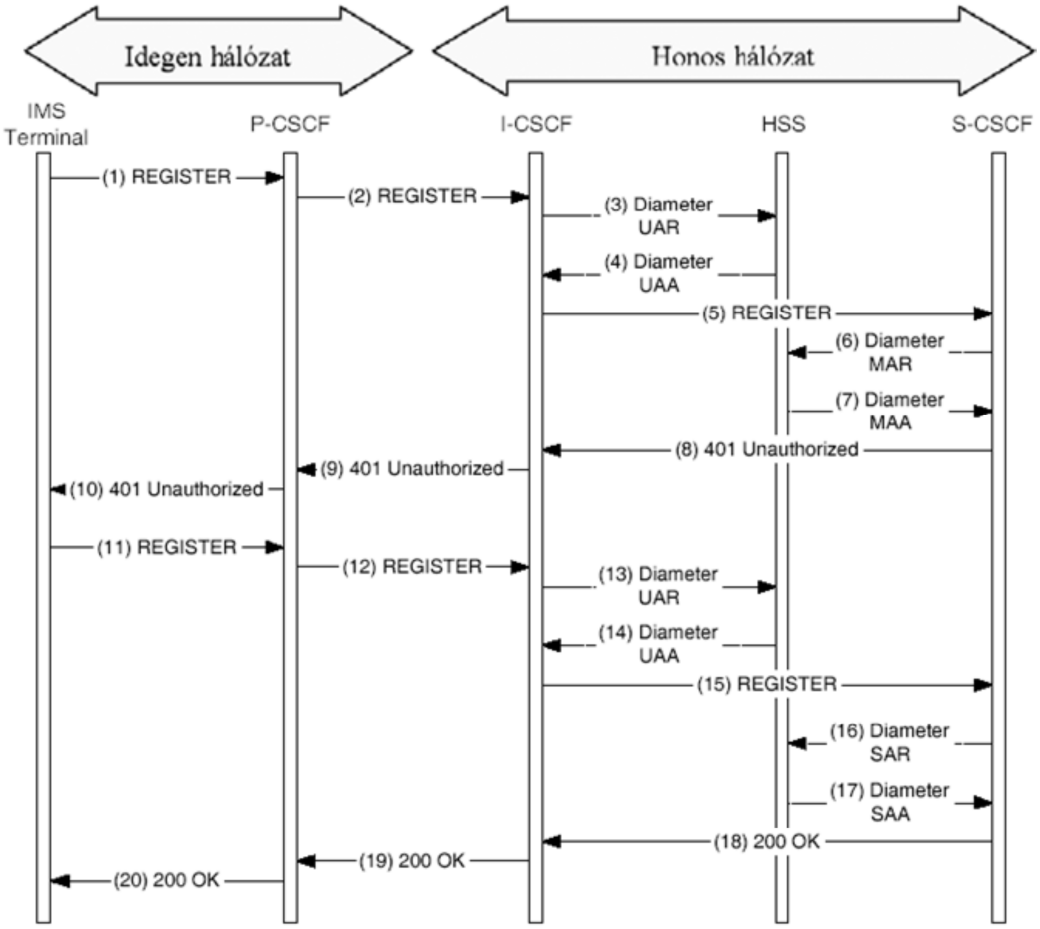
- Az előző példánál maradva, Alice küld egy session leírót Bob-nak
- Azonban ez nem elegendő, a multimédia kapcsolat felépítéséhez Alice-nek tudnia kell Bob IP címét is
- A SIP protokoll biztosít egy kétutas, session leírók cseréjére alkalmas folyamatot, amit kérés/válasz modellnek nevezünk
- Valamely felhasználó (a kérő fél) generál egy session leírót és elküldi a hívott félnek (a válaszoló), aki ezután generál egy új session leírót, amit visszaküld, vagyis megtörténik az egyeztetés
- Az kérés/válasz modell megkövetel bizonyos szabályokat a session leíró generálásra
- Az kérés/válasz csere után a résztvevők ismerni fogják legalább azt, hogy a másik milyen formátumot, milyen kodekeket támogat, illetve ismerik egymás IP címét is

```
v=0
o=Bob 234562566 236376607 IN IP4 192.0.0.2
s=Let's talk about swimming techniques
c=IN IP4 192.0.0.2
t=0 0
m=audio 30000 RTP/AVP 0
a=sendrecv
m=video 30002 RTP/AVP 31
a=sendrecv
```

Tehát Bob visszaküldi az általa generált session leírót. Mivel Bob is támogatja azokat a formátumokat, amit Alice (G.711 és H.261), megkezdődhet a média átvitel.

5. IMS regisztráció és hívásfelépítés (folyamatábra alapján), IETF és 3GPP SIP koncepció összehasonlítása.

Regisztráció folyamata:



Ahhoz, hogy az IMS terminál regisztrálhasson az IMS rendszerbe, előbb IP szintű kapcsolatot kell létesítenie a hozzáférési hálózaton. Ez a hozzáférési hálózat lehet mobil (pl.: GPRS), vezeték nélküli (pl.: WLAN), vagy vezetékes (pl.: ADSL). Ha ez megtörtént, akkor megkezdődhet a regisztráció folyamata SIP üzenetek váltásával.

Regisztráció

A regisztrációt szemléltető ábrán a lehető legösszetettebb esetet feltételezzük:

• A felhasználói terminál idegen hálózatban tartózkodik (roaming)

• A P-CSCF szintén az idegen hálózatban található (a P-CSCF a honos hálózatban is elhelyezhető)

(1) A terminál Register üzenetet küld a P-CSCF-nek

(2) A P-CSCF továbbküldi a Register üzenetet a honos hálózat szélén lévő ICSCF-nek

(3-4) Az I-CSCF a Diameter protokoll segítségével üzenetet vált a HSS-sel, melynek céljai:

• A publikus és privát felhasználói azonosítók ellenőrzése

• Az idegen hálózattal való roaming szerződés meglétének ellenőrzése

• Annak ellenőrzése, hogy a publikus felhasználói azonosító nincs-e regisztrálva másik S-CSCF-ben

(5) A HSS-től kapott pozitív választ követően az I-CSCF továbbküldi a Register üzenetet az S-CSCF felé

(6-7) Az S-CSCF a HSS-től lekéri a felhasználó hitelesítésére szolgáló hitelesítési vektorokat, majd tájékoztatja a HSS-t arról, hogy az adott felhasználó az S-CSCF-hez lett rendelve (A felhasználót csak a regisztráció során hitelesíti a rendszer, vagyis regisztrált állapotban más üzenetváltások alkalmával nem történik felhasználói hitelesítés)

(8-10) Az S-CSCF egy 401 Unauthorized üzenetet küld a terminálnak, ami tartalmaz egy hitelesítési felszólítást a felhasználó felé a szükséges adatokkal, melyre a terminálnak felelnie kell

(11-12) A terminál újból küld egy Register üzenetet a P-CSCF-nek, ami tartalmazza a hitelesítési felszólításra adott választ, majd ezt a P-CSCF továbbítja az I-CSCF felé
(13-14) Az I-CSCF a Diameter protokoll segítségével újra üzenetet vált a HSSsel, mivel:
• Előfordulhat, hogy a terminál második Register kérése nem ugyan ahhoz az I-CSCFhez irányítódik, mint az első
• A HSS-ben viszont nyilván van tartva, hogy melyik S-CSCF várja ezt a második Register üzenetet a terminálótól a hitelesítési felszólításra adott válasszal együtt
(15) Az I-CSCF annak az S-CSCF-nek továbbítja a második Register kérést, amelyiktől a hitelesítési felszólítást kapta a terminál
(16-17) Az S-CSCF és a HSS újbóli üzenetváltása:
• A HSS-ben eltárolásra kerül, hogy a felhasználó az adott S-CSCF-hez lett regisztrálva
• Az S-CSCF letölti a HSS-ből a felhasználói profilt, illetve annak kívánt részét
• A felhasználói profil tartalmazza a privát és a publikus felhasználói azonosítókat az esetlegesen megrendelt szolgáltatásoknak megfelelően, az esetleges szűrőfeltételeket stb.
(18-20) Az S-CSCF egy 200 OK üzenetet küld a terminálnak, ezzel jelezve a sikeres regisztrációt

A sikeres regisztráció után a terminál egy Subscribe kéréssel fordul az S-CSCF felé, ahol az adott terminál jelenléti állapota van nyilvántartva. A terminál így feliratkozik saját jelenléti állapotának figyelésére. Ezt követően ha valamilyen okból kifolyólag törlődik a terminál regisztrációja, a rendszer értesíti erről a terminált.

Hívásfelépítés:

Egy olyan hívásfelépítés kerül bemutatásra, ahol a hívó és a hívott fél is barangol, vagyis nem a honos hálózatukban tartózkodnak. Az egyszerűség kedvéért a kapcsolat során egyik fél sem vesz igénybe szolgáltatásokat, így nincs szükség alkalmazásszerverek közreműködésére. A P-CSCF a hívó és a hívott fél esetében is az idegen hálózatban található. A SIP jelzéseknek minden esetben érinteniük kell a hívó és a hívott félhez rendelt P-CSCF-et, illetve S-CSCF-et.
(1-14) Invite és 100 Trying üzenetek:
• A hívó terminál az Invite üzenetet a regisztrációkor hozzárendelt P-CSCF-nek küldi
• Ez az üzenet tartalmazhat szolgáltatások indítására, vagy a felhasználó helyére vonatkozó információkat (pl.: aktuális cella azonosító)
• Az Invite üzenet SDP-t is tartalmaz, amiben a hívó fél felsorolja az általa támogatott kodekeket
• A hívó P-CSCF ellenőrzi a SIP üzenet tartalmának helyességét:
    • Irányításra vonatkozó információk ellenőrzése
    • Használni kívánt kodekek ellenőrzése
    • Számlázáshoz szükséges mezők illesztése az üzenet fejlécébe
• A 100 Trying üzenet csak ideiglenes üzenet, ami végleges üzenetnek kell majd követnie
A hívó fél S-CSCF-e engedélyezheti az esetleges szolgáltatások indítását a regisztráció során letöltött felhasználói profiladatok alapján
• Az üzenet továbbítódik a hívott fél felé, melynek honos hálózatában az ICSCF kapja meg az üzenetet
• Az I-CSCF a HSS-ből a Diameter protokoll segítségével, hogy a hívott fél melyik S-CSCF-be van beregisztrálva, majd oda továbbítja az Invite üzenetet
• A hívott fél S-CSCF-e szintén engedélyezheti szolgáltatások indítását a hívott fél profiladatai alapján
• A hívott terminál csak akkor fogja jelezni a bejövő hívást, amikor mindkét félnél megtörtént a kívánt hálózati erőforrás lefoglalása
• Ez a kapcsolatban használt média típusoktól és a kodekektől függ, amiket az Invite üzenetben található SDP-vel egyeztetnek a felek
(15-20) 183 Session Progress üzenetek:
• A hívott fél az SDP-ben közli saját IP címét, mivel ez alapján a média átvitel közvetlenül fog menni a felek között
• A beágyazott SDP további médiatípus és kodek egyeztetésre szolgálhat, mivel a felek megpróbálják kiválasztani a mindkettőjük által támogatott, legmegfelelőbb kodekeket

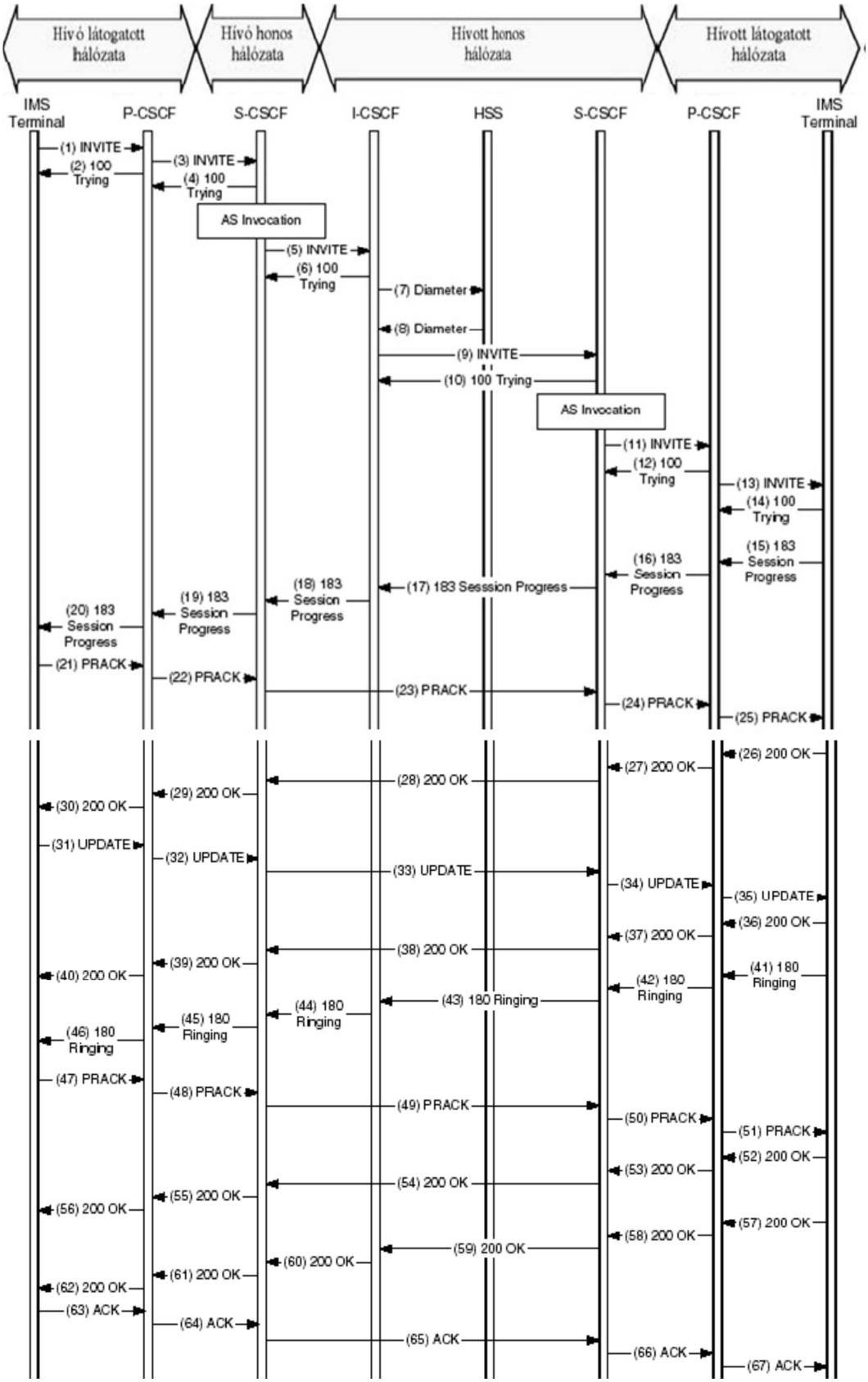
• Ezzel tájékoztatja a hívott fél a hívó felet, hogy a hálózati erőforrás lefoglalás folyamatban van

(21-30) Prack és a hozzá tartozó 200 OK üzenetek

• A Prack üzenetet az előző 183 Session Progress üzenet igényelte

• Erre azért van szükség, mert a hívott fél így bizonyosodik meg arról, hogy a hívó megkapta a 183 Session Progress üzenetet

• A Prack üzenet tartalmazhat új SDP felajánlást, emellett az üzenet feladásakor a hívó fél megkezdi a hálózati erőforrás lefoglalását



(31-40) Update és a hozzá tartozó 200 OK üzenetek:

• A hívó fél jelzi, hogy befejezte az erőforrás lefoglalást

• A hívott fél a 200 OK üzenetbe ágyazott SDP-vel jelzi, hogy ı is lefoglalta a szükséges hálózati erőforrásokat

(41-56) 180 Ringing, Prack és a hozzá tartozó 200 OK üzenetek:

• A 180 Ringing üzenettel jelzi a hívott fél a hívónak, hogy csengeti a végkészüléket

• Ez az üzenet szintén Prack üzenetet igényel a 183 Session Progress üzenethez hasonlóan

(57-67) 200 OK és Ack üzenetek:

• A kapcsolat létrejöttét és a médiafolyam indítását jelzi

• Amikor a hívó fél elfogadja a hívást, a terminál egy 200 OK üzenetet küld

• Erre a hívó fél nyugtázásképpen küld egy Ack üzenetet, majd megkezdődik a média végponttól végpontig történő közvetítése a felek között

(Ha valamelyik fél szeretné megszakítani a kapcsolatot, akkor egy Bye üzenetet küld a másik fél részére, mire az egy 200 OK üzenettel nyugtázza, hogy vette a Bye üzenetet)

Az IETF SIP és a 3GPP SIP összehasonlítása:

Az IETF definiálja a protokollokat, mint például: SIP, SDP, RTP, Diameter

Az IETF SIP a felhasználó centrikus megközelítésen alapul, így a hálózati elemek legfontosabb célja a routing és kismértékben a hívásvezérlés.

A 3GPP az IETF protokollok felhasználását definiálja a 3GPP architektúrában. A 3GPP hálózatcentrikus nézőponttal rendelkezik, vagyis az operátorok szabályozni akarják a hozzáférést, a hívásfelépítést, a hívásbontást, a számlázást, stb.

A problémák oka a 3GPP és az IETF között, hogy megpróbálják a közbenső hálózati eszközök számára lehetővé tenni a végpontok közötti SIP protokoll vezérlést.

A 3GPP további követelményeket támaszt a SIP protokollal szemben:

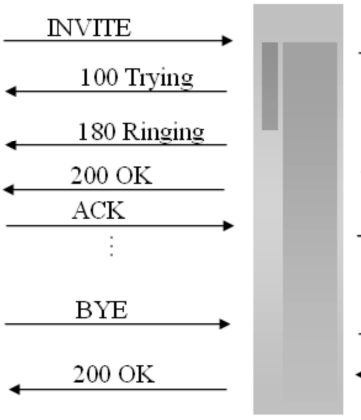
• UMTS-AKA alapú authentikálás

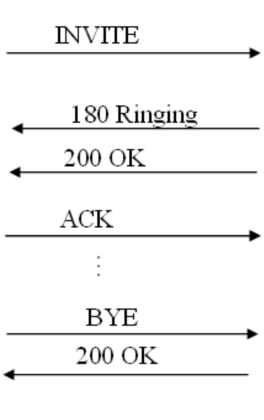
• Hálózat (operátor) által kezdeményezett hívásbontás

• Hálózat (operátor) által kedvezményezett újraazonosítás

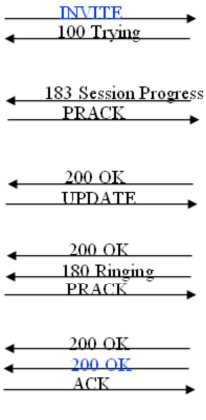
• Path, P-Access-Network-Info, stb.

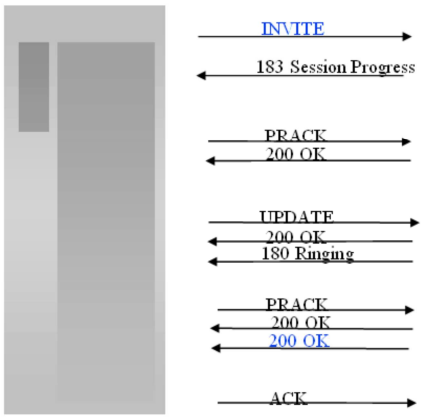
Hívásfelépítés és lebontás az RFC 3261 IETF alapján





Hívásfelépítés és lebontás a 3GPP alapján:





6. QoS biztosítási lehetőségek az IMS-ben. Intserv és Diffserv modell, PDP.

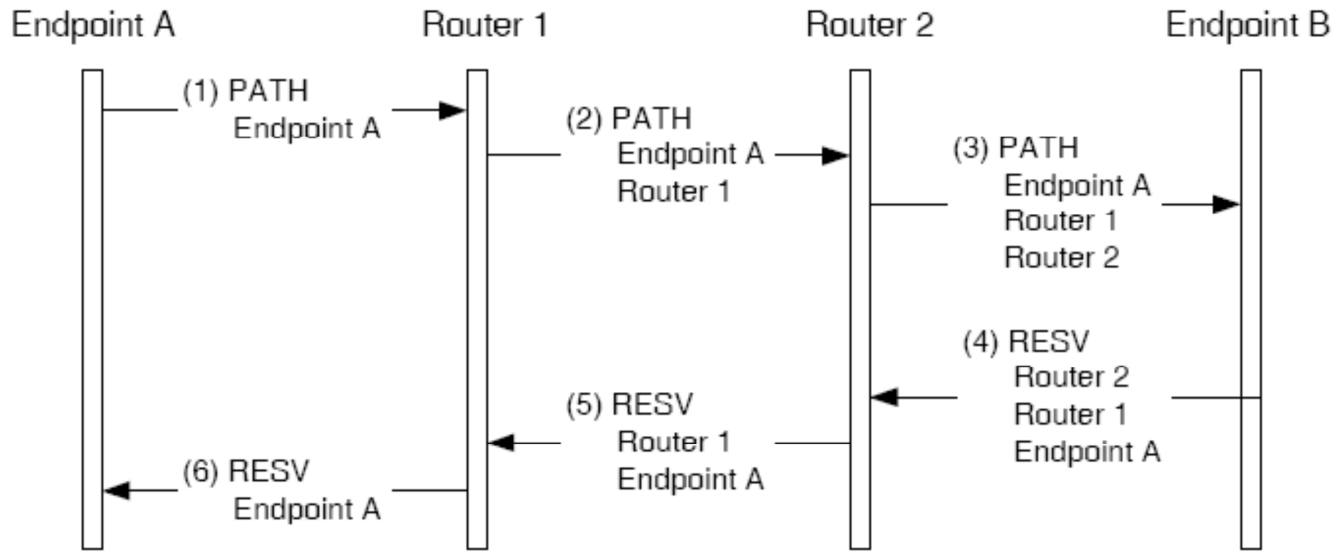
Az Internet best effort jellegő, de egyes alkalmazások igénylik a QoS-t. A QoS alatt nem csak az egyes adatfolyamok prioritásos kezelését értjük, hanem, azt is, hogy bizonyos követelményeknek eleget tegyen. Két modell szerint biztosítanak QoS-t az interneten. Az egyik modell az Integrated Services (IntServ) modell, a másik pedig a Differentiated Services (DiffServ) modell.

Integrated Services:

Végponttól végpontig biztosítja a QoS-t. A végpont egy bizonyos szintű QoS-t igényel a csomagjainak, és ha a hálózat megadja ezt, akkor a routerek ennek megfelelően kezelik a csomagokat.
Két különböző QoS szolgáltatás érhető el:

- Controlled load service
- Guaranteed service

Controlled load services: biztosítja hogy a csomagok úgy kerülnek továbbításra, mint amikor a hálózaton mérsékelt forgalom van jelen. Ezen csomagokat nem érinti a hálózati torlódás. Ennek ellenére a hálózat nem garantál sem meghatározott sávszélességet, sem késleltetést. Jobb mint a best-effort.
Guaranteed service: egy meghatározott sávszélességet, vagy a késleltetés egy bizonyos mértékét garantálja. Ezt általában kevés helyen használják, mert a „controlled load service" általában megfelelő teljesítményt nyújt, és egyszerűbb a kezelése.
Az IntServ RSVP (Resource ReSerVation Protocol) protokollt használ, mint erőforrás foglaló protokoll. RSVP üzenettel a végpontok egy bizonyos szintű QoS-t igényelhetnek. Az RSVP üzenetnek, az adatokkal megegyező útvonalon kell haladniuk. Két speciális üzenet: PATH és RESV. A PATH megjegyzi az útvonalat, amin keresztül eljutott a célállomásra. A RESV ugyanezt az útvonalat használja visszafelé. Az adatok a PATH üzenettel megegyező útvonalon jutnak el a célig.
Az RSVP erőforrás lefoglalás egy kétirányú handshake kapcsolatból áll. Az A pont PATH üzenetet küld B-nek, majd nyugtaként egy RESV üzenetet kap:



Az erőforrásfoglalás akkor történik meg, amikor a routerek megkapják a RESV üzenetet. A protokoll a hálózati topológia változására is tekintettel van. A routerek a bejegyzéseket soft state módon tárolják. Bizonyos időközönként az erőforrás foglalás tényét meg kell erősíteni egy PATH-RESV üzenetváltással. A routerben a bejegyzések az idő lejárta után törlődnek. Ezeken felül a routernek joga van visszautasítani egy kérést, ha nincs elég kapacitás, vagy ha a felhasználónak nincs joga hozzá.

Differentiated Services:

Az IntServ főproblémája, hogy a hálózat állapotáról rengeteg információt kell tárolni. A routernek minden beérkező csomagnál ellenőriznie kell, hogy tartozik-e hozzá már bejegyzés. Ez hatalmas over-headet jelent.
A DiffServ megpróbálja kiküszöbölni az IntServ skálázhatósági problémáját. Azt, hogy egy routernek hogyan kell egy csomagot kezelnie, a Per Hop Behavior (PHB) határozza meg.
A megfelelő PHB-t az IP csomag fejlécében egy 8 bites Differentiated Services CodePoints nevű mező határozza meg. Ezzel a mezővel a hálózat határán jelöli meg a router a csomagokat, a hálózaton belül ez alapján kezelik a routerek a csomagokat.

QoS az IMS-ben:

Az IMS egyik kulcspontja a jól konfigurálható QoS támogatás. Legfontosabb tényező a felhasználó számára biztosított sávszélesség és a kapcsolat állapota, minősége. Az IMS lehetővé teszi a szolgáltatóknak a QoS kontrollálását, és ezáltal a felhasználók bizonyos csoportjaink megkülönbözetését.
Az IMS több QoS modellt is támogat:

- Adatkapcsolati rétegbeli protokollok (pl.: PDP kontextus)
- IntServ
- DiffServ

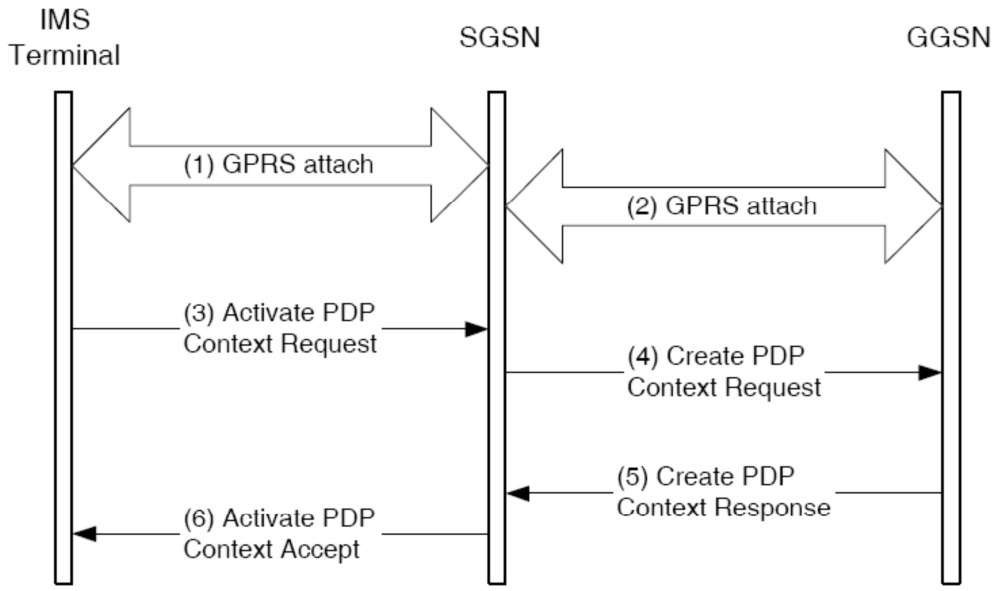
A legáltalánosabb modell szerint az IMS terminálok **PDP** kontextust használnak, a GGSN pedig leképezi azt DiffServ kódokra.
Fontos, hogy a terminál fel tudja térképezni a kapcsolaton áthaladó media stream erıforrás igényeit. Pl.: egy audio + videó adáshoz rendelhet közös, vagy különböző lefoglalást, mely másodlagos PDP kontextus kialakítását, vagy RSVP PATH üzenet küldését tartalmazza. A lefoglalásra a P-CSCF adja ki az utasítást az SDP csoportosító keretrendszer SRF szemantika (Single Reservation Flow) felhasználásával.
Az a = group sor jelzi a csoport szemantikáját (LS, SRF), és a médiafolyamok azonosítóit.
A kapcsolat 2 audio stream-je ugyanazt a PDP kontextust használják, míg a videó a külön hozzá tartozót.

```
v=0
o=- 289083124 289083124 IN IP6 1080::8:800:200C:417A
t=0 0
c=IN IP6 1080::8:800:200C:417A
a=group:SRF 1 2
a=group:SRF 3
m=audio 20000 RTP/AVP 0
a=mid:1
m=audio 20002 RTP/AVP 0
a=mid:2
m=video 20004 RTP/AVP 31
a=mid:3
```

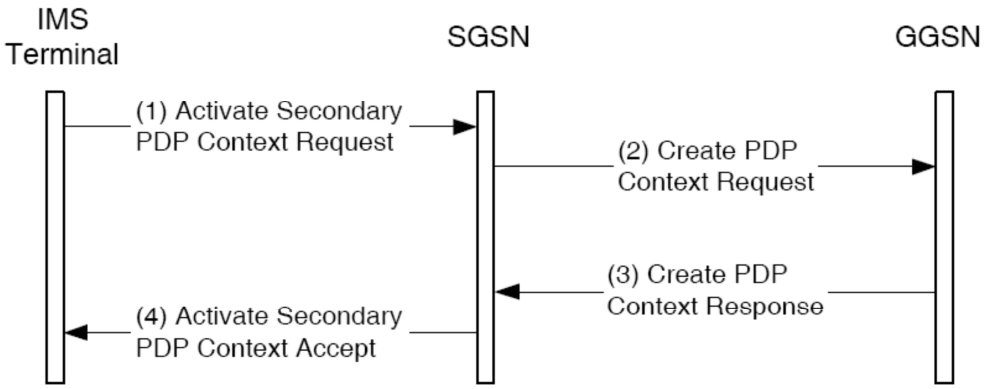
Amennyiben az elérendő hálózat GPRS, az erőforrás lefoglalási folyamat egy PDP kontextus. A PDP-vel kapcsolatban a hálózat információkat tárol, melyek tartalmazzák az IP címet és a QoS karakterisztikát, beleértve a forgalmi osztályokat, melyből 4 fajta van:

- Best effort
- Interactive
- Streaming
- Conversational

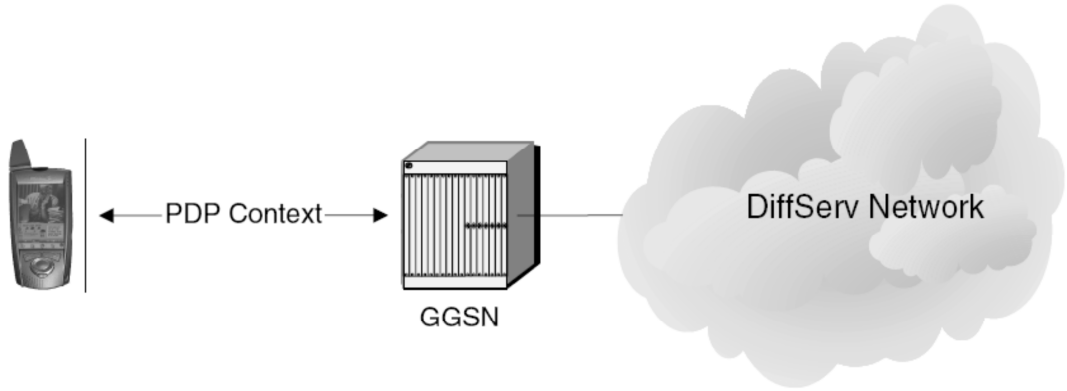
A SIP üzenetek továbbításához mindig conversational forgalmi osztály tartozik.



Az IMS terminálok létrehozhatnak járulékos PDP viszonyokat is médiák küldésére és fogadására. Az IP cím ugyanaz, viszont a QoS karakterisztika lehet más, mint az elsődleges PDP kontextusnál.



A GGSN az adott terminálótól PDP viszonyon keresztül kapott forgalmat egy megfelelő DSCP (Differentiated Service CodePoint)-hoz rendeli, és kiküldi egy DiffServ-enabled hálózatba. A DiffServ csomóponti funkciót a GGSN látja el.



7. Hitelesítés, Engedélyezés, Számlázás (AAA) az IMS-ben, a Diameter protokoll, a felhasználói profil.

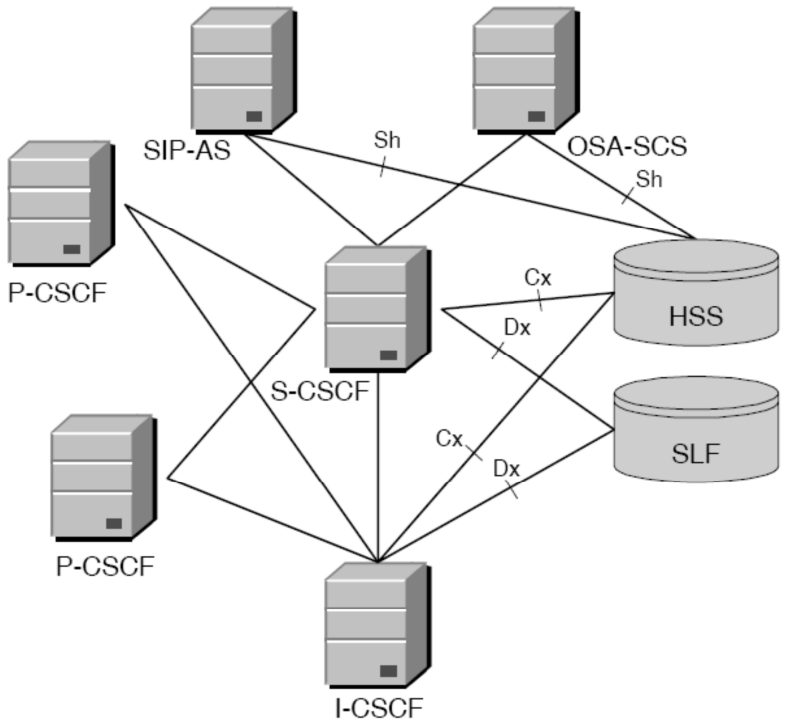
Végfelhasználó számára láthatatlanul működő funkciók, melyek révén a szolgáltató hozzáférés ellenőrzést, monitorozást és számlázást valósíthat meg.

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.

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

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.

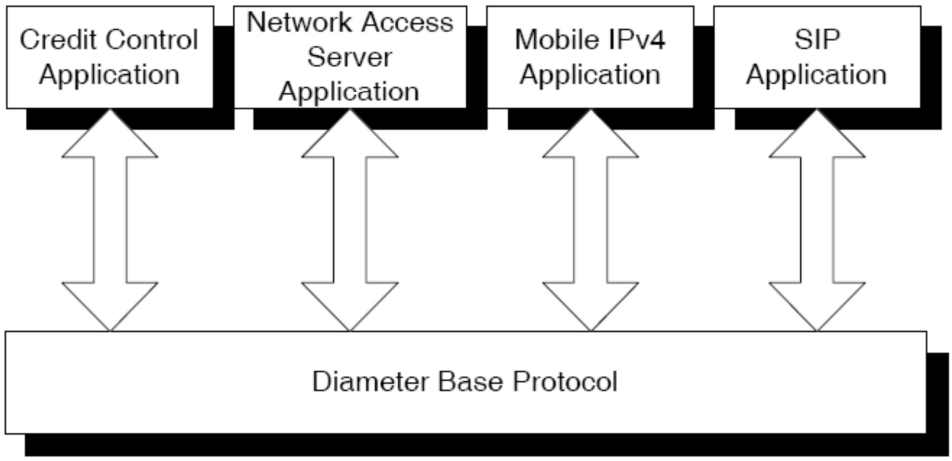


Az I-CSCF és S-CSCF a Cx és Dx interfészeket használja a következő funkciók megvalósítására:
- Felhasználóhoz rendeli a már lefoglalt S-CSCF-et.
- Letölti a felhasználóra vonatkozó hitelesítési vektorokat (HSS-ben vannak tárolva).
- Feljogosítja a felhasználót roaming használatára látogatott hálózatban.

• 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.

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.



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.
• 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.

A 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 SCSCF-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.

8. IMS számlázás. A számlázás fajtái, a számlázás feladatai. Miben különbözik az Immediate Event Charging és Event Charging with Unit Reservation.

Számlázás

- Hívások/szolgáltatások árának meghatározása
- 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.

Számlázás feladatai

Mediation

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

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

Billing

• a havi adatokból a számlainformációk előállítása
    - igényelt szolgáltatások
    - Kedvezmények
• a számla megformálása
• a nyomtatandó / elküldendő file előállítása
• adatok az A/R-nak

Accounts/Receivable (A/R)

• pénzügyek kezelése
• számlabefizetések (banki tranzakciók)
• pre-paid kártyák (top-up) kezelése
• figyelmeztetések, felszólítások

• forgalomfelügyelet (credit limit check)
• pénzügyi kimutatások készítése

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

Az Online számlázásnak 2 típusa van:

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.

9. IMS szolgáltatások: a presence szolgáltatás (általános bemutatás, elemei, példák). Milyen további IMS alkalmazásokat ismer? Milyen előnyökkel jár egy alkalmazásfejlesztési platform alkalmazása?

Presence szolgáltatás

A presence szolgáltatások alapvető célja a felhasználók aktuális elérhetőségeivel kapcsolatos jelenléti információk közzététele és terjesztése a hálózaton belül.
A presence információk tartalmazhatják az adott user online vagy offline helyzetére vonatkozó információkat, illetve az aktuálisan folytatott tevékenységével kapcsolatos adatok is lekérdezhetőek.

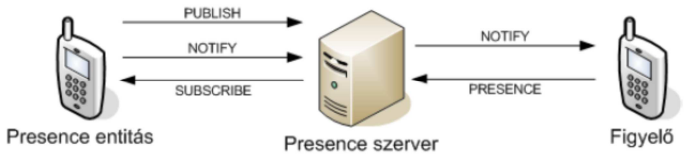
Presence alapötlete

- A hívott fél elérhető jelenleg? (chat, mms, e-mail, video…)
- Vagy éppen mást csinál? (olvas, alszik, megbeszélésen van…)
- Státusz állapota?
- Valóban az adott helyen tartózkodik?

Profilok létrehozása

- pl. az x csoporttól érkezhet bármilyen típusú üzenet, bármikor
- azonban az y csoport esetén a státusz legyen foglalt, illetve csak e-mail engedélyezett
- Hívások legyenek visszautasíthatóak
- Bizonyos státuszinformációk legyenek publikusak
- Néhány státuszinformációt pedig csak az arra jogosultak lássanak

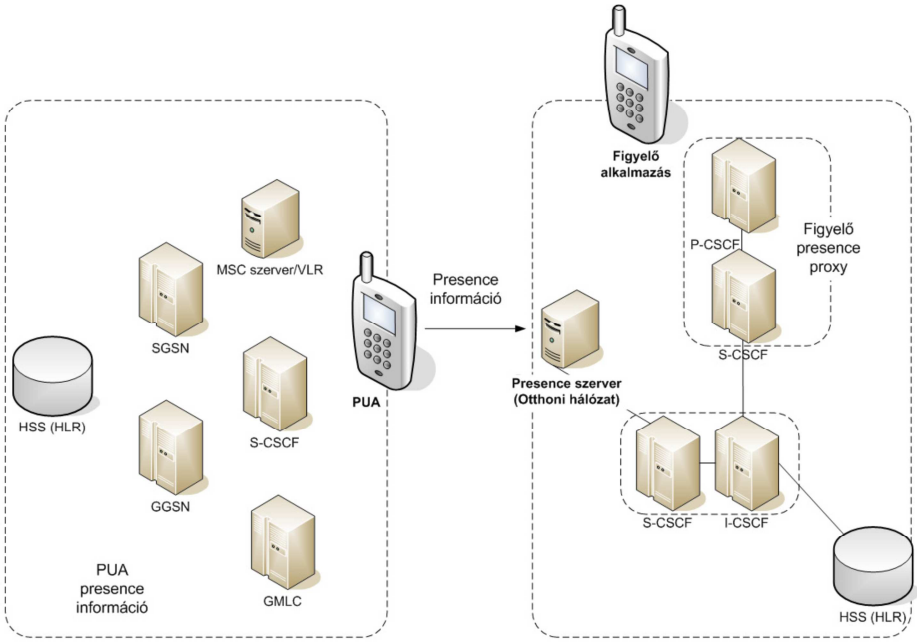
Elemei:



- A PUA egységek a saját információikat a Presence Agent (PA)-nak (presence ágens) továbbítják.
- A Presence Server (PS) egy funkcionális entitás a rendszeren belül. Elsődleges feladata a SUBSCRIBE üzenetek, illetve a további rendszerszintű üzenetek kezelése.
- A rendszer modelljének további résztvevői a figyelők (watchers). Elsődlegesen a PA részére küldenek presence információ lekérdezésére vonatkozó utasításokat, azonban a rendszer többi figyelőjéről is kérhetnek információkat.

Presense az IMS-ben

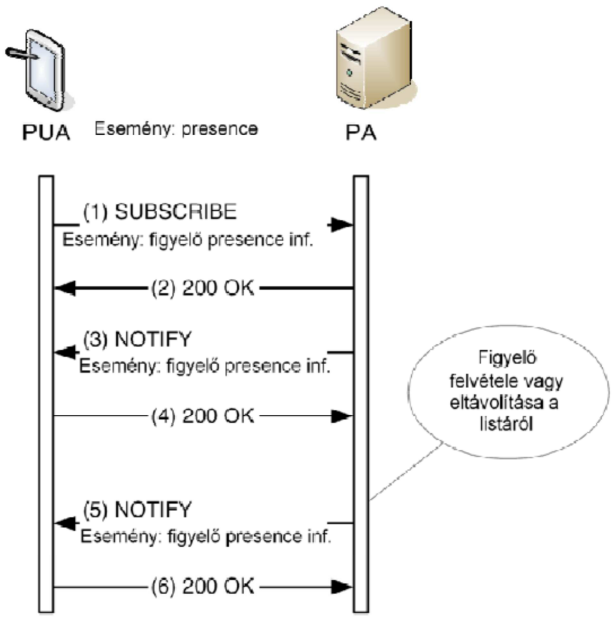
Presence szerver: (PS) A **p**resence szerver feladata a PUA-k által küldött presence információk kezelése, illetve a presence kérések kiszolgálása.
Figyelő presence proxy: Watcher presence proxy. A figyelő presence proxy feladata a presence entitás hálózatának meghatározása, illetve a presence entitás pontosa címének megadása.
Presence proxy: A presence entitáshoz tartozó presence proxy, feladata a presence szerver azonosítása.
PUA: A PUA egységek feladata a presence információ eljuttatása a szerver részére



• A PUBLISH kérés elsődleges célja a SIP jelzésrendszernek megfelelő üzenetek kezelése, illetve a SIP-alapú eseményjelzések továbbítása a rendszeren belül.
• A PUBLISH metódus nem csupán a presence üzenetek közzétételére alkalmazható, bármilyen állapotjelzés továbbítása során felhasználható.

Presence szolgáltatás (példa)

• A figyelő egység a figyelő és a PA között definiált interfészen keresztül jelezheti igényét a presence információk vételére.
• A presence feliratkozási folyamatot egy SIP-alapú SUBSCRIBE metóduson keresztül realizáljuk
• A presence entitáshoz (Alice), csatlakozó figyelőkről maga Alice szeretne egy listát kérni.
• A PUA elsőként egy SUBSCRIBE kérést küld a PA felé.
• A PA ellenőrzi és hitelesíti a kérést, majd egy nyugtával válaszol.
• A PA egy NOTIFY kérést küld, amelyben jelzi feliratkozási szándékát.
• A figyelők listáját a NOTIFY üzenet tartalmazza, a PA frissíti a PUA információit.
• A figyelőkben bekövetkezett további változásokról szintén a NOTIFY üzeneteken keresztül jelzés küldhető, így Alice minden egyes új figyelő belépéséről, vagy egy figyelő leiratkozásáról azonnal értesülhet.

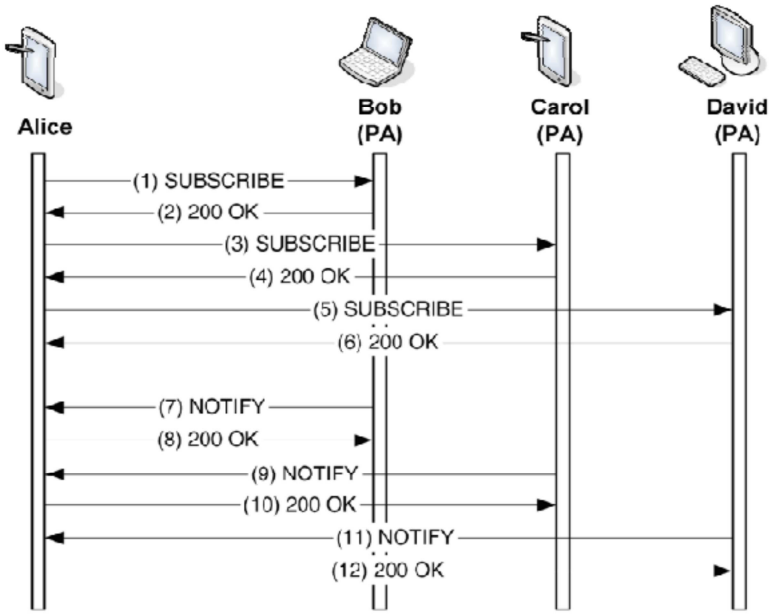


PUA meghatározza a figyelői listáját

Tegyük fel, hogy Alice, barátai – Bob, Carol és David - presence státuszát szeretné megtudni

• Alice figyelő szereplőként elküldi a SUBSCRIBE kéréseket a megfelelő presence ágensek felé. (ezen üzeneteket az 1, 3,5-ös lépés tartalmazza)

• Alice ezt követően, a 7-es, 9- es illetve 11-es üzenetben megkapja a NOTIFY jelzéseket.



Presence lista URI lista nélkül

További IMS szolgáltatások:

- **Push-to-Talk:** A Push-To-Talk egy Walkie-Talkie-szerű half-duplex szolgáltatás, ahol egyszerre több
- mint két felhasználó között is folyhat párbeszéd.
- **IM (Instant Messaging)**: Az IM nagyon elterjedt napjainkban, ezért az IMS is támogatja.
- **Real-time video Sharing**
- **Content Sharing**
- **Interactive Games**

Előnyök szolgáltatásfejlesztési platform esetén:

- Rövidebb fejrövidebb fejlesztési idő
- Biztonsági hibák valószínűsége kisebb
- Kevesebb idő szükséges a tesztelésre, hamarabb bevezethető a szolgáltatás a piacra
- Az egyes szolgáltatások közös részei újra felhasználhatóak: a felhasználó hasonló, már
- megszokott környezettel találkozik, könnyebben megszokja az új szolgáltatásokat
- Szolgáltatói szintű megbízhatóság, rendelkezésre állás, teljesítmény
- Széleskörűen tesztelt
- Komponensenként licenszelhető
- Nagy szolgáltatók által használt (pl. Vodafone, Orange, O2, BTC, stb...)

10. Transzport protokollok. A szállítási réteg feladatai, alkalmazások típusai, vezeték nélküli és mobil hálózatok jellemzői. Hasonlítsa össze a TCP, DCCP és SCTP protokollok tulajdonságait.

Szállítási réteg (transport layer)

A szállítási réteg különböző típusú szolgáltatásokat nyújthat a felsőbb rétegek felé

- hogy milyen típusú szolgáltatásra van szükség, az alkalmazás típusától függ

A szállítási réteg jellemzői:

- A transzport réteg takarja el az alatta levő hálózati architektúrától függő részleteket az alkalmazások elől
- A hálózati topológiát nem ismeri, csak a két végpontban van rá szükség.

Szolgáltatások:

- A szállítási szolgáltatás átlátszó, megbízható és költséghatékony adatátvitelt végez a viszonyentitások között.
- Megbízható kommunikációs csatornát biztosíthat a felette levő protokollrétegeknek
- Feladata a végpontok közötti hibamentes adatátvitel biztosítása, amennyiben szükség van rá

A viszonyrétegnek nyújtott szolgáltatások:

- a viszonyentitások egyértelmű azonosítása szállítási címükkel (port cím)
- szállítási összeköttetések létesítése, fenntartása és bontása
- átlátszó adatátvitel (normál és gyorsított)
- a megválasztott szolgáltatásminőség fenntartása
- összeköttetések nyalábolása és hasítása

A hálózati réteg csak 1db címezhető kommunikációs végpontot biztosít hálózati csatlakozónként, addig a transzport réteg feladata az ennél több címezhető egység biztosítása is.
Erre azért van szükség, mert egy számítógépen több program is futhat - egyidejűleg több is akarhat a hálózaton keresztül más alkalmazásokkal kommunikálni (ekkor fontos, hogy a kommunikáló partnerek csomagjai ne keveredjenek egymással)

Az Internet hálózatban használt transzport protokollok:

- TCP
- UDP/UDP-Lite
- DCCP/DCCP-Lite
- SCTP
- (RTP, RTCP, RTSP)

Alkalmazások típusai

Késleltetésre nem érzékeny, bithibára igen

- Interaktív (Telnet)
- Adat letöltés (HTTP, FTP)
- Ajánlott transzport protokoll: TCP, SCTP

Késleltetésre érzékeny, bithibára kevésbé

- Streaming (video, audio)
- Hangátvitel
- Ajánlott transzport protokoll: UDP, DCCP

Vezeték nélküli és mobil hálózatok jellemzői

A vezeték nélküli közeg használta esetén számos olyan problémával kell megbirkózni, amelyek vezetékes hálózatoknál nem jelentkeznek:

- korlátozott sávszélesség
- sokkal megbízhatatlanabb átvitel, csatornahiba
- nagy zavarérzékenység
- lehallgathatóság
- dinamikus topológia
- jelentős késleltetés és késleltetés-ingadozás (jitter)
- handover – adminisztratív üzenetek - késleltetés

Mobilitástámogatás

Sok probléma merült fel annak köszönhetően, hogy az egyes rétegek elég lazán vannak definiálva
Egyes szolgáltatások több rétegben is megvalósításra kerültek, mások pedig egyikben sem
A mobilitás egyik réteghez sem tartozik egyértelműen
A mobilitást megvalósító rendszerek követelményei:

- Átlátszó átvitel
- Lokáció menedzsment
- Infrastruktúra mentesség

TCP Transmission Control Protocol [RFC-793] - 1981

Az egyik leggyakrabban használt transzport protokoll
A szabványt vezetékes hálózatra dolgozták ki, azonban a ma egyre szélesebb körben használt vezeték nélküli hálózatok karakterisztikái jelentősen különböznek vezetékes hálózatok adatátviteli tulajdonságaitól.
olyan vezetékes összeköttetésekre dolgozták melyeknek a jellemzőik a következők:

- nagy sávszélesség
- kis késleltetés
- kis hibavalószínőség

TCP jellemzői:

Újraküldés

- a TCP feladata, hogy adott esetben (pl. egy bizonyos idő lejártával) az egyes csomagokat újra elküldje, mivel lehet, hogy az előző példány elveszett valahol

Sorrendhelyes átvitel

- A célállomáson a megérkezett csomagok sorrendje nem biztos, hogy az elküldés sorrendjével megegyezik, ezért a TCP feladata ennek a rendezése is (ha szükséges)

Csomagduplázódás

- A TCP a csomagduplázás ellen is védelmet nyújt

Megbízhatóság

- az ún. PAR (Positive Acknowledgement with Retransmission) technikával biztosítja. Ez azt jelenti, hogy a célállomás TCP-t megvalósító szoftvere nyugtázza a csomag kézbesítését, miután a hálózati szinttől (az IP-től) megkapta.

Megbízhatóság és késleltetés

- A TCP esetében a megbízhatóság azt jelenti, hogy az elküldött csomagok biztosan megérkeznek, de az esetleges újraküldések miatti késleltetésre nincs garancia
- Valós idejű szolgáltatások esetén ezért nem javasolt a TCP használata

Kapcsolatorientált

- Kapcsolatkiépítés három-utas kézfogással (sorszám meghatározása)

Több kapcsolat

• Egy hoston egyszerre több TCP kapcsolat is élhet, és itt is, mint az UDP-nél, az egyes kapcsolatok külön-külön TCP-porton (TSAP-on) vannak

Forgalomszabályozás (flow control)

• A küldő nem terheli túl a fogadót

Torlódáskezelés (congestion control)

Full-duplex adatfolyam

• A TCP-kapcsolatok full-duplexek, vagyis kétirányúak, és az elküldött adatokat a TCP strukturálatlan byte- folyamnak tekinti.

• MSS: maximálisszegmens méret (maximum segment size)

DCCP (Datagram Congestion Control Protocol)

Első draft 2001-ben, RFC-4340, 2006 március

Linux kernelben már implementálva

• 2.6.14 – DCCPv4

• 2.6.16 – DCCPv6

Megbízhatatlan transzport protokoll

• Nincs újraküldés

• Van nyugtázás

Kapcsolatorientált

• Kapcsolatkiépítés

Három-utas kézfogással

Torlódásszabályozási algoritmust használ

Sorrendhelyes csomagtovábbítás

Cél: TCP és az UDP előnyeit egy protokollként valósítsák meg

SCTP (Stream Control Transmission Protocol)

A Linux kernel része a 2.6.x verziókban

Megbízható

• Hibamentes

• Duplikáció-mentes

• Nem sorrendhelyes/vagy sorrendhelyes (beállítható)

Több folyam kezelése egy kapcsolaton belül

Multihoming

• Több IP-cím

Torlódásszabályozás

Slow start

MTU (Maximum Transfer Unit) felderítés

SCTP motivációk

A TCP, UDP nem elégíti ki az összes alkalmazás igényeit

Fejlődését leginkább az IP telefónia és az ott alkalmazott

jelzésrendszer indította

A TCP-hez hasonlóan megbízható és full-duplex kapcsolatot alkalmaz

A TCP-vel és UDP-vel ellentétben olyan opciókat is nyújt, amelyek a multimédiás alkalmazások esetén jelent előnyt

TCP-hez hasonló torlódáskezelő algoritmust használ

Azonos hosztok közötti folyamok összefogása

Kapcsolatfelépítés: 4-utas kézfogás

Kapcsolatbontás: 3-utas kézfogás

11. Transzport protokollok. Mi a multihoming, illetve a multistreaming? Mi a torlódásszabályozás? Mi a forgalomszabályozás? Különböző alkalmazástípusokhoz, milyen transzport protokollt javasolt választani? Ismertesse az UDP, RTP/RTCP protokollokat.

Multistreaming

Rendkívül fontos tulajdonsága az SCTP-nek, hogy egy kapcsolaton belül képes több adatfolyamot továbbítani
Míg a TCP-ben ehhez külön kapcsolatokra van szükség
A független adatfolyamok külön chunk-okban kerülnek továbbításra, de egy csomagon belül
Jó felhasználási lehetıség pl. a vezérlő és felhasználói adatok szétválasztása
• TCP esetében meg kell várni, hogy a felhasználói adat továbbítódjon és csak utána
érkezik a nagyobb prioritású vezérlő adat
Az SCTP párhuzamossá teszi a folyamok továbbítását, így csökkentve a késleltetést is
A független folyamokra, különböző tulajdonságokat állíthatunk be, mint pl. a sorrendhelyesség

Multihoming

Egy multihome hoszt azzal a tulajdonsággal rendelkezik, hogy több interfészen érhető el, azaz több IP címe is van
Az SCTP képest tehát egy összeköttetés adatait több interfészen küldeni és fogadni
Jelenleg ez az egyetlen transzport protokoll, amely erre képes
• Ha az elsődleges címen nem lehet elérni, akkor átvált a másik címre

Alkalmazás	Alkalm. réteg protokollja	Szállítási réteg
e-mail	SMTP	TCP
távoli hozzáférés	Telnet	TCP
Web	HTTP	TCP
file átvitel	FTP	TCP
távoli file server	NFS	UDP
Multimédia streaming	egyedi	UDP, DCCP, SCTP
IP telefónia	egyedi	UDP, DCCP
hálózat menedzsment	SNMP	UDP
útvonalválasztás - routing	RIP	UDP

Torlódásszabályozás (TCP)

• Ha egyes hálózatrészek túltelítődnek akkor a csomagok mozgatása lehetetlenné válhat.
• A várakozási sorok, amelyeknek ezeket a csomagokat be kellene fogadniuk, állandóan tele vannak.
• A torlódás a csomaghálózatokban olyan állapot, amelyben a hálózat teljesítménye valamilyen módon lecsökken, mert a hálózatban az áthaladó csomagok száma túlságosan nagy.
• A teljesítménycsökkenés jelentkezhet oly módon hogy
• a hálózat átbocsátóképessége (throughput) lecsökkent, anélkül, hogy a hálózat terhelését csökkentenénk
• a hálózaton áthaladó csomagok késleltetése megnőtt.

Forgalomszaabályozás (TCP)

Cél, hogy a küldő ne terhelje túl a fogadót
• A küldő nem akarja túltölteni a vevő-puffert azzal, hogy túl sokat, túl gyorsan küld

Átviteli sebesség korlátjai
• A vevő kapacitása
• A hálózat kapacitása
Adó oldali csomagok típusai
• Elküldött – nyugtázott
• Elküldött – még nem nyugtázott
• Még nem elküldött – elküldhető
• Még nem elküldött – még nem küldhető el
Vevő oldali csomagok típusai
• Megérkezett (nyugtázott)
• Nem érkezett meg, de megérkezhet (képes fogadni)
• Nem érkezhet meg (nem képes fogadni)
A küldő ne árassza el a vevőt

UDP (User Datagram Protocol)

Az UDP sokkal gyorsabb protokoll, mint a TCP protokoll
Nem megbízható adatátvitel
Multimédiás alkalmazások esetén jól alkalmazható, ahol a késleltetés a kritikus
A TCP-vel ellentétben nem ellenőrzi az adatok sértetlen átvitelét
• ezért nem képes az elveszett vagy sérült csomagok pótlására
Ezen kívül a fogadás sorrendjét sem garantálja a vételi oldalon.

RTP (Real-Time Transport Protocol)

Az RTP protokoll nem egy valódi szállítási rétegbeli szállítási protokoll
Általában alkalmazásokba integrálva jelenik (nem önálló hálózati rétegként)
• audio alkalmazások
• video alkalmazások
• audio és video információk
egyidejű továbbítása
Multicastra készült, de unicast felett is működik

RTCP (Realtime Transport Control Protocol)

Szabályozza az RTP kapcsolatot
• statisztikákat küld
• szinkronizálja az RTP kapcsolatokat (pl. videókonferenciánál a hangot és a képet)
A szolgáltatás minőségével kapcsolatos visszajelzéshez használják.
Periodikus kontroll információkat juttat el a résztvevőkhöz
Feladatai:
• visszajelzési lehetőség az adattovábbítás minőségéről (torlódáskezelés)
minden RTP forrásnak azonosítót továbbít (CNAME)
a résztvevők kontroll üzeneteit elküldi a többi résztvevőnek, szükség esetén saját kontroll csomagokat is küld

12. Web Privacy. Hogyan fejlődtek a nyomkövetéses támadások legalapvetőbb technikái? Sorolja fel ezeket a technológiákat, és röviden írja le, hogyan működnek! Mi az alapelve a History Stealing támadásnak? Mutassa meg, hogy ha a cél a felhasználó profiljának beazonosítása, akkor hogyan hajtaná végre! Milyen anonimizáló szolgáltatás típusokat ismer? Mutasson meg ezek között kapcsolatot, és mindegyiket írja le a jellemzőivel!

Nyomkövetéses technikák

IP alapú nyomkövetés

- kezdeti technikák, egyedi IP címek esetén működik
- A NAT miatt nem hatékony

Böngésző sütik

- sütik ellopássa lehallgatással és munkamenetek eltérítése
- XSS – Cross Site Scripting – sütik ellopása és átküldése a támadó oldalára
- sütimérgezés
- soha le nem járó sütik

Flash

- felhasználás nyomkövetésre, böngésző sütik visszaállítására
- flash egyéb veszélyei
- AJAX
- Felhasználói tevékenység mérése

Egyéb módszerek

- hirdetések, külső szolgálatatók képe (URL-ben azonosító is lehet)
- web poloska (web bug) – 1x1 pixeles átlátszó gifek, sütivel vagy IP és egyéb információk alapján
- meta információk automatikus felderítés
- e-mail mellékletek
- URL referer, előző oldal, de környezet azonosítására is.

History Stealing

- alapkoncepció: a böngészési előzmények nem explicit lekérdezhetőek, csak igen/nem jellegű
- pl. nem látható linkek állapotának lekérdezése
- URL lista látogatottságának ellenőrzése
- mire használható? -> célzott hirdetések, dinamikus árazás, profilírozás
- védelem: előzmények automatikus törlése, private böngészés.
- azonosítási módok: pszeudonim (egyedi URL minta szerint), személyes (közösségi hálózatban is)
- azonosítás közösségi oldalakon (profilinfó gyűjtése, adatbázis építés) csaport tagságok tárolása, amelyeknek egyedi URL-e van, ellenőrzés: milyen csoportokat látogatott meg.
- valódi személy is azonosítható!!!

Felhasználó azonosítása

Kliens oldal:

- spywarek ideális célpontjai – offline hozzáférés, korlátlanul rendelkezésre álló erőforrások
- előzmények adatbázisa (teljes böngészési profil)
- sütik teljes adatbázisa (böngésző és flash sütik, adat és szövegbányászat)
- gyorsítótár

Server oldal

- web logok összemosása (felhasználói tevékenység rekonstrukciója több kiszolgáló logjai szerint
- regisztrációhoz köthető támadások
- publikált adatok elemzése, összekapcsolása

Anonimizáló szolgáltatások

Részleges megoldások:

- böngésző megfelelő beállítása
- weboldalak tartalmának szűrése
- spyware-ek elleni védekezés
- anonim proxyk, anonimizáló hálózatok

komplex megoldások:

- anonim böngészők, teljes anonimitás, identitásmenedzsment.

Böngészőbeállítás: személyes adatok törlése kilépéskor, előzmények, sütik törlése, képek temporary files

Tartalmai elemek szűrése: Flash (adblock, adblock plus), noscript

Anonim proxyk, csak IP címet rejtenek, hagyományos proxyként működik, titkosított kliens-proxy kapcsolat

Anonim böngészők

- Speciális webes proxy-k: beavatkoznak a belső protokollba
- Webes felület, vagy lokális proxy alkalmazás
- Funkciók lehetnek:
  - MIX használata
  - Alternatív csatlakozási pontok, dedikált proxy szervek
  - Titkosított kliens-proxy kapcsolat
  - Sütik tiltása, szűrése
  - Java, Flash, ActiveX objektumok szűrése
  - HTTPS átjászása
  - JavaScript szűrése, tiltása
  - Hibás JavaScript kódok szűrése
  - Reklámok szűrése
  - Pop-up tiltása
  - URL-referrer szűrés
  - Böngésző, rendszerinformációk szűrése
  - Előzmények, gyorsítótár mellőzése

13. Közösségi hálók. Sorolja fel, milyen főbb szereplők érintettek a közösségi hálók privátszférát érintő kérdéseiben, és hogy ezek a szereplők milyen motivációval és lehetőségekkel bírnak! Milyen támadás típusokat ismer, amit harmadik felek hajthatnak végre? Hasonlítsa is össze a leírt típusokat! Írja le egy ismert félig-aktív támadás típus működési elvét! Mi a hátránya ennek a módszernek, és a gyakorlatban miért nehezen alkalmazható?

Szereplők

	Lehetőségek	Célok
Felhasználó	(Szolgáltatásfüggő, de általában nem sok)	▪ Adatok feletti rendelkezés ▪ Hozzáférés szabályozás
Szolgáltató	▪ Mindent lát, bármire képes ▪ Teljes adatbázis, hálózatstruktúra	▪Érdekeik az adatok exportálásához, eladásához vezethetnek: ○ Anyagi haszon előteremtése ○ Együttműködés harmadik féllel ○ Szolgáltatás üzleti értékének növelése, márkanév építése
Többi felhasználó	▪ Nyilvános kapcsolatok listázása ▪ Publikus események megfigyelése ▪ Új regisztrációk készítése ▪ Új kapcsolatok létesítése	▪ Állapot, tevékenység kompromittálása ▪ Profilok közötti kapcsolat megmutatása ▪ Egyéni adatgyűjtő akciók
Harmadik fél	▪ Publikus adatok, mint kiegészítő források ▪ Anonimizált adatbázis exportok ▪ Kis mértékű beavatkozások (ld. többi felhasználó)	▪ Profilozás ▪ Megfigyelés ▪ Személyre szabott szolgáltatások: ○ Hirdetések ○ Dinamikus árak

Támadástípusok:

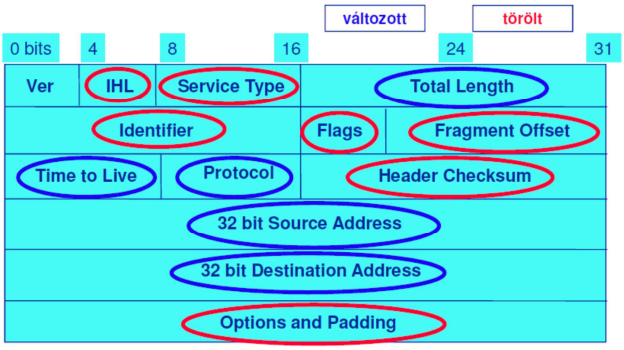
- aktív
- félig aktív
- passzív: egy másik hálózat publikus adatainak, mint kiegészítő információforrásnak alkalmazása

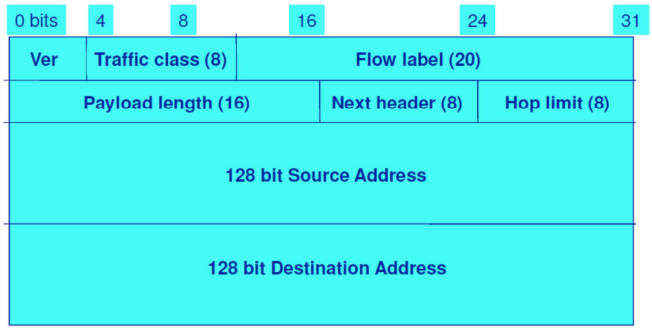
félig aktív támadás hibája:

- működik, de sokszor nem lehet új értéket, regisztrációkat létrehozni
- drága lehet az új él, csomópont
- néha a hálózat sem elérhető csak anonimizálás után
- kétirányú megerősítés kellhet
- csak a szomszédokat azonosítja

14. Ismertesse az IPv4 és az IPv6 fejléc-struktúráinak különbségeit! Mutassa be az IPv4 legfontosabb hátrányait, hiányosságait! Hogyan kezeli az IPv6 az Internet felhasználóinak egyre növekvő számát? Mire szolgál az IPv6-ban a Destination Option kiegészítő fejléc?

IPv4 vs IPv6 (jobb oldal lett)





Ami eltűnt:

- Fejléc hossz (fix 40 byte)
- Azonosító
- Flags
- Fragment offset
- Fejléc ellenőrzőösszeg

Ami átalakult:

Type-of-Service => forgalmi osztály (traffic class)
- prioritások kezelése

Protocol Type => Next header
- TCP, UDP, de kiegészítı fejlécek is, lásd késıbb

Time To Live (TTL) => Hop Limit

Címzett és feladó címe (hosszabb)

Új mező: Folyam azonosító (flow label)
- hatékonyabb csomagtovábbítás

IPv4 hibái

Az IPv4 korlátozott
- 4,3 milliárd cím, 60% az USA-ban
- egyre növekvő felhasználói populáció

(pl. ADSL, mobil készülékek, játék konzolok)
- KEVÉS CÍM (a NAT nem megoldás)

IPv4 – 32 bit
- 2^{32} = 4,29 10^9 darab cím (elvileg)
  - már több, mint 6,5 milliárd ember a Földön
- összesen 2 113 389 darab hálózat

IPv6 – 128 bit
- 2^{128} = 3,4 10^{38} darab cím (elvileg)
  - 6,65 10^{23} darab cím/m^2
- 2^{45} darab /48-as hálózat (global unicast 001)
  - 3,5 10^{15} darab hálózat
  - mindegyikből további 65 535 /64-es alhálózat

Destination options fejléc

Ez is egy opciós kiegészítő fejléc
- Formátuma az opciós fejlécé

A végállomásnak kell feldolgoznia

Kétszer is előfordulhat
- Ha a routing fejlécet is használjuk
- Elsı (routing header előtti)
- A routing headerben előírt állomások dolgozzák fel
- Az utolsó (routing header utáni)
- A célállomás dolgozza fel

15. Milyen IPv6-os címtípusokat ismer? Mi váltja az IPv6-ban az IPv4-es ARP és RARP funkciókat? Hogyan működik az IPv6-os állapotmentes (stateless) autokonfiguráció? Mi az a Path MTU discovery és hogyan működik az IPv6-ban?

Címtípusok IPv6

Címzett alapján

- Unicast (egyes küldéses)
- Multicast (többes küldéses)
- Anycast

Route-olhatóság alapján

- globális (global)
- nem globális (non-global)
- link-local
- egyedi lokális IPv6 cím (régen site-local)

ARP, RARP helyett - Internet Control Message Protocol 6-os verzió (ICMPv6)

Sokkal fejlettebb, mint az ICMPv4

- Multicast management (IGMP helyett)
- ***Neighbor Discovery (ARP, RARP helyett)***
    - a szomszéd állomások, routerek, elérhető szomszédok és változó adatkapcsolati címek feltérképezésére
- Echo request/echo reply (ping)
- Packet too big (fragment fejlécek helyett)

ICMPv6 autoconfiguration

Két típus: stateless és stateful

- Stateful = DHCP az IPv4-ben hívják: ~ autoconfiguration, ~ DHCP
- Stateless: hálózati prefix alapján
    - vagy MAC cím, vagy random ID
    - duplikált címek szűrése DAD-del

A kettő kombinálható

- pl. stateless a címhez
- stateful a DNS-ek címéért

Path MTU discovery

Az IPv6-nál nincs fragmentálás

Ha a csomag nagy (> MTU):

- eldobja a router
- küld egy ICMPv6 üzenetet a forrásnak (PTB)
- A PTB tartalmazza a következő link MTU-ját

Módszer:

- küldjünk echo requestet a címre
- kezdjünk nagy MTU-val, majd lépdeljünk lefelé
- az új MTU-val próbálkozik
- soha nem megy 1280 byte alá
- GOTO eleje

16. Hogyan csoportosíthatók az IPv4-IPv6 együttélést megvalósító módszerek? Mit nevezünk anycast kommunikációnak, és hogyan támogatja az IPv6 ezt a kommunikáció típust? Hogyan működik a broadcast átvitel IPv6-ban? Milyen ICMPv6 üzeneteket ismer?

Együttműködés

Az IPv4 és az IPv6 sokáig együtt fog élni egymás mellett
• IPv4 világ kész, az IPv6 világ most épül
Három módszer
• kettős protokoll stack (dual stack)
• alagút (tunneling, vagy encapsulation)
• IPv6 szigetek összekötése IPv4 felett
• fordítás (translation)
• IPv6 hosztok kommunikációja IPv4 hosztokkal
A fentiek kombinálhatóak is

Anycast címek

A nagy terhelésű eszközökhöz találták ki
• számítógépek egy csoportjából egyetlen (tipikusan a legközelebbi) állomást címzi
Az unicast tartományból szabadon
Subnet-router anycast
• [n_bitnyi_subnet_prefix]:[128-n_bitnyi_0]
• az első router fogja feldolgozni a linken

Broadcast

Broadcast nincs IPv6-ban csak helyette multicast

FF[0RPT][4_bitnyi_scope][Csoport_ID]
- 0RPT flagek (bitek)
  - R=0 Randevú pont nincs beágyazva
  - P=0 Multicast cím prefix infó nélkül
  - T=0 Jól ismert multicast cím (1: ideiglenes)
- Scope példák
  - 1: Interface-local scope
  - 2: Link-local scope
  - 5: Site-local scope
  - E: Global scope

Minden node
- a küldővel azonos linken FF02::1
- a küldővel azonos site-on FF05::1

Minden router
- a küldővel azonos linken FF02::2
- a küldővel azonos site-on FF05::2

Minden DHCP ügyfél FF02::1:2
Minden DHCP szerver FF05::1:3
Minden NTP szerver
- a küldővel azonos site-on FF05::101
- az Interneten FF0E::101

ICMPv6 üzenetek (hiba vagy információs)

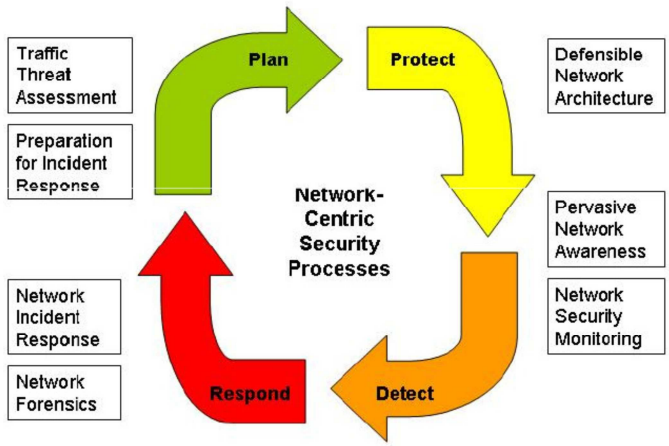
hiba:
Címzett elérhetetlen (destination unreachable)
• ha az IP datagram nem továbbítható
• Nincs route a célhoz, cím/port elérhetetlen, adminisztratíve tiltott
Túl nagy csomag (Packet Too Big)
• az MTU a köv. linken kisebb a csomagméretnél
Lejárt az idő (Time Exceeded)
• ha a hop számláló nullára csökkent
Paraméter probléma (Parameter problem)

információs:
Echo request / echo reply
multicast felderíti üzenetek
• router
• listener
router felderítő (router discovery)
szomszéd felderítő (neighbor discovery)
hálózat újraszámozás (router renumbering)
mobilitás támogatáshoz kapcsolódó üzenetek

17. Mit mondott Bruce Schneier a biztonságról? Milyen lépésekre lehet bontani a körforgást? Miért támadnak a támadók? Definiálja a következőket: Sértetlenség, Hitelesség, Letagadhatatlanság. Definiálja a következőket: Bizalmasság, Távoli azonosítás.

Bruce Schneier : „A biztonság nem egy termék, hanem egy folyamat.”

Lépések:



Miért támadnak?

• A támadó haszonszerzésre törekszik
• A támadó a szolgáltató hírnevét próbája gyengíteni
• Jó szándékú támadó, csak a rendszer hibáira szeretné felhívni a figyelmet
• Erőfitogtatás, szórakozás
• Ugródeszka más gépek feltöréséhez

A támadásokat két nagy csoportba osztjuk:

• Passzív támadások
• Aktív támadások

Definíciók

Sértetlenség

• Az elküldött üzenet változtatás nélkül ér célba
• Esetleges módosítás detektálható

Hitelesség

• Az üzenetet valóban az küldte, akit feltételezünk és a hálózati továbbítás során nem módosult

Letagadhatatlanság

• Nemcsak a vevő, hanem tetszőleges harmadik fél felé is igazolható, hogy egy adott üzenetet tényleg a valódi küldő küldött, letagadni azt nem tudja

Bizalmasság

• Az üzenetet egy támadó hiába hallgatja le, azt nem tudja értelmezni a titkos kulcs nélkül, mivel kriptográfiai módszerekkel titkosítva van.
• Az emberek többnyire ezt értik biztonságos kommunikáción

Távoli azonosítás

• Akkor, ha két fél még nem ismeri egymást, és közöttük nincs egy biztonságos csatorna, akkor egyéb módszerek segítségével rendszerint harmadik fél bevonásával mutatkozhatnak be egymásnak biztonságosan. Rendszerint

18. Milyen két nagy csoportra osztjuk a támadásokat? Jellemezze ezeket. Milyen passzív támadástípusokat ismer? Mi jellemzi a passzív támadásokat? Milyen aktív támadástípusokat ismer? Mi jellemzi az aktív támadásokat? Mi az a DoS támadás? Ismertessen két DoS típusú támadást! Mi az a Social Engineering?

A támadásokat két nagy csoportba osztjuk:
• Passzív támadások
• Aktív támadások

Passzív támadások

A támadó csak megfigyelést végez, vagy információt gyűjt az információ tartalmának és továbbítási módjának megváltoztatása nélkül.

Két fő típus:
Üzenet tartalmának felfedése
• Üzenetek lehallgatása, küldött adatállományok tartalmának megfigyelése
• Védekezés: titkosítással és/vagy a kommunikáló felek azonosításával
Forgalomanalízis
• A kommunikáló felek helyét, a kommunikáció gyakoriságát, idejét, időtartamát határozza meg
• Ezen támadások ellen nem segít a titkosítás, azonosítás

Általánosságban elmondható, hogy a passzív támadások ellen védekezni nagyon nehéz, a megelőzés a legjobb mód. A támadó személyének, helyének felderítése nagyon nehéz, mivel a támadás nem hagy nyomot az üzenetekben.

Aktív támadások

Aktív támadás esetén, a támadó valamilyen módon megváltoztatja az üzeneteket, vagy hamis üzeneteket generál. Az aktív támadásoknak négy fő típusa létezik:
Álcázás (masquerade), megszemélyesítés (impersonation), hamisítás (spoofing)
• A támadó egy legális partnernek adja ki magát
• Példa 1: FTP felhasználónév és jelszó lehallgatása, majd később ezen adatok felhasználása kapcsolat kiépítésére
• Példa 2: Csomagban forrás IP cím cseréje
Visszajátszás (replay)
• Korában megszerzett üzenet / üzenetváltás későbbi időpontban történő újraküldése
Módosítás (modification)
• Egy szabályos üzenet bizonyos részeit a támadó módosítja, kitörli, vagy új részeket illeszt bele
• Nem szükséges hozzá a teljes üzenet ismerete
• Real time alkalmazása Man-In-The-Middle támadással lehetséges

Szolgáltatásmegtagadás (Denial of Service – DoS)

• A kommunikációs infrastruktúra normális működését zavarják meg, rontják el
• Célja lehet egy adott számítógép, vagy adott program megbénítása, de adott esetben egy egész hálózat működésképtelenné tétele is
• Például egy számítógép elárasztása hamis kérésekkel, így a valós kérdésekre nem tud válaszolni
• Amikor a támadás egyszerre több gépről érkezik DDoS –Distributed Denial of Service támadásról beszélünk

Social Engineering

A social engineering az emberek bizalomra való hajlamát használja ki, nem a hardver, szoftver, vagy a hálózat hibáit. Napjainkban nagyon népszerű.