VoIP technológiák összehasonlítása (H.323, SIP)

Ebben a fejezetben a VoIP (Voice over IP) különböző ma elterjedt lehetőségeinek összehasonlítását mutatjuk be, a hívás felépítést, a DNS segítségével való telefonszám feloldást, foglalkozunk a különböző VoIP-et érintő problémákkal: NAT, rendelkezésre állás, minőség.

VoIP

Az elmúlt években a széles sávú hálózatok terjedésével felmerült az igény, hogy a hálózatokon nem csak adatokat, hanem hangot és képet vigyünk át, ezzel lényegesen csökkentve a telefonálásra költött összeget. Ugyanakkor rájöttek arra is, hogy teljesen felesleges két külön hálózatot kiépíteni, amikor egy is ellátja az általunk igényelt feladatokat. Ezek az igények biztosítják a VoIP elterjedését, a már meglévő és kiforrott PSTN hálózat mellett. Két típus terjedt el az évek folyamán, ezek az ITU-T által ajánlott H.323 és az IETF SIP protokollja.

VoIP előnyei

- jobb kihasználtság, költséghatékonyság,
- hely és távolság független: bárhol rádugjuk a hálózatra a telefonunkat, a VoIP szolgáltatón belül beszélhetek (és ez a szolgáltatónak is jó), hiszen az előfizetőt nem az előfizetés helye alapján különböztetjük meg,
- adatátvitel beszéd közben
- Ha telephelyeinket kötjük össze már meglévő internetkapcsolaton keresztül, akkor a telephelyek közötti kommunikáció ingyenes, sőt ha különböző országokban vannak, akkor a gateway-ek segítségével helyi tarifákkal érhetjük el az adott ország PSTN előfizetőit.

A VoIP hangminőségét a következő zavaró tényezők befolyásolhatják:

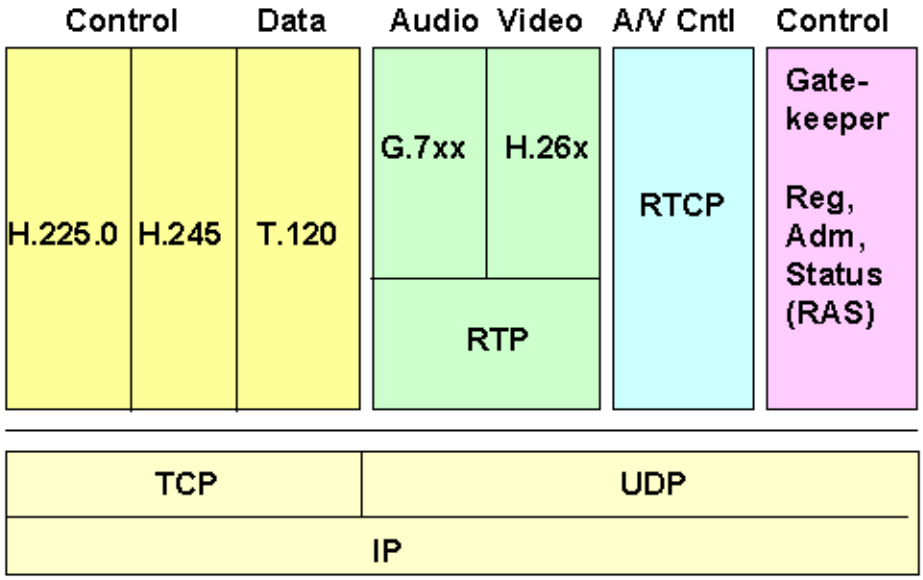
- **bithibák:** Ha a hálózatot „zavarja” valamilyen jel, előfordulhat, hogy az adatfolyamban bitek értéke megváltozik. ezért szükséges mérni a BER-t (Bit Error Rate), hogy megtudjuk az egyes codec-ekre milyen hatása van a bithibáknak (mekkora BER érték, amelyet még képesek javítani)
- **jitter:** pl.: hang csomagok időbeni eltolódása az ideálishoz képest.
- **visszhang:** visszhang akkor lép fel amikor, ha a mikrofon és a hangszóró között akusztikus kapcsolat van. Ez kis érték esetén nem annyira zavaró (200ms alatt).

H.323

A H.323 egy keretajánlás mely több ajánlást tartalmaz VoIP kapcsolatok felépítésére, és az ITU-T dolgozta ki 1996-ban. A H.323 felépítését tekintve az ISDN-re hasonlít. A H.323 csak a szabványban rögzített hangkodekeket támogatja. A következő eszközök vesznek részt a H.323 kommunikációban:

- **Terminal:** a H.323 végberendezése (IP telefon, PC softphone-nal)
- **Gateway:** H.323 és egyéb hálózatok közötti átjáró (GSM, PSTN, ISDN gatewayek)
- **Gatekeeper:** A kapcsolat felépítéséért felelős eszközök.
- **MCU (Multipoint Control Unit):** Konferencia hívásokért felelős egység. Konferencia híváskor az összes készülék ide csatlakozik be. Itt tárgyalják meg a használatos kodeket és a sávszélesség igényt.

A kapcsolatok felépítésének szempontjából fontos megjegyeznünk, hogy a Terminal és a Gatekeeper között egy állandó TCP kapcsolat van. Ez ugyan kis forgalmi igény alacsony számú eszköznél, de sok eszköz esetén problémát okozhat, ha a Gatekeepernek nincs megfelelő sávszélessége.



A H.323 protokollcsalád elemei

- **H.225:** Hívás felépítésért bontásért felelős protokollokat foglalja össze
- **H.225.0 (RAS):** A terminal és a gatekeeper közötti kommunikációt írja le.
- **H.245:** az eszközök képességeit egyeztetik ennek segítségével (kódolást)
- **RTP:** Valós idejű adatfolyamokért felelős protokoll (SIP, H.323 is használja)
- **RTCP:** RTP kapcsolatok vezérlőinformációi (SIP, H.323 is használja)

RTP

A VoIP csomagok átvitelére a TCP/IP nem használható elég hatékonyan, a kapcsolatfelépítés és bontás plusz csomagokat jelentenek, adatvesztés esetén újrakéri az adatot, ami időkiesést okoz. Ezen megfontolásokból a „streaming media" (valós idejű adatfolyam) az UDP/IP protokollt használja de ez meg nem képes megbízható adatátvitelre (csomagvesztés, más sorrend). Ezért az RTP (Real-time Transport Protocol) felel az adatok érkezési sorrendjéért. A szokásostól eltérően nem kötött port számon, hanem a 16384-32767 portok egyikén nyit kapcsolatot, az e feletti porton pedig a RTCP protokoll kap helyet.

RTCP

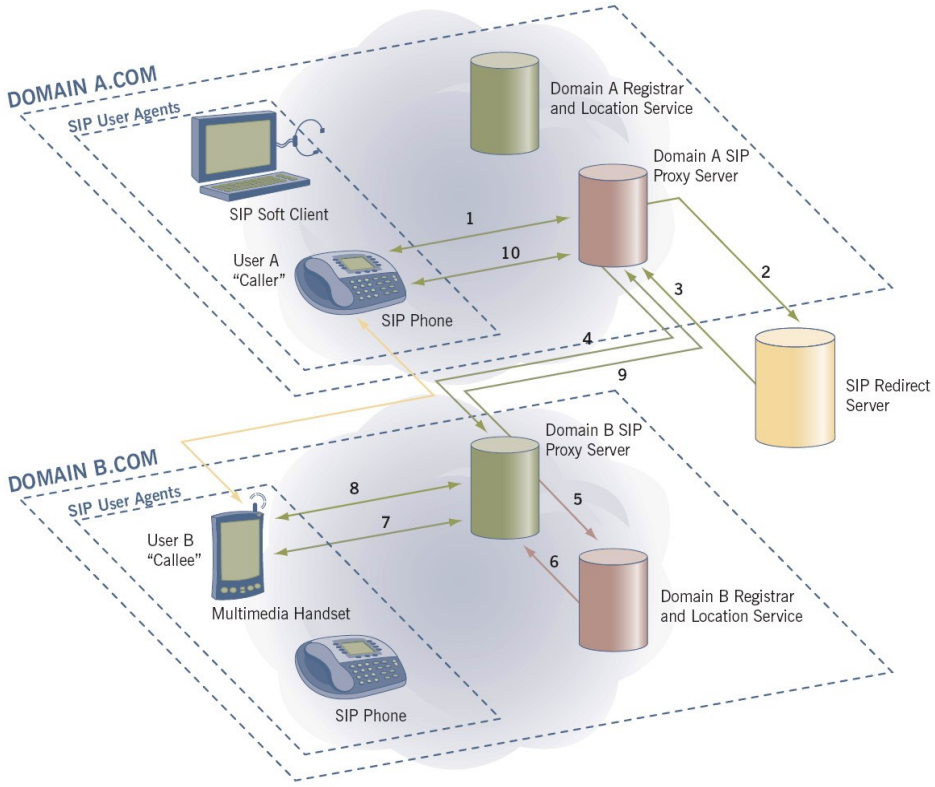
Az RTCP (Real-time Transport Control Protocol) Minden egyes RTP kapcsolathoz tartozik egy RTCP kapcsolat is, mely a kapcsolat minőségéről, vezérlésével kapcsolatban közöl információt a küldővel.

SIP

A SIP (Session Initiation Protocol) a kapcsolat felépítését és kezelését írja le. Míg a H.323 fixen dokumentálva tartalmazza a kapcsolat felépítésére vonatkozó eljárásokat, a SIP – mivel szöveg alapú protokoll – rugalmasan változtatható. Például, ha olyan hangtömörítést szeretnénk használni, mely nincs dokumentálva a H.323-ban, a SIP esetében ez nem okoz gondot, hiszen ha a kliensek ismerik az általuk használni kívánt kodeket, minden további nélkül megtehetik ezt. A formátuma leginkább a HTTP-re hasonlít, ez annak köszönhető, hogy elsősorban internetes kommunikáció felépítésére találták ki.

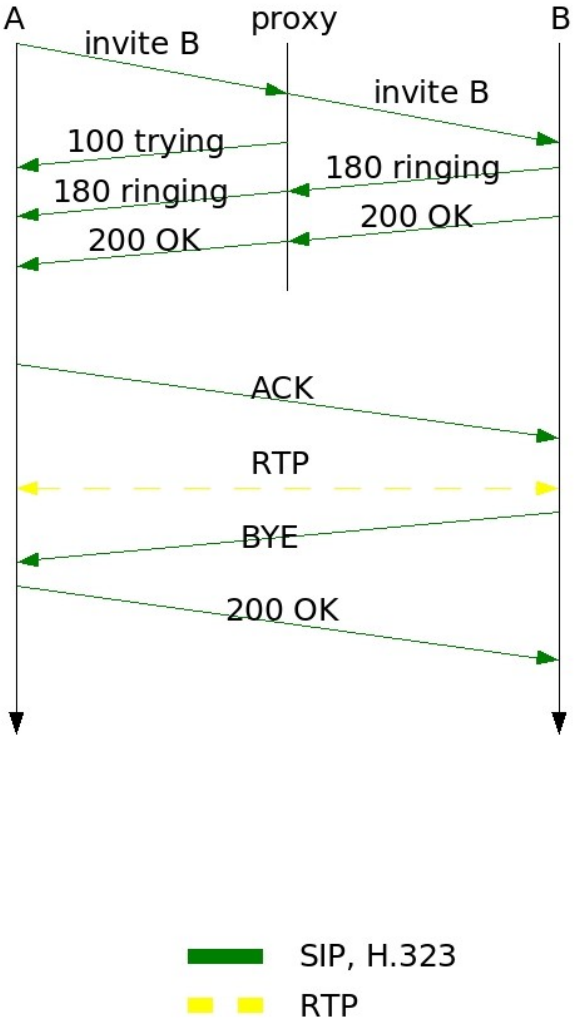
A SIP kommunikációban résztvevő eszközök:

- **SIP User Agent:** a végberendezés. Lehet hardveres IP-telefon vagy szoftver is.
- **SIP Registrar szerver:** DNS szerver megfelelő NAPTR rekordokkal
- **SIP proxy szerver:** ezekkel kommunikálnak a kliensek, és ezek kérdezik le a Registrar szerverektől a kliensek helyét.
- **SIP Redirect szerver:** Domainek közötti kommunikációnál van szerepe a SIP proxy szerverek fordulnak hozzá.

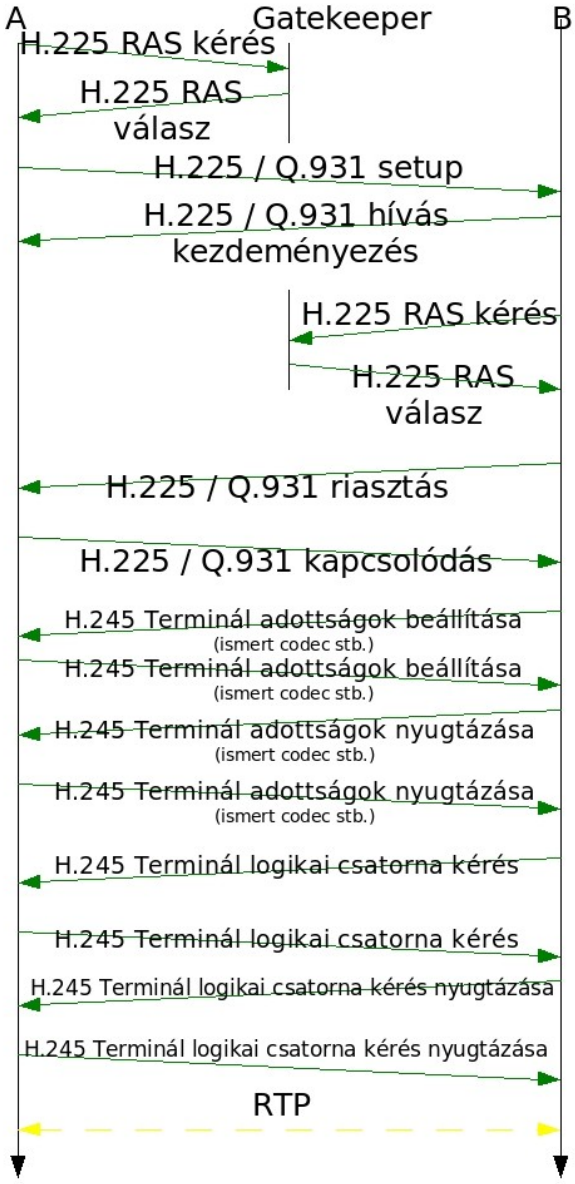


A SIP kapcsolat felépítése. Az A hívja B-t (1), a SIP proxy szerveren (H.323 gatekeeper-éhez hasonlít) keresztül. A proxy szerver a Redirect szervert megkérdezi, hogy B proxy szervere hol található (2) a Redirect a kérésre válaszol (3). Az A proxy szervere B proxy szerver felé jelzi, hogy A hívja B-t (4). A B proxy szervere B domain és helymeghatározó szerverétől megkérdezi B hol található (5 a válasz a 6). A B proxy szervere közli B-vel, hogy hívták (7). B a szervereken keresztül válaszol A-nak (8-10). Az RTP kapcsolat felépül a két VoIP eszköz között. Az ábrán a SIP kapcsolatok zöld színnel, az RTP sárga színűek.

SIP



H.323



A fenti ábra egy domainen belüli kapcsolat felépítését mutatja be. Mint az ábrákból is jól látható a SIP kapcsolat, a H.323-hoz képest lényegesen egyszerűbben épül fel, ami szintén időmegtakarítás. A kommunikációba nem rajzoltuk bele az RTCP protokollt és a H.323 esetén a kapcsolat bontását.

SIP, H.323 Gateway-ek

Mivel a SIP és a H.323 sokszor ugyan azokat a hangtömörítési eljárásokat alkalmazza, a SIP H.323 gatewaynek csak a SIP kapcsolat felépítését segítő protokollokat kell „átfordítania”.

VoIP stream átültetése PSTN hálózatba

Attól még hogy a VoIP egy jól működő viszonylag biztonságos rendszer szükségünk lehet a már meglévő PSTN hálózat elérhetőségére is. Erre külön vásárolnunk kell egy VoIP PSTN gateway-t mellyel akár SIP akár H.323 telefonunkkal képesek vagyunk analóg készüléket hívni. A VoIP PSTN gateway kicsomagolja a IP telefon által küldött adatot, majd ezt az analóg készülék számára értelmezhető formára alakítja.

DNS protokoll, és biztonsági kérdései

Ahhoz, hogy elérjük a SIP, H.323 hálózatokban lévő VoIP készülékekről a PSTN hálózatokban lévőket, szükségünk van DNS használatára. A PSTN telefonok telefonszámát az ITU-T e.164 írja le (legalábbis az ország hívókódokat, Magyarországé a +36).

Az rfc3761 leírja, hogyan lehet egy ENUM (e.164) számot DNS segítségével feloldani. Az RFC a következő példával mutatja be:

A e.164 nek megfelelő +442079460148 telefonszám elől eltávolítjuk a „+”-t, az így kapott 442079460148 szám számjegyei közé pontokat teszünk és „megfordítjuk”, 8.4.1.0.6.4.9.7.0.2.4.4 ezt kiegészítjük a .e164.arpa domainnel, ezzel a PTR rekordokat is tartalmazó arpa. TLD része lesz. Ezután DNS szerverben NAPTR (Naming Authority Pointer) rekordként bejegyezhetjük a következőképp:

```
$ORIGIN 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa.
  NAPTR 10 100 "u" "E2U+sip" "!^.*$!sip:info@example.com!" .
  NAPTR 10 101 "u" "E2U+h323" "!^.*$!h323:info@example.com!" .
  NAPTR 10 102 "u" "E2U+msg" "!^.*$!mailto:info@example.com!" .
```

A NAPTR egy újabb DNS rekord. Segítségével a névfeloldás sorrendjét határozhatjuk meg. Példánkban először SIP, majd H.323 legvégül SMTP URN-t (Uniform Resource Name) ad vissza a DNS szerver. Elvileg bármennyi NAPTR bejegyzés tartozhat egy rekordhoz.

A magyar E.164 tartomány (+36) névszerverei (és lekérdezésük módja):

```
laptop:~# host -t ns 6.3.e164.arpa
     6.3.e164.arpa          NS      ns2.sztaki.hu
     6.3.e164.arpa          NS      ns.nic.hu
```

Sajnálatos módon a DNS sohasem volt biztonságos protokoll. Ez a VoIP megjelenésével fokozottabb problémákat vet fel, hiszen egy hívás közben, ha PSTN telefont hívunk, a névfeloldás sima szöveg alapú volta miatt egyszerűen megszerezhetik a hívott számát.
A jelenlegi problémák a DNS-sel és ez nem csak az ENUM feloldásra érvényes:

- Csomag elfogás (lehallgatás)
- ID becslés, jóslás (hamisításhoz)
- Név alapú
- Védett szerver elhagyása
- Szolgáltatás megtagadás
- Erőforrás rekord hiánya

A fenti hibák majd mindegyike ellen védekezhetünk a DNSSEC-el, – ez jelenleg még nem elfogadott technológia és állandóan változik – Egyedül a DoS (szolgáltatás megtagadás) mely ellen a DNSSEC nem fog védeni.

NAT

Mivel a 32 bites IPv4 címek száma „csak” 4 milliárd, a személyenkénti publikus IP-címek száma meglehetősen kevésnek bizonyult. A megoldást a NAT (Network Address Translation) jelentette. Ez a megoldás lehetővé tette, hogy a NAT-olt tartományban lévő eszközök is használják az Internetet, de ezt a publikus tartomány felől „láthatatlanul” teszik. Sajnos ez problémát okoz a VoIP kapcsolatok között, ahol a két végberendezés közvetlenül egymással kommunikálna. Ezen probléma megoldására született a STUN és a TURN.

A NAT-nak 4 típusát különböztetjük meg:

- „FULL CONE” NAT: A belső hoszt egy portot kap az átjáró gépen, ennek a portnak az ismeretében kérés nélkül tudunk adatot küldeni a belső gépnek

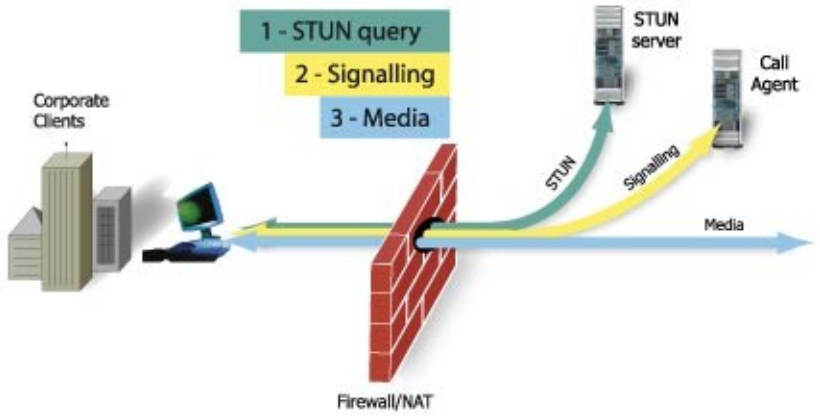
- RESTRICTED CONE NAT**:** A belső hoszt egy portot kap az átjáró gépen, külső géptől csak akkor kapja meg a csomagokat a belső gép, ha előzőleg a küldő felé volt kérés

- PORT RESTRICTED CONE NAT**:** A belső hoszt egy portot kap az átjáró gépen, külső géptől csak akkor kapja meg a csomagokat a belső gép, ha előzőleg a küldő felé volt kérés a belső gép számára fenntartott portról, a válasz csak erre a portra érkezhet

- SYMMETRIC NAT: a belső gép felől irányuló összes kérés más portszámot kap az átjáró gépen.

STUN

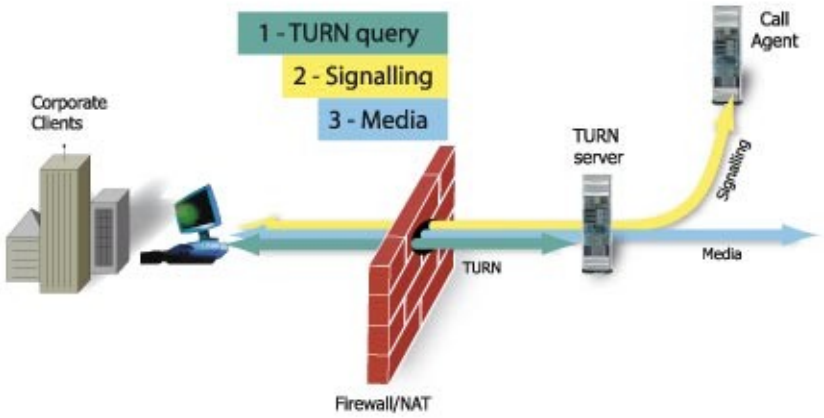
A STUN (Simple Traversal of User Datagram Protocol (UDP) Through NAT) kliens-szerver alapú protokoll. A fent említett négy NAT típus közül az utolsó kivételével mindegyikkel együttműködik.



Mint a fenti rajzon is láthatjuk, a STUN esetében a kommunikáció úgy kezdődik, hogy a kliens információkat kér hálózati környezetéről egy publikus IP-vel rendelkező STUN szervertől. A STUN megmondja, hogy milyen publikus IP-ről és portszámról jött a kliens kérése. Ezek segítségével a kliens már képes SIP vagy H.323 típusú VoIP kapcsolat kezdeményezésére.

TURN

A TURN (Traversal Using Relay NAT) egyelőre az IETF RFC tervezete. A symmetric NAT mögött lévő kliensek elérésére nyújt megoldást.



A TURN esetében a válaszok nem a klienshez, hanem egy TURN szerverhez érkeznek, amely kapcsolatban áll a NAT mögött lévő klienssel. A hívásfelépítést és a hívást is a TURN szerver kezeli, ezzel téve „publikussá” a NAT-olt klienst.

VoIP a vezeték nélküli hálózaton

A GSM rendszerek megjelenésével a helyhez kötött VoIP-nek igen kis esélye lenne elterjedni. Ezért mindenféleképpen vizsgálnunk kell a vezeték nélküli hálózatok feletti átvitel erőforrásigényeit, és biztonságát. A sajnos még mindig igen elterjedt WEP miatt a vezeték nélküli hálózatok nagy része megbízhatatlan. Legalább WPA-PSK-t (PreShared Key) kell használnunk az ilyen eszközök esetében. Egy nagy cégnél az egész céget lefedő vezeték nélküli hálózat további problémákat vet fel. A több Access Pointból (AP) álló vezeték nélküli hálózatok esetében, gondoskodnunk kell a roaming közbeni AP váltás zökkenőmentes voltáról. Mind a WEP-et mind a WPA-PSK-t úgy támadják, hogy a hálózatra csatlakozott eszközöket lelökik. Ilyenkor a készülékek újracsatlakoznak. Ezt ismételgetve jutnak a támadók az IV csomagokhoz, melyek segítségével képesek például a WEP-et percek alatt törni. Mindamellett, hogy érdemes vizsgálni, hogy a készülék tud-e erősebb hitelesítést mint a WEP, számunkra érdekes, hogy a „lelökött” készülék újracsatlakozása észlelhető-e az hangátvitelben.

Rendelkezésre állás

A PSTN hálózatok végberendezéseit a telefonközpontok táplálják, akár több kilométeren keresztül. Ezzel szemben a VoIP eszközök tápellátását lokálisan kell biztosítanunk. Ha a készülék PoE képes, akkor lehetőségünk van „távoli” tápellátásra megfelelő hálózati eszközök segítségével (PoE-s (Powe Over Ethernet) switch). Ez a távolság ugyanakkor a PSTN több kilométeréhez képest maximálisan 100m. Áramszünet esetén a PSTN központokat szünetmentes tápegységek védik, és ha az áthidalni kívánt idő hosszabb, mint amit a szünetmentes tápegység képes ellátni, akkor a szolgáltató robbanómotoros áramgenerátorral táplálja a központot, így biztosítva az előfizetői végpontok működőképességét.

Hasonló elvet alkalmazhatunk VoIP hálózatok esetén. Célszerű olyan eszközöket beszerezni, melyek képesek PoE használatra (így nem kell minden telefon mellé szünetmentes tápegységet elhelyezni), ezeket PoE injektoros switchekkel meghajtani. Mivel az esetleges segélyhívások is történhetnek a VoIP hálózatról, ezek működőképességét – és a hozzákapcsolódó infrastruktúráét – mindenképpen biztosítanunk kell. Ugyan ilyen megfontolásokból érdemes a vezeték nélküli AP-ket is szünetmentes tápellátással ellátni, ha használunk vezeték nélküli VoIP készülékeket.

Sávszélesség biztosítása

A streaming média számára valamilyen módon biztosítani kell, hogy az átvitel zökkenőmentes legyen. Erre használhatjuk a QoS-t (Quality of Service) vagy választhatjuk azt a megoldást – ha a készülék ismeri –; hogy a VoIP eszközök külön VLAN-ban helyezkedjenek el, így az esetlegesen használni kívánt eszközök számától és a hálózat kihasználtságától függően az adott VLAN-nak biztosítjuk az igényelt sávot. Ez utóbbi megoldás a biztonság szempontjából is hasznos.