

Hálózatba kapcsolt erőforrás platformok és alkalmazásaik

Simon Csaba

TMIT

2018

Anonimitás - elosztott módon

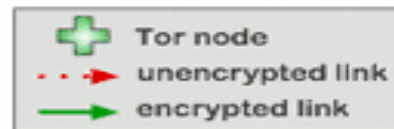
A decorative graphic consisting of several horizontal lines of varying lengths and colors (blue and white) extending from the right side of the slide.

Anonimitás

- Első lépés
 - Követők, lehallgatók összezavarása
 - Nem tudják, hogy ki is tölt le
 - P2P módon együttműködnek a felhasználók
 - „relay”

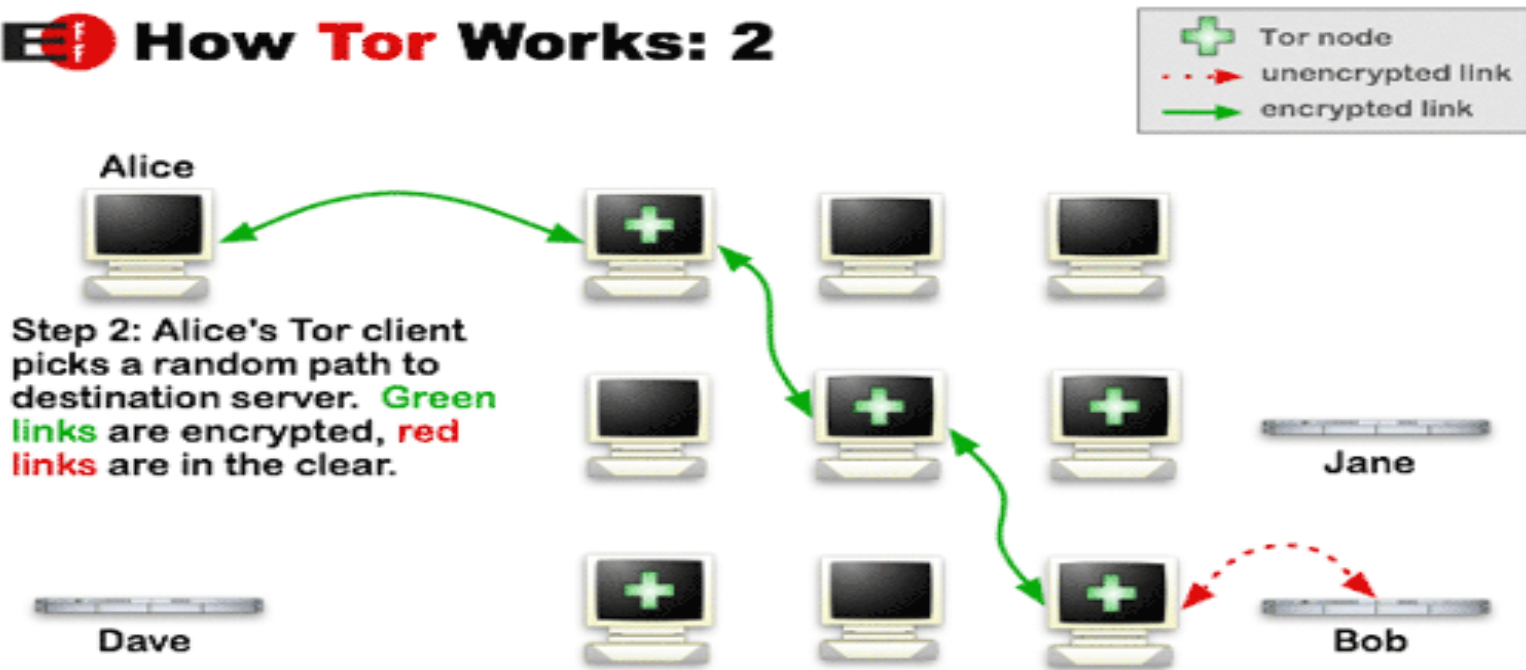
Tor

EFF How Tor Works: 1



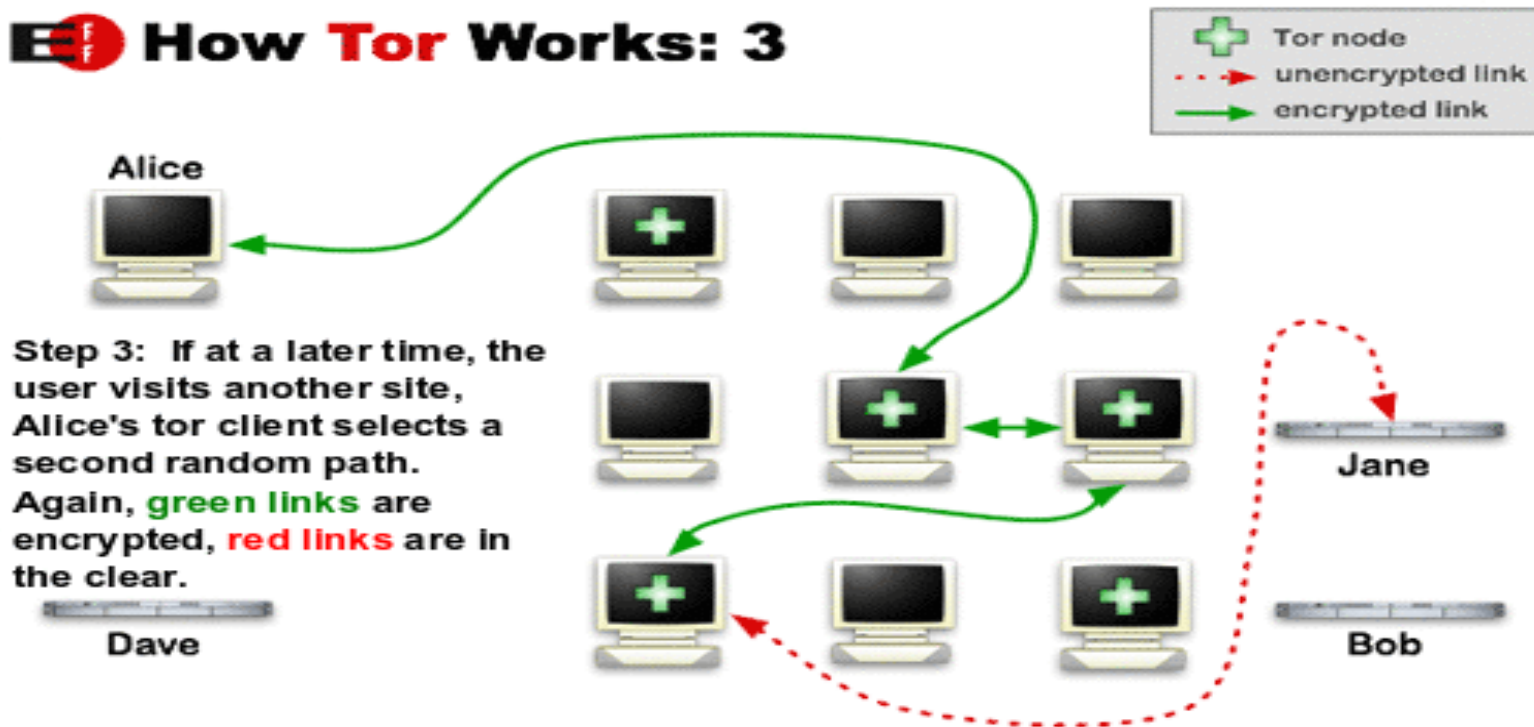
Tor

How Tor Works: 2



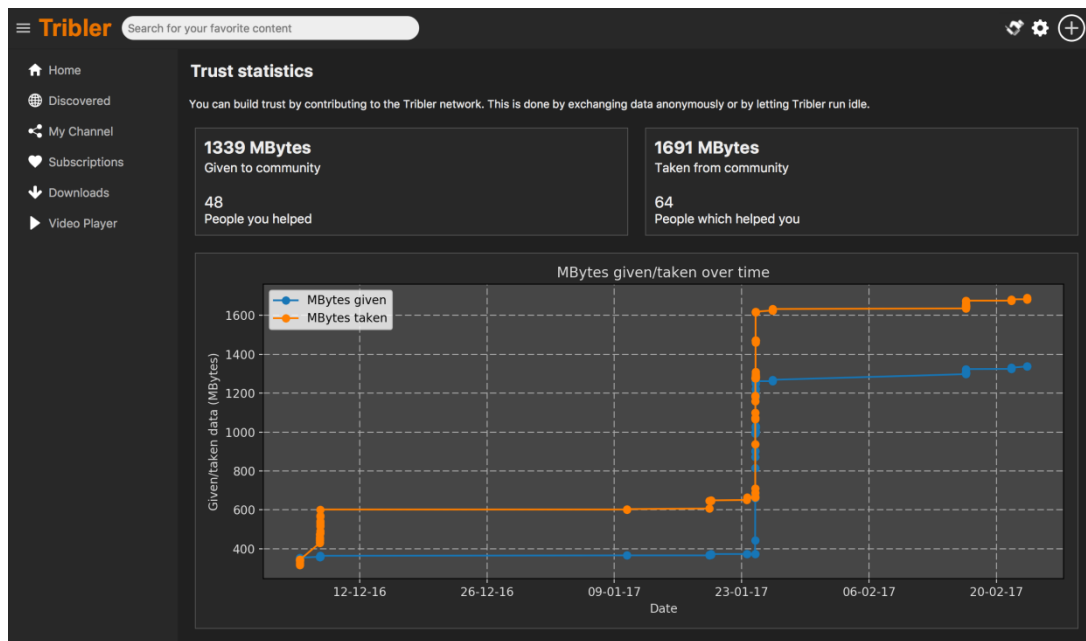
Tor

How Tor Works: 3

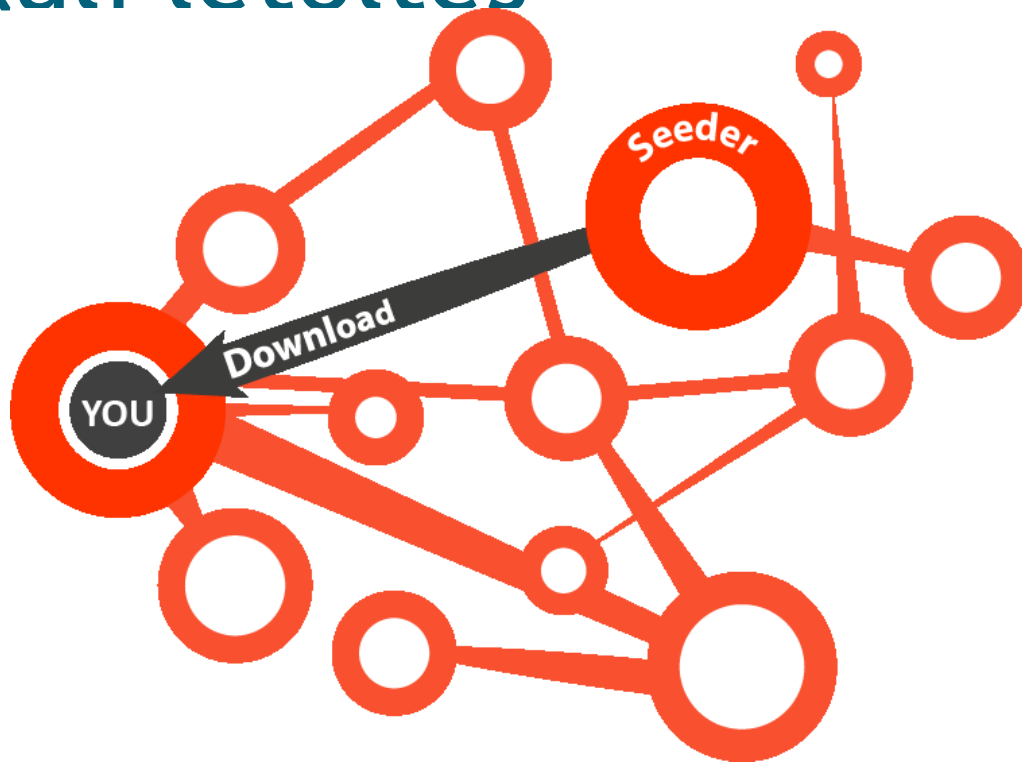


Tribler

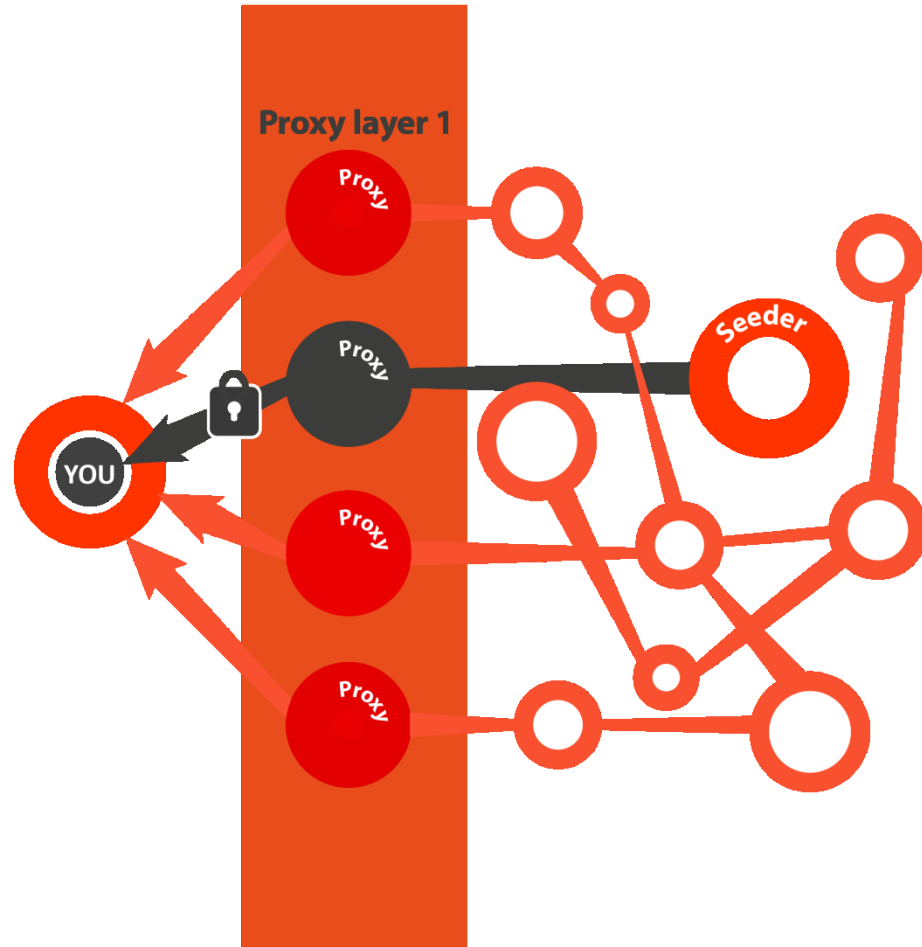
Reputation



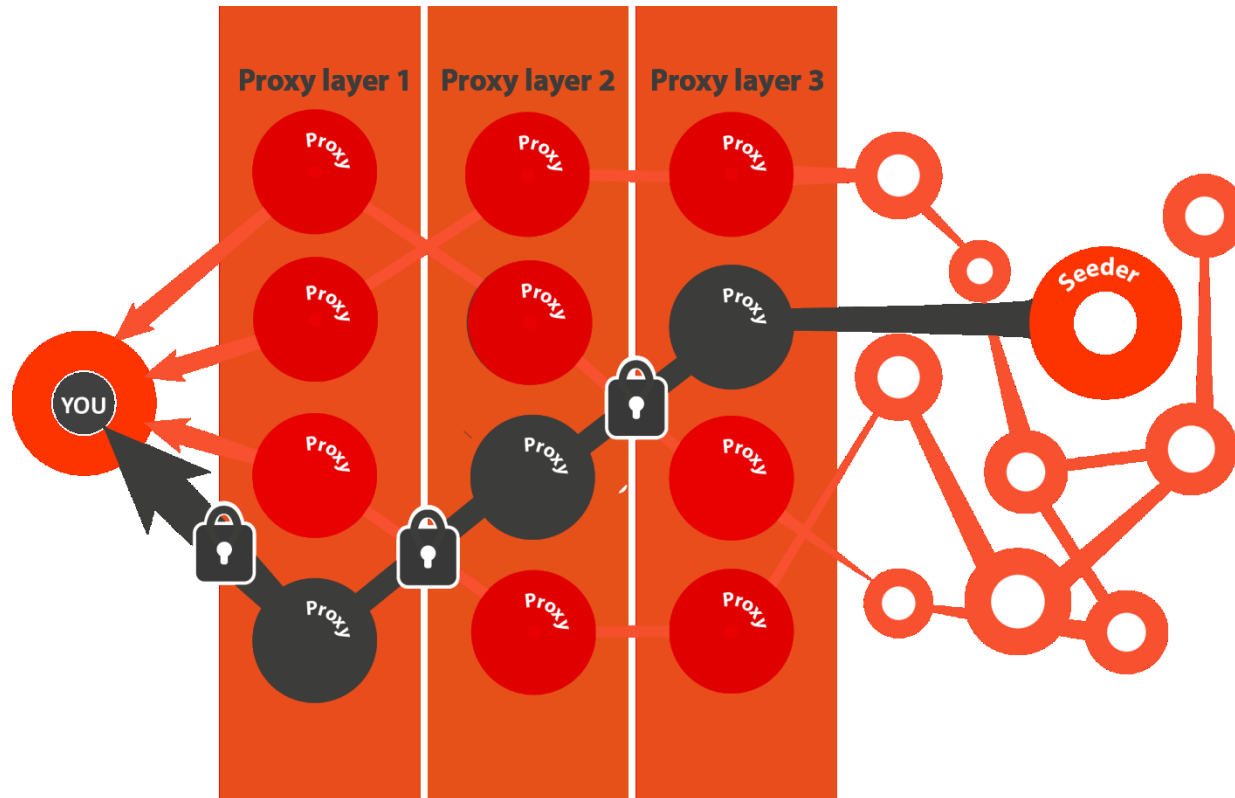
Védelem nélküli letöltés



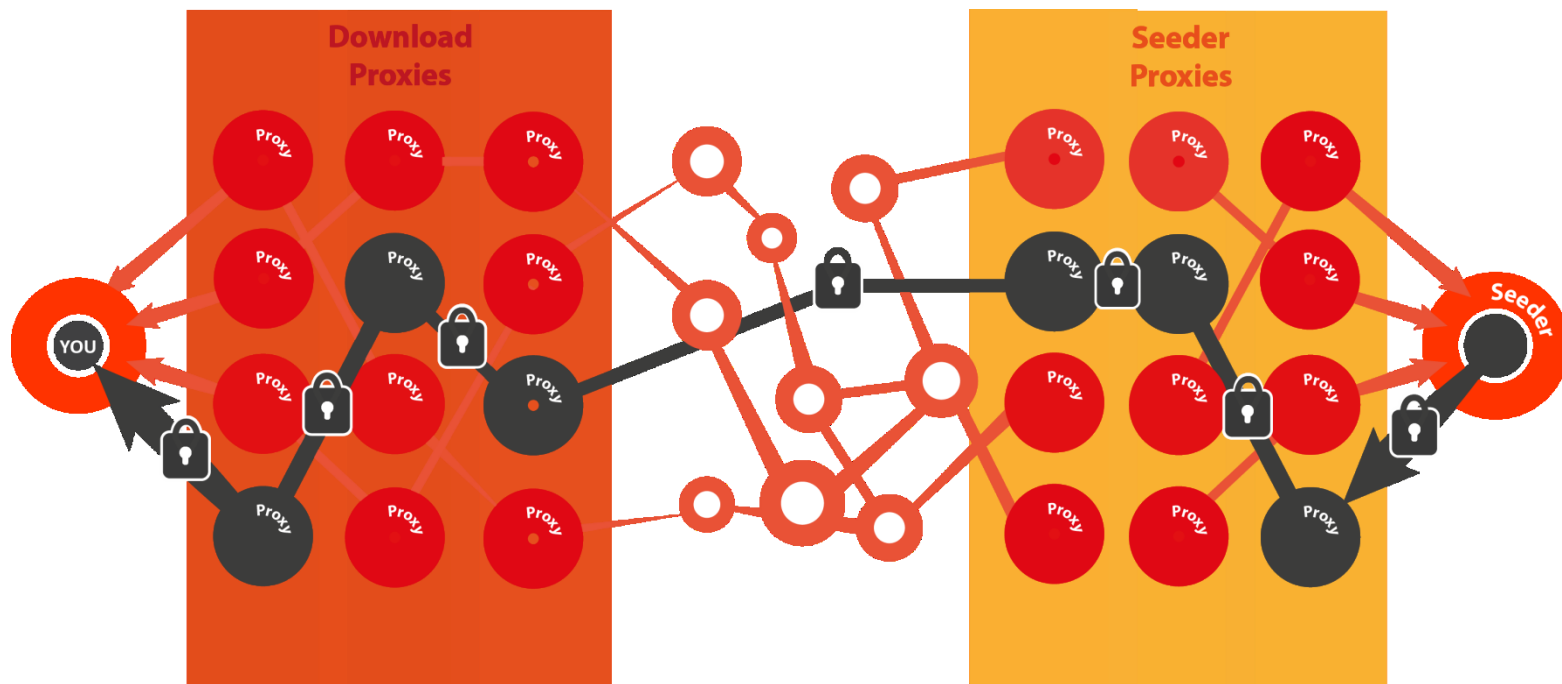
Leacher proxy



3szoros proxy



Seeder proxy



Anonimitás - elosztott módon

Anonimitás

- Második lépés
 - Követők, lehallgatók összezavarása
 - P2P rendszerben történik a routolás is
 - Adatot is szétszjtjuk
 - ELOSZTOTT ADATBÁZIS
 - Igazából egy elosztott cache
 - Keresés

Freenet



- Ian Clarke, végzős hallgató
- University of Edinburgh
- Teljesen elosztott, egyenrangú hálózat
- A peer-ek tárolófelületet és sávszélességet „ajánlanak” fel a rendszernek
 - Nem tudják a rendszer mit tárol ott
 - Minden adat kódolva van
- Freenet – *„földrajzilag elosztott nagyméretű virtuális merevlemez, névtelen (anonymous) hozzáféréssel”*



Freenet



- Biztosítja a „szerzők” és az „olvasók” anonimitását
 - Nem lehet megállapítani az adatok forrását és célállomását
 - Az adatokat *kulcsok* azonosítják
 - A peer-ek nem tudják mit tárol a rendszer a gépükön
 - Nem (vagy nehezen) vonhatóak felelősségre
- A keresést abba az irányba továbbítja, ahol a legvalószínűbb a találat
 - Nincs központi szerver (Napster)
 - Nincs elárasztás (Gnutella)
- A fájlok azonosítása tárolási helyüktől független

Freenet



- Az adatok dinamikus elosztása a rendszerben
- A hálózati topológia (gráfstruktúra) folyamatosan változik
 - Új kapcsolatok jönnek létre a peer-ek között
 - Az állományok vándorolnak a rendszerben
 - Dinamikus, adaptív útválasztás

Freenet fejléc



- UniqueID (64 bit)
 - Azonosítja az üzenetet
 - A hurkok elkerülésére szolgál
- Hops To Live
 - Még hányszor lehet továbbküldeni a csomagot
- Depth
 - Hányat ugrott már a küldés óta
- Source
 - Az üzenet forrását azonosítja

Üzenet típusok



- HandshakeRequest
 - Kapcsolatot kezdeményez egy peer-el
- HandshakeReply
 - Válasz a HandshakeRequest-re
- DataRequest
 - A megadott kulcsnak megfelelő adatot kéri
- DataReply
 - Válasz a DataRequest-re
 - A közbeeső peer-ek cache-ben tárolják az adatot
 - A következő hasonló kérésre már tudnak közvetlenül válaszolni
- RequestFailed
 - Sikertelen keresés esetén

Üzenet típusok



- **InsertRequest**

- Megegyezik a DataRequest-el
- Azt ellenőrzi, hogy a megadott kulcsnak megfelelő fájl megtalálható-e a rendszerben
- Ha igen, egy DataReply érkezik
- Ha nem, egy InsertReply üzenet

- **DataInsert**

- Kérés a megadott adat és kulcs tárolására a rendszerben
- Az InsertRequest útvonalán halad
 - Ott tárolja ahol majd keresni fogják
- A közbeeső peer-ek cache-ben tárolják az adatot

Data Store



- Minden peer-nek tudnia kell...
 - Merre továbbítani egy kérést
 - Merre továbbítani egy választ
 - Meddig tárolni egy adott dokumentumot



Data Store

Key	Data	Address
8e47683isdd0932uje89	ZT38hwe01h02hdhgdzu	tcp/125.45.12.56:6474
456r5wero04d903iksd0	Rhweui12340jhd091230	tcp/67.12.4.65:4711
f3682jkjdn9ndaqmmxia	eqwe1089341ih0zuhge3	tcp/127.156.78.20:8811
wen09hjfdh03uhn4218	erwq038382hjh3728ee7	tcp/78.6.6.7:2544
712345jb89b8nbopledh		tcp/40.56.123.234:1111
d0ui43203803ujoejqhh		tcp/128.121.89.12:9991

Lista tetején – „friss”, gyakran kért fájlok

- Kulcs, adat, származási cím

Lista alján – régi, ritkán kért fájlok

- Kulcs, elérhetőségi cím

Ha egy kulcs lefele mozog a listán, egy idő után
az adatok törlődnek

Keresés



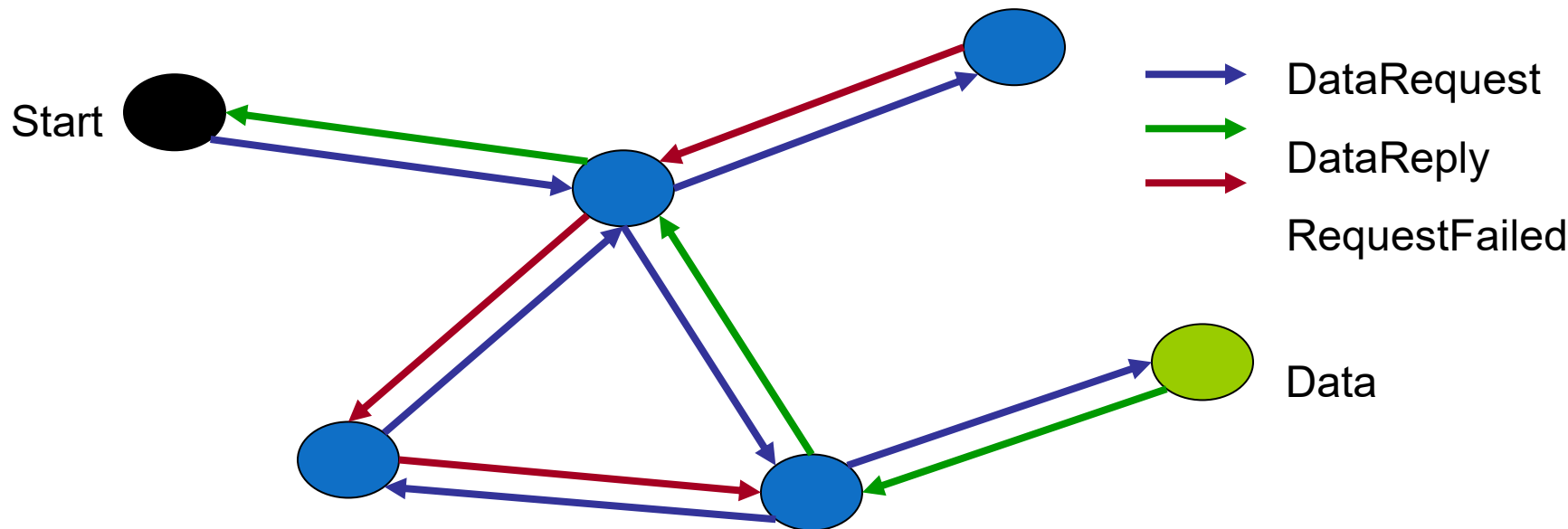
- A peer-ek által tárolt kulcsok alapján
 - Korlátozott számú ugrás, de nagyobb mint a Gnutella esetében
 - Tipikusan 500
 - Az üzenetek azonosítója alapján szűri a hurkokat
- Egy kérés érkezésekor
 - Ha már kezelte a kérést (hurok), visszaválaszol hogy a küldő próbálja másfelé továbbítani („next-best choice”)
 - Ha rendelkezik az állománnyal, válaszol
 - Ha nem, továbbküldi a keresett kulcshoz legközelebb álló kulcsnak megfelelő cím felé



Keresés (II)

- Ha egy válasz érkezik
 - A kulcs és az adat bekerül a cache-be
 - A legrégebbi kulcs kikerül a data store-ból
- Találat esetén az állomány küldése nem pont-pont közötti
 - A keresés útvonalán terjed vissza
 - Segíti a cache működését
 - Növeli az anonimitást

Keresés - példa



Keresés



- Az elején a Data Store üres
 - A peer véletlenszerűen választja ki merre küldje a keresési, illetve adatbeviteli kéréseit
 - Az adatok eloszlása is véletlenszerű lesz
- A keresés (útválasztás) minősége idővel javul
 - Lavina effektus
 - Egy tárolt fájl alapján a peer bekerül más peer-ek adatbázisába, a megfelelő kulccsal
 - Hasonló kulcsok iránti kérések elkezdenek érkezni
 - A válaszok bekerülnek a cache-be
 - Egyre több hasonló kulcsú állományt tárol
- A peer nem döntheti el milyen kulcstartományra „specializálódik”
 - A többi peer által tárolt kulcsoktól függ
 - Növeli a rendszer „ellenőrizhetetlenségét”

Freenet keresés - példa



k10	B
k36	A
k36	B
k7	B

k10
k36
k9

A

B

k7

k9	A
k11	B
k10	A

k9
k11

F

C

k36

k41

E

k9 ?

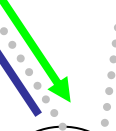
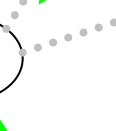
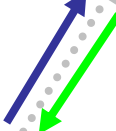
D

k34

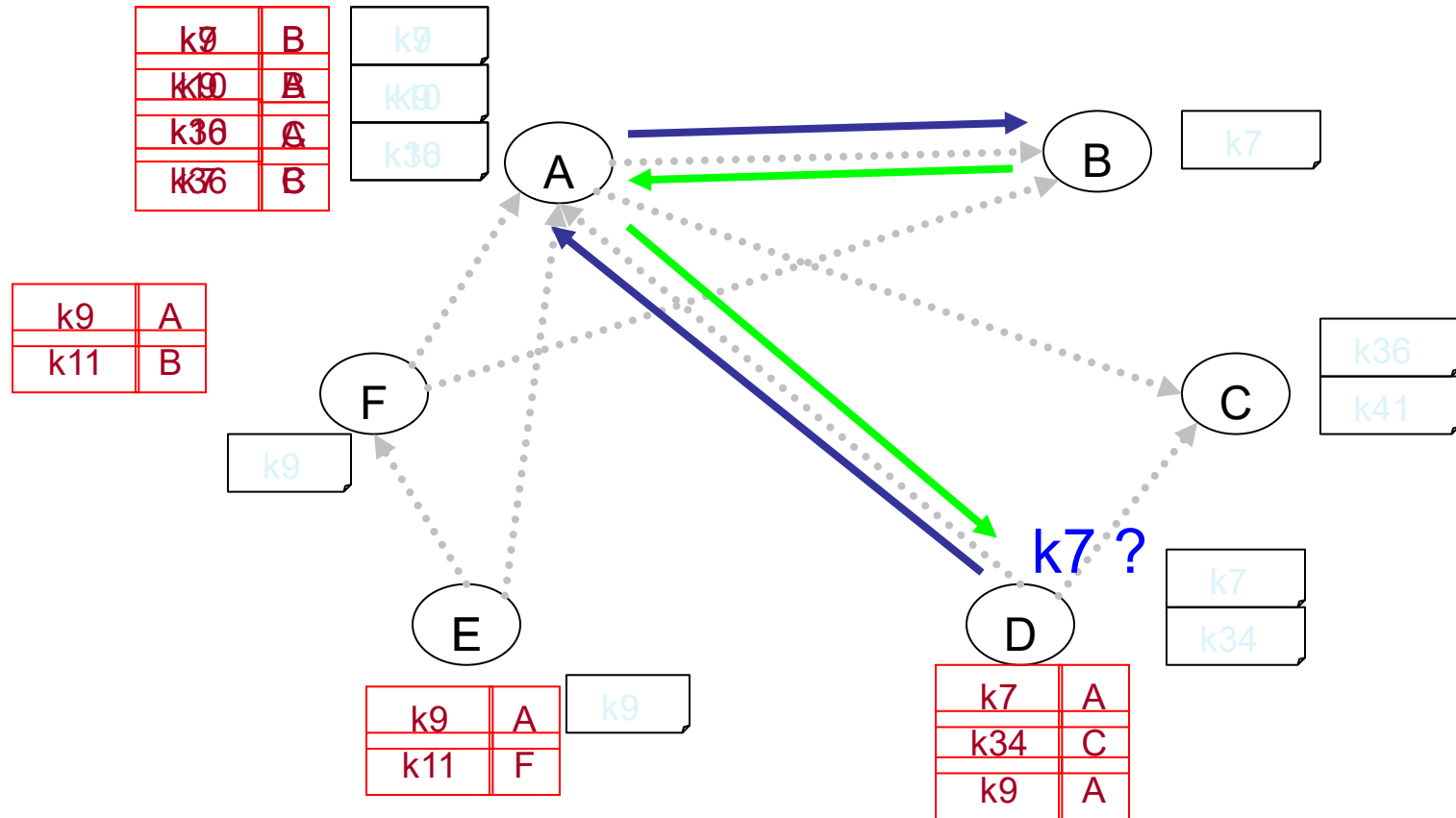
k9	A
k11	F
k34	D

k9
k11

k34	C
k9	A



Freenet keresés - példa





Lavina effektus példa



Animáció, klikkelj a „vonalkódra”



Keresések eloszlása

- Slashdot effektus (<http://slashdot.org/>)
 - Népszerű számítástechnikai hírportál
 - „News for nerds, stuff that matters”
 - Ha egy érdekes hír jelenik meg rajta, mindenki ráklikkel a linkre
 - A hirtelen terhelés megbéníthatja a kisebb kapacitású gépeket
- A Freenet elkerüli a Slashdot effektust
 - A cache-elés miatt a keresések eloszlanak
 - A források nem kerülnek túl nagy terhelés alá
- A kulcsok hash-ek
 - Szemantikailag egymáshoz közel álló tartalmak teljesen különböző kulcsokat kaphatnak
 - Egy „hot topic”-hoz tartozó különböző állományok eloszlanak a rendszerben



Hash függvény

- Nagy értelmezési tartományt képez le egy „szűk” értékkészletre
 - Változó hosszúságú x paramétert képez le fix hosszúságú $h = H(x)$ értékre
- Kriptografikus hash függvények
 - Ha adott x , $H(x)$ relatív egyszerűen kiszámítható
 - $H(x)$ egyirányú
 - Ha adott h hash érték, túlzottan számításigényes olyan x -et találni, amire $H(x) = h$
 - $H(x)$ ütközésmentes
 - H „gyengén ütközésmentes” ha egy adott x -re, túlzottan számításigényes egy olyan y megtalálása ($x \neq y$), melyre $H(x) = H(y)$
 - H „erősen ütközésmentes” ha túlzottan számításigényes bármilyen olyan x és y értékeket találni ($x \neq y$), melyre $H(x) = H(y)$



Hash függvény

- Népszerű algoritmusok

- MD5 – (Message Digest Algorithm 5)
 - Ronald Rivest (MIT), 1991
 - <http://www.ietf.org/rfc/rfc1321.txt>
- SHA-1 (Secure Hash Algorithm)
 - <http://www.itl.nist.gov/fipspubs/fip180-1.htm>



Kulcsok

- Minden állományt egy kulcs azonosít
- A kulcs egy globális azonosító része
 - Uniform Resource Identifiers (URIs): *freenet:keytype@data*
- Több fajta kulcs létezik
 - Keyword Signed Key (KSK)
 - Signature Verification Key (SVK)
 - SVK Subspace Key (SSK)
 - Content Hash Key (CHK)



Keresés

- A kereséshez tudni kell az adott kulcsot
- A publikáló félnek ezt nyilvánosan meg kell hirdetni
 - Anonymous hirdetési lehetőség Freenet portálokon
 - Rövid leírás, kulcs
 - Freenet levelező listákon
 - Freenet IRC csatorna
 - [irc.freenode.net #freenet](https://irc.freenode.net/#freenet)
 - Privát e-mail, web
 - Graffiti, hőlégballonon, repülő által húzott reklámszalagon

Anonimitás



- A peer-ek véletlenszerűen „hazudhatnak” a kérésekkel kapcsolatban
 - A Depth és a Hop-To-Live értékek változtathatóak
- Lehetetlen kideríteni kitől kapod meg a dokumentumot
 - A forrás címet bármely csomópont az útvonalon átírhatja a sajátjára
- Lehetetlen kideríteni ki publikált először a rendszerben egy adott fájlt
- Igyekeznek a réseket is betömni
 - „the Javascript exploit mentioned would not have worked on Freenet because Freenet removes Javascript by default. ”
- Nem biztosít igazi anonimitást
 - A nem triviális támadások ellen valószínűleg nem képes védekezni
 - Forgalomanalízis, nagyszámú csomópont kompromittálása



Előnyök

- Teljesen elosztott rendszer
- Nagy hibatűrés
- Robusztus, skálázható
- Másolatok automatikus generálása
- Jól alkalmazkodik a felhasználók dinamizmusához
- Adaptív, hatékony útválasztás
- Anonim szerzők és olvasók
- Freeriding nem lehetséges

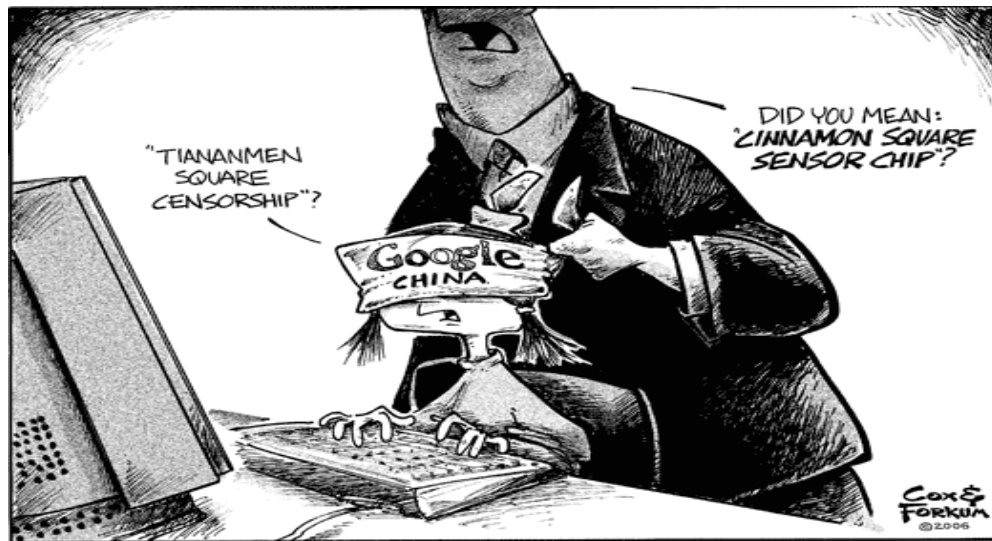


Hátrányok

- Nem garantálható a keresések ideje
- Nem garantálható a keresések sikere
- Ismeretlen topológia
 - A kereső algoritmusok nem tudják ezt kihasználni
- Nem biztosítja a tartós tárolást
 - Egy ma publikált fájl holnapra lehet hogy „kihal” a rendszerből
- Nagyméretű állományoknál nem előnyös egy hosszú útvonal mentén küldeni a választ
 - Nagy a hibalehetőség
 - „Elpocsékolt” sávszélesség

Anonimitás vs. hatékonyság

- A Freenet fő célja a cenzúra elkerülése és az anonimitás,
- nem a hatékonyság
 - Főként kisméretű fájlok, szöveges dokumentumok tárolására és terjesztésére kiváló
 - Freenet China
<http://freenet-china.org/>



Irodalom



- I. Clarke, O. Sandberg, B. Wiley, T. W. Hong, , "*Freenet: A distributed anonymous information storage and retrieval system*", in Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, July 2000.
 - <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.4919>
 - 2000 legtöbbször hivatkozott cikke a Citeseer-ben
 - Jelenleg 773 hivatkozás a Citeseer-ben, 2236 hivatkozás a Google Scholar-ban
- The Free Network Project
 - <http://www.freenetproject.org/>
 - <http://freenetproject.org/papers.html>

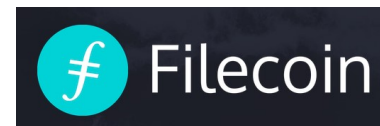


Blockchain alapú P2P megoldások



IPFS

- Interplanetary File System
 - combines the concept of linking the distributed file sharing to a file system
 - Hashing individual files
- Ethereum
 - a single shared computer that is run by the network of users and on which resources are parceled out and paid for by *Ether*
 - *finance, the internet-of-things, farm-to-table produce, electricity sourcing and pricing, and sports betting*
- Filecoin
 - incentive for storage, on top of IPFS
 - distributed electronic currency similar to Bitcoin
 - proof-of-retrievability component, which re-quires nodes to prove they store a particular file



Zeronet

- Dynamic Web
 - P2P
 - Integrated BitCoin
-
- ZeroNet and IPFS: uncensorable auto-scaling BitTorrent powered websites
 - ZeroNet is created for fast, dynamic websites, IPFS is more like a storage solution



SWARM



SWARM

SERVERLESS HOSTING
INCENTIVISED
PEER-TO-PEER
STORAGE AND
CONTENT
DISTRIBUTION

- Distributed **storage** platform and content distribution service
 - a native base layer service of the ethereum web 3 stack
- Features
 - DDOS-resistant, zero-downtime, fault-tolerant, censorship-resistant
 - self-sustaining due to a built-in incentive system
 - uses peer to peer accounting
 - allows trading resources for payment

<http://www.epointsystem.org/~nagydani/homepage>



Összefoglalás

- P2P > fájlcsere
 - Lehetőség van a résztvevők identitásának elrejtésére
 - DHT alapú
- Blockchain alapú új javaslatok (2014/15-től kezdődően)
 - Distributed storage
 - Cenzorship
 - Incentive
 - Dynamic

P2P alkalmazás - SKYPE



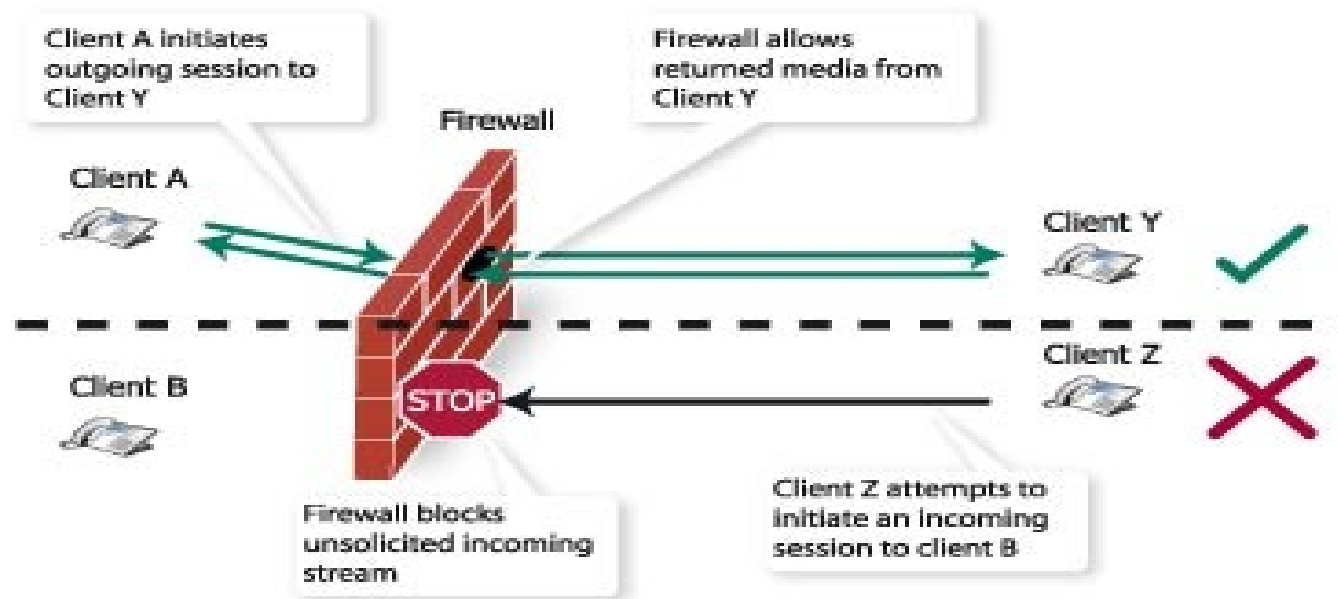
Tűzfal és NAT

VoIP

- Voice over IP
 - Internetes telefonszolgáltatás
 - A hagyományos telefonhálózatok „versenytársa”
- Előnyök:
 - „Ingyenes”
 - az Internet kapcsolaton kívül nincs más költsége a felhasználónak
 - Sok társított szolgáltatás lehetséges
 - Chat, jelenlét követés, stb.
- Hátrányok
 - A hangátvitel érzékeny a csomagvesztésre, késleltetésre és a jitter-re
 - Torlódás esetén rossz hangminőség, megszakadó kapcsolatok
 - A tűzfalak és a NAT megakadályozzák sok VoIP szolgáltatás működését

Tűzfalak

- Tűzfalak mindenhol
 - üzleti/céges hálózatok
 - otthoni felhasználók
 - DSL, kábel modem kapcsolatot használók
- Védik a hálózatot a jogosulatlan forrásoktól
 - Forrás-, célcím és forgalom típus alapján szűrnek
 - Bejövő forgalmat csak akkor engednek be, ha a kapcsolatot belülről kezdeményezték
 - VoIP alkalmazások nem tudnak hívásokat fogadni



„NAT Traversal Solutions for Multimedia over IP Services”, White Paper, Newport Networks.
<http://www.newport-networks.com/whitepapers/nat-traversal.html>

NAT

- Network Address Translation
- (Hálózati címfordítás)
 - Lokális „magán” IP címeket fordít át publikus IP címekké, és vissza
 - Korlátolt számú publikus IP cím elegendő egy nagyméretű hálózat kiszolgálására
 - IPv4-ben kevés az IP cím
- Hogy működik?
 - Minden belső gépnek van egy lokális címe
 - Az általa küldött csomagokat a NAT átírja
 - (lokális cím, port1) → (publikus cím, port2)
 - Táblában őrzi a megfeleltetéseket

Private Address Space

Public Address Space

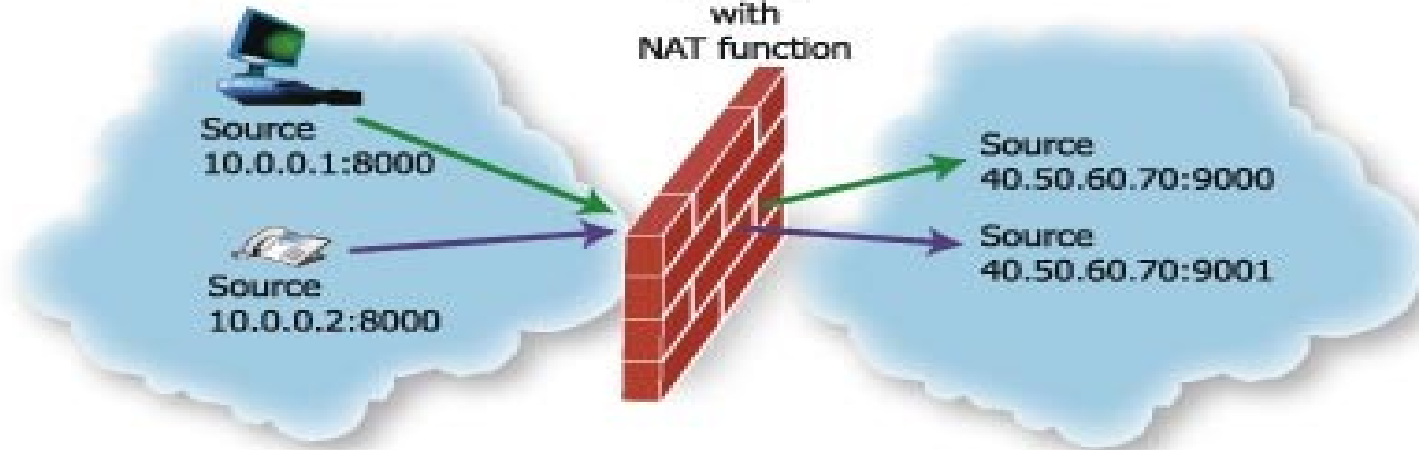
Firewall
with
NAT function

Source
10.0.0.1:8000

Source
10.0.0.2:8000

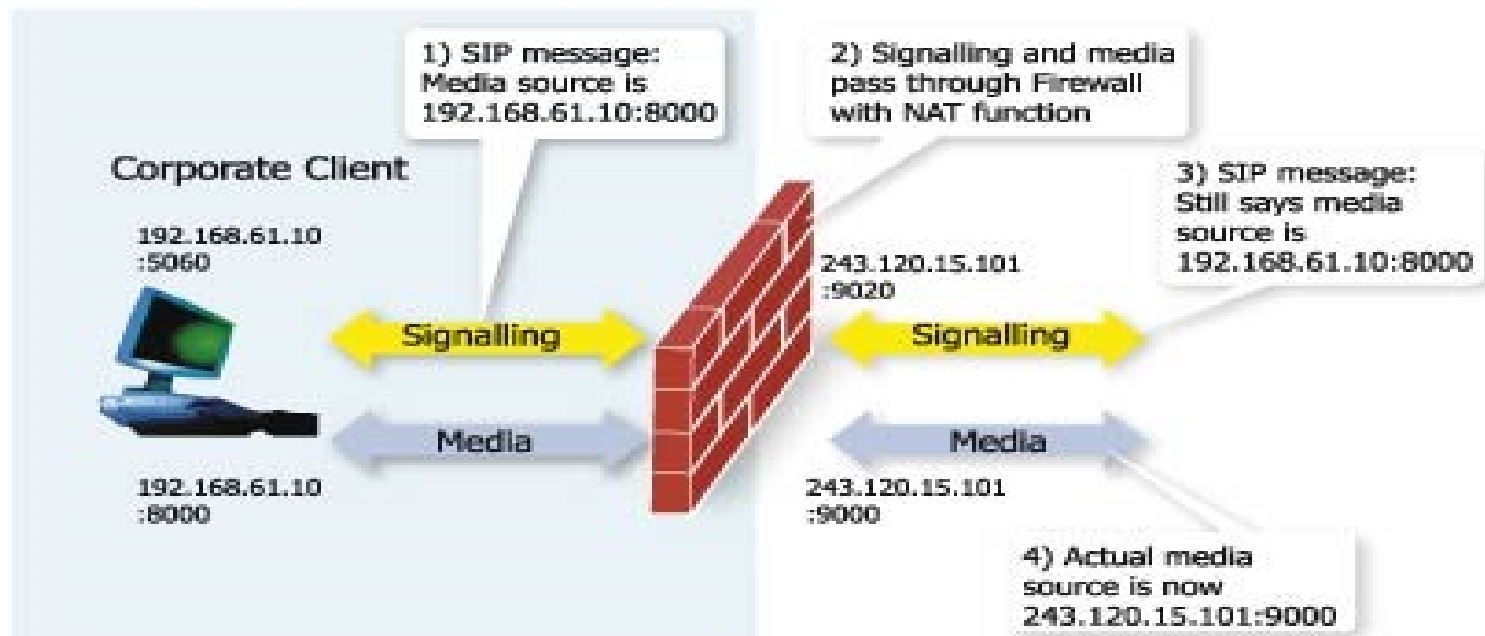
Source
40.50.60.70:9000

Source
40.50.60.70:9001



A „NAT probléma”

- Signaling protokollok audio-video konferenciákhoz, VoIP szolgáltatásokhoz
 - H.323 – ITU-T
 - SIP (Session Initiation Protocol) – IETF
- NAT probléma
 - A SIP signaling csomagok tartalmazzák a VoIP kliens lokális címét
 - A csomag forrás címét átírja a NAT, de a tartalmát nem

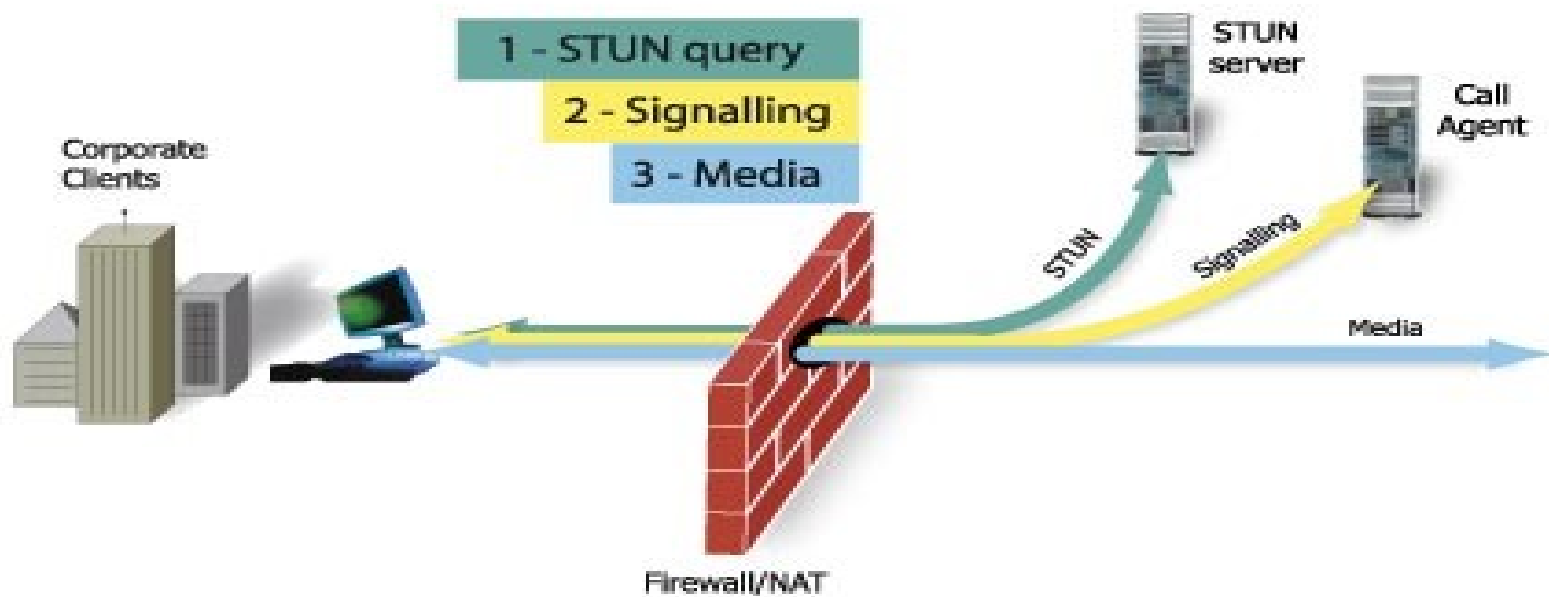


NAT átjárás (traversal)

- Több megoldás
 - Universal Plug and Play (UPnP)
 - Simple Traversal of UDP Through Network Address Translation devices (STUN)
 - Application Layer Gateway
 - manuális konfiguráció
 - alagutazás

STUN

- STUN szerver a tűzfalon kívül
 - A VoIP kliens a STUN szervernek küld egy felderítő csomagot
 - A NAT átírja a csomagot a saját publikus IP címével és egy választott port-al
 - A STUN szerver visszaküldi ezt az infót a kliensnek
 - A kliens ezekkel a paraméterekkel küldi ki a SIP csomagot

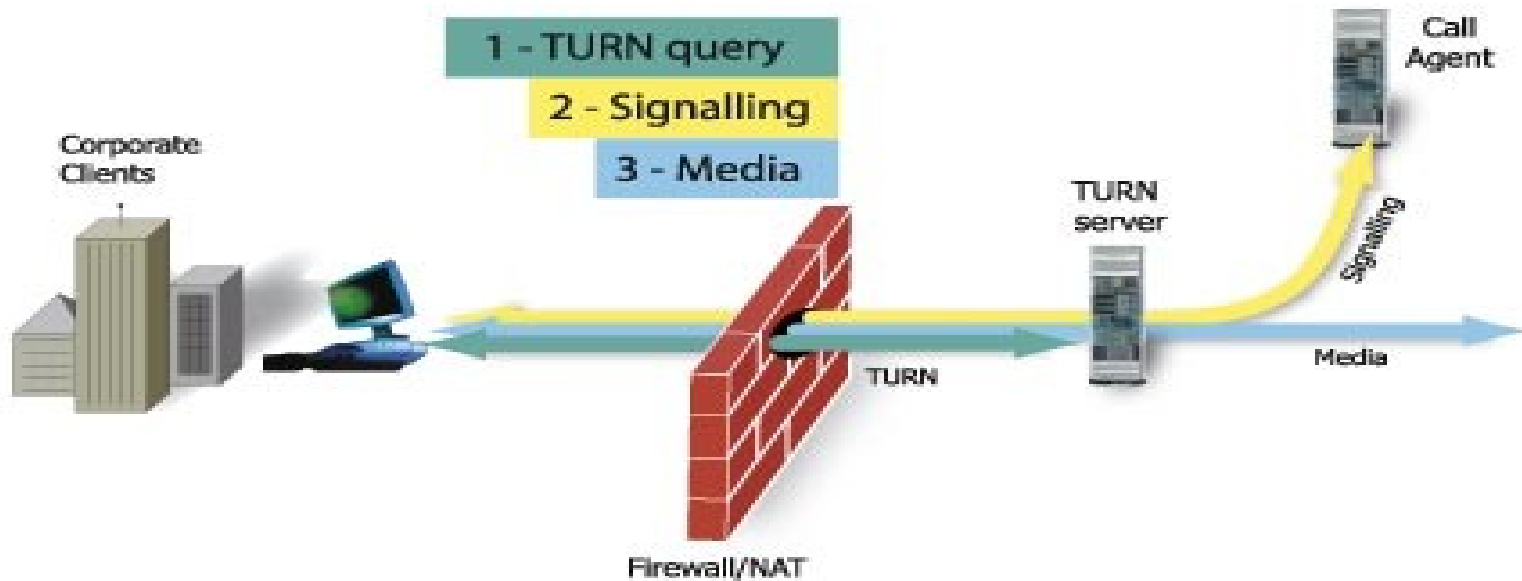


Szimetrikus NAT

- Szimetrikus NAT-ok nagyon elterjedtek
- Minden célcímhez más portot társít
 - A STUN címe eltér a VoIP célállomás címétől
 - A STUN által küldött információ használhatatlan

TURN

- Traversal Using Relay NAT (IETF)
- A TURN szerver proxy-ként működik
 - Minden signalling (jelzési) és adat csomag rajta megy keresztül
 - A címzett mindig a TURN szerver, a NAT ugyanazt a portot generálja
 - A TURN szerver továbbküldi ...
 - a signalling csomagokat a SIP szervernek
 - az adatcsomagokat a VoIP célállomásnak



Skype

Skype

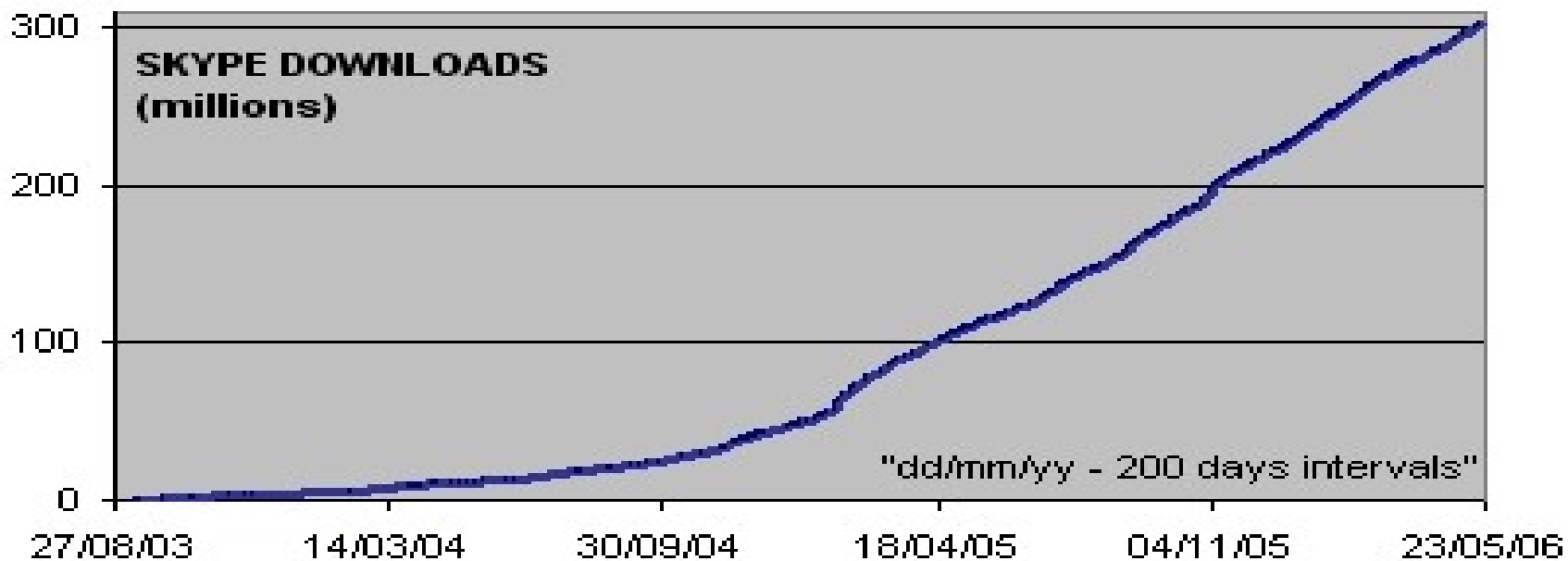


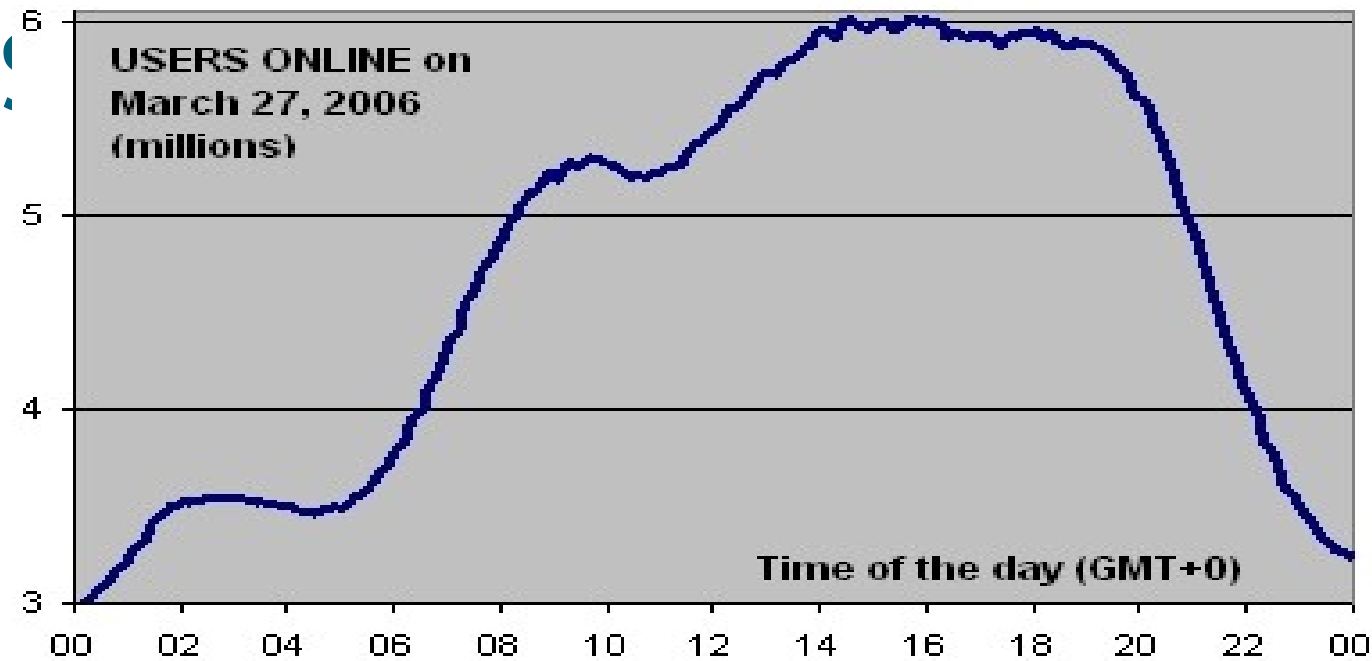
- Az internetes telefonszolgáltatás (VoIP) már évek óta használt
- Több ok miatt nem terjedt el
 - A hagyományos telefonnál olcsóbb megoldások nem kínálnak hasonló minőséget
 - Tűzfalak és NAT miatt az otthoni felhasználók kb 50%-a nem tudja a hagyományos VoIP szoftvereket használni
 - Nehézkes User Interface, bonyolult konfiguráció

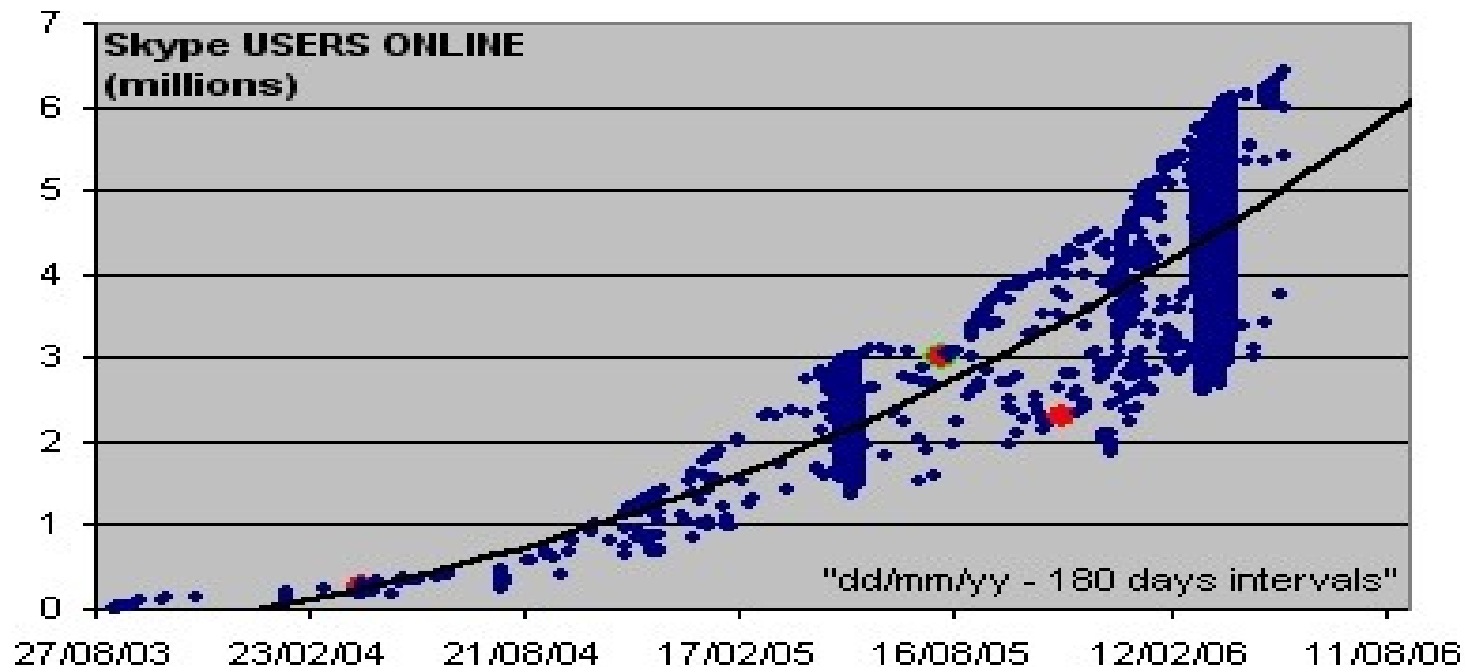


Skype számokban

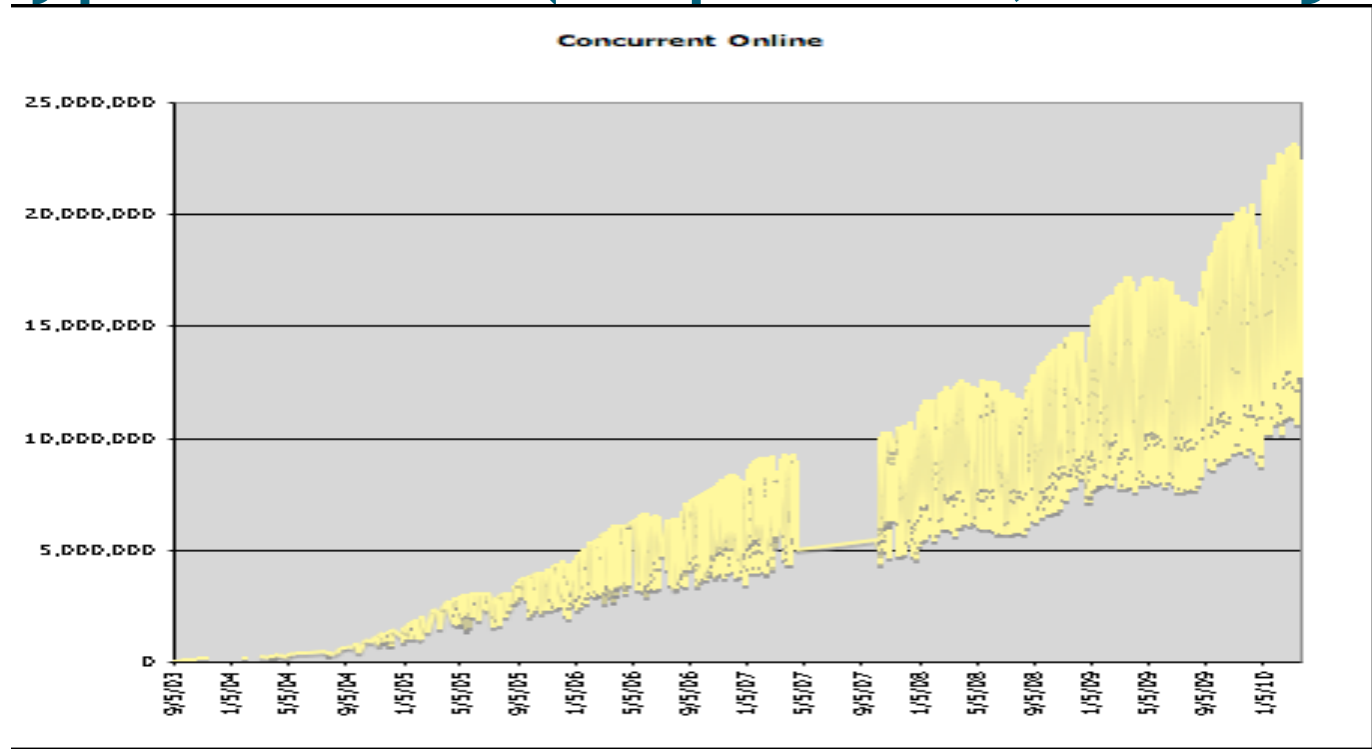
- Niklas Zensström és Janus Friis (KaZaa) alapította
 - 2003 augusztus
- Az egyik jelenlegi legelterjedtebb P2P és VoIP alkalmazás
 - 6.9 milliárd perc (2006 Q1)
 - A világ távolsági hívásainak 7%-a
 - Több mint 381 millió letöltés (2006.09)
 - Több mint 113 millió regisztrált felhasználó (2006.05)
 - Átlagban több mint 6 millió felhasználó egyidőben (2006.09)
 - 14-15 millió 2009 elején
 - Átlagban több mint 52.000 párhuzamos hívás (2006.09)





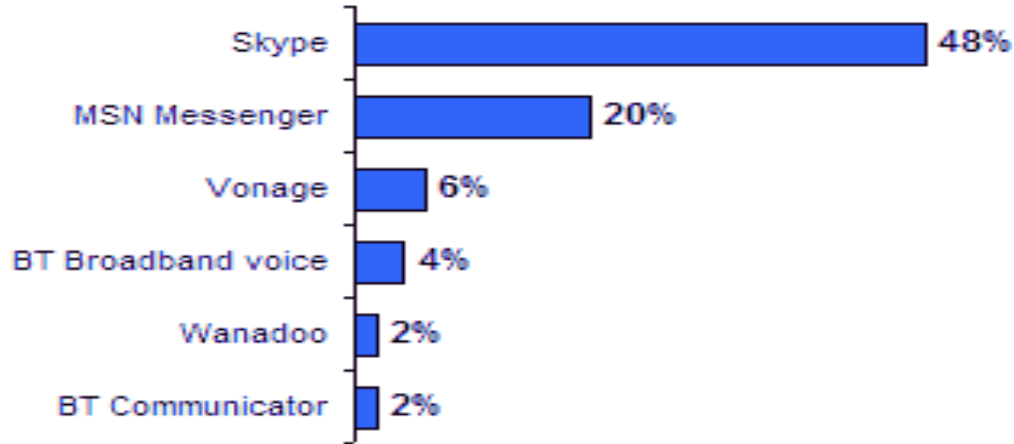


Skype on-line (ckipe.com, 2010 január)



Skype és a konkurencia (Anglia, 2006.04)

Provider used to make calls over the Internet



Base: all who have made a phone/video call in the last 12 months 123

Skype - mit tud?



- Jobb minőség mint a hagyományos telefon
 - Hagományos telefonnál: 300 Hz – 3 kHz
 - Beszédjel + védősávok = 4 kHz-es beszédcsatorna
 - Skype: 50 Hz – 8 kHz
- Nem igényel tűzfal vagy router konfigurációt
 - P2P alapú NAT és tűzfal átjárás
- Biztonságos
 - end-to-end encryption
- Egyszerű user interface
- Szinte minden platformon fut
 - Windows, Mac OS X, Linux, Pocket PC
- Telefonkonferencia (5 résztvevővel), videotelefon, IM, file transfer,
- üzenetrögzítő



- Ingyenes internetes telefonszolgáltatás (VoIP)
 - Két számítógép között
 - Skype
 - Számítógép és hagyományos vezetékes vagy mobil telefon között
 - SkypeOut
 - Vezetékes vagy mobil telefon és számítógép között
 - SkypeIn



Skype szolgáltatások

- Egyszerű user interface
- Szinte minden platformon fut
 - Windows, Mac OS X, Linux, Pocket PC
- Telefonkonferencia – 4 résztvevővel
- Telefon, instant messaging, file transfer
- irodalom: Skype és SIP kapcsolata
 - http://www.theregister.co.uk/2004/06/22/sip_versus_skype/page2.html

Skype működése





Hogy működik?

- Titkos forráskód
- Kódvisszafejtés
 - S. Baset, H. Schulzrinne, „An Analysis of the Skype Peer-to-Peer Internal Telephony Protocol”, Columbia University, September 15, 2004.
- Mérések
 - Neil Daswani, Ravi Jain, „An Experimental Study of the Skype Peer-to-Peer VoIP System”, white paper.
<http://saikat.guha.cc/pub/iptps06-skype/>
 - Mérések 2005 szeptembere és 2006 januárja között, Cornell University

Hogy működik?



- Hierarchikus rendszer

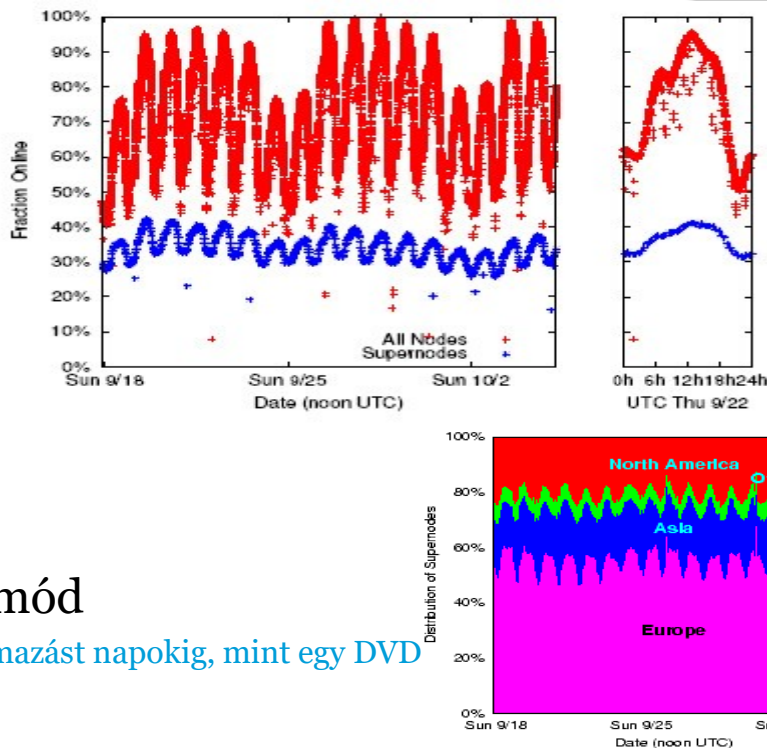
- peer, supernode, Skype login szerver
- Kb. 20-25.000 supernode
 - Mások szerint 150-200.000 supernode
- A supernode-ok stabilabbak mint a peer-ek
 - 50-60% Európában

- A fájlcsereelőkhöz képest más viselkedésmód

- Munkaórákhoz köthető, nem hagyják futni az alkalmazást napokig, mint egy DVD letöltésénél

- Nincs benne csendelnyomás, 33 csomag/sec bármilyen beszélgetésre

- Jelentősen lehetne csökkenteni a supernode-ok terhelését



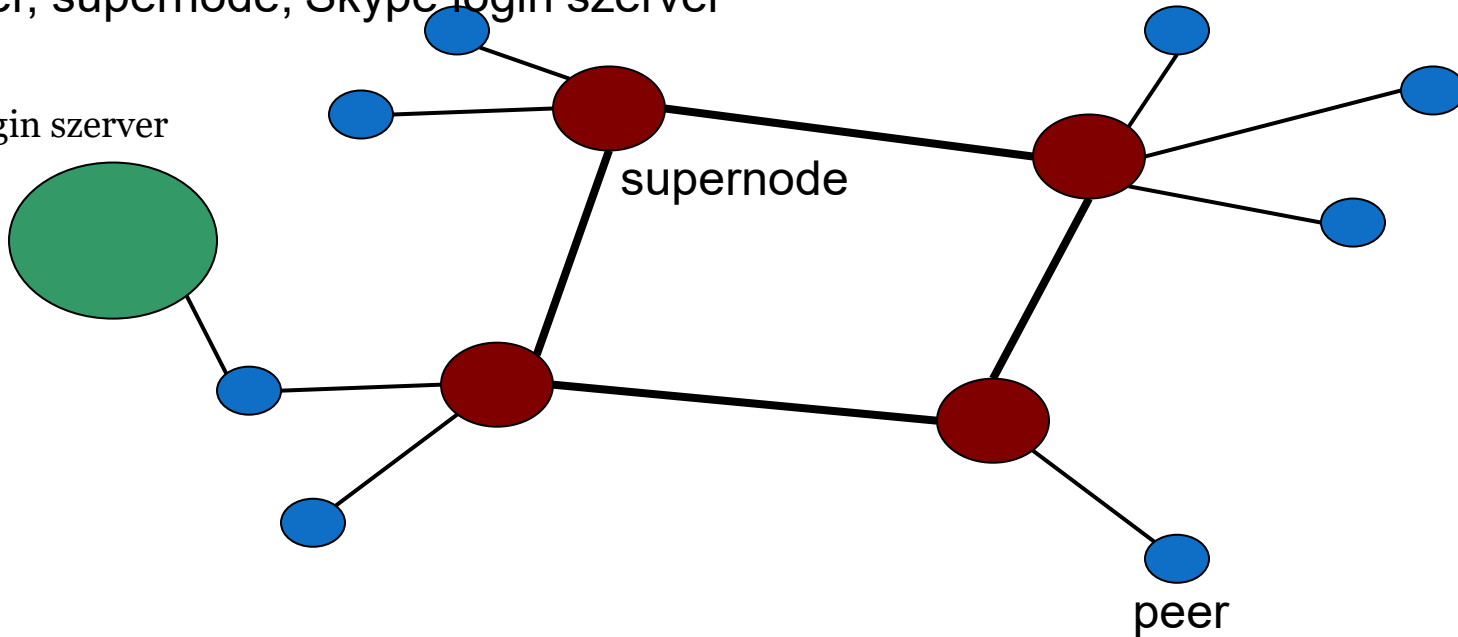
Skype architektúra

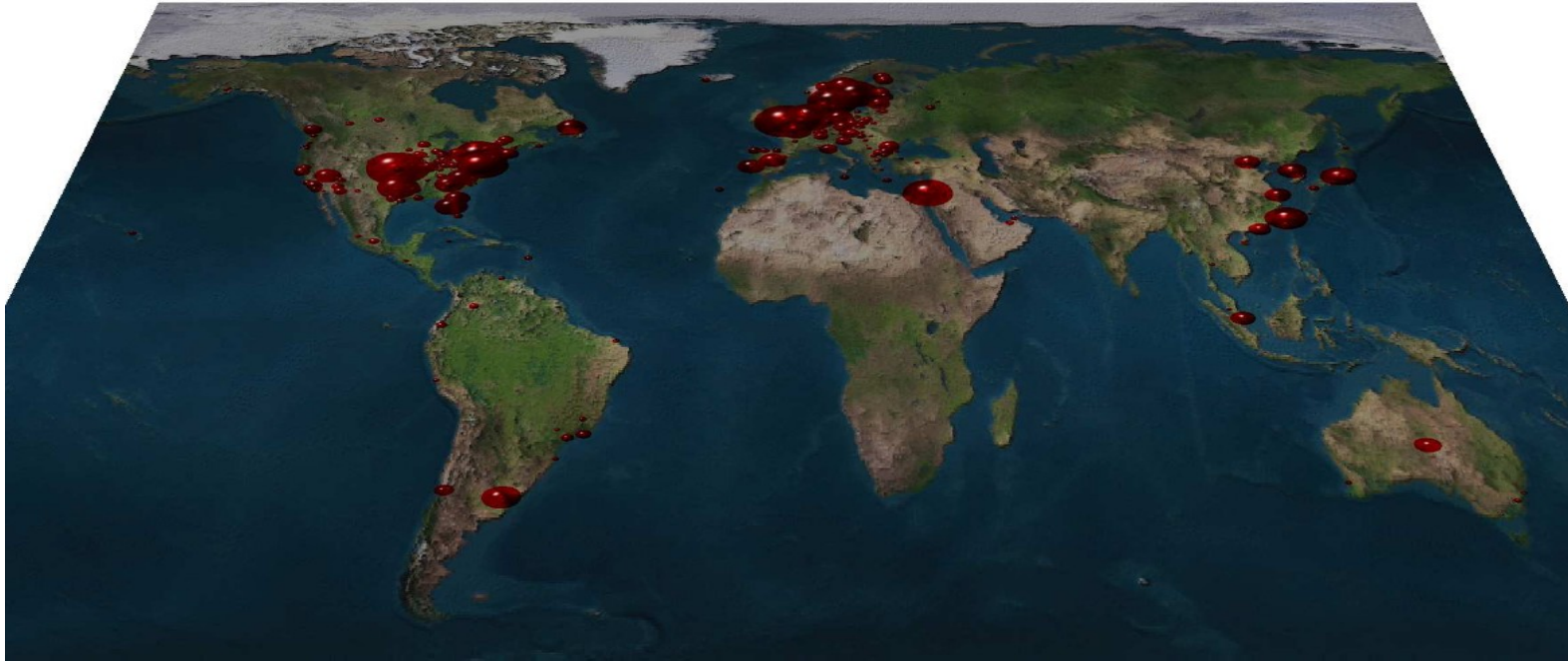


Elemek:

• peer, supernode, Skype login szerver

• Skype login szerver





Forrás: Biondi, Desclaux: Silver Needle in the Skype

Becsatlakozás



- Host Cache (HC)
 - Lista supernode-ok (SN) IP címével és portjával
 - Legalább egy érvényes bejegyzés kell, különben nem tud csatlakozni
- Kiépít egy TCP kapcsolatot az SN-el
- Authentikáció a login szervernél
 - Egyetlen központosított elem a rendszerben
 - Ellenőrzi a felhasználónevet és a jelszót
 - Felelős a felhasználónevek egyediségéért a címtérben
 - Kódvisszafejtés során egy dán ISP hálózatán belüli login szervert mutattak ki

SN redundancia



- Becsatlakozás után feltölti a HC-t érvényes adatokkal
 - Más supernode-ok adatai
 - Ha az aktuális SN meghal, automatikusan újhoz kapcsolódik a HC-ből választva

Kontakt keresés



- Global decentralized User Directory
 - Lehet keresni benne
 - Ha valaki a kontakt listán van, lehet követni az állapotát
 - online, offline, busy, stb.
- A hagyományos Instant Messaging szolgáltatásoknál központosított directory
 - Egy azonosítóhoz (user name) milyen IP cím tartozik
 - Dinamikus IP címek (DHCP) és mobilitás támogatása
 - Nem skálázható ha több millió felhasználó

Skype keresés



- A Skype-ban P2P alapú elosztott megoldás
 - A hagyományos fájlmegosztó alkalmazás elegendő lenne, de...
 - a keresés nem determinisztikus, nem ér el minden peer-t
 - 3G P2P megoldás – Global Index (DHT)?
 - Többretegű hálózat, a supernode-ok által bármelyik peer globális képet kaphat az összes elérhető erőforrásról, minimális késleltetéssel
 - Titkos, nem visszafejthető
 - Nem nézhetünk be a csomagokba melyeket az SN küld tovább
 - Valószínűleg hullámokban keres, új és új SN-on
 - Átlagban 3-4 másodperc
 - Cache működik a SN-on

Tűzfal/NAT átjárás



- Hagyományos NAT es tűzfal elkerülés
 - A hívások egy központi gépen keresztül mennek
- Túl nagy erőforrást igényel, túl drága megoldás
- Az erőforrás igény arányosan nő a hálózat méretével
 - Egy-egy felhasználónak nagyon kevés erőforrást biztosítanak
 - Rossz minőségű kapcsolatok

Skype megoldás



- Tűzfalakon kívüli és publikus IP címekkel rendelkező peer-ek (proxy) segítenek a forgalom továbbításában
- A végpontok közötti titkosítás miatt a proxy nem jelent gondot a biztonság szempontjából
- Csak olyan proxy-t választ ki a rendszer, amelyiknek van elegendő erőforrása
 - A kapcsolat minősége nem romlik

Skype routing



- Multipath routing

- Több útvonalat is fenntart a két kommunikáló fél között
- Mindig a legjobbat, a legtöbb erőforrással rendelkezőt használja

Skype biztonság



- Vitatéma szakértői körökben
 - A titkos forráskód miatt nehéz megállapítani mennyire biztonságos
- A teljes forgalom titkosítva van, nem lehet beavatkozni
- A felhasználó nincs bevonva a kriptografikus folyamatokba
- Viszonylag kisméretű kulcsok
 - „Security through obscurity”
 - Ha nyilvánossá tennék a forráskódot, támadhatóvá válna
- Bármelyik másik Skype-ot beszélő gépben megbízik, nincs hitelesítés
 - Támadási felület
- A kód számos helyen akarattal össze van zavarva, megnehezítve a visszafejtést
- Rengeteg checksum az integritás ellenőrzésére
- P. Biondi & F. Desclaux, „Silver Needle in the Skype”, Black Hat Europe 2006.
 - <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-biondi/bh-eu-06-biondi-up.pdf>

Skype vírusok

- Wormok
- Ismeretlentől egy fájlt kell letölteni
 - Pl képet tölts le, de egy script
 - Ez rátelepedik a Skype kliensre és üzeneteket küld az ismerősöknek
- W32/Ramex.A
- <http://www.thedailynewsegypt.com/article.aspx?ArticleID=9436>

Bepillantás a Skype falai mögé

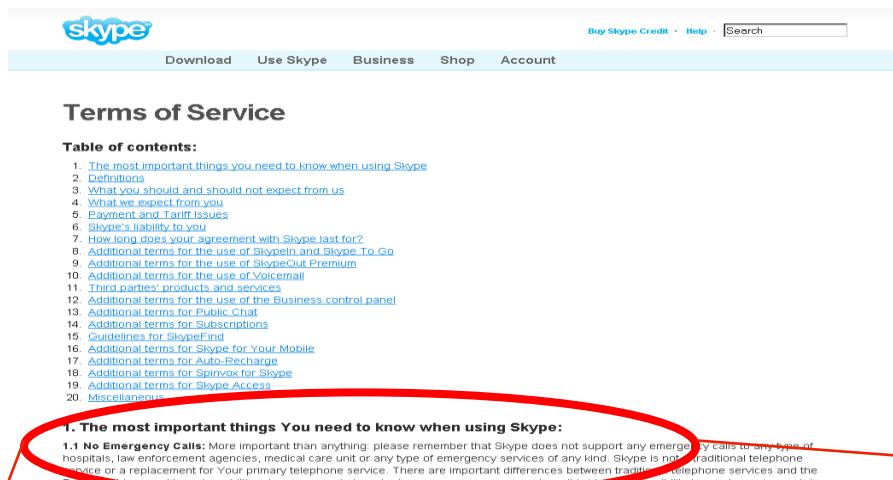
A decorative graphic consisting of several horizontal lines of varying lengths and colors (white and blue) extending from the right side of the title area towards the right edge of the slide.

Skype rendelkezésre állás

- 2007 augusztus 16.án megszakadt a Skype szolgáltatás
 - **Rejtett hiba, 2003tól a kliensben!**
- „Skype, the online phone company, was today working to fix an outage that left its 220 million users unable to make cheap calls over the internet.”
- **Probléma: a Skype szakított a klasszikus telefóniában szokásos rendelkezésre állás biztosításával**
 - **Skálázhatósági problémákkal próbálták magyarázni**
 - **Skype-ban nem törekednek olyan szigorúan a rendelkezésre állás biztosítására**
 - Kevesebb infrastruktúra, megengedőbb szerződések 3. féllel


THE SUNDAY TIMES
TIMES**ONLINE**

Zárójel: Skype korlátozása



skype

Buy Skype Credit · Help · Search

Download Use Skype Business Shop Account

Terms of Service

Table of contents:

1. The most important things you need to know when using Skype
2. Definitions
3. What you should and should not expect from us
4. What we expect from you
5. Payment and Tariff issues
6. Skype's liability to you
7. How long does your agreement with Skype last for?
8. Additional terms for the use of SkypeIn and Skype To Go
9. Additional terms for the use of SkypeOut Premium
10. Additional terms for the use of Voicemail
11. Third parties' products and services
12. Additional terms for the use of the Business control panel
13. Additional terms for Public Chat
14. Additional terms for Subscriptions
15. Guidelines for SkypeFind
16. Additional terms for Skype for Your Mobile
17. Additional terms for Auto-Recharge
18. Additional terms for Spinvox for Skype
19. Additional terms for Skype Access
20. Miscellaneous

1. The most important things You need to know when using Skype:

1.1 No Emergency Calls: More important than anything: please remember that Skype does not support any emergency calls to any type of hospitals, law enforcement agencies, medical care unit or any type of emergency services of any kind. Skype is not a replacement for your primary telephone service. There are important differences between traditional telephone services and the

- Pl: Informatikai Tárcaközi Bizottság ajánlása 12 számú Ajánlása 1996
- Megbízható működési
 - alapszintű (MM-A) osztály (95,5 %)
 - fokozott biztonságú (MMF) osztály (99,5 %)
 - kiemelt biztonságú (MMK) osztály (99,95 %)
- MM-K osztályban a szolgáltatás megszakítás mértéke: 16 perc/hónap, DE 1perc/alkalom

1. The most important things You need to know when using Skype:

1.1 No Emergency Calls: More important than anything: please remember that Skype does not support hospitals, law enforcement agencies, medical care unit or any type of emergency services of any kind. \$

Skype rendelkezésre állás (2)



<http://heartbeat.skype.com/>:



[RESOLVED] Problems with Skype login

By  Joosep on August 16, 2007.

UPDATED 14:02 GMT: Some of you may be having problems logging into Skype. Our engineering team has determined that it's a software issue. We expect this to be resolved within 12 to 24 hours. Meanwhile, you can simply leave your Skype client running and as soon as the issue is resolved, you will be logged in. We apologize for the inconvenience.

Additionally, downloads of Skype have been temporarily disabled. We will make downloads available again as quickly as possible.

- Miért akkor és miért pont azért omlott össze?
 - Kívülről nehéz volt belelátni a rendszerbe

Miért omlott össze a Skype?

Skype néhány közleménye tisztázta a kérdést (aug.20. és aug.21.)

„The disruption was triggered by a massive restart of our users' computers across the globe within a very short timeframe as they re-booted after receiving a routine set of patches through Windows Update. (...) Flood of log-in requests, which, combined with the lack of peer-to-peer network resources, prompted a chain reaction that had a critical impact”

Egy DoS támadással felérő Microsoft Update következménye

- Egy blogger kitalálta ☺

<http://blog.tmcnet.com/blog/tom-keating/skype-outage.asp>

Az erőforrás-elosztó rendszer nem tudta tartani a lépést

- Lavina hatás: megismételt login-kérések (?)
 - Többen jelezték, hogy a Skype-login nem volt sikeres
 - Mások észrevették, hogy sikeres skype-login után rövidesen „kidobta” őket a rendszer
- Supernode-kérések (?)
 - a Host Cache alapján ismételt csatlakozási kísérletek

Skype magyarázat (folyt)

- Négy pontban finomította a Skype a közleményt
 - Microsoft Update patches were merely a catalyst
 - [Skype's] P2P network management algorithm was not tuned to take into account a combination of high load and supernode rebooting
 - [Previously] there had not been such a combination of high usage load during supernode rebooting
 - We've tuned Skype's P2P core so that it can cope with simultaneous P2P network load and core size changes

Skype összeomlások

- 2010.12.22.
 - IM szolgáltatást kezelő gépek túlterhelés miatt leálltak
 - Skype v.5.0.0.152 for Windows alkalmazás a késleltetés miatt meghalt
 - Pech: a felhasználók 50%-ánál ez a verzió futott ☺
 - Ezek között sok supernode is volt
 - A leállt supernodok forgalma átkerült a még működő supernodeokhoz
 - Ezért az elvileg érintetlen, működőképes supernodeok túlterhelés miatt estek ki
 - 24 órás szolgáltatás kiesés, amíg 100-as nagyságrendű pót-supernodeokat (mega-supernode) állított üzembe a Microsoft
- 2011.05.26.
 - Megint a Windows verzióval volt a gond, kiléptette a felhasználót
 - Nem tudtak újra belépni
 - Nem nyilatkoztak, mi volt a baj („fairly technical issue”)
 - Kérték a *shared.xml* fájl törlését – itt tárolja a supernode listát ☺ Ismerős hiba ;)
- 2016.12.15.
 - „Skype multiple service outages” - sign-in, PSTN calls, SMS sending (ekkor a Skype már nem P2P!)



http://readwrite.com/2010/12/23/skype_outage_continues_30_percent_functional/
http://heartbeat.skype.com/2011/05/problems_signing_into_skype_an.html
http://heartbeat.skype.com/2016/12/skype_multiple_service_outage.html

Skype és a PSTN

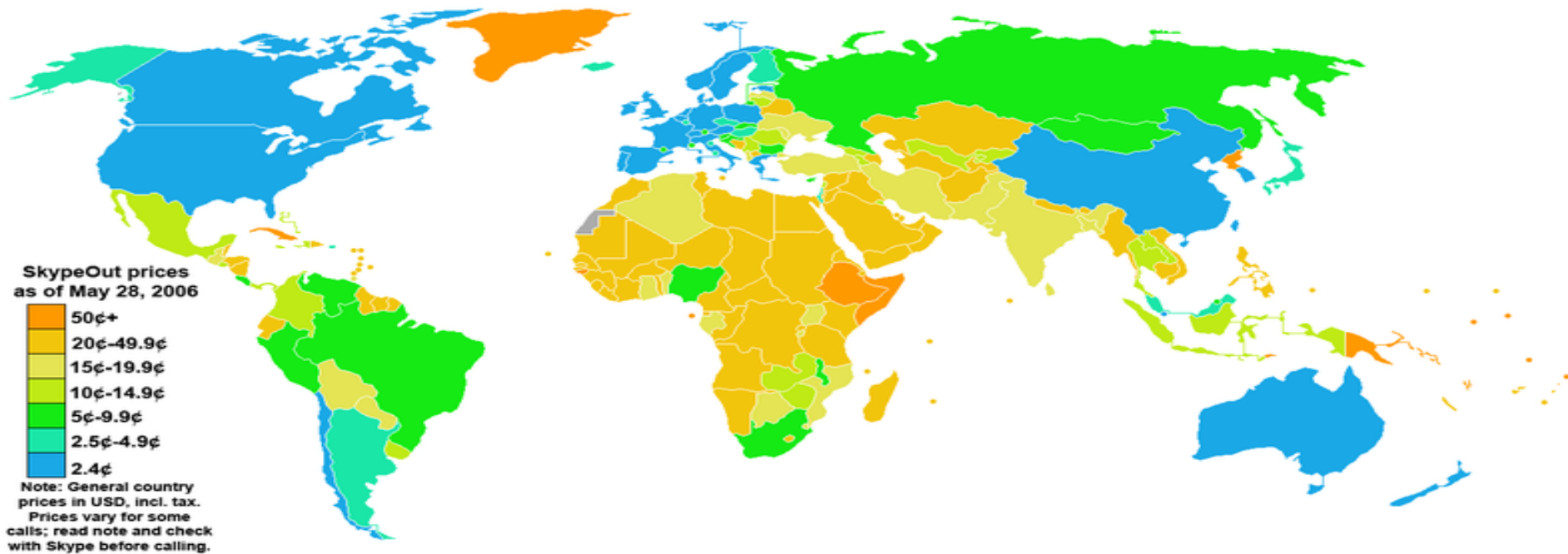
A decorative graphic consisting of several horizontal lines of varying lengths and colors (white and light blue) extending from the right edge of the slide.

SkypeOut



- A hagyományos vezetékes és mobil telefonhálózatok integrációja
 - Számítógépről lehet hívni egy hagyományos telefont
- Nem ingyenes, de nagyon olcsó
 - Internetes számlafeltöltés - PREPAID
 - Flat rate naptól, napszaktól függetlenül
 - Interneten keresztül jut el a célországba, ott a helyi hívást kell fizetni
 - Kinában 2005-ben rövid időre betiltották
 - A helyi telco-k nem szerették a versenyt
 - A Skype támogatja a kínai állami cenzúrát (a Google, AOL, Microsoft, Yahoo és Cisco is)
- SkypeOut árak:
 - Magyarország 3 cent (8 forint/perc) – bárhonnan a világból
 - Magyar mobil: 20 cent (55 forint/perc, 30 forint/SMS)
 - Europa, USA, Kanada, Ausztrália: 1.7 cent (4 forint/perc, 28 forint/SMS)
 - 2006 végéig ingyenes minden belföldi hívás – USA, Kanada, Franciaország
- 1 millió regisztrált felhasználó (2005.03)

SkypeOut árak





SkypeIn

- Április 15, 2005
- 10 SkypeIn számot választhatunk (bárhol) a világban
 - USA, UK, Franciaország, Hong Kong, Dánia, Lengyelország, stb.
 - Kapunk egy hagyományos telefonszámot a kért országban, megyében
 - country + area code
 - Előfizetés: 3 hónap – 10 euró

SkypeIn



- Bárki hívhatja ezt a számot, és elér bennünket ha fel vagyunk kapcsolódva az Internetre és fut a Skype
 - Csak a helyi hívást fizeti a hívó, attól függetlenül, hogy mi hol netezünk
 - Mint a roaming, csak a hívott fél nem fizet a roamingért
 - Ha nem vagyunk elérhetőek, ingyenes VoiceMail szolgáltatás
 - 60 napig tárolva a rendszerben
 - meghallgatás után átmásolódik a felhasználó gépére
 - max 10 perc hosszú lehet az üzenet

Skyepcasts

- 2006 májusában indult
- Moderált konferenciabeszélgetés, max 100 résztvevővel
 - A moderátor megadja vagy megvonja a szót
- Nem támogat párhuzamos chat ablakot
- Ingyenes szolgáltatás, Skype felhasználóknak

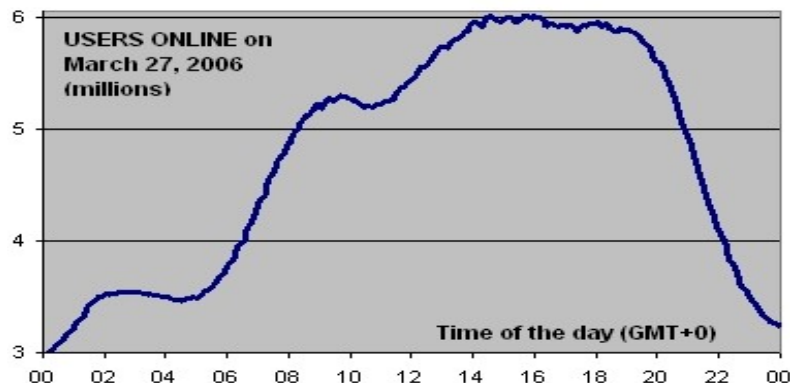
Skype a piacon

A decorative graphic consisting of several horizontal lines of varying lengths and colors (white and light blue) extending from the right edge of the slide.

Skype előfizetők

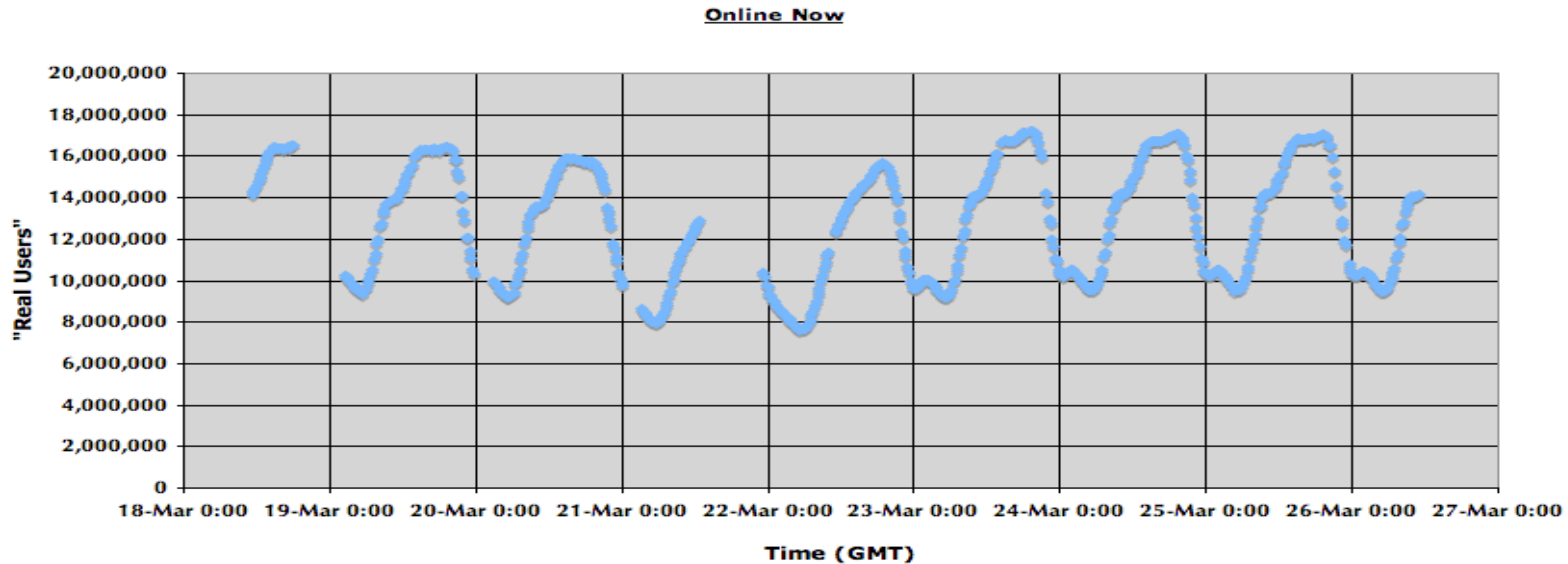


- Európában van a legaktívabb közösség
- Jelenleg 400millió feletti felhasználói bázis
 - 390e belépő NAPONTA
 - 2.2mill belébő HAVONTA



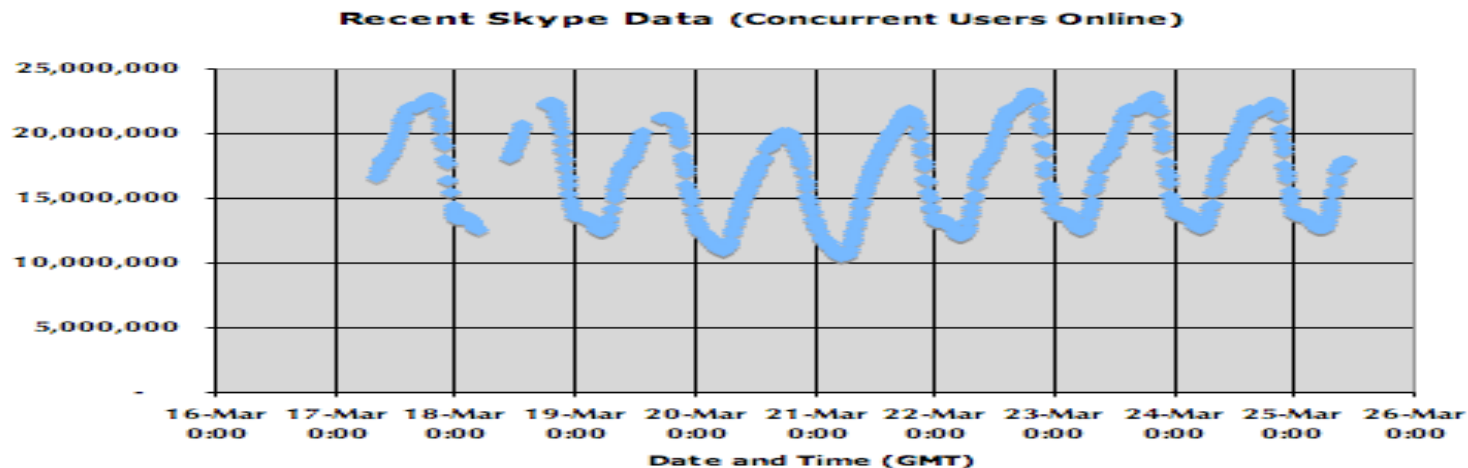
Skype felhasználók

- <http://glimfeather.com/borderless/OnlineNow.htm>
- Skype Users Online Now:14,074,794 3/26/09
- Skype "Real Users" Total:42,046,587 3/26/09
- All-Time peak of concurrent users:17,186,245 3/23/09



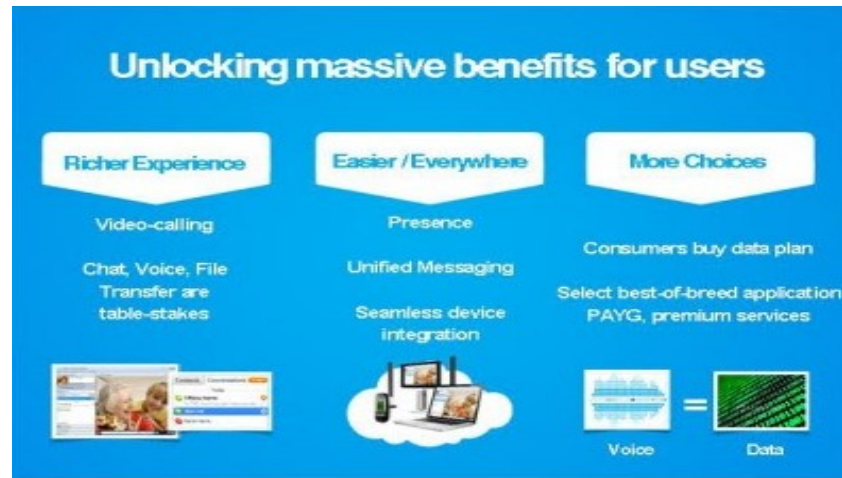
Skype felhasználók (+1 év)

- <http://ckipe.com/borderless>
- Skype Users Online Now: 17,850,544 3/25/10
- Skype "Real Users" Total: 55,720,059 3/25/10



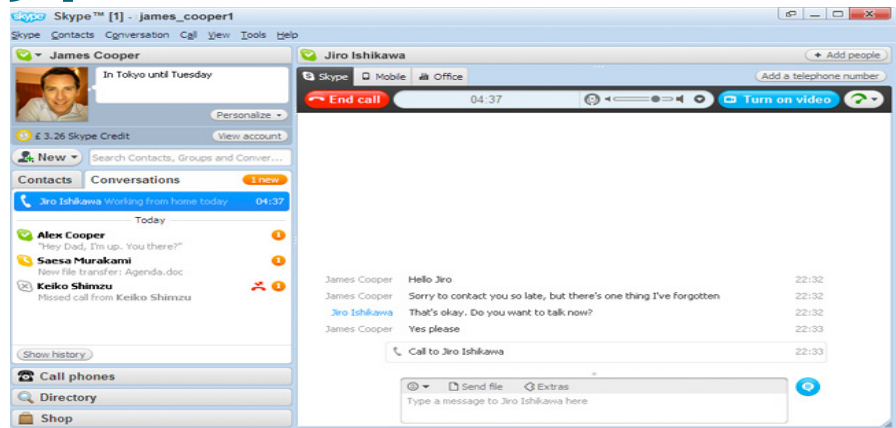
Miért éri meg a Skype-nak?

- Miért érte meg az eBay-nek 3.4 mld USD-t fizetni érte?
- Marketing hatásos, de nem magyarázza az árat
- \$45mill. Q4/2008 profit
 - FOLYAMATOSAN a 8. nyereséges negyedév
- 2.6 mld. SkypeOut perc beszélgetés
 - Negyedévente 60%-os növekedés



Miért éri meg a Skype-nak?

- Miért érte meg az eBay-nek 3.4 mld USD-t fizetni érte?
- Marketing hatásos, de nem magyarázza az árat
- \$45mill. Q4/2008 profit
 - FOLYAMATOSAN a 8. nyereséges negyedév
- 2.6 mld. SkypeOut perc beszélgetés
 - Negyedévente 60%-os növekedés
- Skype v4 február óta
 - Csak Windows (egyelőre)
 - Hang és videó minősége jobb
 - Architektúra, algoritmus ???
- A Microsoft 8.5 mld USD-t fizetett érte 2011-ben
 - Pedig az MSN messenger megoldása évtizedes múltra tekint vissza
 - Kiváltotta a Live Messenger és Lync szolgáltatásokat



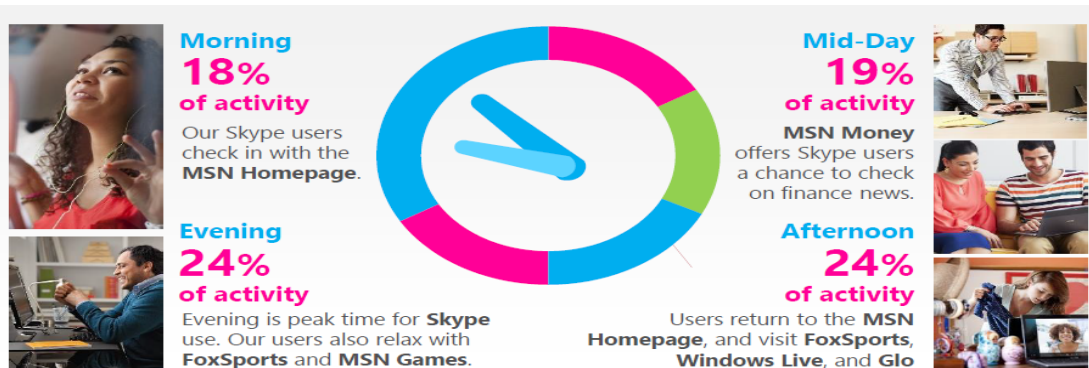
Skype Business Model



- Miből van pénzük, miért éri meg?
 - SkypeOut és SkypeIn előfizetések
 - Szerződés több ISP-vel
 - Naponta \$318.000 (2006 elején)
 - Szerződések gyártókkal
 - Headset, „skype-ready” mobil eszközök
 - A telefonálás ingyenes, de az Internetért fizetni kell
 - Több szolgáltatás, egyre több felhasználó (pl. DSL)
- Az eBay megvette 2005 végén
 - 2.6 milliárd dollár (készpénz, részvények)
 - További 1.5 milliárd ha bizonyos célszámokat elérnek

Skype by Microsoft

- 2011-ben felvásárolta a Microsoft
- 300 millió felhasználó (47 millió/US)
- 2016 óta már nem P2P!
 - Sok mobil kliens számára előnytelen a P2P modell (pl. folyamatos feltöltés)
 - Már úgyis sok „mega-supernode”-ot kellett üzemben tartani
 - A felhő alapú rendszerek már jól skálázódnak



Skype Business Model



- Skype és a Broadreach Networks – Voice over WiFi
 - Az egyik legnagyobb angol internet szolgáltató
 - 350 hotspot: repterek, vasútállomások, plázák, szállodák
 - Ingyenes Skype használat
 - A felhasználók a hagyományos internet szolgáltatásokért fizetnek
 - web, e-mail
- SkypeZones
 - Tesztelés alatt
 - WiFi hotspotok elérése olcsón (18.000 hotspot jelenleg)
- Spyware?
 - Hatalmas adatbázis, amit ki lehetne használni
 - Saját bevallásuk szerint nem teszik
 - A Kazaa híres volt a spyware-ekről

Skype protokoll

- Supernode
 - *slot-okba* vannak csoportosítva (9-10 supernode egy slotban)
 - *A slot-ok block-okba* vannak szervezve (8 slot egy blokkban)
- Jellemző rövidítések
 - SN (Skype Network) Skype hálózat
 - SC (Skype Client) Skype kliens, felhasználó, peer
 - HC (Host Cache)
- Egy SC jellemző funkciói
 - Bejelentkezés, regisztráció (login)
 - Keresés (user search)
 - Hívás kezdeményezés, végeztetés (start and end calls)
 - Média átvitel – video-kép-adat fájlok (media transfer)
 - Szöveges üzenetek, állapot kijelzés (presence messages)