“Odprtokodni oblak”

Opredelitev problema

- Oblak
  - Software as a service (SaaS, IaaS, PaaS)
  - Prednosti
    - Dostop kjerkoli, kadarkoli
    - Kolaboracija, funkcije “socialnega omrežja”
    - Enkratne posodobitve
    - Avtomatična sinhronizacija
    - Centralizacija podatkov → “big data”

[1] [2]

Opredelitev problema

- Oblak
  - Šibke točke
    - Centraliziran model → "Single point of failure"
    - Odvzem nadzora uporabniku
    - Kršenje vseh štirih svoboščin prostega programja
    - Vprašljiva zasebnost

"Software as a service always subjects you to the power of the server operator, and the only remedy is to avoid it."

Richard M. Stallman[1]

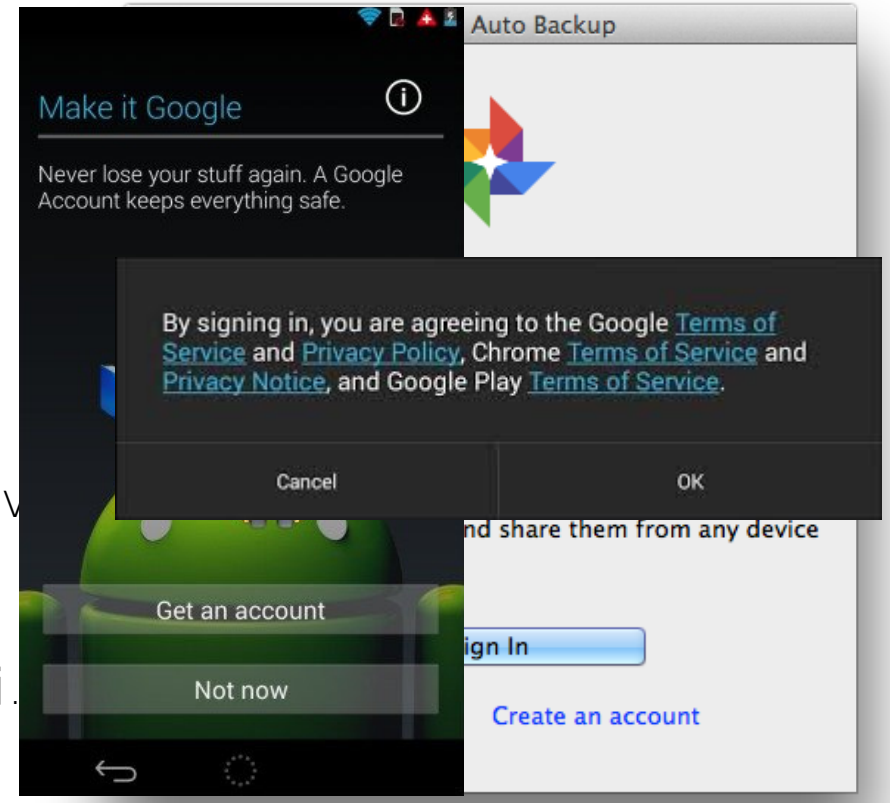
[1] Stallman, Richard (18. marec 2010). "Who does the server really serve?". Boston Revirew.

Opredelitev problema

- Ponudniki storitev v oblaku

- Pridobivanje povratnih informacij
- Izboljšave storitev

- **Invazivno** širjenje zaprtokodnih storitev[*]
- Poseg v uporabnikovo **zasebnost**.
- Izročitev in trženje z **osebnimi podatki**.



[*] Lastniška programska oprema, angl. Proprietary software.

Opredelitev problema

Tehnologija je odlično sredstvo, ki pa je lahko bodi si **uporabljeno**, bodi si **zlorabljeno**.

Žal kapital in korporacija marsikdaj prevladata nad pravicami posameznika.

Kaj storiti?

“Odprtokodni oblak”

- Lasten strežnik s prosto programsko opremo
  - Nadzor nad strojno opremo
  - Preverljiva programska oprema
  - Zaupanja vredna fizična lokacija
  - Uporabnik = Administrator

} OpenSaaS

“With great power comes great responsibility”

varnost – zanesljivost - zasebnost

Storitve v oblaku

- LAMP (spletni strežnik)
- DNS strežnik
- E-poštni strežnik

} OSNOVNE STORITVE

- Oddaljen dostop do datotek iz različnih naprav in operacijskih sistemov
- Urejanje dokumentov in pregled medijev na strežniku
- Spletni vmesnik za pošiljanje e-pošte
- Inicializacija prenosov na daljavo
- Samodejne varnostne kopije
- Avtomatična sinhronizacija

OBLAK

- Sinhronizacija zaznamkov, računov in bralnega seznama (brskalnik)
- Sinhronizacija telefonskega imenika
- Sinhronizacija SMS sporočil
- Sinhronizacija koledarjev
- Sinhronizacija opravil
- Sinhronizacija beležk

PIM

- Medijski strežnik na lokalnem omrežju
- Omrežni disk (NFS, SMB/CIFS)
- Krmiljenje naprav na lokalnem omrežju

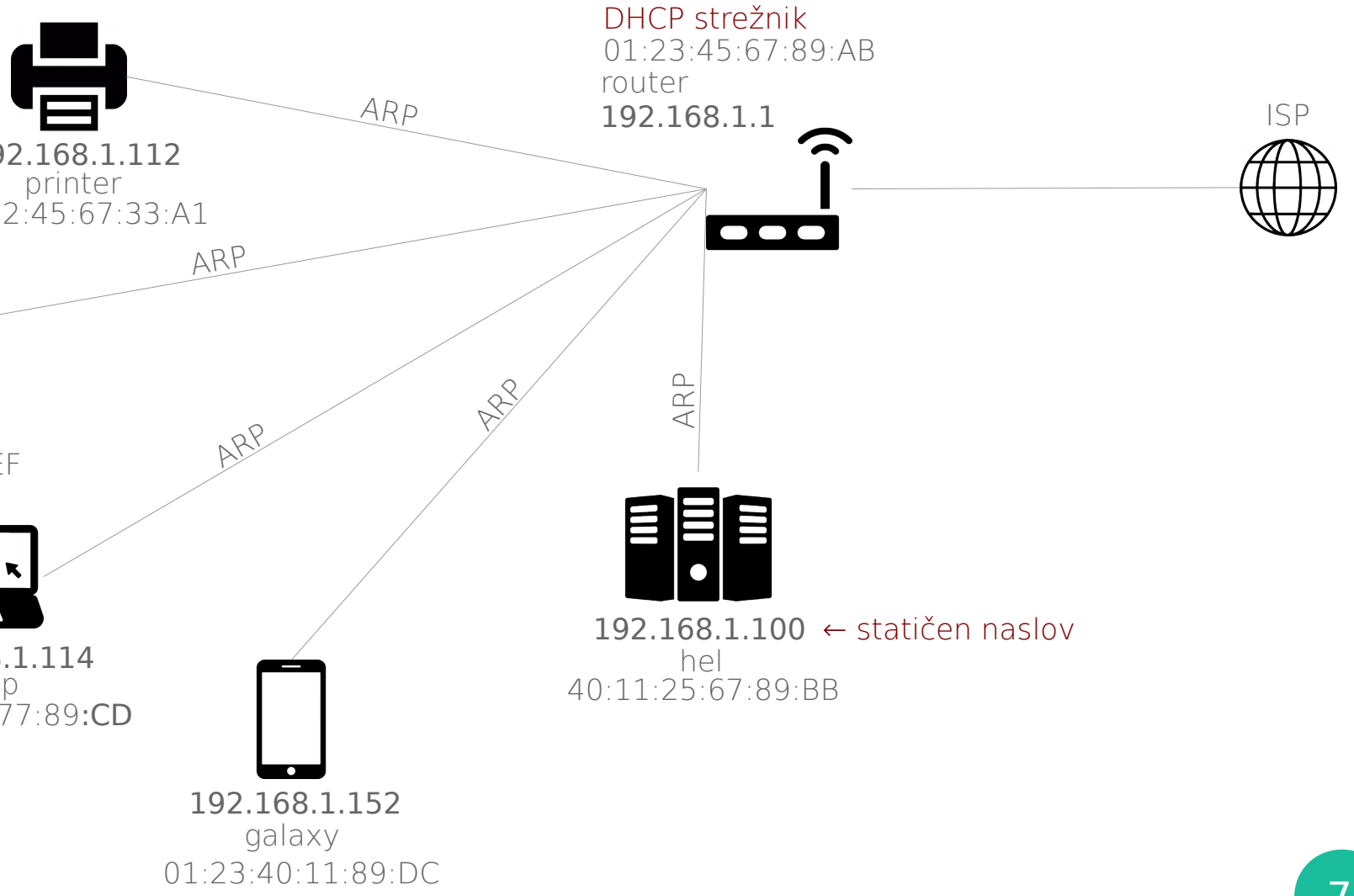
} LOKALNE STORITVE

...

Lokalno omrežje (LAN, IPv4)

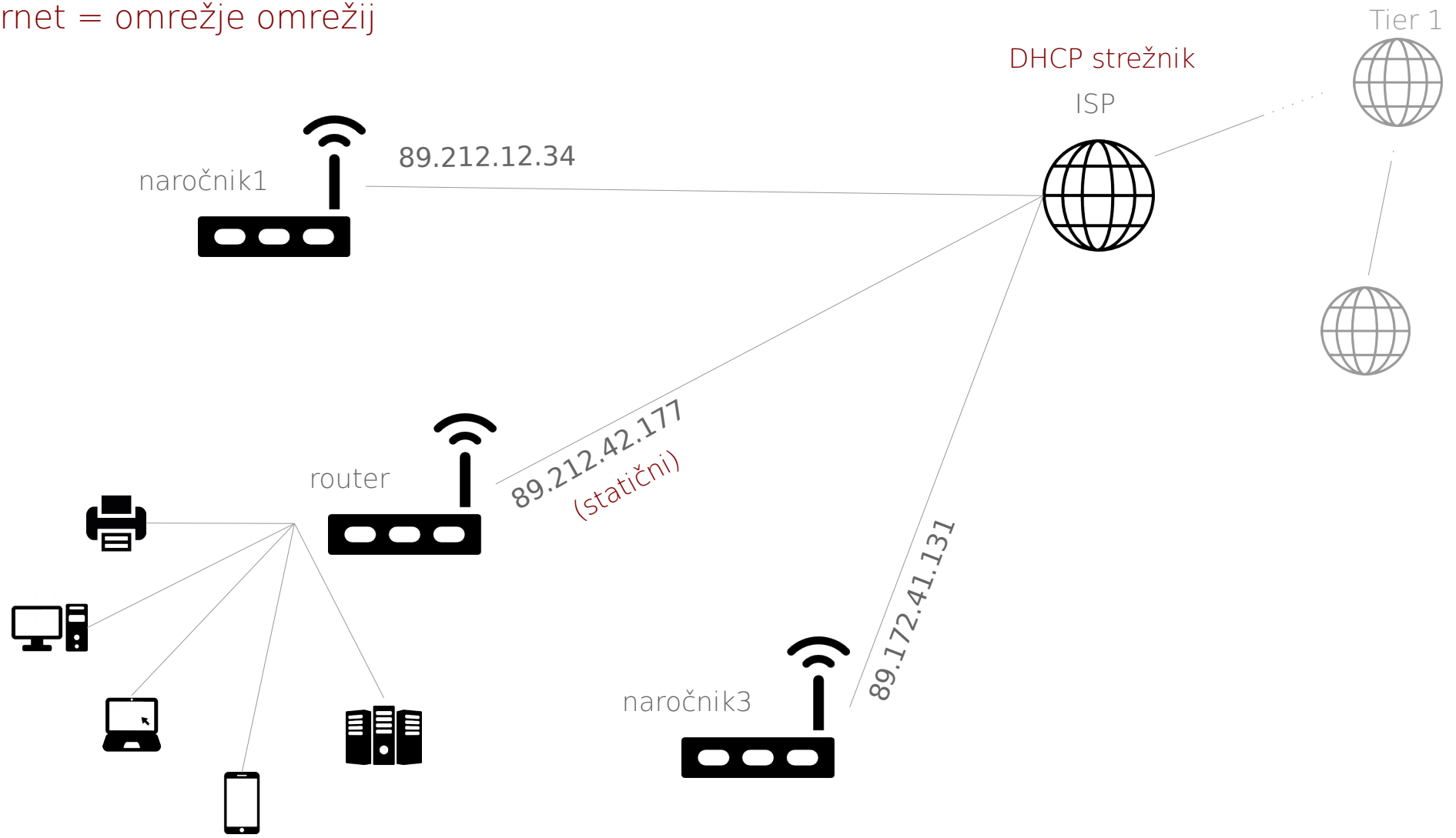
Zasebna (lokalna) IP območja:

- 10.0.0.0
- 172.16.0.0
- 192.168.0.0

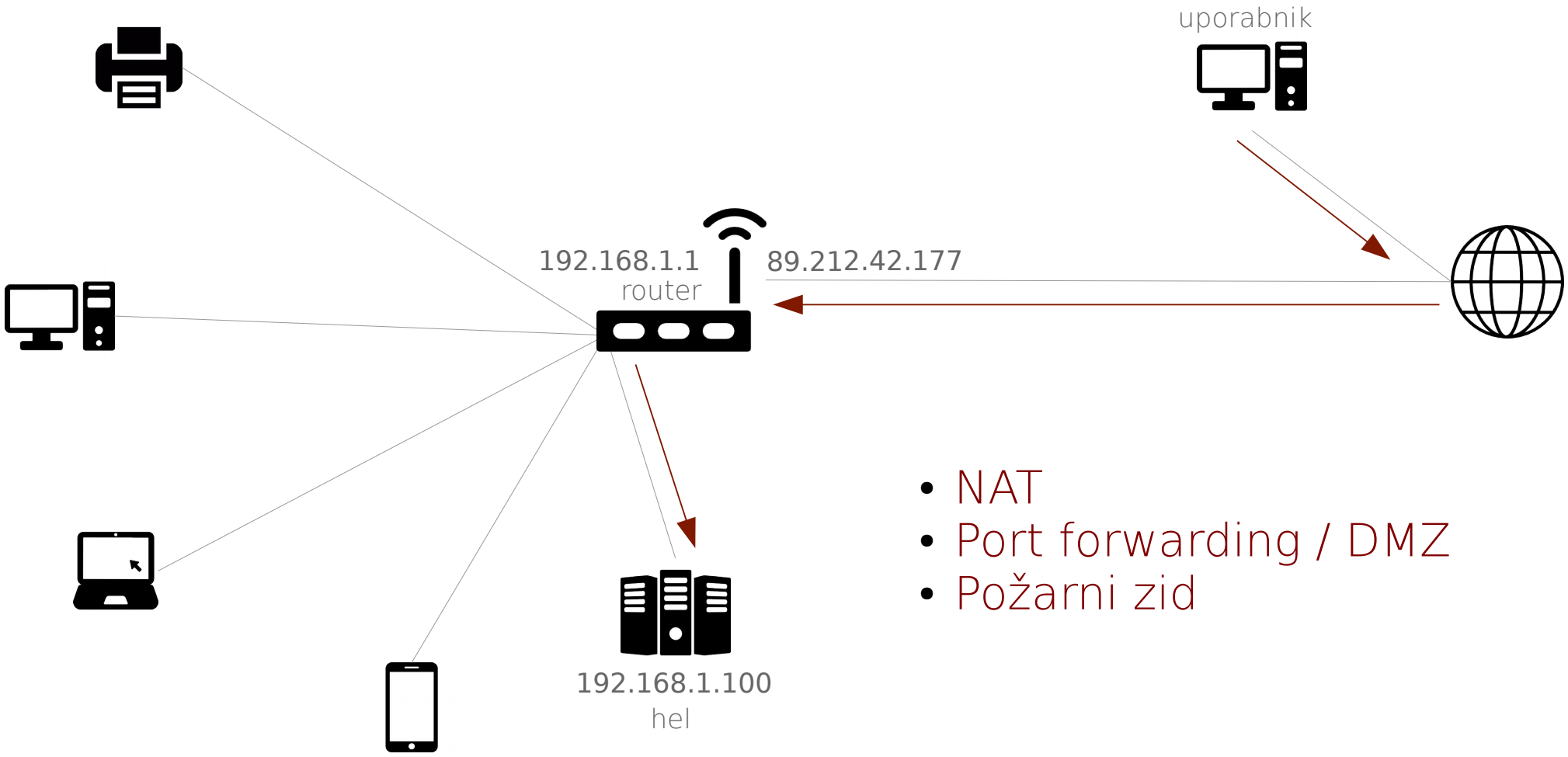


WAN omrežje (IPv4)

- Internet = omrežje omrežij



Translacija IP naslovov (IPv4)



- NAT
- Port forwarding / DMZ
- Požarni zid

Nekaj besed o ~~prihodnosti~~ (IPv6)

- Naslovni prostor IPv4 je premajhen (32 bitov)
- Standard IPv6 ponuja 128 bitov za naslavljanje
  - Teoretično bi to pomenilo 2^{128} IP naslovov

Kaj to pomeni za nas?

- Za IPv6 naslov moramo zaprositi
- Uporabniku ni dodeljen en naslov, temveč celotno podomrežje
  - Zasebni uporabniki običajno prejmejo subneto z masko /64
- IPv6 podpira avtomatično konfiguracijo (SLAAC)
  - Poskrbeti moramo za "Privacy Extension"
- DHCPv6 se za naslavljanje ne sklicuje na MAC, temveč na DUID
- NDP namesto ARP (usmerjevalniki potrebujejo RAdvd)
- Vsi IPv6 naslovi so javni (izjema link-local) → NAT ne obstaja

Predlogi strežniških operacijskih sistemov

Usmerjevalnik

WARNING: Security warning: unpatched http/tftp backdoor in **original** firmware: http://sekurak.pl/tp-link-httptftp-backdoor/

- Je pravzaprav miniaturna GNU/Linux distribucija
- …kih paketov (opkg)
- …nikom

History of the bug

12.02.2013 – TP-Link e-mailed with details – no response

22.02.2013 – TP-Link again e-mailed with details – no response

12.03.2013 – public disclosure

14.03.2013 – UPDATE: contact from TP-Link Poland. They asked for some more detailed information. Additional PoC sent.

15.03.2013 – UDPATE: confirmation of the issue (it is WAN exploitable if h… available from WAN side)

```
 W I R E L E S S   F R E E D O M
-----------------------------------------------------
BARRIER BREAKER (14.07)
-----------------------------------------------------
 * 1/2 oz Galliano         Pour all ingredients into
 * 4 oz cold Coffee        an irish coffee mug filled
 * 1 1/2 oz Dark Rum       with crushed ice. Stir.
 * 2 tsp. Creme de Cacao
-----------------------------------------------------
```

- LibreWRT
- DD-WRT
- Tomato

} Odprtokoden le backend

Predlogi strežniških operacijskih sistemov

Strežnik

- Izbirni kriteriji
  - Podpora za našo strojno opremo
  - Dolžina programske izdaje (release cycle)
  - Količina programskih paketov v repozitorijih
  - Podpora storitev, ki jih bomo uporabljali
  - Stabilnost

V vseh pogledih najboljše distribucije ni!

Predlogi strežniških operacijskih sistemov

Strežnik

Distribucija	CentOS	debian	fedora	ubuntu	archlinux
Ključne lastnosti	Stabilen; Zanesljiv; Namenjen strežnikom; Konservativna politika zagotavlja stabilnost, a starejšo programsko opremo.	Stabilen; Zanesljiv; Veliko programskih paketov; Odličen package manager. Zelo konservativen	Posodobljene različice programske opreme; Posledično nekoliko manjša stabilnost; Veliko paketov;	Osnovan na Debianu; Dobra podpora in velika količina gradiva; Primeren za začetnike; Ni v celoti prosta programska oprema!	Najnovejša programska oprema; Rolling release; Predaja uporabniku popoln nadzor nad sistemom; Posodobitve vedno zahtevajo uporabniško intervencijo;

Nasveti glede namestitve sistema

- Virtualizacija
  - Je danes standard pri postavljanju strežnikov
  - Tehnologije: KVM, Xen, OpenVZ, LXC, Docker ...
  - Omogoča sočasno izvajanje več OS na isti strojni opremi
  - Separacija virtualiziranih strežnikov lahko pripomore k varnosti
  - Virtualna strojna oprema (omrežni vmesniki)

Nasveti glede namestitve sistema

- Izkoristite LVM *(Logical volume management)*
  - Omogoča kasnejše prilagajanje particij (on-line)
  - Ponuja snapshote (olajša varnostno kopiranje)
  - Posamezno logično enoto lahko razpnemo preko večih fizičnih diskov
- Šifriranje diska
  - Zaščita zasebnosti v primeru zasega/tatvine naprave
  - Potrebna je implementacija daljinskega odklepanja (Dropbead SSH → initrd)
  - *Standardna implementacija (LUKS) ne ščiti podatkov pred vdori v strežnik, ko je ta v teku!*

Varnostne kopije, redundanca

- Varnostno kopiranje
  - GNU/Linux → datoteke, direktoriji
  - LVM Snapshoti (ločen root)
  - Nizkonivojsko kopiranje (dd, ddrescue)
  - Kopije posameznih datotek (rsync)
  - Celovite rešitve (Bacula)

- Redundanca
  - Podatkovni nivo: RAID
  - Omrežni nivo: HAProxy
  - Primer odpovedi strežnika → sekundarni strežnik

Domena

- Domena je "kazalec" na IP naslov strežnika
  - Primer: rabzelj.si → 89.212.42.177
- Zapisi the kazalcev se nahajajo na DNS strežnikih

Zakup domene

- Vsaka domena je unikatna, zato jo je potrebno zakupiti
- Zakup opravimo pri registrarju
  - Informativno: cene domen v .si coni se gibljejo okoli 10€/leto
  - Pozor: zakup domene navadno ne vključuje DNS gostovanja

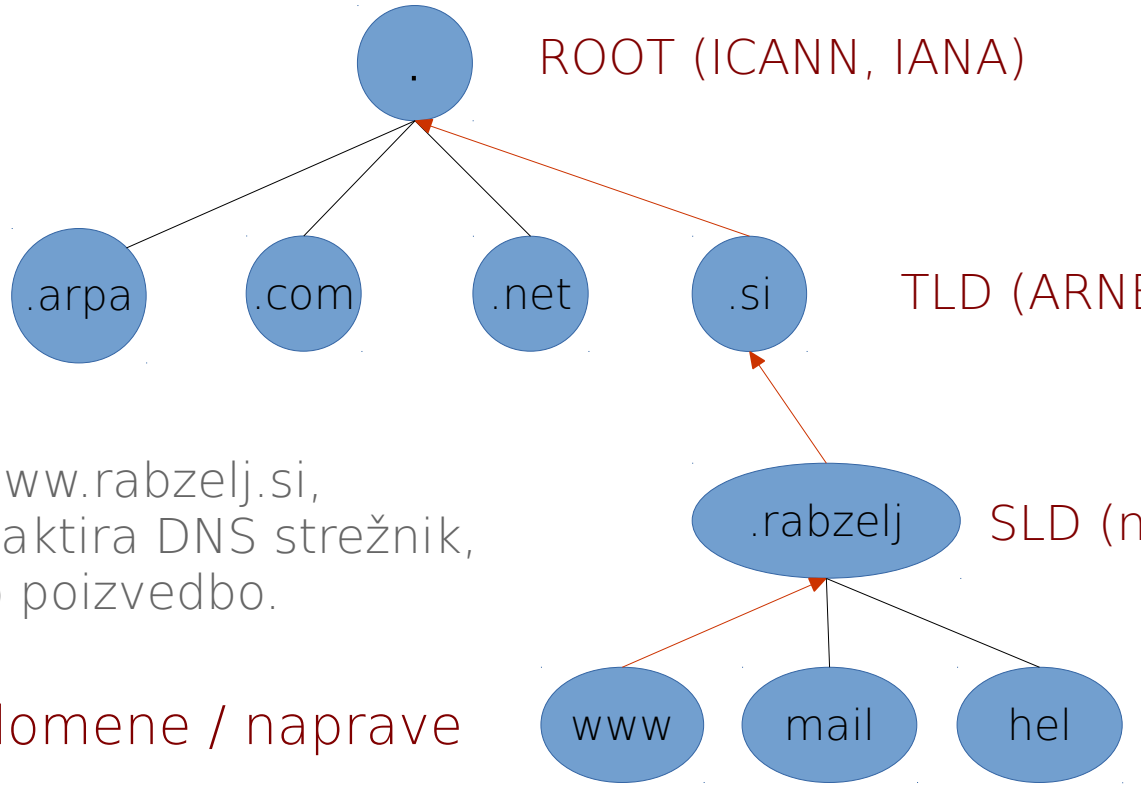
Možne alternative

- Brezplačne domene (.tt, .tk, ...)
- Dinamični DNS (no-ip.org, ...)

} Tuje storitve!

DNS (Domain Name System)

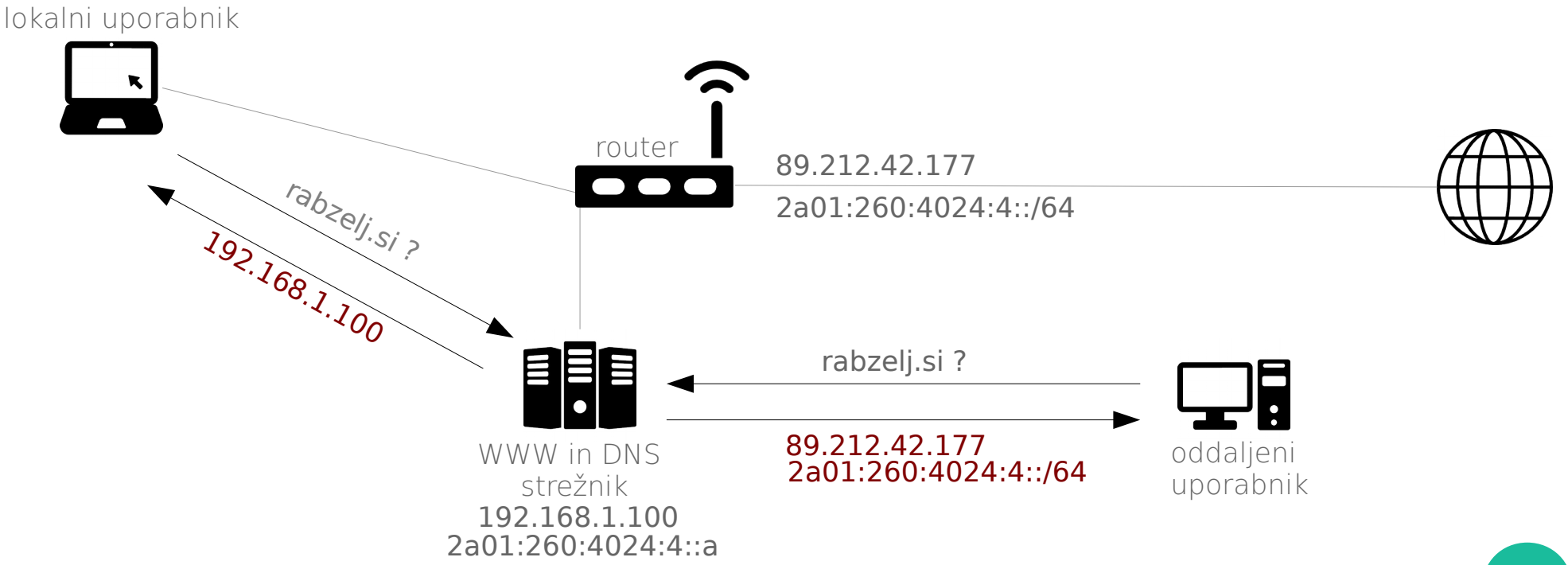
- Skrbi za razreševanje domen v IP naslove in obratno
- Za pravilno delovanje potrebuje natančno določeno strukturo



Ko navigiramo na www.rabzelj.si,
naš računalnik kontaktira DNS strežnik,
ki opravi rekurzivno poizvedbo.

DNS (Domain Name System)

- Split-horizon / Brain-split DNS
  - Naš DNS strežnik ne opravlja rekurzivnih poizvedb (obremenitev)
  - Kategorizacija klientov glede na njihovo omrežje
  - Lokalnim klientom postrežemo z lokalnimi IP naslovi



DNS (Domain Name System)

- Priporočen DNS strežnik za okolje GNU/Linux
  - BIND *(Berkeley Internet Name Domain, named)*
    - De facto standard DNS strežnikov
    - ISC licenca (kompatibilna z GNU GPL)
    - Urejanje DNS con z besedilnimi datotekami

- Alternative
  - djbdns
  - MaraDNS
  - DNS gostovanje – *tuje storitve!*
    - vaš registrar
    - dns.siel.si, freedns.afraid.org (brezplačno)

LAMP

- Linux, Apache, MySQL/MariaDB, PHP/Pearl
  - Najbolj razširjen sklop programske opreme spletnega strežnika
  - Podlaga za spletne aplikacije (večina ostalih storitev)
  - Združljivost posameznih programskih paketov

- Alternative
  - Spletni strežniki:
    - Nginx
    - Lighthttpd
  - Baze podatkov:
    - PostgreSQL
    - SQLite
    - LDAP
  - Skripti jeziki:
    - JavaScript (Node.js)

E-poštni strežnik (Virtual User Mail System)

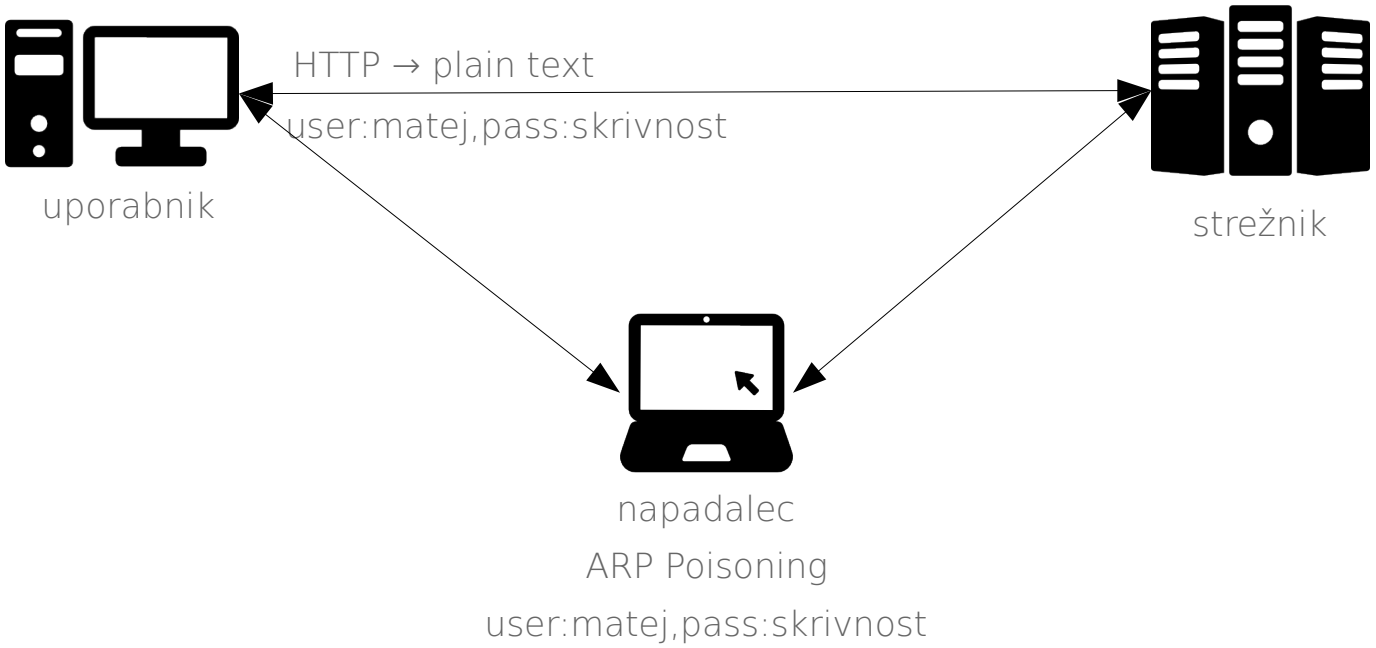
- Za najboljšo uporabniško izkušnjo uporabimo kombinacijo storitev
  - Postfix ali Exim (SMTP)
  - Dovecot ali Cyrus (IMAP)
  - Amavisd-new (ClamAV, SpamAssassin)
  - DNSBL, ZEN (Spamhaus)
  - Roundcubemail, Rainloop, Squirrelmail (Webmail)

- Upoštevamo RFC priporočila
  - HELO
  - SPF
  - DKIM
  - Obvezna domena in statični IP
  - Reverzni DNS (PTR na FQDN)

Nastavitev je zamuda in kompleksna, zato lahko posežemo po že pripravljenih programskih paketih (npr.: iRedMail).

Varna povezava

- MITM (Man In The Middle)



Varna povezava

- Uporaba varnih protokolov
  - HTTP → HTTPS
  - FTP → SFTP, FTPS
  - …
- Šifritanje prometa
  - TLS/SSL
  - VPN
  - …
- Certifikati
  - Self-signed
  - Nakup, ~~StartSSL~~ Let's Encrypt
  - Web-of-trust

Kolaborativi in PIM projekti

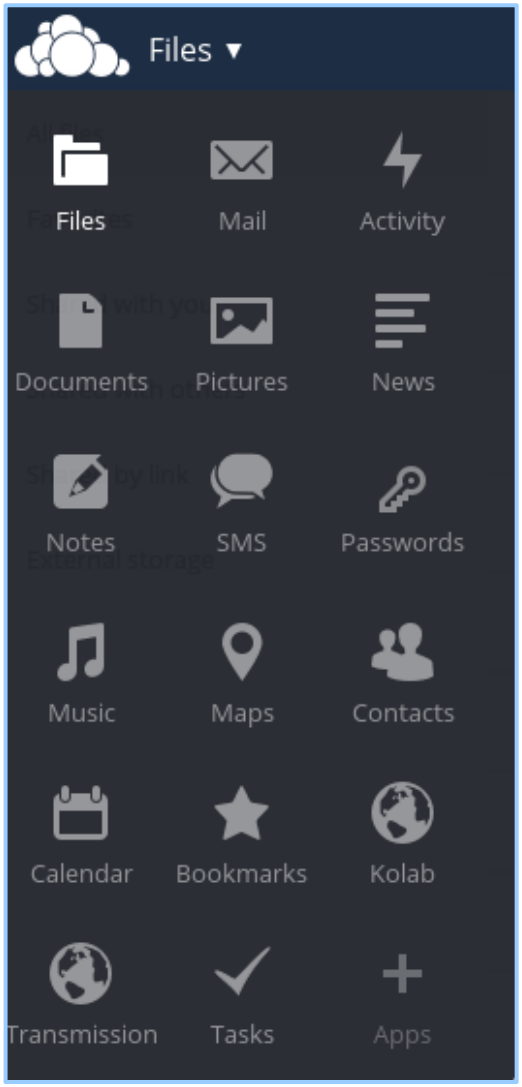
KOLAB

COLLABORATE IN CONFIDENCE

- Vrhunska "groupware" programska oprema
- Integriran odličen e-poštni strežnik
- Pokriva celoten sklop PIM (Koledarji, Imenik, Beležke, Opravila)
- Odjemalec, ki deluje na večih platformah (Kontact)
- Ni primeren za shranjevanje večjih količin datotek!

- Alternative
  - Zimbra
  - Horde
  - SOGo
  - phpGroupware
  - Citadel
  - Open-eXchange

~~ownCloud~~ Nextcloud



- Izredno razširljiva spletna aplikacija
- Zelo preprosta namestitev
- Upravljanje z datotekami in dokumenti
- Odjemalci za vse najpopularnejše platforme

- Alternative
  - Seafile
  - Pydio
  - Sparkleshare

Sinhronizacija brskalnika

- Firefox Sync
  - Omogoča postavitev lastnega strežnika za sinhronizacijo
  - Strežnik sestoji iz treh komponent
    - Strežnik Firefox računov
    - Shramba podatkov brskalnika
    - API, ki ju povezuje

Sinhronizacija zgodovine, zaznamkov, računov, odprtih zavihkov, vtičnikov in bralnega seznama

- Alternative
  - Wallabag

Ostale storitve

- Prenašanje datotek
  - Transmission, Deluge
  - PyLoad



- Spletna administracija strežnika
  - Ajenti, ISPConfig

- Simbolično in numerično računanje v oblaku

SageMathCloud™ collaborative computational mathematics

SageMath, IPython, LaTeX, and terminals in your browser

- Zaščita izgubljenih naprav
  - Prey

Storitve v lokalnem omrežju

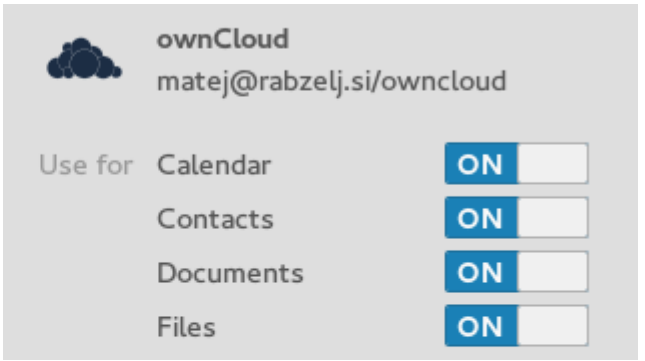
- Centralizirana shramba (NFS, SMB/CIFS)
- Medijski strežnik (UPnP PS3 Media Server)
- Print server
- Wake-On-Lan
- OpenELEC (RaspberryPi)
- Sekundarni usmerjevalnik

openelec
embedded linux entertainment center

Odjemalci

- Android (AOSP, CyanogenMod)
  - K-9 Mail
  - Mirakel
  - MyOwnNotes
  - ownCloud
  - Wallabag
  - Just Player
  - DAVdroid
  - ownCloud-SMS
  - pyLoad
  - Firefox
  - Transdroid
  - VLC
  - DeskCon
  - KDE Connect
  - …

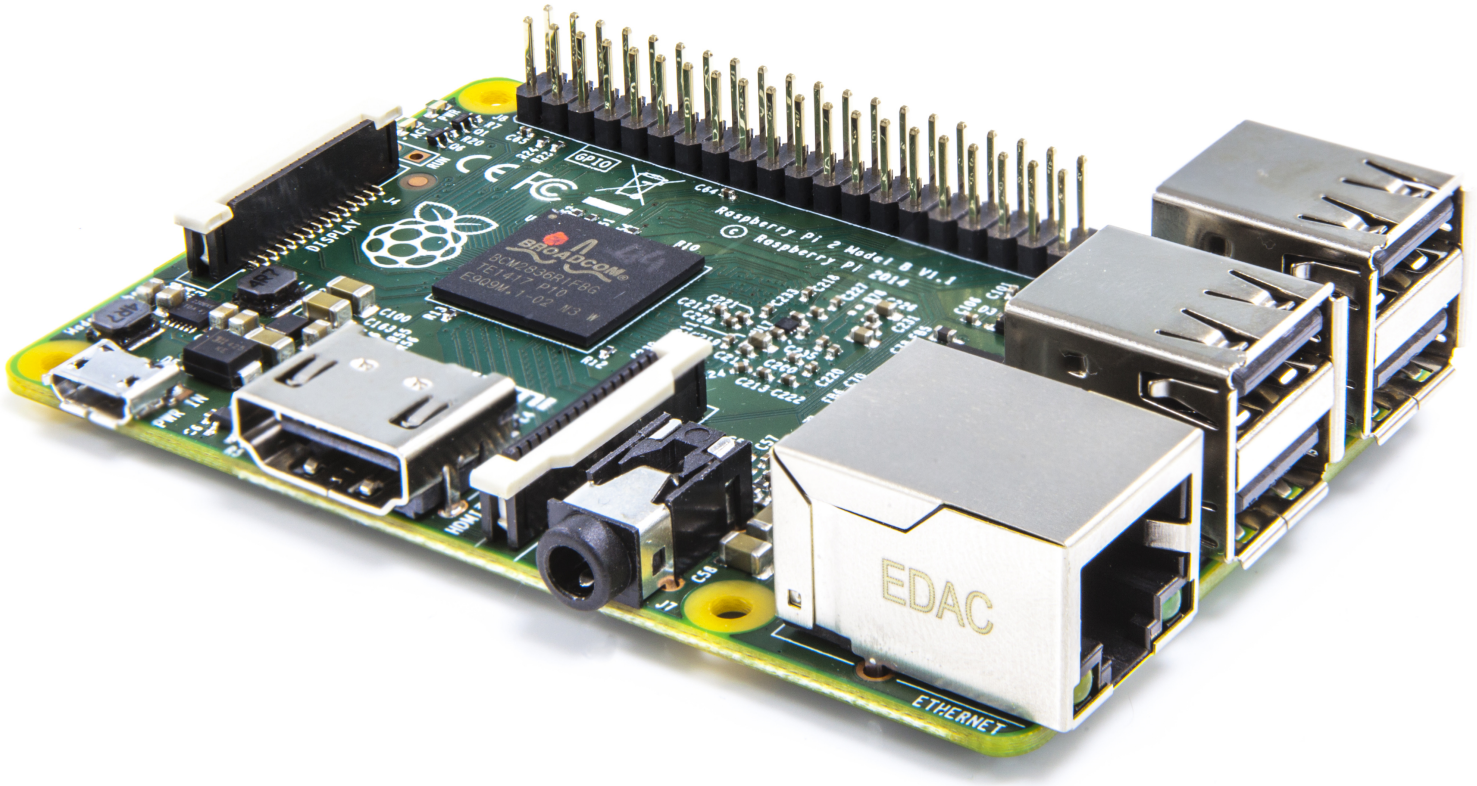
- GNU/Linux
  - ownCloud
  - ownCloud GNOME
  - Evolution
  - KMail
  - Kontact (Kolab)
  - Firefox
  - …



Strojna oprema

Koliko procesorske moči v resnici potrebujemo?

Strojna oprema



Strojna oprema

Hvala za pozornost!