Sicurezza VOIP

Un’Introduzione

VOIP in Crescita

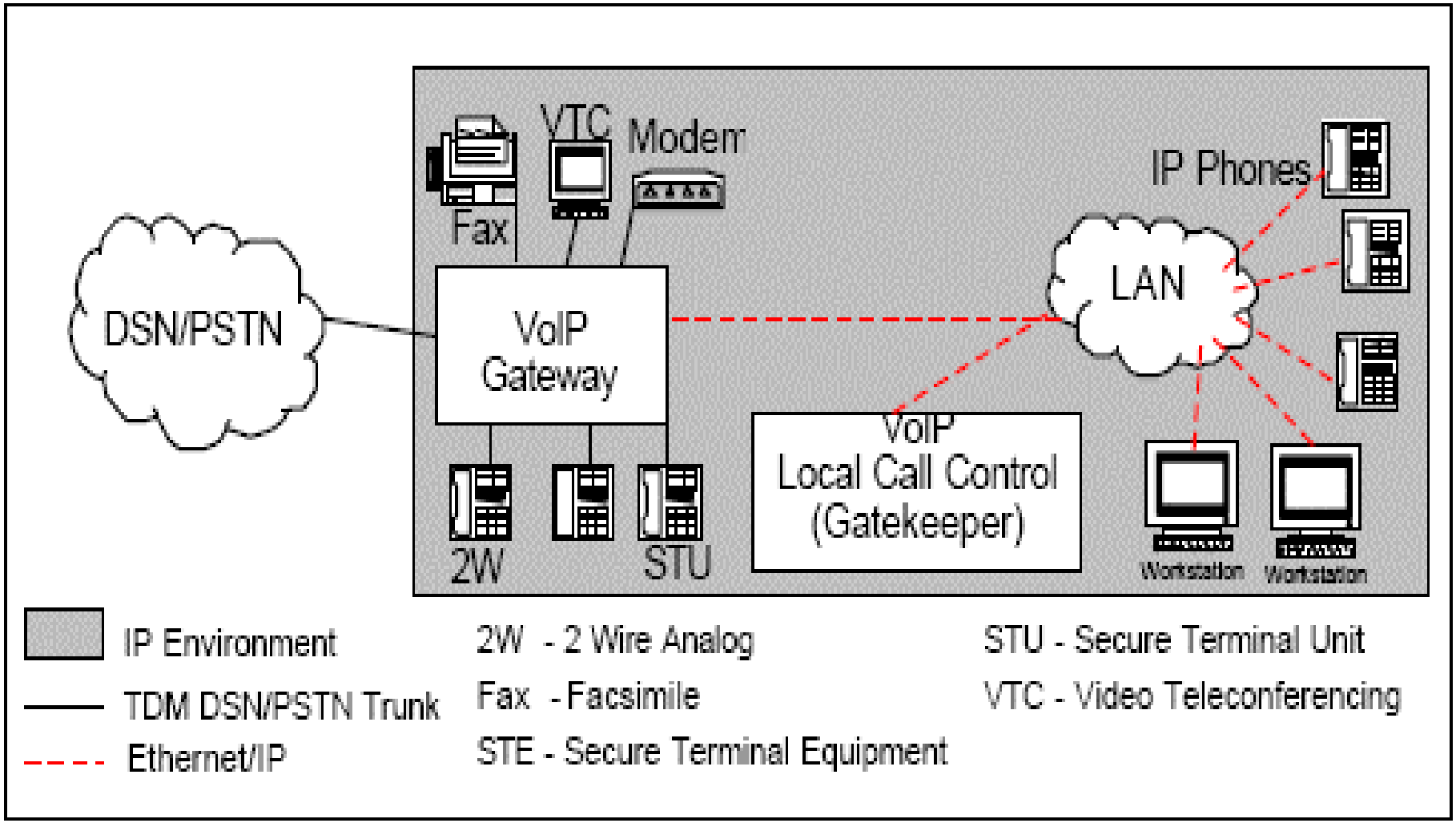
- VOIP è già ora un metodo di comunicazione molto popolare e sempre più lo diventerà
- Molti ISP e Telco cominciano a fornire servizi più o meno avanzati di telefonia VOIP
- Il traffico VOIP ha una alta aspettativa di confidenzialità, come tutto il traffico telefonico

Tipi di Telefono

- Softphone

- Hardphone

Tipica Architettura VOIP



VOIP: Attacchi

- Cattura del traffico di rete
- Bootp
- Vulnerabilità del telefono
- Attacchi alle interfacce di gestione

Attacchi: Conseguenze

- Ascolto o registrazione delle telefonate
- Inserimento di contenuto non autorizzato all'interno di una telefonata
- *Spoofing* del ID del chiamante
- Crash dei telefoni
- DOS
- Spamming

VOIP: Protocolli

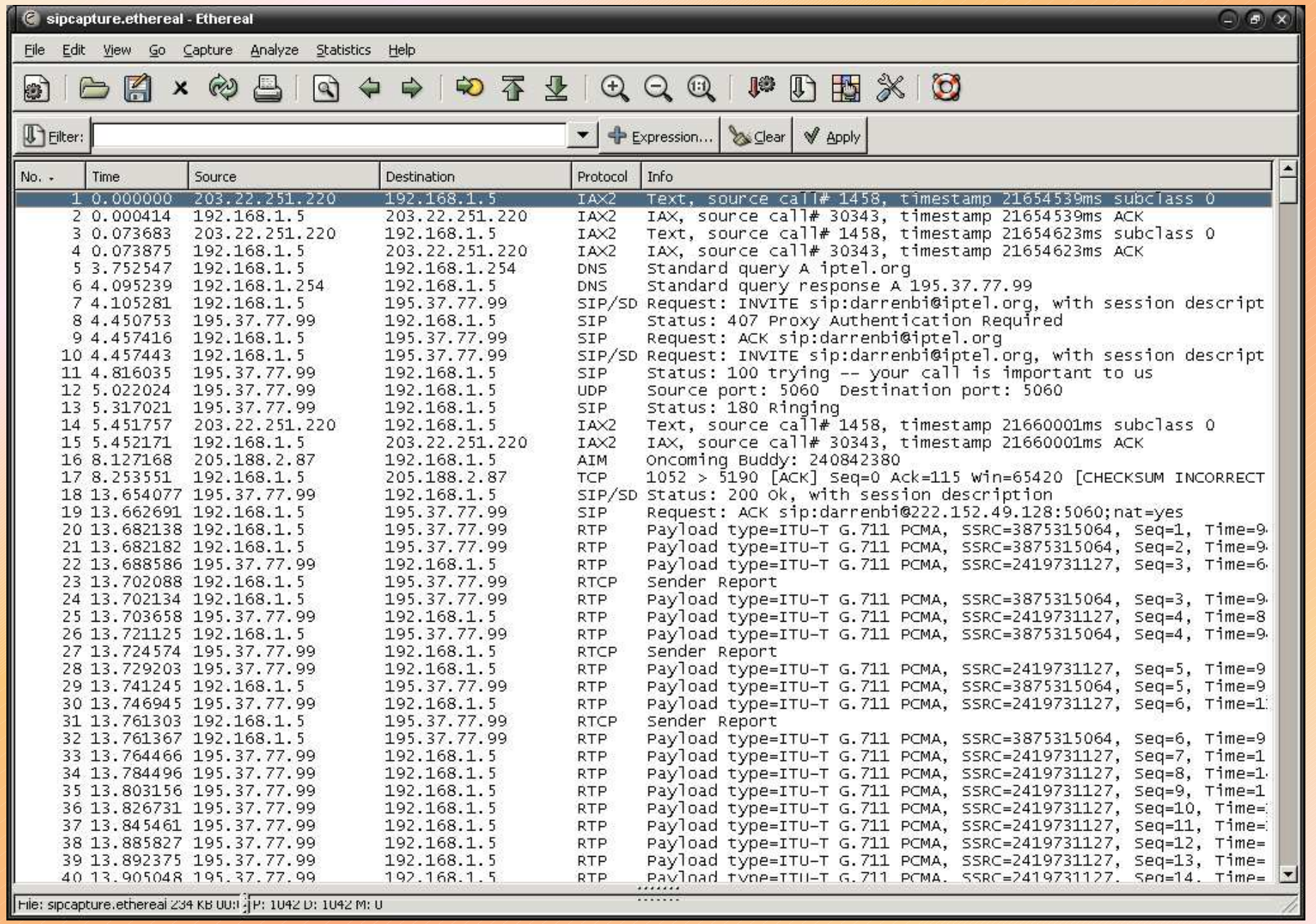
- H.323
  - Il protocollo più vecchio, ma ancora utilizzato
  - Fornisce metodi per la cifratura e l'autenticazione del traffico
- SIP
  - Autenticazione di tipo Digest basata su HTTP, ma molte volte risulta disabilitata
  - Non fornisce metodi di cifratura
- MGCP
  - Si basa sul protocollo IPSec per quanto riguarda la sicurezza, ma purtroppo la maggior parte dei telefoni non supporta IPSec

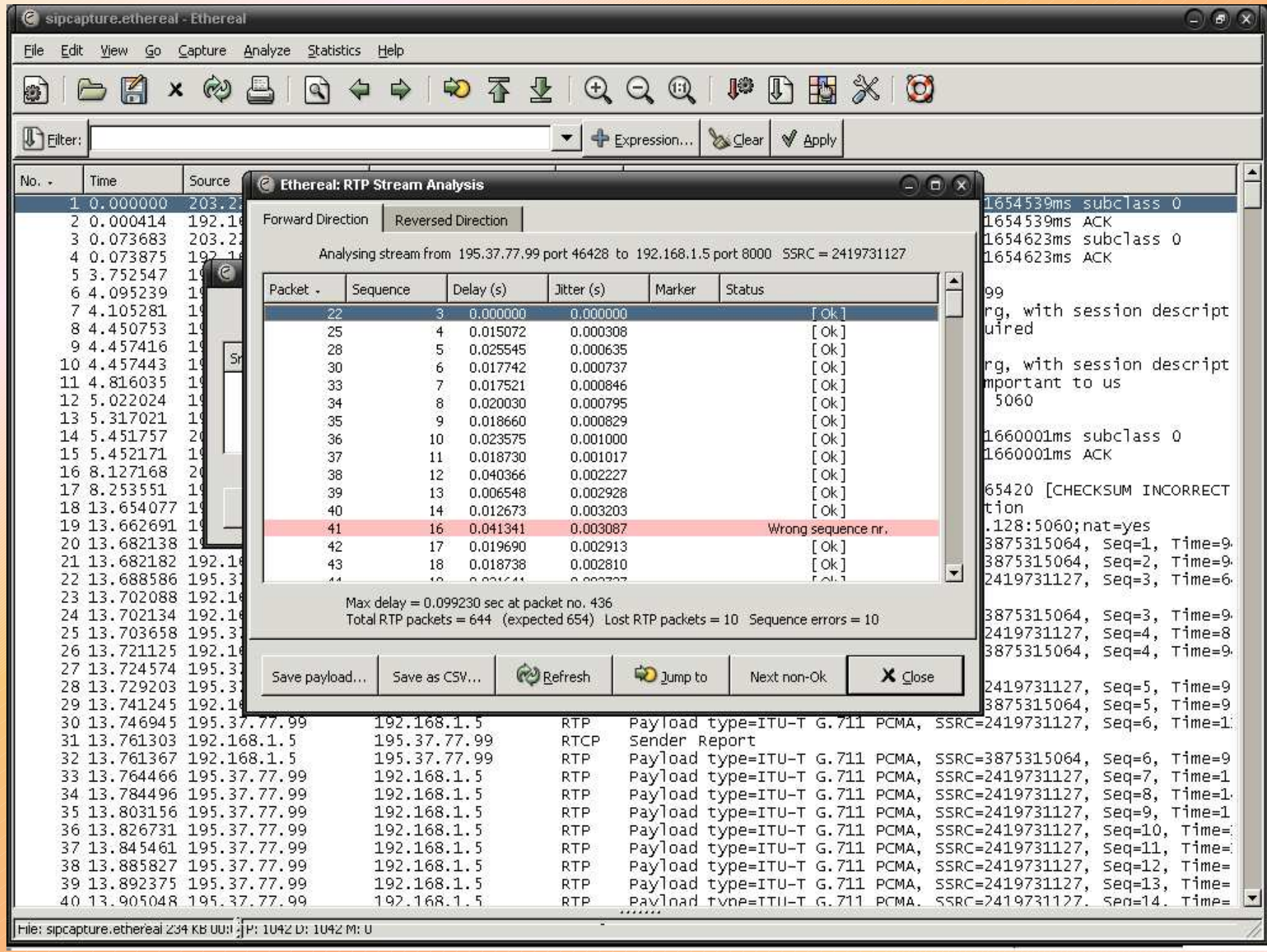
Uso delle VLANs

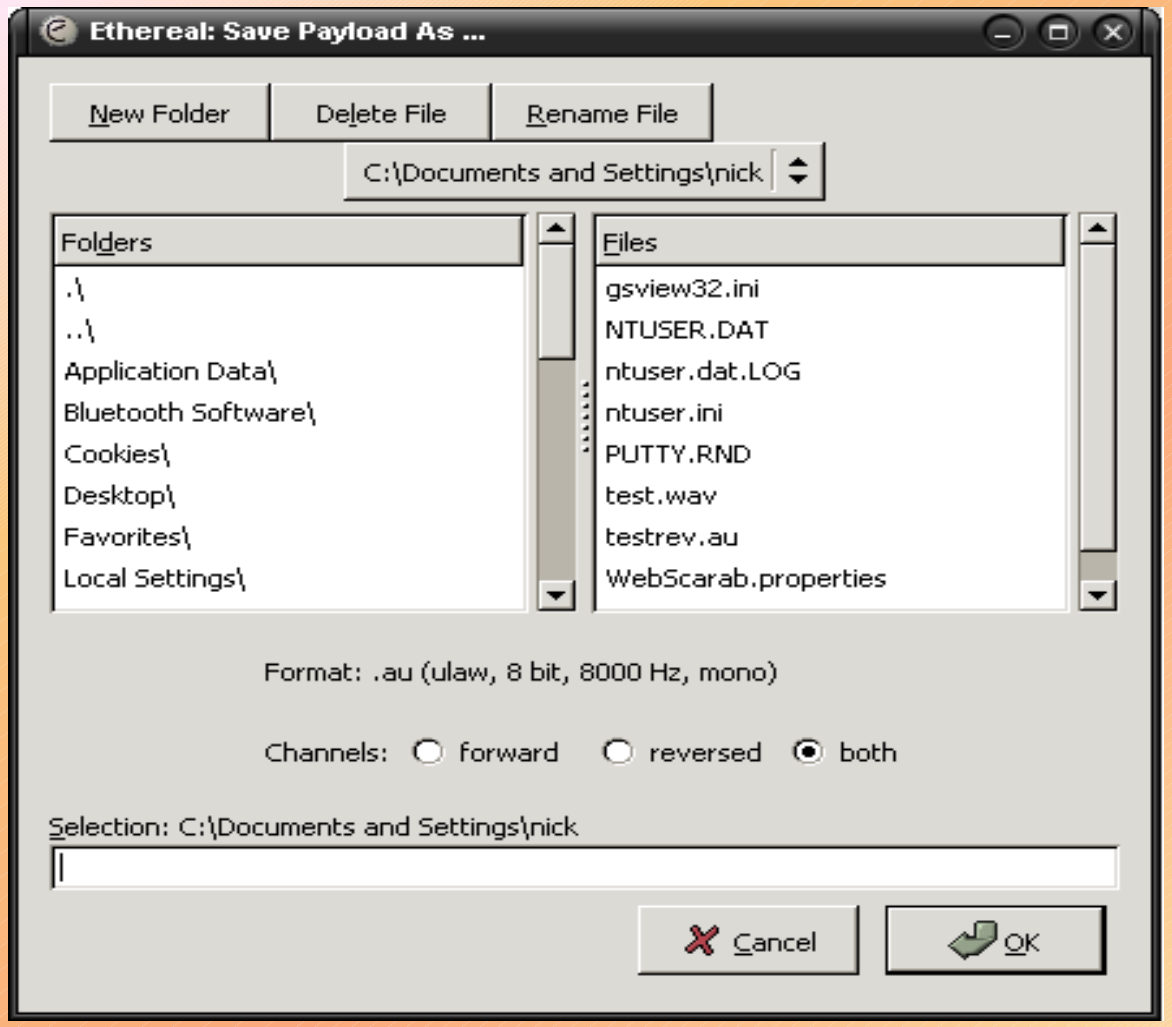
- Cisco raccomanda VLAN separate per il traffico voce ed il traffico dati
- MA…
- Molti telefoni VOIP consentono di condividere le connessioni di rete con i PC Desktop
- Inoltre, Voip permette l'uso di Softohones installati direttamente sui PC
- Perciò, a volte non si può separare il traffico voce dal resto della rete

VOIP: Cattura Traffico

- Ethereal ha il supporto per alcuni dei protocolli VOIP
- Permette quindi di catturare il traffico VOIP
- Ed anche di convertire tale traffico in un file .wav di tipo audio


sipcapture.ethereal - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 203.22.251.220 192.168.1.5 IAX2 Text, source call# 1458, timestamp 21654539ms subclass 0
2 0.000414 192.168.1.5 203.22.251.220 IAX2 IAX, source call# 30343, timestamp 21654539ms ACK
3 0.073683 203.22.251.220 192.168.1.5 IAX2 Text, source call# 1458, timestamp 21654623ms subclass 0
4 0.073875 192.168.1.5 203.22.251.220 IAX2 IAX, source call# 30343, timestamp 21654623ms ACK
5 3.752547 192.168.1.5 192.168.1.254 DNS Standard query A iptel.org
6 4.095239 192.168.1.254 192.168.1.5 DNS Standard query response A 195.37.77.99
7 4.105281 192.168.1.5 195.37.77.99 SIP/SD Request: INVITE sip:darrenbi@iptel.org, with session descript
8 4.450753 195.37.77.99 192.168.1.5 SIP Status: 407 Proxy Authentication Required
9 4.457416 192.168.1.5 195.37.77.99 SIP Request: ACK sip:darrenbi@iptel.org
10 4.457443 192.168.1.5 195.37.77.99 SIP/SD Request: INVITE sip:darrenbi@iptel.org, with session descript
11 4.816035 195.37.77.99 192.168.1.5 SIP Status: 100 trying -- your call is important to us
12 5.022024 195.37.77.99 192.168.1.5 UDP Source port: 5060 Destination port: 5060
13 5.317021 195.37.77.99 192.168.1.5 SIP Status: 180 Ringing
14 5.451757 203.22.251.220 192.168.1.5 IAX2 Text, source call# 1458, timestamp 21660001ms subclass 0
15 5.452171 192.168.1.5 203.22.251.220 IAX2 IAX, source call# 30343, timestamp 21660001ms ACK
16 8.127168 205.188.2.87 192.168.1.5 AIM Oncoming Buddy: 240842380
17 8.253551 192.168.1.5 205.188.2.87 TCP 1052 > 5190 [ACK] Seq=0 Ack=115 Win=65420 [CHECKSUM INCORRECT
18 13.654077 195.37.77.99 192.168.1.5 SIP/SD Status: 200 Ok, with session description
19 13.662691 192.168.1.5 195.37.77.99 SIP Request: ACK sip:darrenbi@222.152.49.128:5060;nat=yes
20 13.682138 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=1, Time=9
21 13.682182 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=2, Time=9
22 13.688586 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=3, Time=6
23 13.702088 192.168.1.5 195.37.77.99 RTCP Sender Report
24 13.702134 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=3, Time=9
25 13.703658 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=4, Time=8
26 13.721125 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=4, Time=9
27 13.724574 195.37.77.99 192.168.1.5 RTCP Sender Report
28 13.729203 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=5, Time=9
29 13.741245 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=5, Time=9
30 13.746945 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=6, Time=1
31 13.761303 192.168.1.5 195.37.77.99 RTCP Sender Report
32 13.761367 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=6, Time=9
33 13.764466 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=7, Time=1
34 13.784496 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=8, Time=1
35 13.803156 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=9, Time=1
36 13.826731 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=10, Time=
37 13.845461 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=11, Time=
38 13.885827 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=12, Time=
39 13.892375 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=13, Time=
40 13.905048 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=14, Time=
File: sipcapture.ethereal 234 KB 00:1 P: 1042 D: 1042 M: 0


sipcapture.ethereal - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source
Ethereal: RTP Stream Analysis
Forward Direction
Reversed Direction
Analysing stream from 195.37.77.99 port 46428 to 192.168.1.5 port 8000 SSRC = 2419731127
Packet Sequence Delay (s) Jitter (s) Marker Status
22 3 0.000000 0.000000 [Ok]
25 4 0.015072 0.000308 [Ok]
28 5 0.025545 0.000635 [Ok]
30 6 0.017742 0.000737 [Ok]
33 7 0.017521 0.000846 [Ok]
34 8 0.020030 0.000795 [Ok]
35 9 0.018660 0.000829 [Ok]
36 10 0.023575 0.001000 [Ok]
37 11 0.018730 0.001017 [Ok]
38 12 0.040366 0.002227 [Ok]
39 13 0.006548 0.002928 [Ok]
40 14 0.012673 0.003203 [Ok]
41 16 0.041341 0.003087 Wrong sequence nr.
42 17 0.019690 0.002913 [Ok]
43 18 0.018738 0.002810 [Ok]
Max delay = 0.099230 sec at packet no. 436
Total RTP packets = 644 (expected 654) Lost RTP packets = 10 Sequence errors = 10
Save payload... Save as CSV... Refresh Jump to Next non-Ok Close
30 13.746945 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=6, Time=1
31 13.761303 192.168.1.5 195.37.77.99 RTCP Sender Report
32 13.761367 192.168.1.5 195.37.77.99 RTP Payload type=ITU-T G.711 PCMA, SSRC=3875315064, Seq=6, Time=9
33 13.764466 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=7, Time=1
34 13.784496 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=8, Time=1
35 13.803156 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=9, Time=1
36 13.826731 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=10, Time=
37 13.845461 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=11, Time=
38 13.885827 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=12, Time=
39 13.892375 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=13, Time=
40 13.905048 195.37.77.99 192.168.1.5 RTP Payload type=ITU-T G.711 PCMA, SSRC=2419731127, Seq=14, Time=
File: sipcapture.ethereal 234 KB 00:1 P: 1042 D: 1042 M: 0


Ethereal: Save Payload As ...
New Folder
Delete File
Rename File
C:\Documents and Settings\nick
Folders
.\
..\
Application Data\
Bluetooth Software\
Cookies\
Desktop\
Favorites\
Local Settings\
Files
gsview32.ini
NTUSER.DAT
ntuser.dat.LOG
ntuser.ini
PUTTY.RND
test.wav
testrev.au
WebScarab.properties
Format: .au (ulaw, 8 bit, 8000 Hz, mono)
Channels: forward reversed both
Selection: C:\Documents and Settings\nick
Cancel
OK

Altri Tools

- Vomit
  - Inserisce file audio all’interno di una conversazione VOIP
- Tourettes
  - Inserisce parole a caso durante una conversazione VOIP

VOIP Phones

- Un’altra cosa da patchare !!!

- Esempio:
  - Inviando una richiesta POST di un solo byte all’interfaccia HTTP dell’adapter, viene rivelata la configurazione completa del telefono compresa la password dell’amministratore !!!

Caller *ID: Spoofing*

- Il Caller ID si basa su un Calling Party Number (CPN)
- Questo viene sempre inviato quando ha luogo una chiamata
- Un flag indica se è possibile per il ricevente verificare o meno il numero del chiamante
- Anche con i PBX classici era possibile lo spoofing del Caller ID, ma richiedeva una strumentazione sofisticata
- Con i PBX VOIP, lo spoofing è molto più facile