VoIP Security

Studenti: Angelo Reppucci matr. 0521/000728
Antonio Picardi matr. 0521/000730

Docente:
Alfredo De Santis

Anno accademico 2007/2008

Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Public Switched Telephone Network

- Progettate principalmente per trasmissioni vocali non per invio di dati.

- Costi di manutenzione per mantenere sicura la linea PSTN sono molto elevati.

PSTN e VoIP

- **Sebbene Internet condivida molti aspetti della PSTN, presenta alcune caratteristiche peculiari.**

- **Rete a commutazione di circuito ottimizzata per le comunicazioni vocali in sincrono e in tempo reale con una qualità di servizio garantita (QoS:Quality of Service).**

-

PSTN e VoIP

- Quando una comunicazione viene iniziata, si stabilisce un circuito fra la parte chiamante e quella chiamata. La PSTN garantisce la qualità del servizio (QoS) dedicando alla conversazione un circuito full-duplex con una larghezza di banda 64KHz.

- Tale larghezza di banda rimane inalterata indipendentemente dal fatto che le parti siano in conversazione attiva o in silenzio.

PSTN e VoIP(2)

- **Internet, invece, è una rete a commutazione di pacchetto e, storicamente, è sempre stata usata per applicazioni dove una QoS variabile poteva essere un parametro tollerabile (e-mail, ftp..).**

- **Le reti a commutazione di pacchetto non dedicano un circuito (a meno di non considerare i circuiti virtuali) tra le parti in conversazione , perciò non possono garantire la qualità del servizio.**

PSTN e VoIP(2)

- Per come sono strutturati i protocolli di comunicazione e per come è stata concepita Internet, il costo primario per un'applicazione di telefonia IP non è né la distanza né il tempo ma l'ampiezza di banda usata nella comunicazione.

- Il servizio a tali utenti è infatti fornito solitamente dagli ISP (Internet Service Provider) che gestiscono direttamente il costo delle connessioni.

Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Vantaggi del VoIP

- **Collegamento telefonico senza costi aggiuntivi rispetto alla connessione dati**
- **Integrazione delle applicazioni**
- **Flessibilità**
- **Condivisione degli apparati di rete tra servizi dati e voce.**
- **Semplificazione (utilizzo di un solo protocollo di rete – IP - per tutte le applicazioni permette di ridurre la complessità della rete ed aumentare la sua flessibilità).**
- **Applicazioni avanzate: sviluppo di applicazioni multimediali.**

Successo del VoIP

- **Dovuto alla crescente diffusione della banda larga, la possibilità di risparmiare sulle chiamate, i costi relativamente bassi delle attrezzature.**

- **Per quanto riguarda l'utente finale, la telefonia IP diventa dunque il mezzo per comunicare a distanze intercontinentali ai prezzi di una telefonata all'interno della locale rete PSTN.**

- **Soprattutto per questo motivo il mercato VoIP promette una crescita esponenziale per i prossimi anni in tutti i suoi principali settori.**

Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Implementazioni VoIP

- Ad oggi, le due maggiori suite di protocolli che caratterizzano VoIP sono SIP e H.323.

- H.323 definisce esplicitamente i protocolli di livello più basso della segnalazione;

- SIP invece è un application-layer control framework che definisce il carattere della chiamata in termini di servizi, indirizzi e caratteristiche di protocollo.

Implementazioni VoIP

- Oltre a questi due protocolli più importanti, VoIP si serve di altri protocolli come RTP,RTCP,STCP…

- Inoltre VoIP richiede altri protocolli, usati per garantire la QoS, per sincronizzare i clock, per permettere aggiornamenti firmware e software, monitorare le performance, tracciare rotte efficientemente.

Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Protocollo H.323

- H.323 e' uno standard della International Telecommunications Union-Telecommunications Standardization (ITU-T)

- E' uno standard che specifica le componenti, i protocolli e i meccanismi per la trasmissione di dati multimediali su reti a commutazione di pacchetto senza garanzie di qualità del servizio.

Componenti Architettura H.323

- **Terminal**

- **Gateway**

- **Gatekeeper**

- **MCU (Multipoint Control Unit)**

- **Border Elements**

Terminal

- Un H.323 terminal è il nodo finale della rete (endpoint) che consente la comunicazione audio (o opzionalmente video e dati) bi-direzionale con un altro H.323 terminal, gateway o MCU

Esempi:

- Telefono tradizionale
- Dispositivo IVR (Interactive Voice Response)
- Voicemail system
- “Soft phones” (es. NetMeeting)

MCU (Multipoint Control Unit)

- L'MCU fornisce il supporto per conferenze di più terminali H.323

- Contiene un "Multipoint Controller" (MC) che gestisce la segnalazione di chiamata e (opzionalmente) un "Multipoint Processor" (MP) che processa l'audio/video (ad esempio mixing dei media, conversione tra codec, etc)

- Gestisce chiamate in conferenza tra molteplici terminali/gateway
  - Il MC stabilisce quale formato di media va utilizzato (si deve avere compatibilita' mutua trai partecipanti)
  - Cio' avviene trasmetterndo ai partecipanti un capability set
  - Il capability set puo' essere cambiato dinamicamente dal MC in seguito a join/leave durante la conferenza

Gateway

- Il gateway ha la funzione di connettere una rete H.323 con un'altra non H.323, traducendo opportunamente i formati di trasmissione e le procedure di comunicazione.

- Un lato del gateway H.323 supporta segnalazione e media nei formati standard H.323. L'altro lato supporta segnalazione e media di una rete esterna (per esempio SS7 per la PSTN).
  Sul lato H.323, il gateway si comporta come un H.323 terminal, sul lato esterno, si comporta come una centrale telefonica.

- È composto da un "Media Gateway Controller" (MGC) e da un "Media Gateway" (MG).
  - MGC → gestisce la segnalazione
    - Q.931 / H.225.0
  - MG → gestisce l'audio
    - multiplex, rate matching, audio transcoding

Gatekeeper

- Il gatekeeper è indicato come elemento opzionale.

- Se presente, possiede le seguenti funzionalità:
  - Address translation (routing): determina l'indirizzo di destinazione di un endpoint H. 323 per una chiamata.
  - H.323 Alias → indirizzi IP (durante la registrazione del terminale)
  - "email-like" name & "phone number like" name
  - Admission control: determina se ad un endpoint è permesso o meno accedere al sistema.
  - Bandwidth control. Processa al minimo le richieste di banda.
  - Zone management.

Gatekeeper (2)

Funzionalità opzionali:

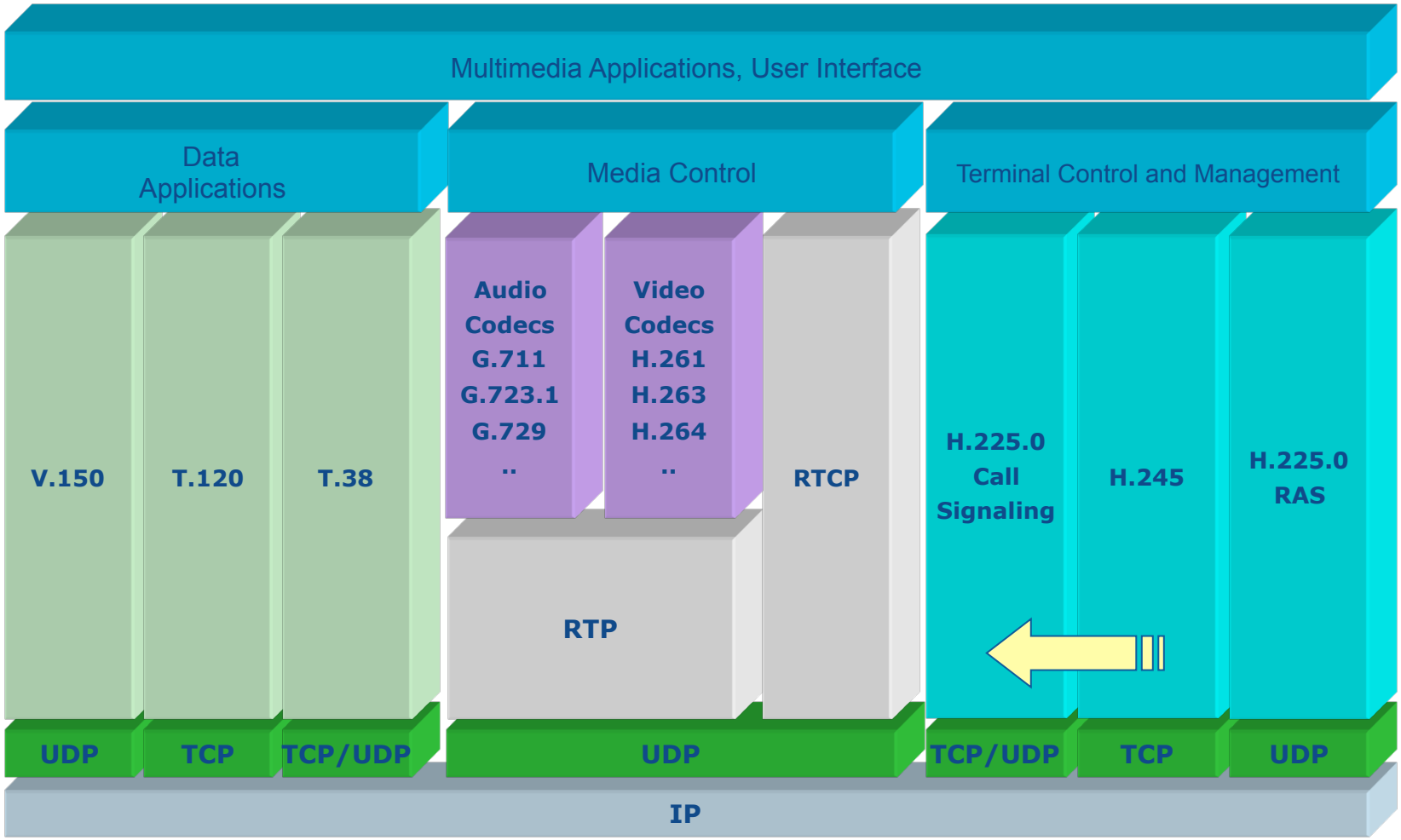
- **Call control signalling: gestione della segnalazione H.225/Q.931 tra endpoint H.323.**
- **Call authorization: concede o meno l'autorizzazione ad effettuare una chiamata utilizzando opportune policy (es. stato della sottoscrizione al servizio dell'endpoint)**
- **Bandwidth management: processa le richieste di banda utilizzando policy (es. condizioni della banda in quel momento)**
- **Call management: processa le richieste di chiamata usando policy (es. stato dell'endpoint)**
- **Gatekeeper management information (MIB).**
- **Bandwidth reservation: riserva la banda per quei terminali che non sono in grado di farlo.**
- **Directory services.**

Border Elements

- Scambiano informazioni sugli indirizzi e sono coinvolti nella call authorization tra diversi domini amministrativi (utilizzano o meno una clearing house).

- Possono aggregare informazioni sugli indirizzi per ridurre il volume del traffico dovuto ai messaggi di routing che passano in rete.

Stack H.323


Multimedia Applications, User Interface
Data Applications
Media Control
Terminal Control and Management
V.150
T.120
T.38
Audio Codecs G.711 G.723.1 G.729 ..
Video Codecs H.261 H.263 H.264 ..
RTCP
RTP
H.225.0 Call Signaling
H.245
H.225.0 RAS
UDP
TCP
TCP/UDP
UDP
TCP/UDP
TCP
UDP
IP

Protocolli VoIP

- H.225/Q.931 definisce la segnalazione per call setup e teardown,includendo indirizzo IP sorgente e destinazione, porte e informazioni sulla porta H.245
- H.225.0/RAS Specifica i messaggi che descrivono la segnalazione, Registration Admission and Status (RAS) e informazioni sugli stream media.
- H.245 specifica i messaggi che sono scambiati per determinare l'insieme delle capacità dei terminali, le relazioni master/slave, e l'informazioni del canale logico per gli stream media
- Real Time Protocol (RTP) descrive il trasporto END-to-END per i dati real time
- Real Time Control Protocol (RTCP) descrive il monitoring dell'END-TO-END della consegna dati e QoS.

Codecs G.700

- Per quanto riguarda i codecs, la serie G.700 dei codec usati per VoIP includono:
- G.711. Non usa compressione, così la qualità della voce è eccellente (stesso codec usato da PSTN e ISDN), consuma molta banda.
- G.723.1. Codec usato per la conferenza/videofonia sulle linee standard ed è ottimizzato per la codifica/decodifica veloce. (Qualità voce media)
- G.729 Usato principalmente per le applicazioni VoIP perchè richiede poca banda.

H.225/Q.931

- Definisce 2 importanti tappe per il setup della chiamata: Call signaling e RAS
- I messaggi sono codificati nel formato ASN.1 PER (Packed Encoding Rules)
- Inoltre , H.225.0 il canale per il signaling può essere implementato sul top dell'UDP.
- Vengono definiti i messaggi tra comunicazione endpoint-gatekeeper and gatekeeper-gatekeeper — questa parte di H.225 è conosciuta come RAS (Registration, Admission, Status), e rispetto alla fase di call signaling, gira su UDP.

H.245 Call Control Messages

- Dopo che la fase di setup è stata fatta il protocollo H.245 stabilisce canali logici tra gli endpoint mediante i quali e' possibile selezionare e parametrizzare i codec.
- H.245 viene usato tra gli endpoint di una connessione
- H.245 serve principalmente per gestire i media utilizzati
- Si deve per esempio verificare che entrambi i partecipanti dispongono di terminali in grado di capire i codec scelti.

Indirizzamento H.323

- Per ogni indirizzo di rete, una entita' H.323 ha uno o piu' Transport Service Access Points (TSAPs)
- Il TSAP identifica un canale logico (servizio) e funziona come un socket
- Quindi, dato un indirizzo IP ed una porta di servizio, se e' disponibile un DNS si puo' indirizzare il servizio tramite una URL (es.: ras://gatekeeper1@domain.com)
- In generale, e' opportuno fare in modo che tutti i device interni alla stessa area gatekeeper abbino lo stesso dominio nella URL
- Per comodita', all'interno di una zona si possono avere degli alias, che pero' vanno risolti correttamente nel relativo indirizzo IP
- La traslazione tra alias e indirizzi IP e' eseguita dal gatekeeper ed e' supportata dalla segnalazione RAS
- L'unico vincolo e' che un alias deve essere unico in una zona

Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

SIP (Session Initiation Protocol)

- SIP e' un'alternativa ad H.323, considerata molto buona
- E' uno standard della IETF ed e' utilizzato congiuntamente ad altri protocolli come il Session Description Protocol (SDP) , il Real Time Streaming Protocol (RTSP) e il Session Announcement Protocol (SAP)
- SIP e' un protocollo di segnalazione e gestisce il setup, tear down e gestione delle sessioni multimediali
- SIP e' in crescita e sempre piu' costituisce una alternativa valida ad H.323
- Nella rete IP, la messaggistica di controllo SIP passa su un canale logico distinto da quello dei media (analogamente ad H.323)

SIP (2)

- SIP definisce due categorie di entita':
  - client, denominato anche user agent client: è un'applicazione che invia richieste SIP
  - server: è un'applicazione che risponde a richieste SIP

- Una chiamata VoIP SIP ha come endpoint
  - un user agent client (che puo' essere un PC)
  - un user agent server

- Si definiscono quattro tipi di server
  - proxy server
  - redirect server
  - user agent server
  - registrar

Proxy Server

- Il proxy server agisce ricevendo richieste di connessione e gestendole, per esempio rinviandole ad altri server
- I messaggi gestiti dal proxy sono percepiti dai server destinatari come generati dal proxy stesso, piuttosto che da qualche applicazione nascosta dietro di esso
- Ovviamente, il proxy server riceve e trasmette richieste quindi ha sia un lato client che un lato server

Redirect Server

- Il redirect server riceve richieste SIP, mappa l'indirizzo del destinatario su un altro indirizzo (o piu' indirizzi) e restituisce i nuovi indirizzi al richiedente
- Il richiedente poi fara' la chiamata specificando il nuovo indirizzo
- Il redirect server non reinstrada le chiamate, ma traduce gli indirizzi

User agent server

- Tipicamente presente nei terminali d'utente
- Un terminale d'utente implementa sia il client che il server
- Il client viene usato per inviare richieste di chiamata
- Il server per ricevere richieste di chiamata e rispondere

Registrar

- Il registrar e' un server che accetta le richieste SIP REGISTER
- SIP prevede le procedure di registrazione di un utente (si come il gatekeeper in H.323)
- Le registrazioni sono comode per tracciare la posizione dell'utente e trasmettergli le richieste di chiamata
- La procedura di registrazione migliora il controllo sulla rete VoIP

Caratteristiche di SIP

- **SIP e' molto semplice e flessibile**
- **Non si occupa in dettaglio della negoziazione dei media, ci pensano gli utenti mediante campi appositi che sono adattabili e anche non-standard**
- **Un esempio e' il campo "subject" del messaggio INVITE:**
  l'utente puo' specificare, come in una mail, il motivo della chiamata e il chiamato puo' accettare o rigettare anche sulla base del subject
- **Altro esempio: la chiamata è per un utente in quel momento non raggiungibile, la risposta puo' contenere l'informazione che (ad esempio) l'utente chiamato sara' raggiungibile a partire dalle ore 16:00.**

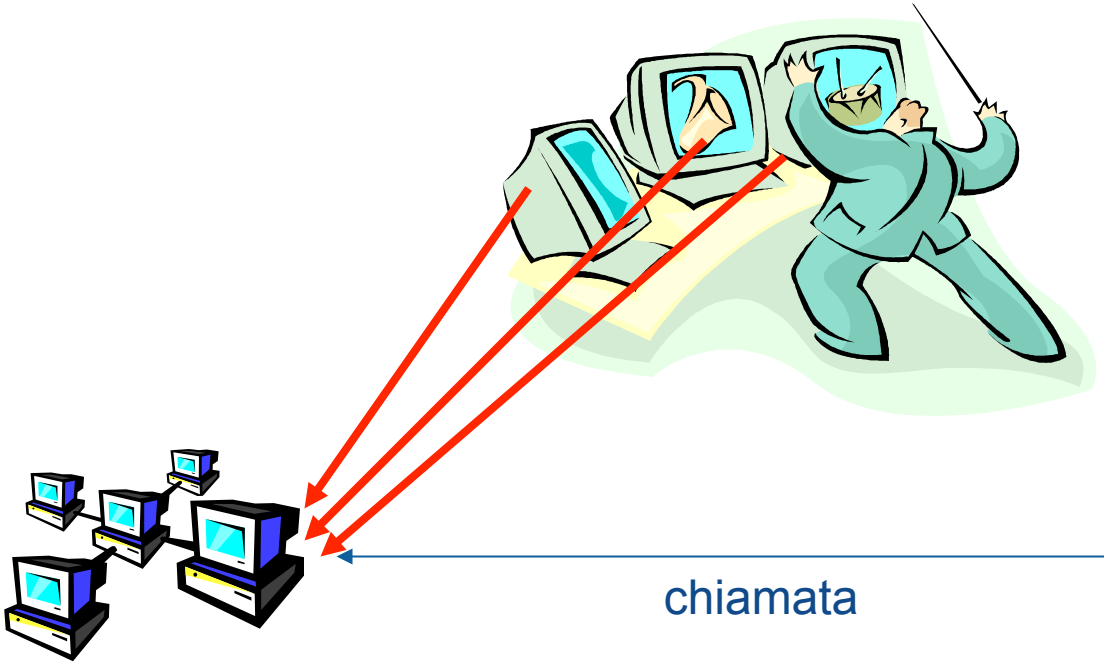
Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Perchè la sicurezza VoIP è un problema?

- Possibilità di spiare e registrare le chiamate telefoniche
- Le chiamate possono essere tracciate
- Furto di informazioni confidenziali
- Modifica delle chiamate telefoniche
- Possibilità di effettuare chiamate gratis
- Falsificazione dell'ID del chiamante
- Spam over IP Telephony (SPIT)
- Un altro punto di accesso alla rete

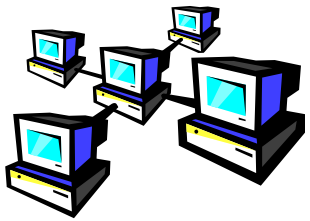
DDoS Attack

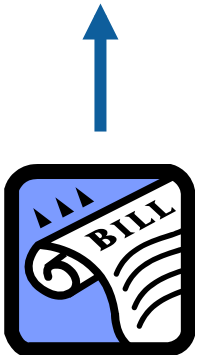


?

chiamata

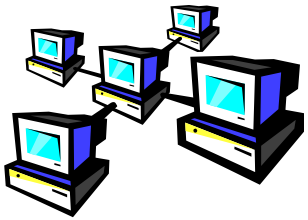
Frodi

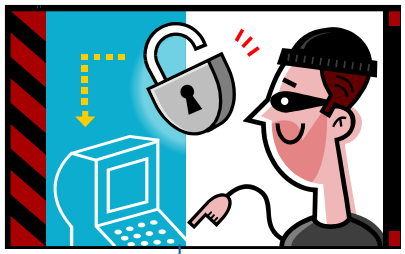




Un hacker potrebbe vendere informazioni riservate sulle aziende

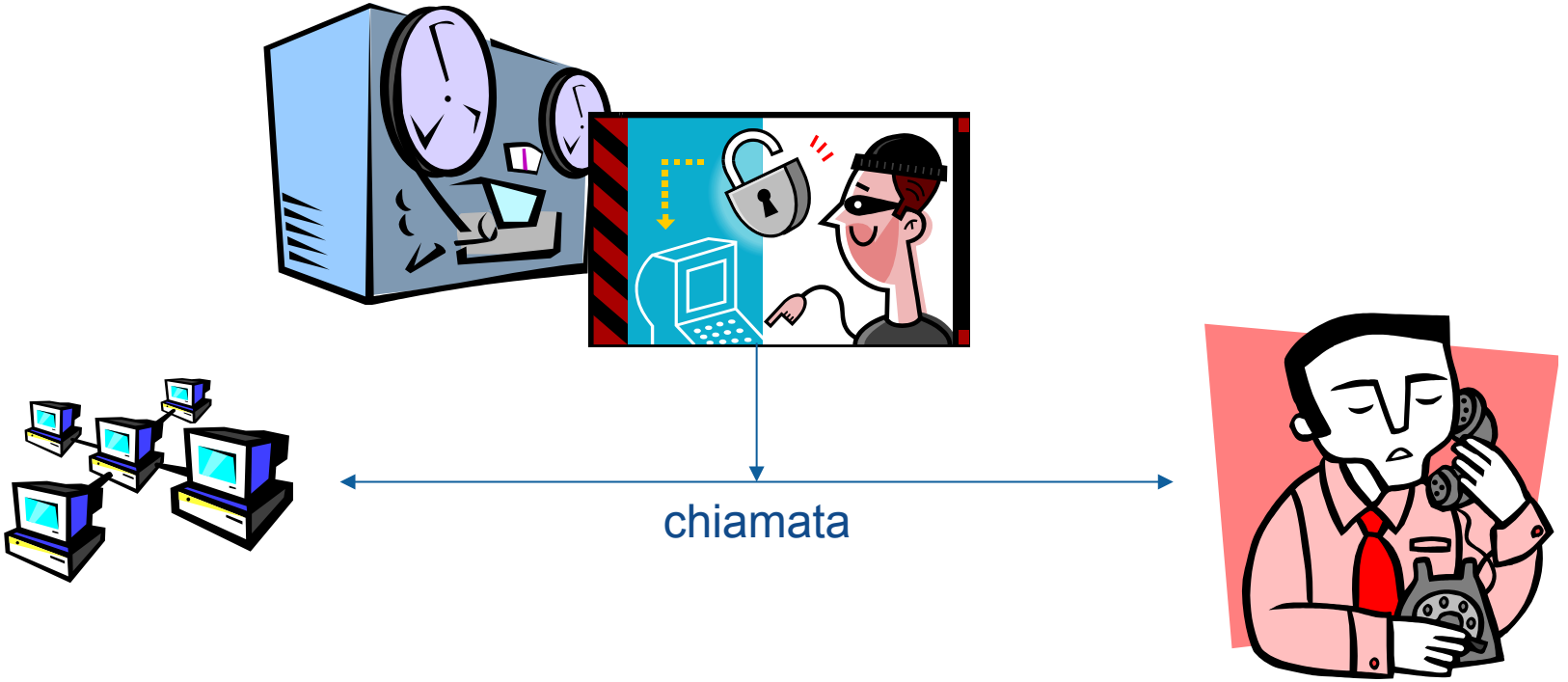
Eavesdropping





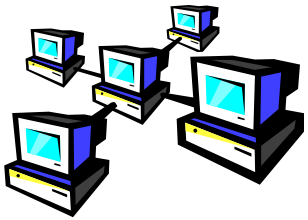
chiamata

Recording



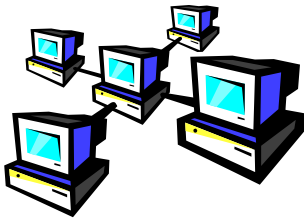
Hijacking/Injection Attack

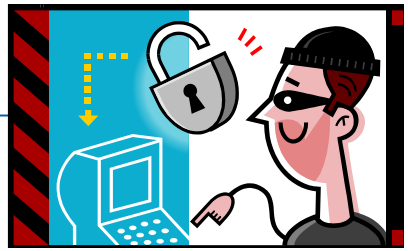
Call Forwarding/Spoofing



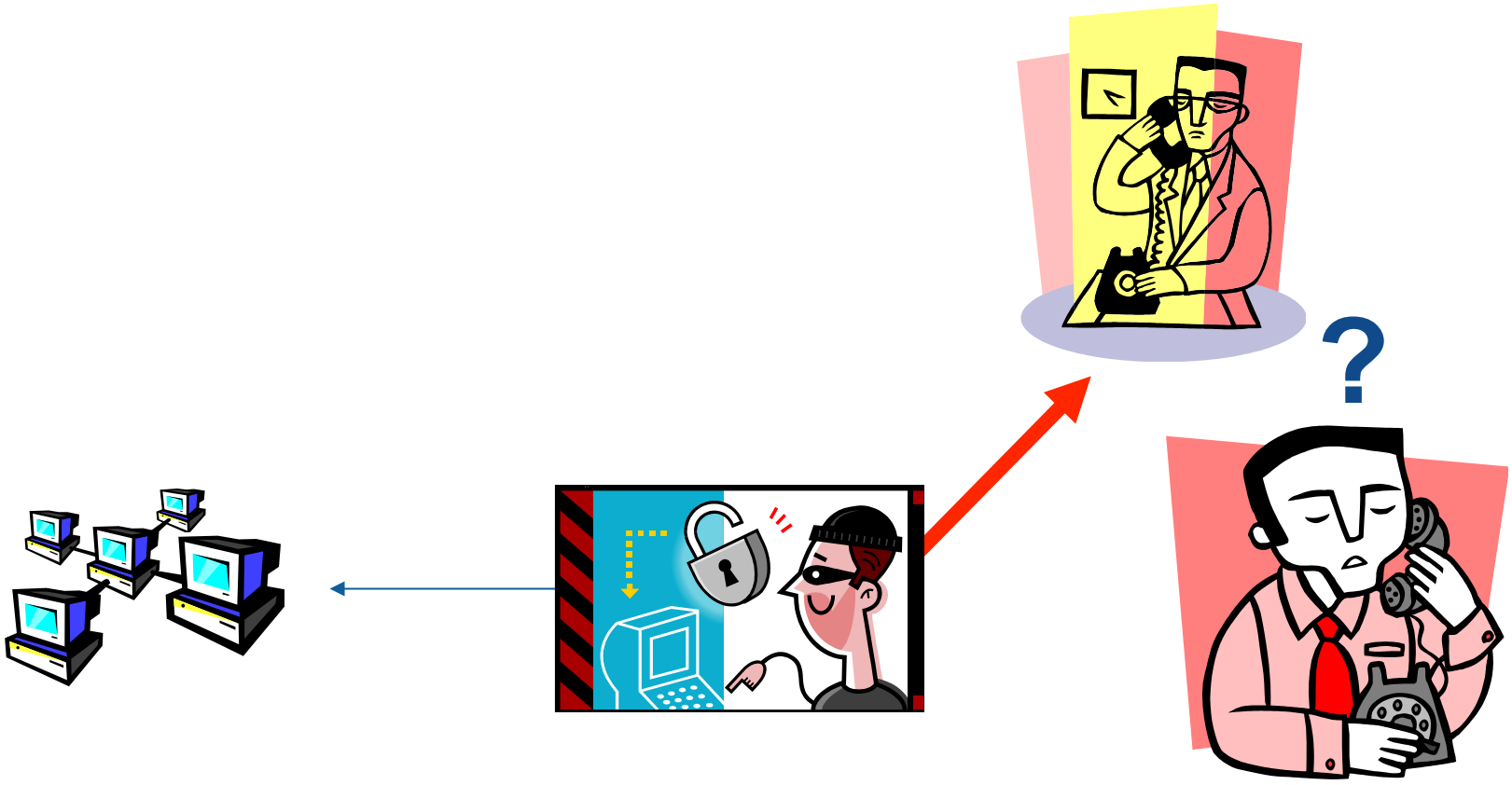
chiamata

Call Forwarding/Spoofing

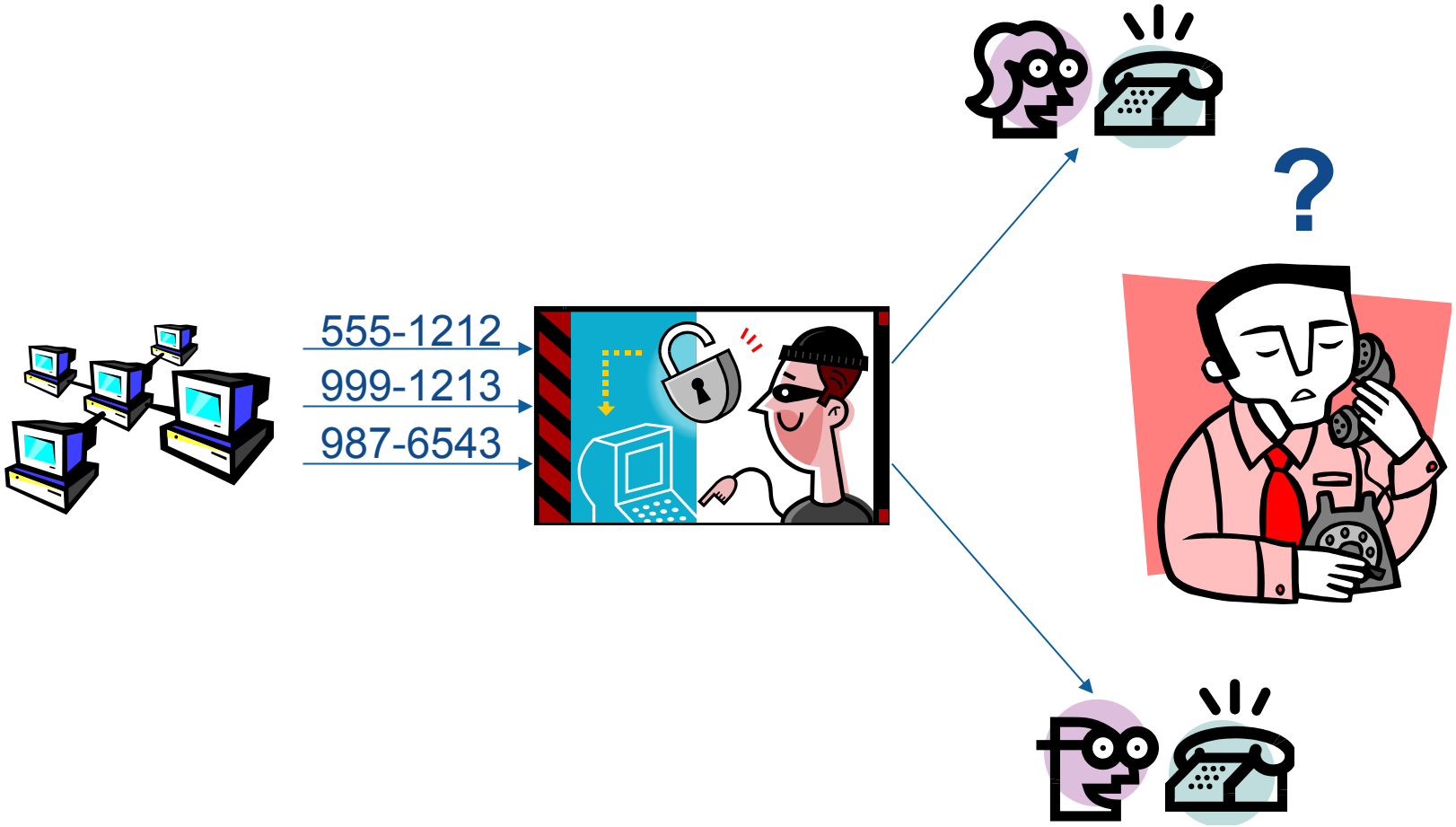




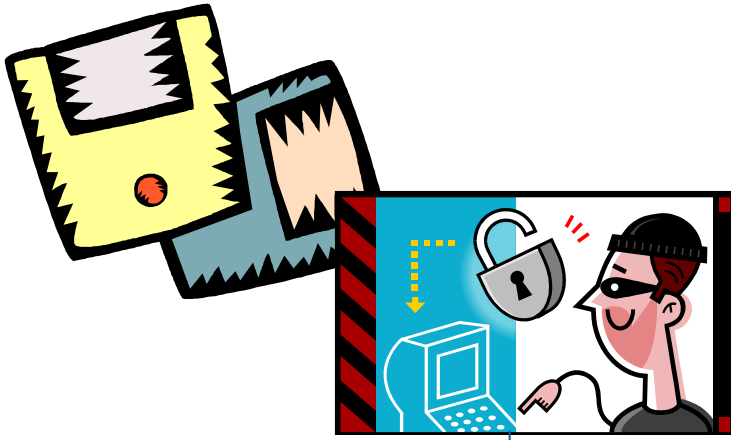
Call Forwarding/Spoofing

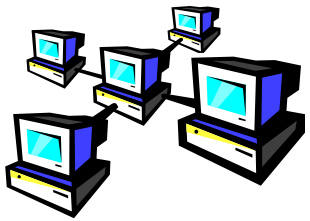


Blocco di determinate chiamate



Logging delle attività delle chiamate



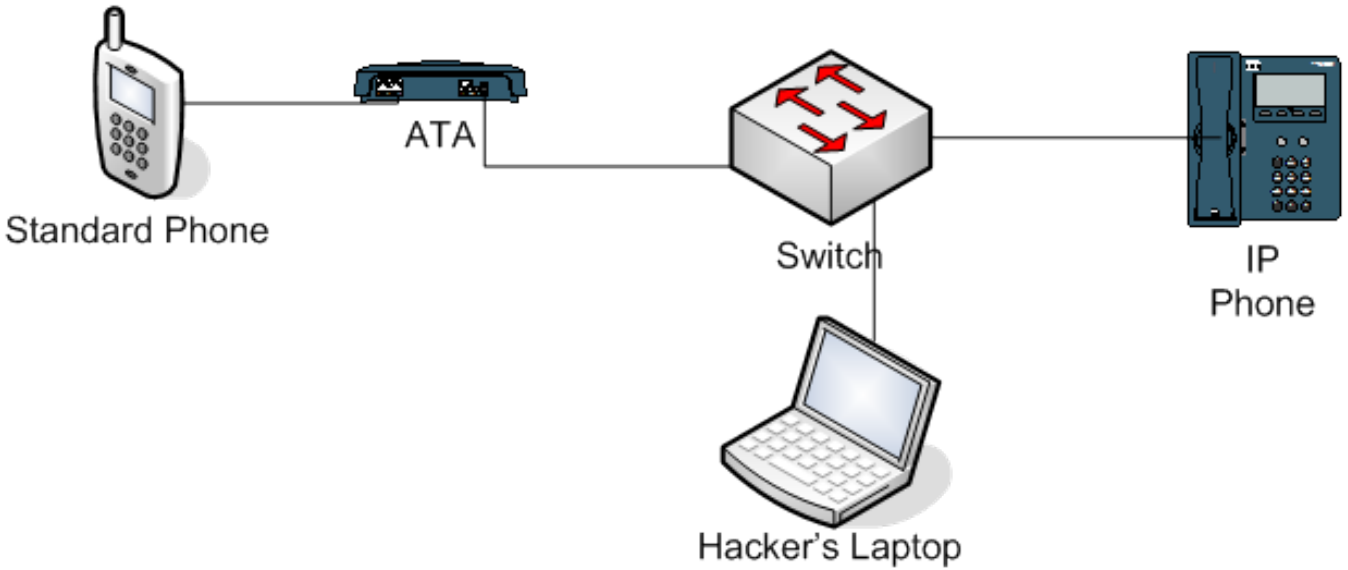


call

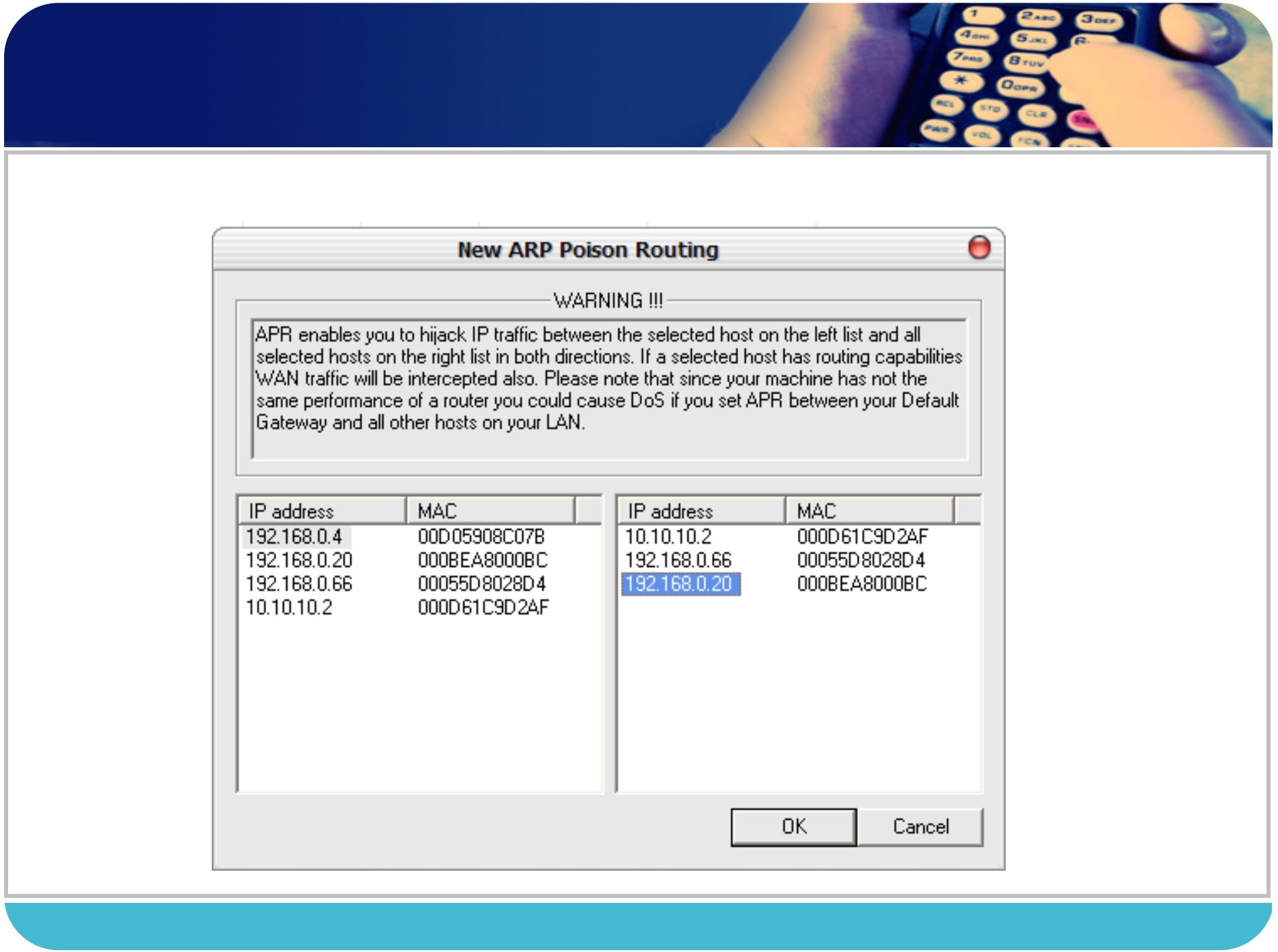
Esempio 1 – Raccolta di informazioni Industriali

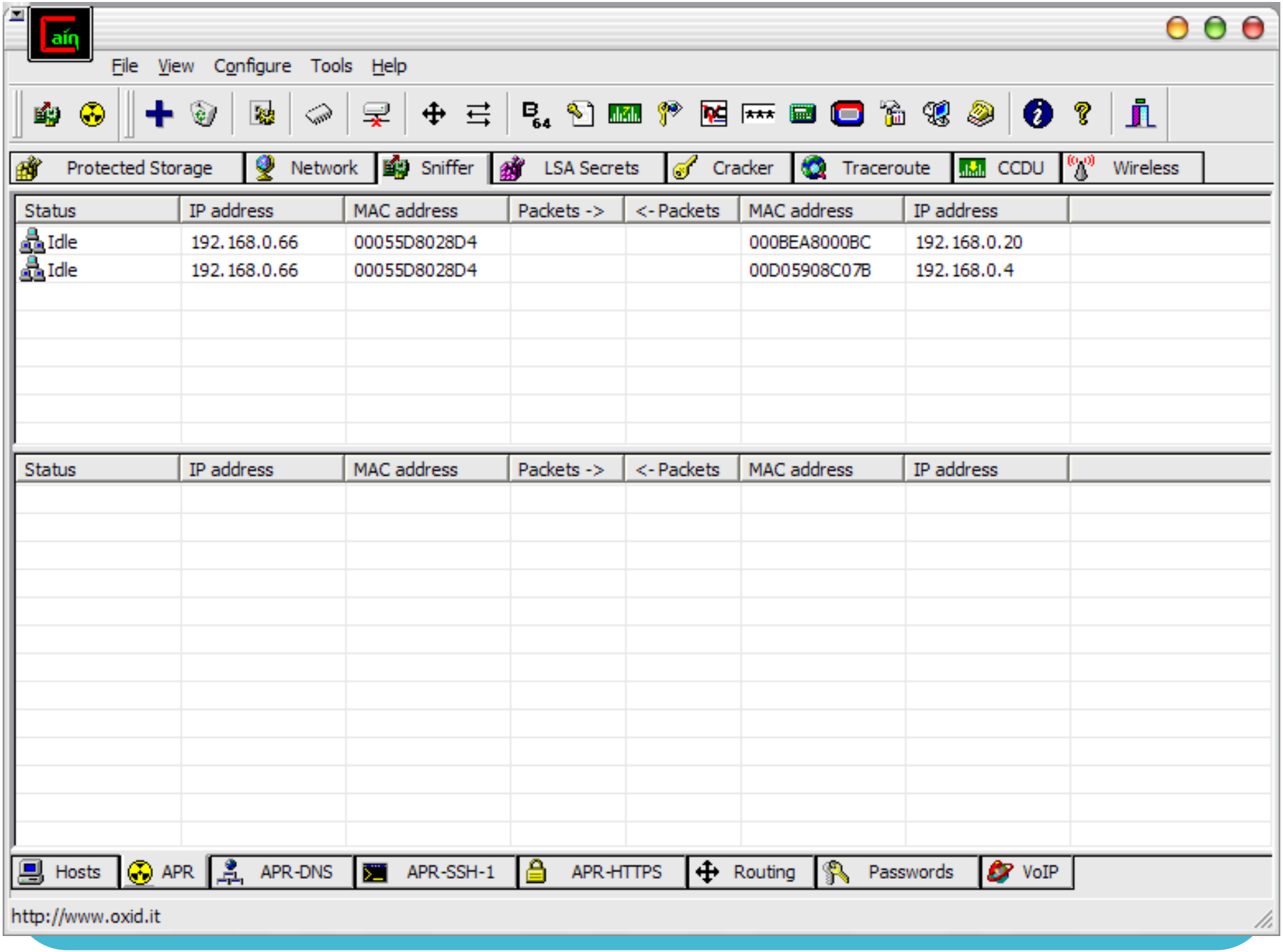
- Un impiegato usa la rete VoIP per spiare le chiamate del proprio direttore
- Ottenere informazioni personali
- Inoltrare le informazioni raccolte ai concorrenti

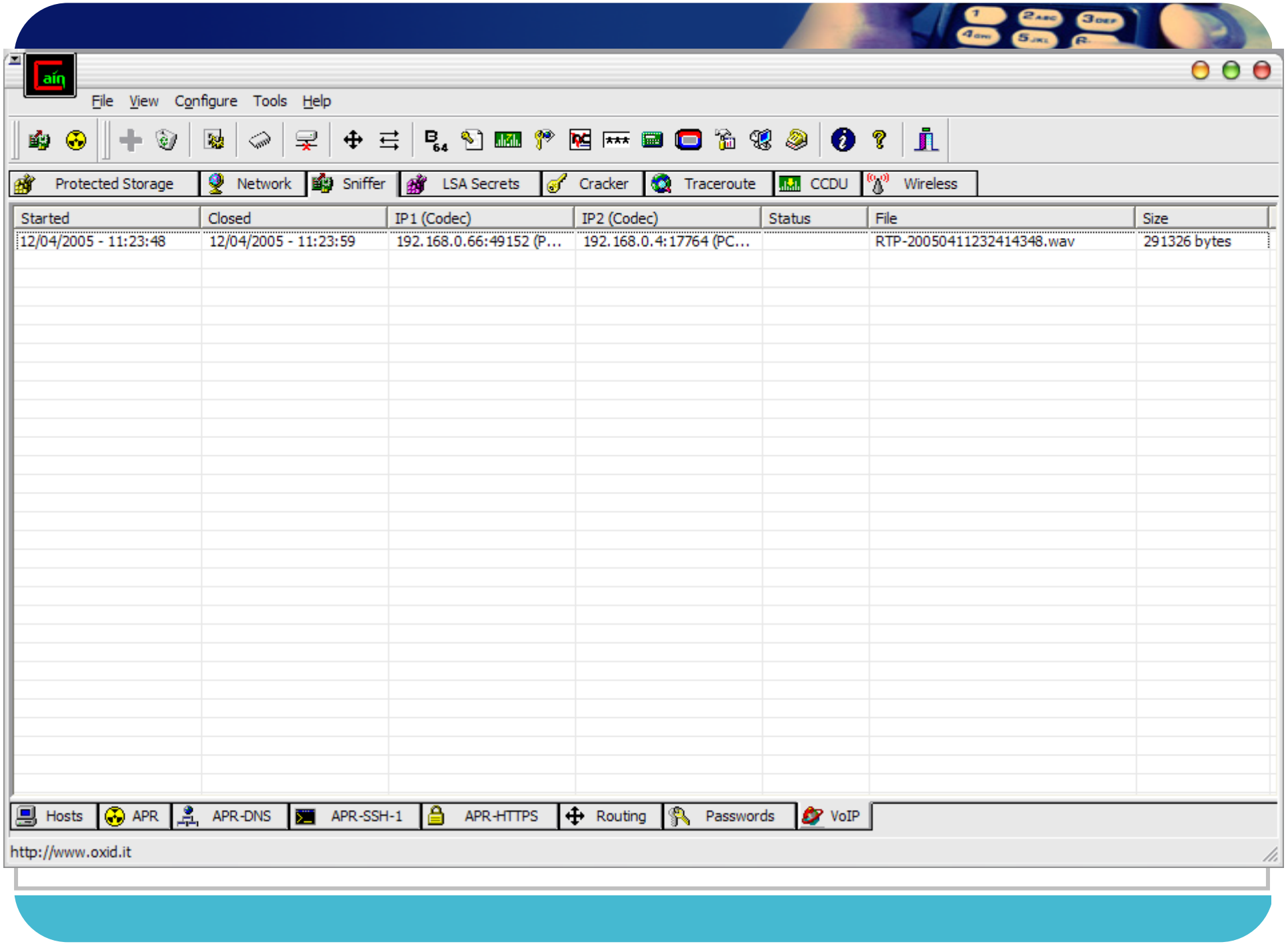
Demo

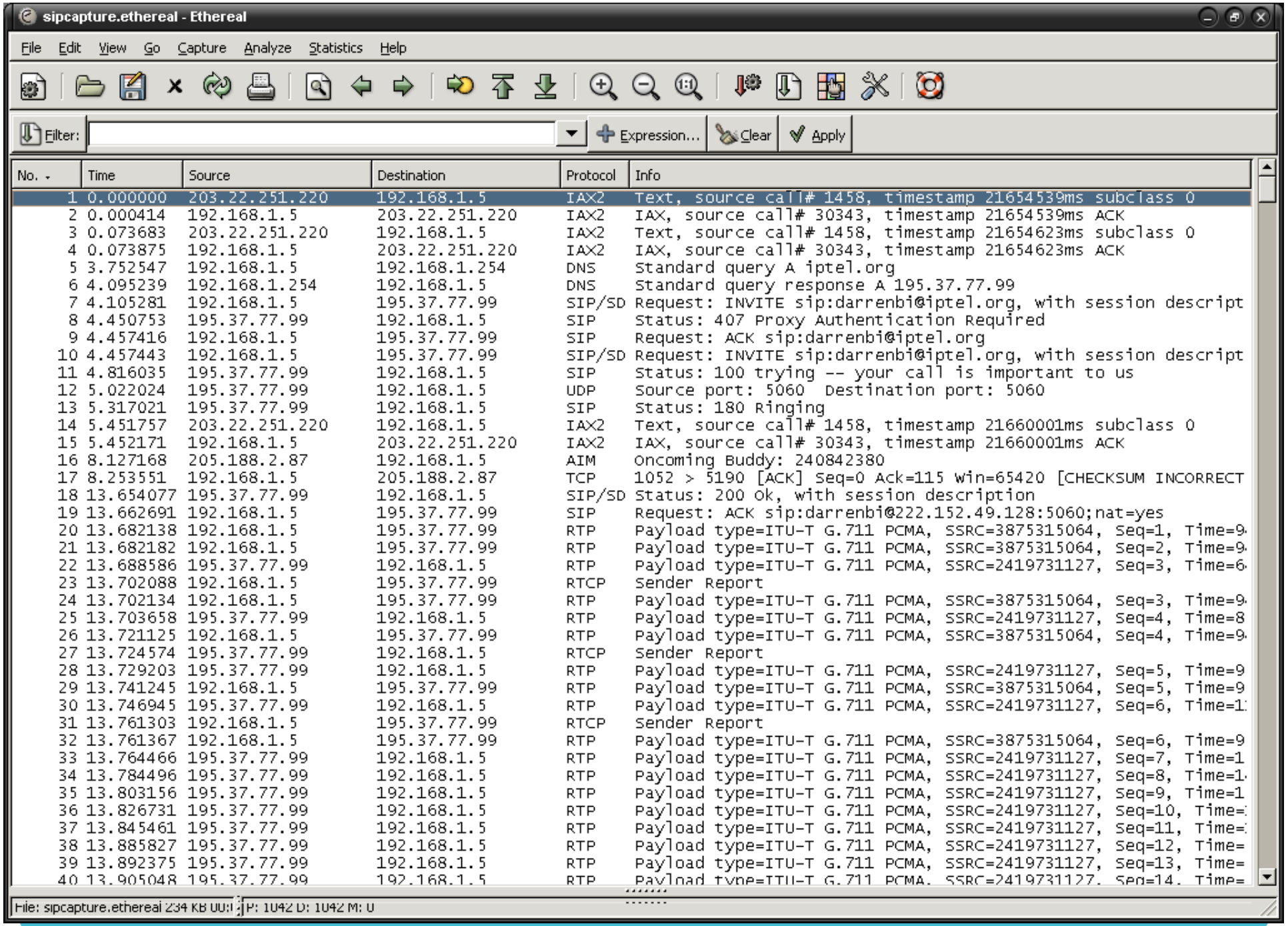


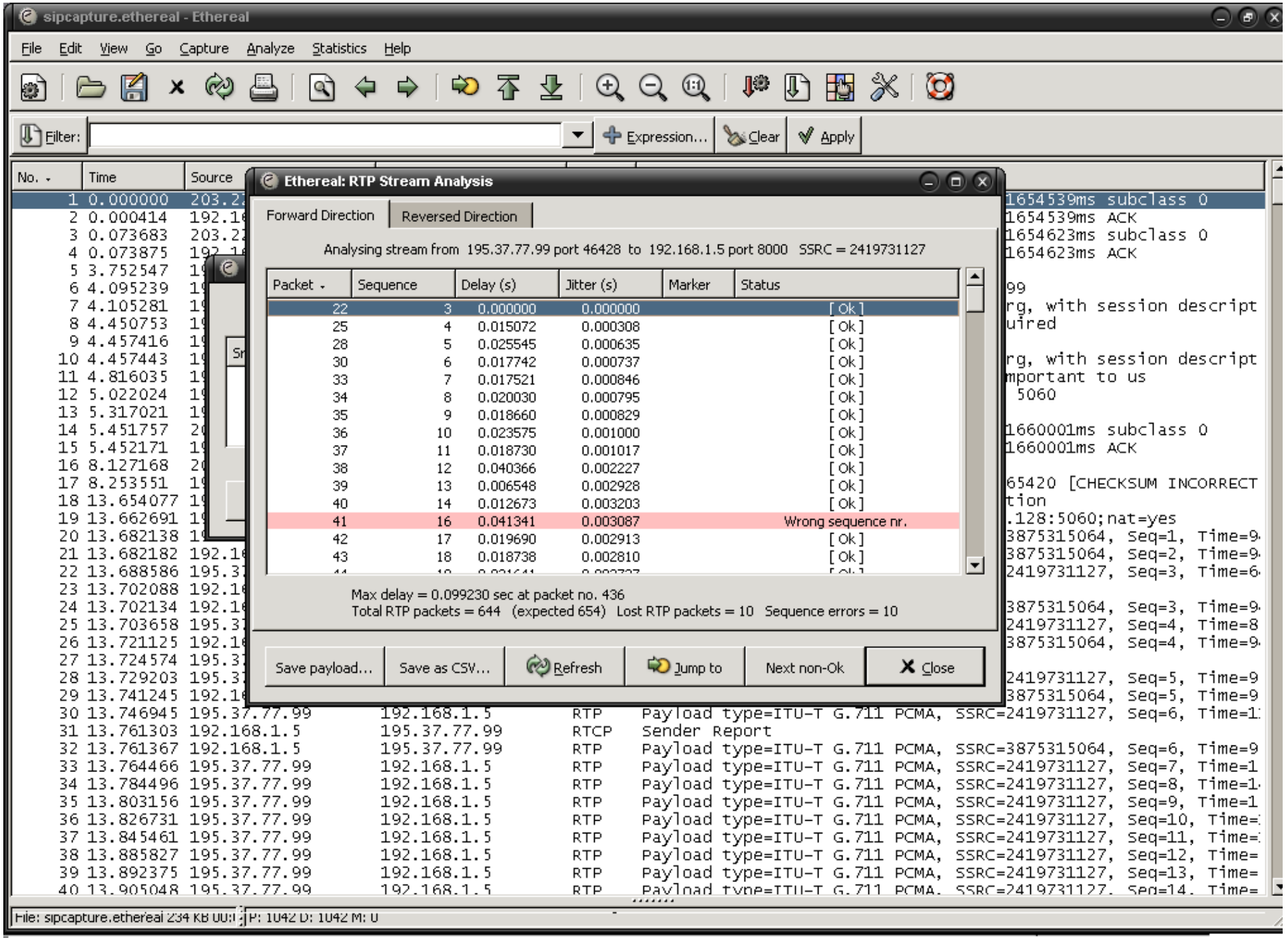
- Cain - http://www.oxid.it
- Ettercap – http://ettercap.sourceforge.net
- Ethereal – http://www.ethereal.com
- Vomit - http://vomit.xtdnet.nl

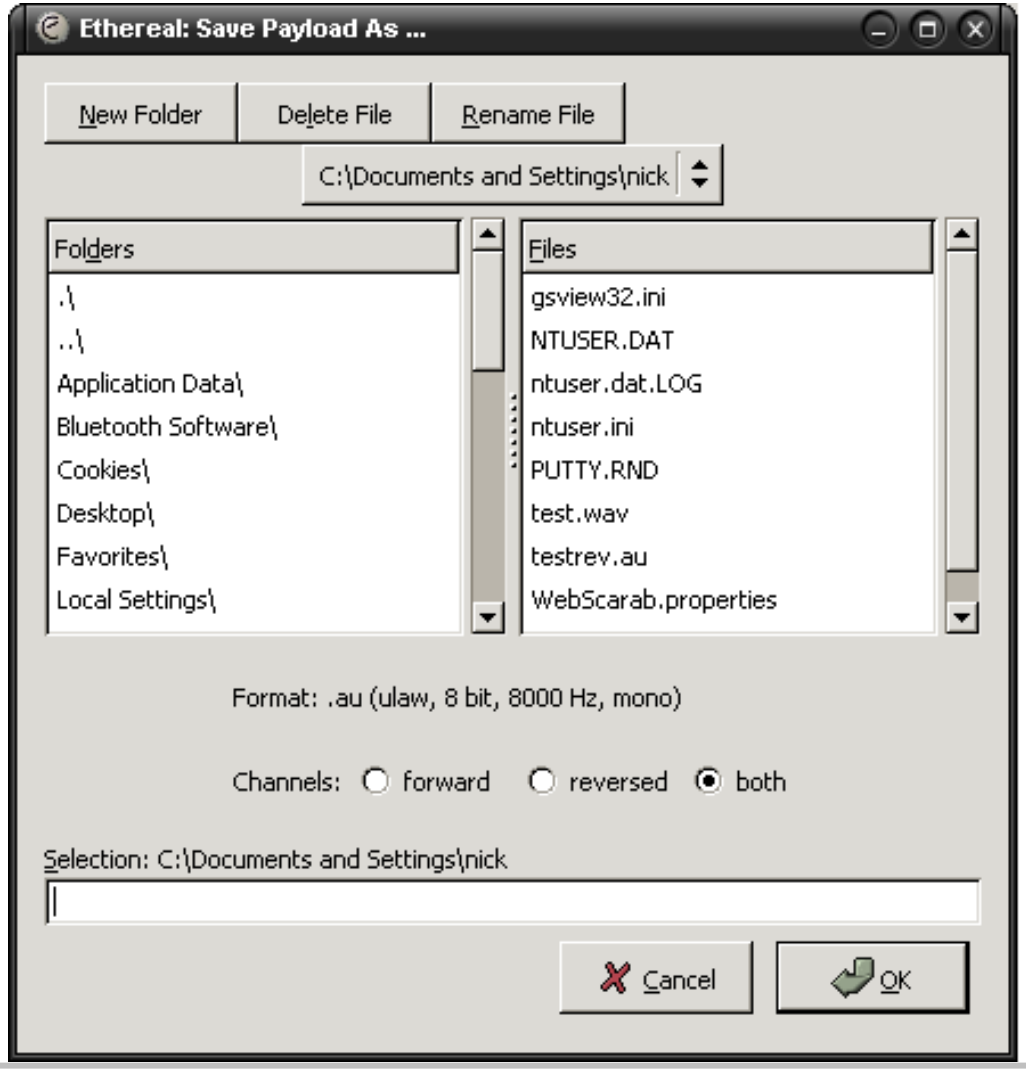

New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted also. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address
MAC
192.168.0.4
00D05908C07B
192.168.0.20
000BEA8000BC
192.168.0.66
00055D8028D4
10.10.10.2
000D61C9D2AF
IP address
MAC
10.10.10.2
000D61C9D2AF
192.168.0.66
00055D8028D4
192.168.0.20
000BEA8000BC
OK
Cancel


Cain
File View Configure Tools Help
Protected Storage
Network
Sniffer
LSA Secrets
Cracker
Traceroute
CCDU
Wireless
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.0.66 00055D8028D4 000BEA8000BC 192.168.0.20
Idle 192.168.0.66 00055D8028D4 00D05908C07B 192.168.0.4
Status IP address MAC address Packets -> <- Packets MAC address IP address
Hosts
APR
APR-DNS
APR-SSH-1
APR-HTTPS
Routing
Passwords
VoIP
http://www.oxid.it


File View Configure Tools Help
Protected Storage
Network
Sniffer
LSA Secrets
Cracker
Traceroute
CCDU
Wireless
Started
Closed
IP1 (Codec)
IP2 (Codec)
Status
File
Size
12/04/2005 - 11:23:48
12/04/2005 - 11:23:59
192.168.0.66:49152 (P...
192.168.0.4:17764 (PC...
RTP-20050411232414348.wav
291326 bytes
Hosts
APR
APR-DNS
APR-SSH-1
APR-HTTPS
Routing
Passwords
VoIP
http://www.oxid.it

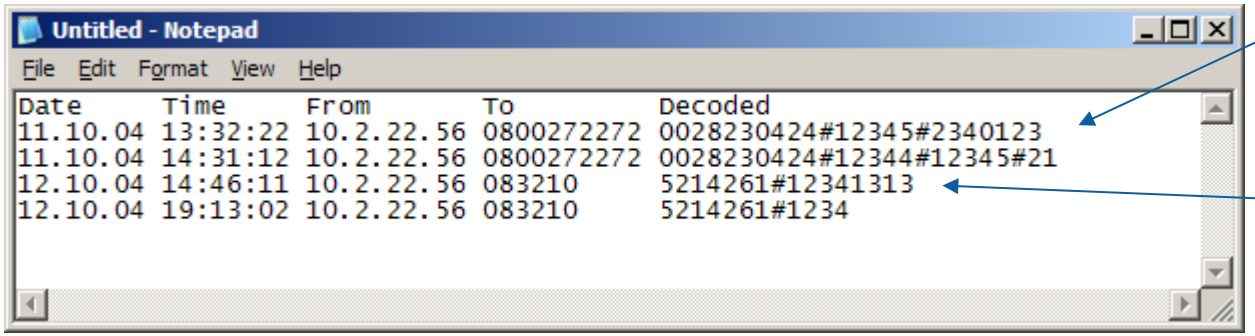

sipcapture.ethereal - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
1 0.000000 203.22.251.220 192.168.1.5 IAX2 Text, source call# 1458, timestamp 21654539ms subclass 0
2 0.000414 192.168.1.5 203.22.251.220 IAX2 IAX, 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=


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

Scenario 2 – Frodi

- Un impiegato di un grande ufficio usa la redirezione ARP per registrare tutte le chiamate
- Effettua le registrazioni e il logging per una settimana
- Usa DTMF decoder per ottenere accesso ai dettagli bancari degli altri impiegati, voice mailboxes etc



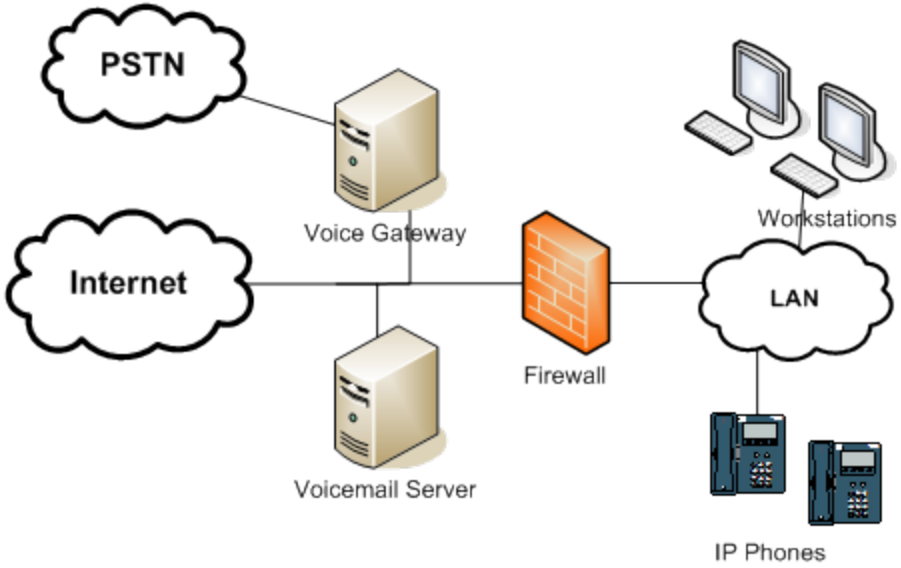
Indice

- **Public Switched Telephone Network**
- **Vantaggi del VoIP**
- **Implementazione & protocolli VoIP**
  - H.323
  - SIP
- **Rischi per la Sicurezza**
- **Soluzioni per la Sicurezza**
  - Sicurezza dei dispositivi
  - Separazione logica del traffico
  - Autenticazione
  - Cifratura

Cosa bisogna fare per rendere tutto sicuro?

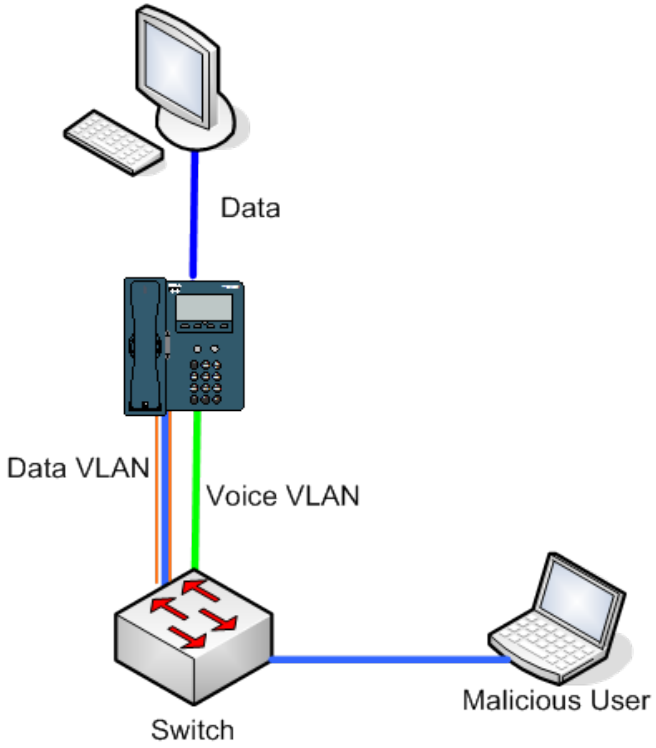
- Sicurezza dei Dispositivi
- Separazione logica della rete
- Cifratura del traffico
- Intrusion Detection

Sicurezza dei Dispositivi



- Nulla che non debba essere visto al di fuori dovrebbe essere esposto su Internet
- Rafforzare la sicurezza dei server VoIP
- Applicare le patch di sicureza

Separazione Logica del traffico



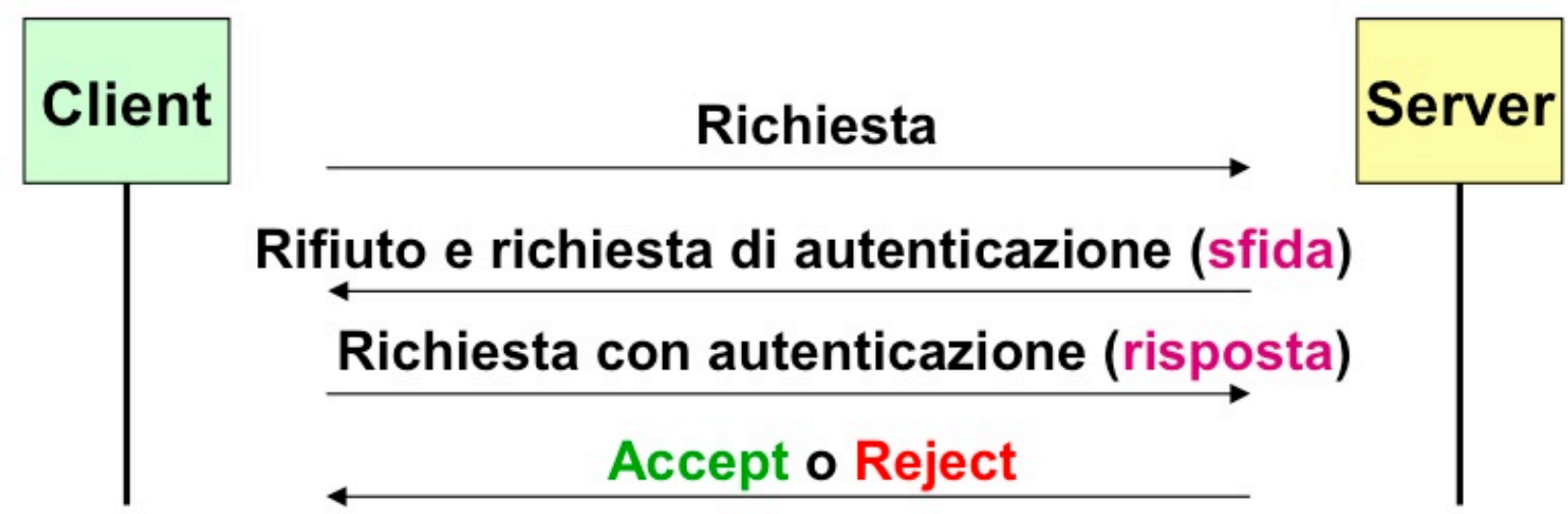
Autenticazione

- **L'autenticazione consente ad un Server di verificare l'autenticità di un Client che sottopone una certa richiesta di servizio**

- **In SIP (RFC 3261) si utilizza il "*Digest Authentication Scheme*";**

Autenticazione

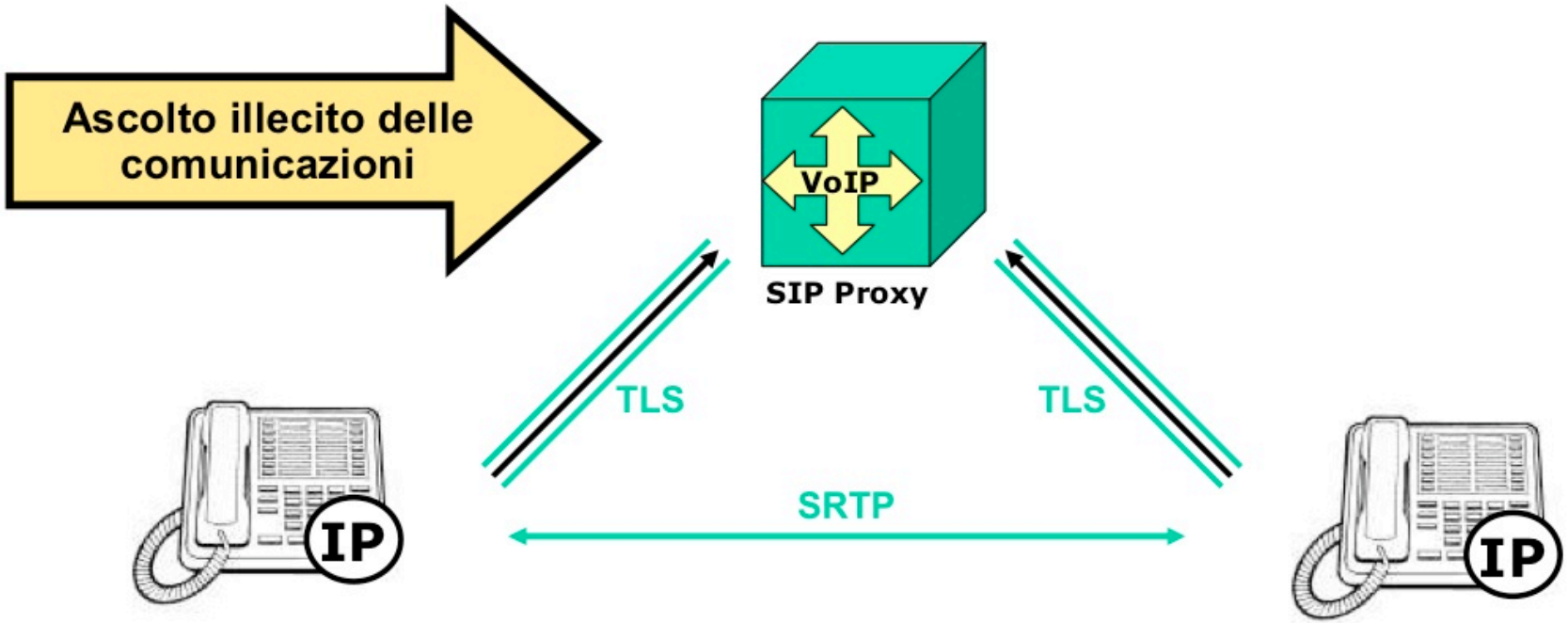
- SIP utilizza meccanismi di autenticazione basati sul paradigma challenge-response : il Server "sfida" il Client a "dimostrare" la propria identità
- Se il Client vince la sfida la richiesta di servizio viene portata avanti dal Server, in caso contrario il Server rilascia la transazione.
- Le response utilizzate per richiedere l'autenticazione sono:
  - Risposta "401 – Unauthorized " per i Server di tipo UA
  - Risposta "407 – Proxy authentication required" per i server di tipo Proxy



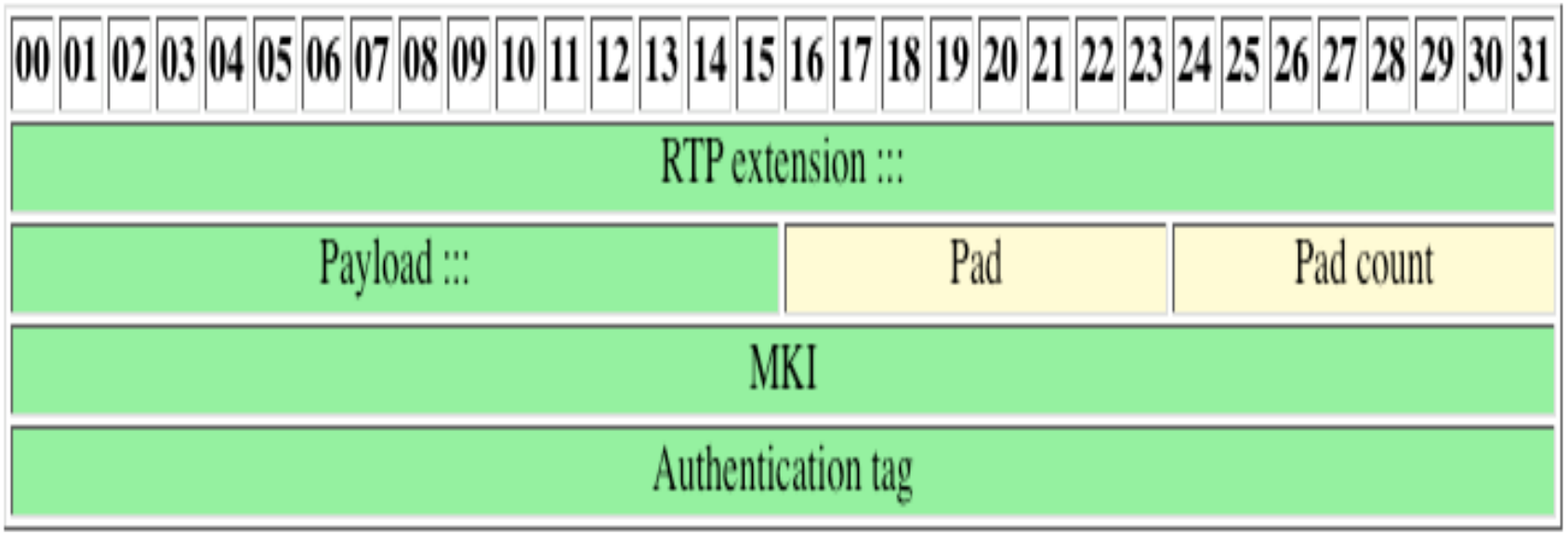
SRTP - Secure Real-time Transport Protocol

- **Estensione RTP/RTCP**
- **End to End**
- **IETF RFC 3711**
- **Aggiunte**
  - Riservatezza (AES128)
  - Autenticazione dei Messaggi(HMAC-SHA1)
  - Protezione contro gli attacchi a ripetizione
- **Non influisce sulla compressione e Qos**
- **Scalabile**

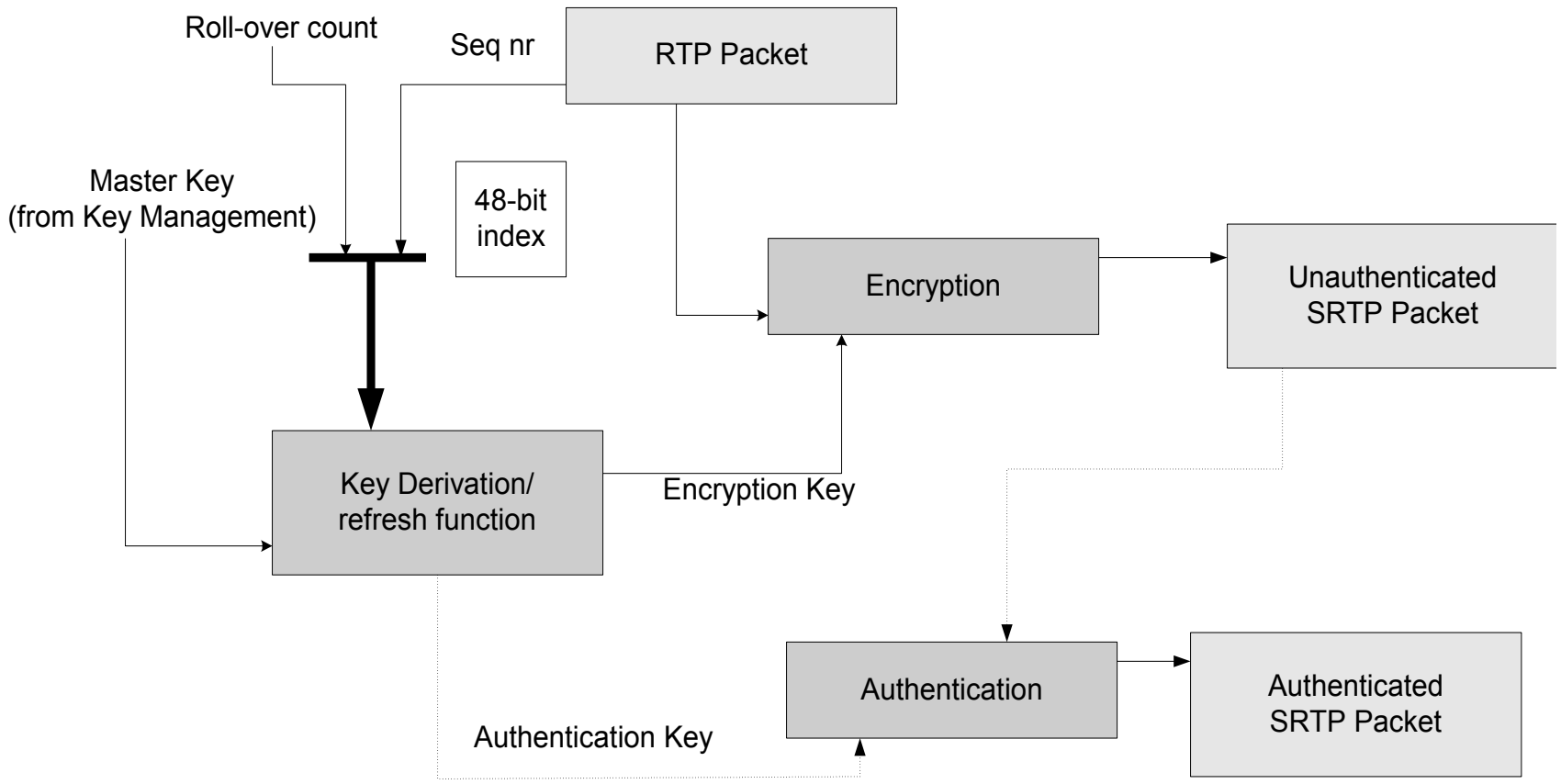
SRTP - Secure Real-time Transport Protocol



SRTP - Secure Real-time Transport Protocol



SRTP - Secure Real-time Transport Protocol



Link Utili

- **Alcuni likn utili per approfondire la conoscenza su VoIP**

Voip-Info.org	http://www.voip-info.org
VoP Security	http://www.vopsecurity.org
Cain and Abel	http://www.oxid.it
Vomit	http://vomit.xtdnet.nl/
VoipSA	http://www.voipsa.org


Grazie!