ISEL
INSTITUTO SUPERIOR DE ENGENHARIA DE LISBOA

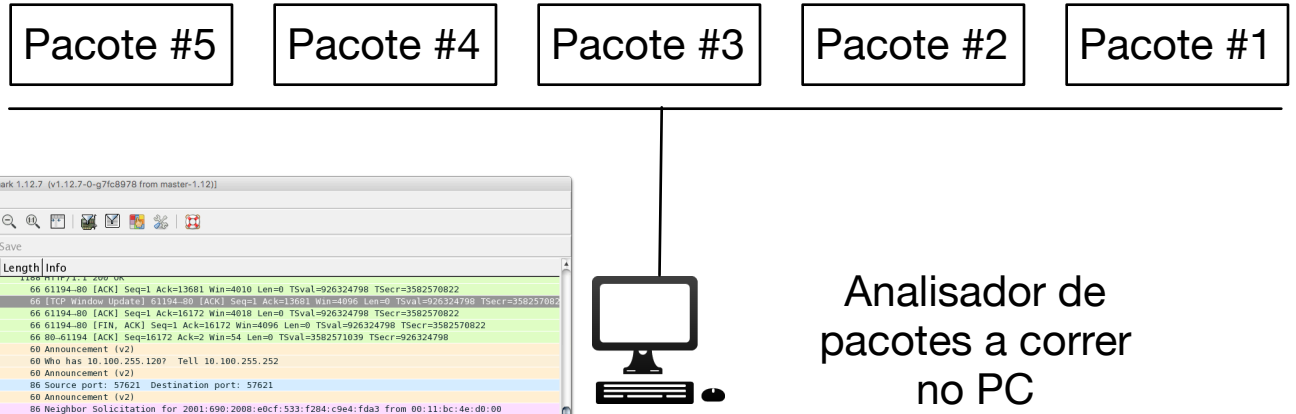
Análise de tráfego

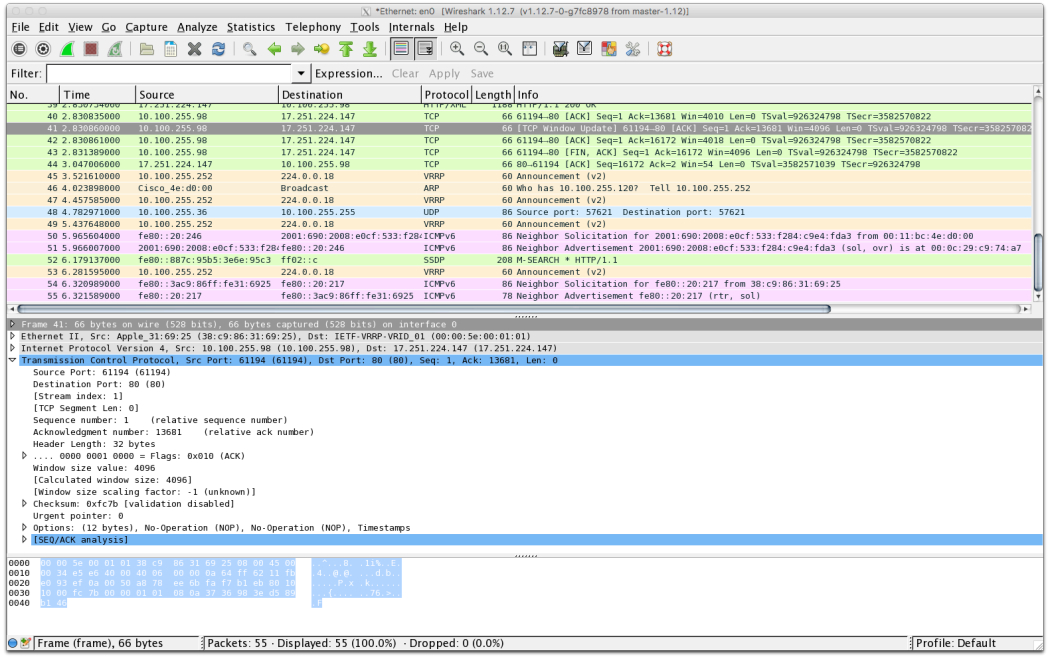
ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

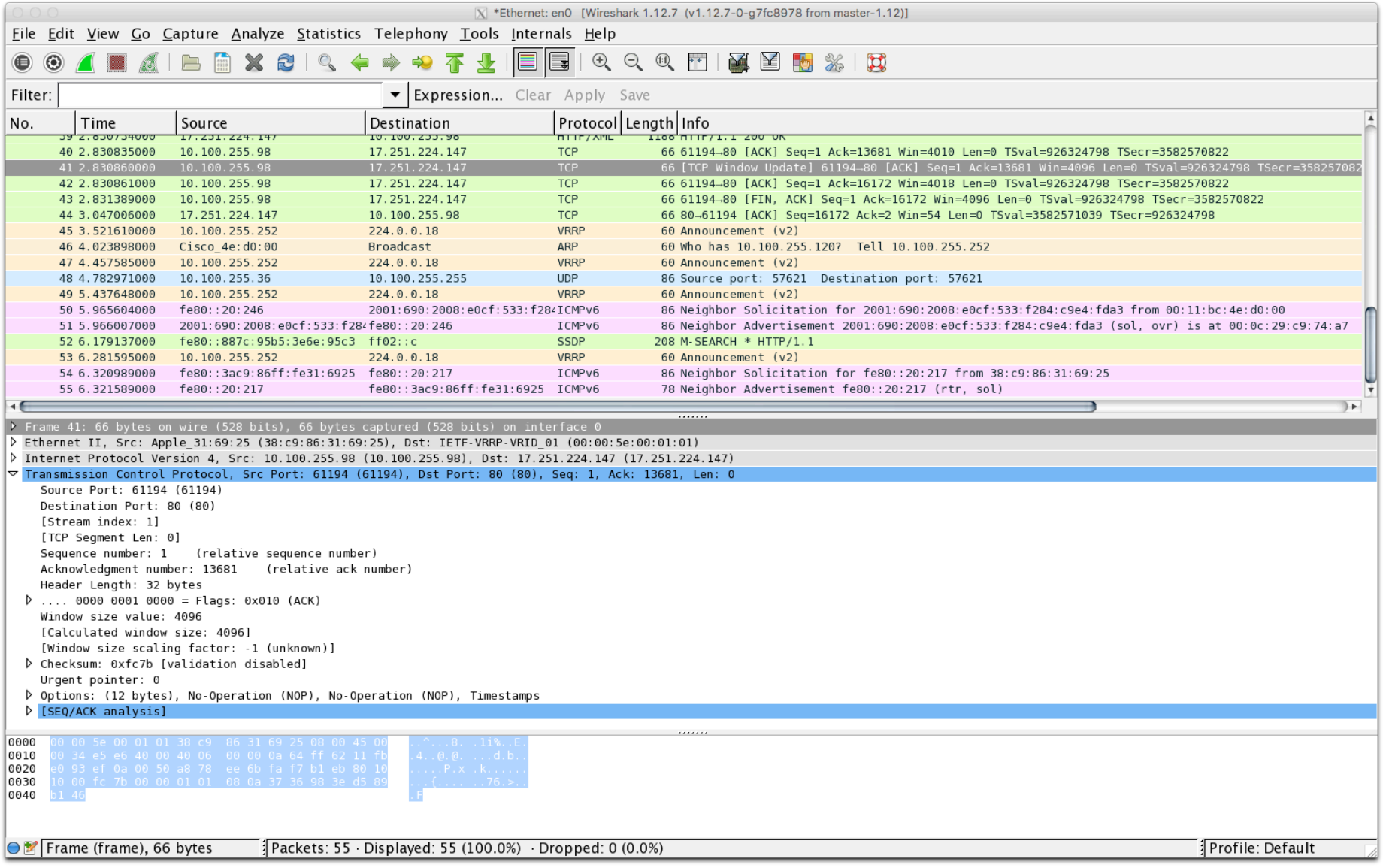
Ferramentas para captura de tráfego

- Wireshark
  - Ambiente gráfico
- Tcpdump
  - Ferramenta de linha de comandos
- Ngrep
  - Ferramenta de linha de comandos

Como funciona?



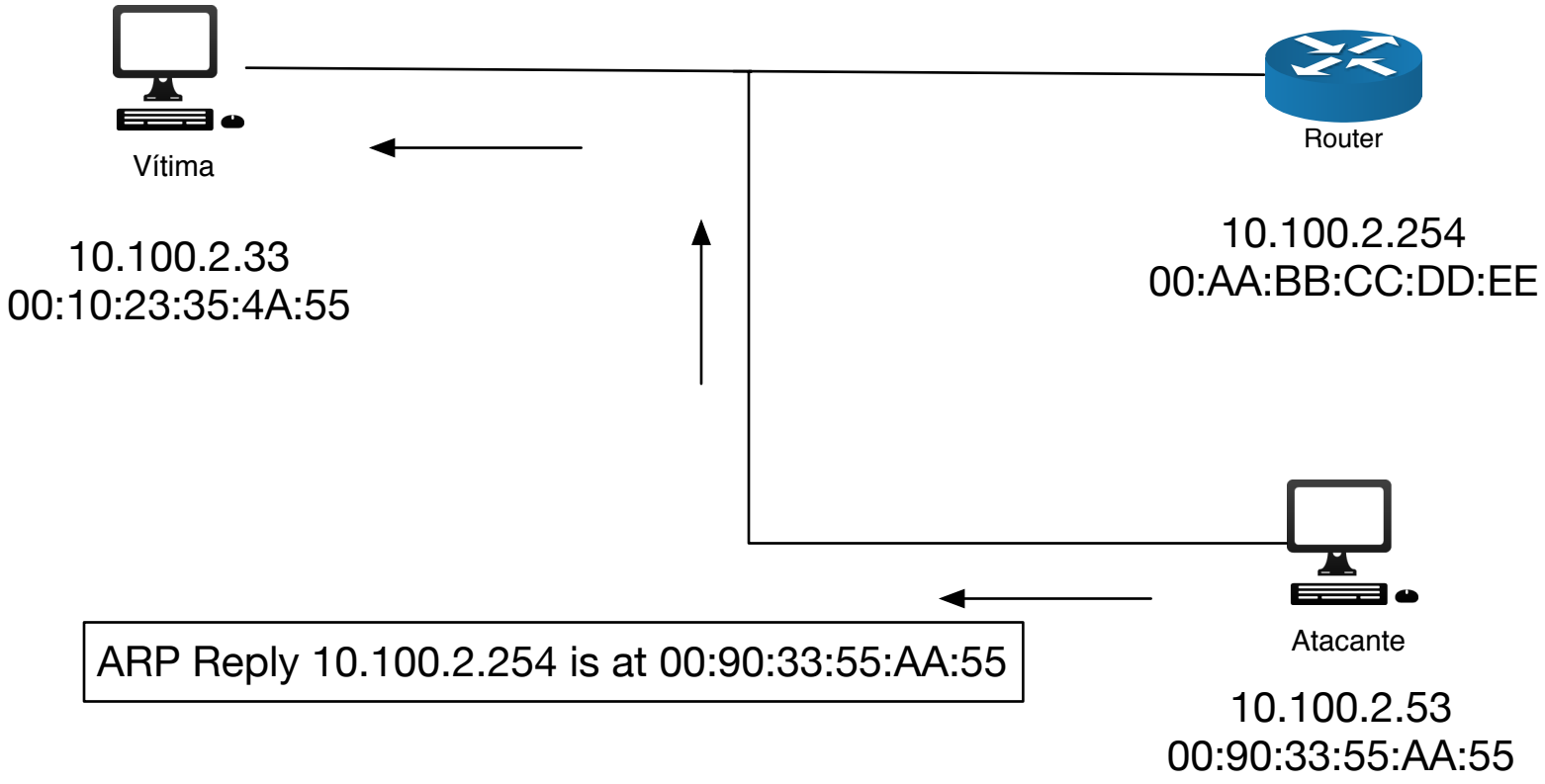



*Ethernet: en0 [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
40 2.830835000 10.100.255.98 17.251.224.147 TCP 66 61194→80 [ACK] Seq=1 Ack=13681 Win=4010 Len=0 TSval=926324798 TSecr=3582570822
41 2.830860000 10.100.255.98 17.251.224.147 TCP 66 [TCP Window Update] 61194→80 [ACK] Seq=1 Ack=13681 Win=4096 Len=0 TSval=926324798 TSecr=358257082
42 2.830861000 10.100.255.98 17.251.224.147 TCP 66 61194→80 [ACK] Seq=1 Ack=16172 Win=4018 Len=0 TSval=926324798 TSecr=3582570822
43 2.831389000 10.100.255.98 17.251.224.147 TCP 66 61194→80 [FIN, ACK] Seq=1 Ack=16172 Win=4096 Len=0 TSval=926324798 TSecr=3582570822
44 3.047006000 17.251.224.147 10.100.255.98 TCP 66 80→61194 [ACK] Seq=16172 Ack=2 Win=54 Len=0 TSval=3582571039 TSecr=926324798
45 3.521610000 10.100.255.252 224.0.0.18 VRRP 60 Announcement (v2)
46 4.023898000 Cisco_4e:d0:00 Broadcast ARP 60 Who has 10.100.255.120? Tell 10.100.255.252
47 4.457585000 10.100.255.252 224.0.0.18 VRRP 60 Announcement (v2)
48 4.782971000 10.100.255.36 10.100.255.255 UDP 86 Source port: 57621 Destination port: 57621
49 5.437648000 10.100.255.252 224.0.0.18 VRRP 60 Announcement (v2)
50 5.965604000 fe80::20:246 2001:690:2008:e0cf:533:f284 ICMPv6 86 Neighbor Solicitation for 2001:690:2008:e0cf:533:f284:c9e4:fda3 from 00:11:bc:4e:d0:00
51 5.966007000 2001:690:2008:e0cf:533:f284 fe80::20:246 ICMPv6 86 Neighbor Advertisement 2001:690:2008:e0cf:533:f284:c9e4:fda3 (sol, ovr) is at 00:0c:29:c9:74:a7
52 6.179137000 fe80::887c:95b5:3e6e:95c3 ff02::c SSDP 208 M-SEARCH * HTTP/1.1
53 6.281595000 10.100.255.252 224.0.0.18 VRRP 60 Announcement (v2)
54 6.320989000 fe80::3ac9:86ff:fe31:6925 fe80::20:217 ICMPv6 86 Neighbor Solicitation for fe80::20:217 from 38:c9:86:31:69:25
55 6.321589000 fe80::20:217 fe80::3ac9:86ff:fe31:6925 ICMPv6 78 Neighbor Advertisement fe80::20:217 (rtr, sol)
Frame 41: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Apple_31:69:25 (38:c9:86:31:69:25), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
Internet Protocol Version 4, Src: 10.100.255.98 (10.100.255.98), Dst: 17.251.224.147 (17.251.224.147)
Transmission Control Protocol, Src Port: 61194 (61194), Dst Port: 80 (80), Seq: 1, Ack: 13681, Len: 0
Source Port: 61194 (61194)
Destination Port: 80 (80)
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 13681 (relative ack number)
Header Length: 32 bytes
.... 0000 0001 0000 = Flags: 0x010 (ACK)
Window size value: 4096
[Calculated window size: 4096]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xfc7b [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
0000 00 00 5e 00 01 01 38 c9 86 31 69 25 08 00 45 00 ..^...8. .1i%..E.
0010 00 34 e5 e6 40 00 40 06 00 00 0a 64 ff 62 11 fb .4..@.@. ...d.b..
0020 e0 93 ef 0a 00 50 a8 78 ee 6b fa f7 b1 eb 80 10 .....P.x .k......
0030 10 00 fc 7b 00 00 01 01 08 0a 37 36 98 3e d5 89 ...{.... ..76.>..
0040 b1 46 .F
Frame (frame), 66 bytes
Packets: 55 · Displayed: 55 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

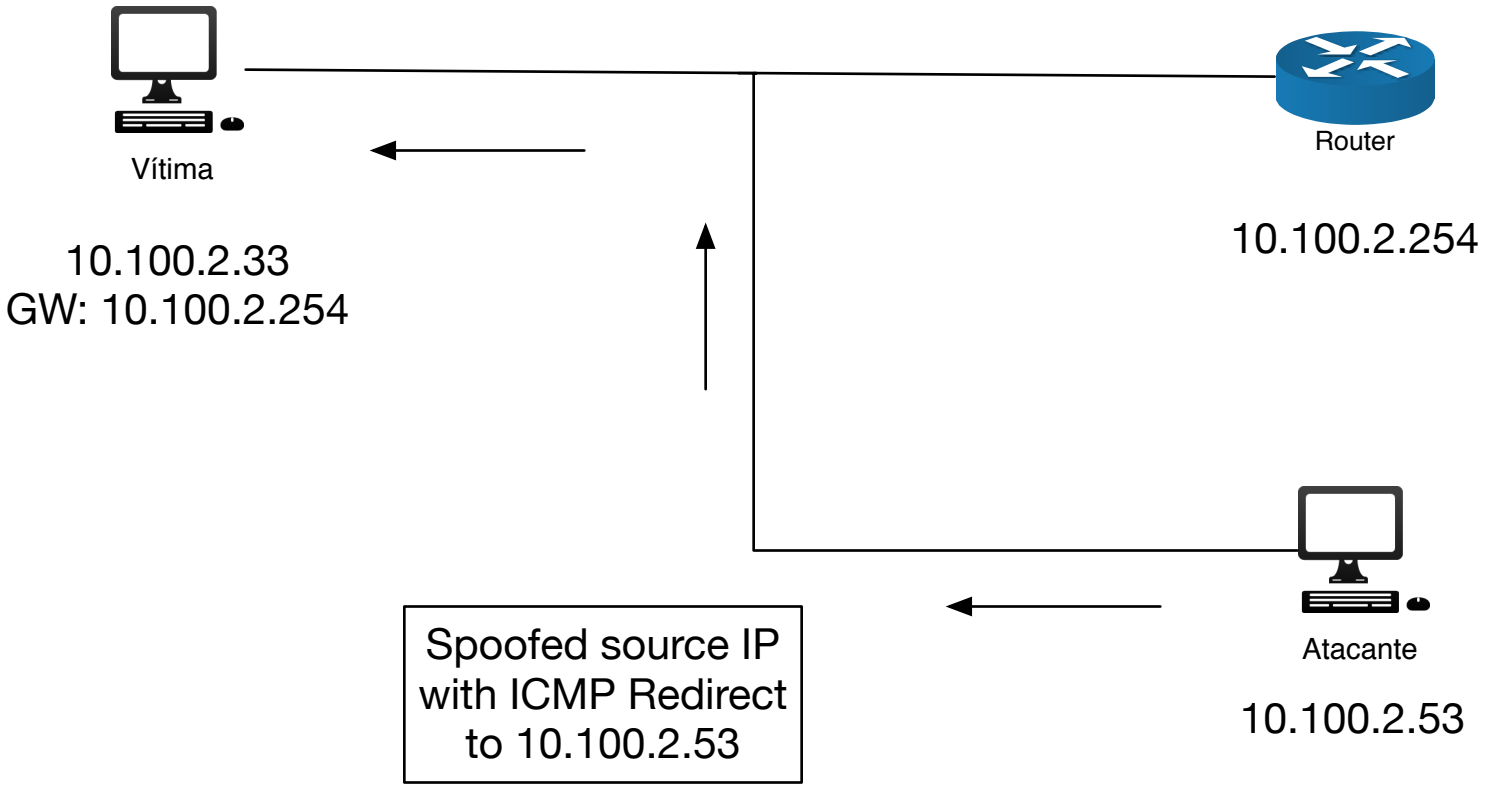
Captura de tráfego

- A captura só é possível se as tramas chegarem fisicamente ao *host*
  - Meio partilhado
- Ataques para manipular o caminho do tráfego
  - ARP *Poisoning*
  - ARP cache *flooding*
  - ICMP Redirect
  - DHCP/DHCPv6 *spoofing*
  - IPv6 Neighbour Advertisement/SLAAC *spoof*
  - WPAD (Web Proxy Auto Discovery)

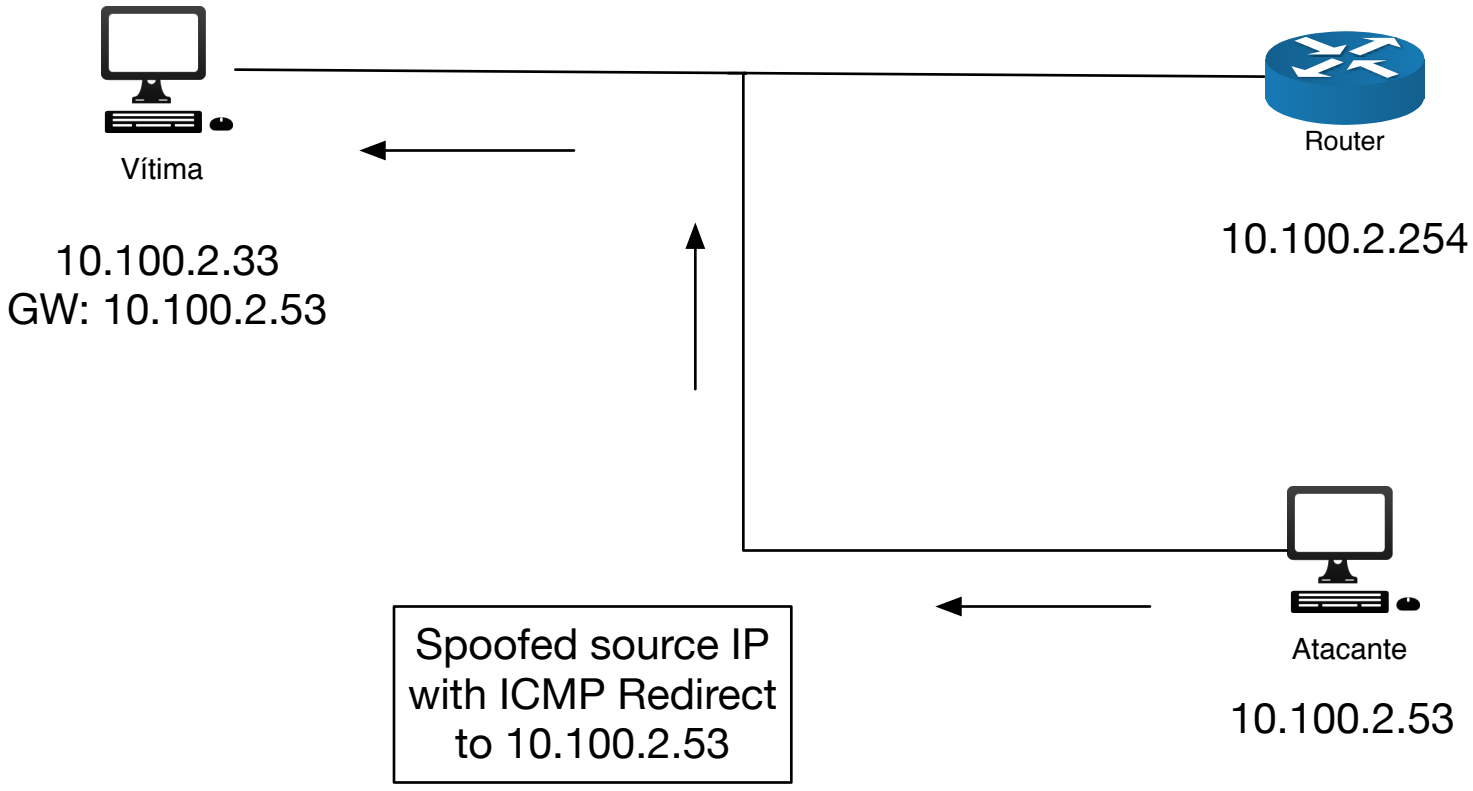
Pacotes ARP maliciosos



ICMP Redirect



ICMP Redirect



Medidas de prevenção

- ARP inspection
  - Os *switches* controlam o conteúdo dos pacotes ARP
- DHCP snooping
  - Os *switches* controlam o conteúdo dos pacotes DHCP
- Port security
  - Limitar o número de endereços MAC numa porta
- ICMP redirects
  - Configurar os clientes para ignorarem ICMP redirects