



Capturing IP Resolution

ARP & IP Resolution

» **What is IP resolution?**

» **What does ARP do?**

- Helps resolve IP address to corresponding hardware addresses (Ethernet, MAC, BIA)

» **Why capture this resolution with Wireshark?**

- Determine why a host may not be connecting to a network
- Table instability
- Spoofing
- More

IP Resolution

ARP Request

Device tries to find the hardware address for a node based on the IP address it knows.



ARP Reply

Correct device provides the requested hardware address.

Wireshark & ARP

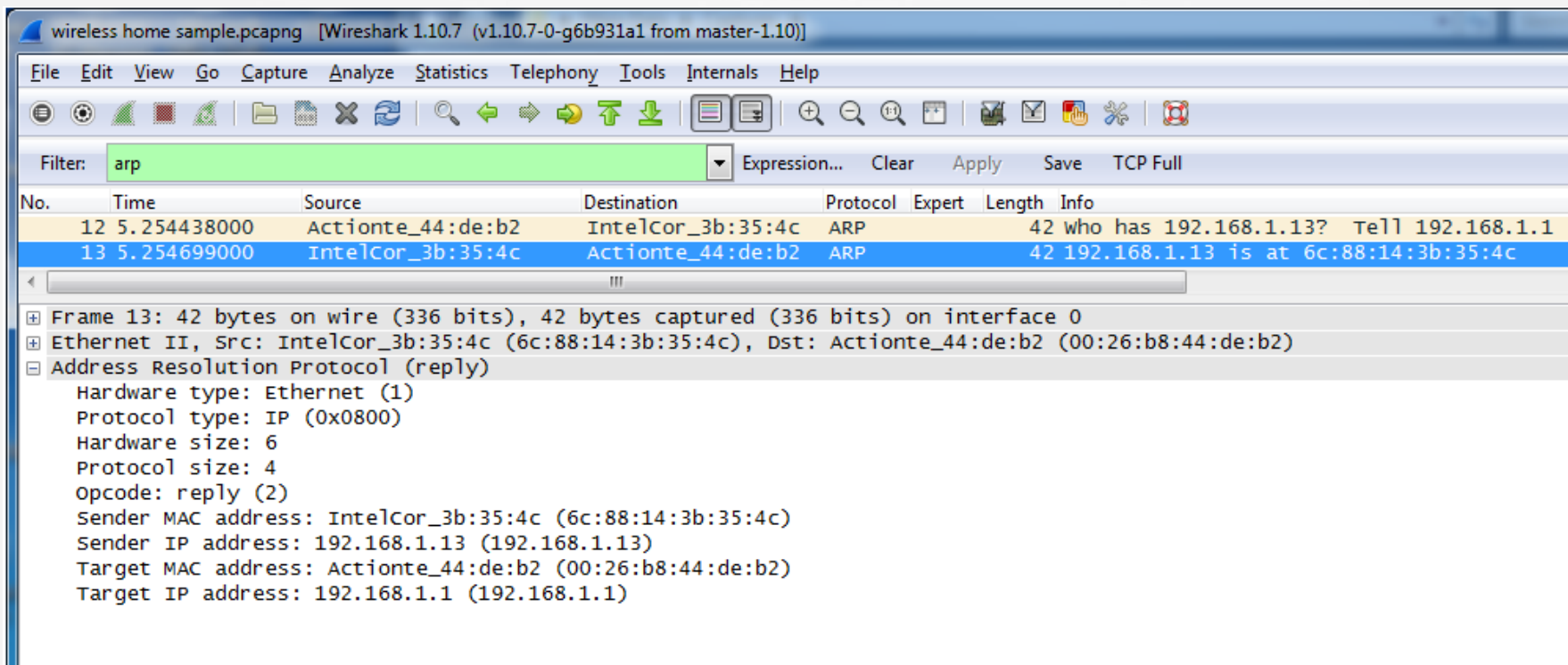
» ARP fundamentals

- Resolves IP addresses to MAC addresses
- Broadcast based
- Works in conjunction with other network devices

» Possible issues

- Sticky
- Storms
- Chattering
- Spoofing
- Sweeps
- Proxy
- Cache
- More

IP Resolution



wireless home sample.pcapng [Wireshark 1.10.7 (v1.10.7-0-g6b931a1 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **arp** Expression... Clear Apply Save TCP Full

No.	Time	Source	Destination	Protocol	Expert	Length	Info
12	5.254438000	Actionte_44:de:b2	IntelCor_3b:35:4c	ARP		42	who has 192.168.1.13? Tell 192.168.1.1
13	5.254699000	IntelCor_3b:35:4c	Actionte_44:de:b2	ARP		42	192.168.1.13 is at 6c:88:14:3b:35:4c

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0

- Ethernet II, Src: IntelCor_3b:35:4c (6c:88:14:3b:35:4c), Dst: Actionte_44:de:b2 (00:26:b8:44:de:b2)
- Address Resolution Protocol (reply)
 - Hardware type: Ethernet (1)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - opcode: reply (2)
 - Sender MAC address: IntelCor_3b:35:4c (6c:88:14:3b:35:4c)
 - Sender IP address: 192.168.1.13 (192.168.1.13)
 - Target MAC address: Actionte_44:de:b2 (00:26:b8:44:de:b2)
 - Target IP address: 192.168.1.1 (192.168.1.1)

Questions?