



Network Layers & the OSI Model

Understanding Networking Concepts

- » **Fundamental network knowledge needed to use Wireshark**
- » **How data traverses a network**
 - Traffic flow concepts from source to destination
- » **OSI model**
 - 7 layers and mapping of different protocol stacks
 - Understanding of encapsulation of data and the protocol stack (headers)

Wireshark & Protocols

The screenshot displays the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the 'Local Area Connection' using Wireshark 1.10.6. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, Internals, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar shows the active filter: 'arp.src.proto_ipv4'. The main display area is a table of captured packets, with the first packet selected. Below the table, the packet details pane shows the raw data in hexadecimal and ASCII format.

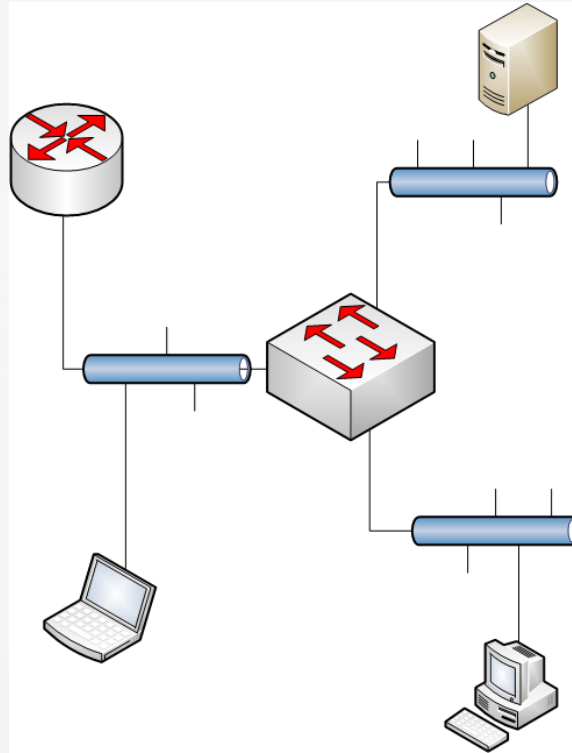
No.	Time	Source	Destination	Protocol	Length	Info
9	0.16381100	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.183? Tell 10.121.90.3
10	0.16702300	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.189? Tell 10.121.90.2
86	0.51021400	LcfHeFe_05:39:ea	Broadcast	ARP	60	who has 169.254.62.40? Tell 10.121.90.194
89	0.54091900	NecInfro_ef:98:26	Broadcast	ARP	60	who has 10.121.78.1? Tell 10.121.79.77
91	0.70289800	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.158? Tell 10.121.90.3
92	0.71242300	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.157? Tell 10.121.90.3
101	0.77457200	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.188? Tell 10.121.90.2
104	1.04457300	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.250? Tell 10.121.90.3
115	1.50206600	NecInfro_ef:85:08	Broadcast	ARP	60	who has 10.121.78.1? Tell 10.121.79.67
122	2.05647200	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.160? Tell 10.121.90.3
130	2.76470600	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.109? Tell 10.121.90.2
136	3.00008200	Dell_6a:e3:92	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.170
137	3.00981900	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.172? Tell 10.121.90.3
147	3.43614200	Elitegro_31:c9:12	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.179
151	3.59697500	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.160? Tell 10.121.90.2
153	3.73305400	Microsof_5a:62:00	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.203
159	4.16513400	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.183? Tell 10.121.90.3
161	4.17099100	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.189? Tell 10.121.90.2
162	4.18950400	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.160? Tell 10.121.90.3
166	4.34280000	Elitegro_1e:f7:91	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.181
167	4.40938600	LcfHeFe_1d:86:2f	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.126
170	4.78534500	Cisco_56:dd:c7	Broadcast	ARP	60	who has 10.121.90.188? Tell 10.121.90.2
173	4.85251100	Dell_36:75:6f	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.148
174	4.94340700	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.250? Tell 10.121.90.3
175	4.95062000	Micro-st_c8:97:3a	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.153
179	5.09502000	Micro-st_c8:96:57	Broadcast	ARP	60	who has 10.121.90.194? Tell 10.121.90.154
182	5.25176800	Cisco_e2:7b:47	Broadcast	ARP	60	who has 10.121.90.157? Tell 10.121.90.3

```
0000 ff ff ff ff ff ff 10 f3 11 e2 7b 47 08 06 00 01 .....:G...
0010 08 00 06 04 00 01 10 f3 11 e2 7b 47 0a 79 5a 03 .....:G.yz.
0020 00 00 00 00 00 00 0a 79 5a b7 00 00 00 00 00 00 .....yZ.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....:..
```

Network Lab

- » Simple network with Layer 2 and Layer 3, multiple segments and common scenarios
- » How to capture traffic
 - Port mirroring
 - Endpoints
- » Troubleshooting problems
 - Use Wireshark to capture traffic
 - Review traffic to analyze network, protocols, and traffic flow

Network Lab



Connectivity & the OSI Model

» Layer 1

- Cabling and electrical signals
- Wireless

» Layers 2–7

- As data flows from endpoints on a network, it changes while traversing different layer devices
- Data is encapsulated and addresses are changed

» Ports, sockets, etc.

- Higher-layer protocols use other functionality to establish connections

Hardware Connectivity

» Network interfaces

- NIC card
- Ports
- Probes

» Other hardware

- Switches, routers, firewalls, IPS units, load balancers, and other hardware change way data is captured and interpreted

Traffic Flow Analysis

» Data captured for analysis can reveal many issues

- Bandwidth
- Corruption
- Incorrect path
- Latency
- Many others

» Source to destination

- Data is commonly captured and analyzed from a source computer to a destination computer
- Data is analyzed to isolate and find root cause of a known or unknown problem

Encapsulation

» Traffic flow and the OSI model

» Data encapsulation

- Headers
- Protocol analysis of traffic flow

» Protocol decode and inspection

- When data is captured, it can be analyzed at all applicable layers to show the “under the hood” details needed to solve problems

Network Lab

```
101 0.774572000 Cisco_56:dd:c7 Broadcast ARP 60 Who has 10.121.90.188? Tell 10.121.90.2

[-] Frame 101: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
    Interface id: 0
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr 22, 2014 08:27:28.604954000 Eastern Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1398169648.604954000 seconds
    [Time delta from previous captured frame: 0.044593000 seconds]
    [Time delta from previous displayed frame: 0.062149000 seconds]
    [Time since reference or first frame: 0.774572000 seconds]
    Frame Number: 101
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
    [+ Ethernet II, src: Cisco_56:dd:c7 (f0:f7:55:56:dd:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    [+ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff f0 f7  55 56 dd c7 08 06 00 01  ..... UV.....
0010  08 00 06 04 00 01 f0 f7  55 56 dd c7 0a 79 5a 02  ..... UV...yZ.
0020  00 00 00 00 00 00 0a 79  5a bc 00 00 00 00 00  .....y Z.....
0030  00 00 00 00 00 00 00 00  00 00 00 00  ..... .....
```

Capturing Protocol Data

- » **Captured protocol data can be inspected for issues**
- » **Protocol analysis**
 - Opens up the data for inspection
 - Helps find problems you cannot see without capturing data for inspection
- » **Traffic analysis**
 - Used to find bandwidth, latency, and other network issues