



EMT2455 Data Communications
§ 4. Network Layer

Dr. Xiaohai Li

xhli@citytech.cuny.edu

Dept. of Computer Eng. Tech., NYCCT

Last Update: Nov. 2014



Copyright Notice

- *The slides include pictures, figures, diagrams, tables and other contents from a variety of sources. Use them for educational purpose ONLY. Copyrights are reserved by their original authors and/or publishers.*

Copyright of all other contents are reserved.



Contents

- **Ch4.1. ICMP, IGMP and ARP**
- **Ch4.2. IP Addressing**



Contents

- **Ch4.1. ICMP, IGMP and ARP**
- **Ch4.2. IP Addressing**



Protocols Defined on Network Layer

- ARP: Address Resolution Protocol
- NDP: Neighbor Discovery Protocol (similar to ARP, but used for IPv6)
- IP: Internet Protocol, including Internet Protocol version 4 (IPv4) and IPv6
- ICMP: Internet Control Message Protocol. Defines the “ping” command
- IGMP: Internet Group Message Protocol



TCP/IP Model

- Application Layer: HTTP, FTP, DHCP, DNS...
- Transport Layer: TCP, UDP
- Internet Layer: IP, ICMP, IGMP
- Link Layer: ARP, NDP, MAC, PPP



ICMP

- **ICMP:** Internet Control Message Protocol
- **PING (Packet InterNet Groper):** A very important network troubleshooting tool provided by ICMP.
- **How “ping” works?** By sending *ICMP echo request packet* to a target host, then waiting for ICMP response, and measuring the time duration.
- **What “ping” can do?** To verify connectivity with another host in the network. The destination host could be in a LAN, a WAN, or even the Internet.
- **Limits of PING:** If the destination host turns OFF, it cannot verify the connection.



IGMP

- **IGMP: Internet Group Message Protocol.**
- IGMP is used for **multicasting** (sending data to many destination hosts).
- The addresses used to send a multicast data packet are called **multicast addresses**.
- An example of an application that uses IGMP packets is when a router uses multicasting to share routing tables.



IGMP

- Another example of using IGMP: to stream video/audio to multiple hosts.
- Streaming means the data are sent without waiting for any acknowledgement that the data packets were delivered. In fact, in the IGMP protocol, the source doesn't care if the destination receives a packet.



ARP

- **ARP** (Address Resolution Protocol): to resolve an IP address to a hardware address for final delivery of data packets to the destination IP.
- Packets being used by ARP: **ARP Request** and **ARP Response**



ARP Procedure

- Suppose computer *Alpha* wants to access a destination IP of 120.200.56.10
- **Step 1:** *Alpha* issues a query in the network by broadcasting a **ARP Request** packet, asking which NIC has this IP address (120.200.56.10).
- **Step 2:** the host with the IP address 120.200.56.10 replies with an **ARP Response** packet that contains the hardware address (MAC address) of the destination host.

ARP Revealed by Capsa

- **Capsa:** a popular packet/protocol analyzer. Easy to use. Supports Windows ONLY by now
- Find the MAC and IP Addresses of your computer first!
 - Windows command:
ipconfig/all
 - Linux/Unix command:
ifconfig

See instructor's demonstration

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig/all

Windows IP Configuration

Host Name . . . . . : U646XLI
Primary Dns Suffix . . . . . : citytech.cuny.edu
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : citytech.cuny.edu
                                citytech.cuny.edu
                                cuny.edu

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : citytech.cuny.edu
   Description . . . . .           : Intel(R) 82567LM-3 Gigabit Network C
onnection
   Physical Address. . . . .       : B8-AC-6F-20-2B-68
   Dhcp Enabled. . . . .           : Yes
   Autoconfiguration Enabled . . . : Yes
   IP Address. . . . .             : 10.15.60.137
   Subnet Mask . . . . .           : 255.255.255.0
   Default Gateway . . . . .       : 10.15.60.1
   DHCP Server . . . . .           : 10.10.200.10
   DNS Servers . . . . .           : 10.10.200.10
                                       10.10.200.11
                                       128.228.1.10
   Primary WINS Server . . . . .   : 10.10.200.10
   Secondary WINS Server . . . . . : 10.10.200.11
   Lease Obtained. . . . .         : Monday, April 08, 2013 3:45:30 PM
   Lease Expires . . . . .         : Tuesday, April 16, 2013 3:45:30 PM

C:\>
```

Address Resolving Procedure Revealed by Capsa

Step 1. An **ARP Request** packet is sent by source host B8:AC:6F:20:2B:68 (with IP: 10.15.60.137): “Who is 10.15.60.22? Tell 10.15.60.137” (interpretation by Capsa).

Note: Pay attention at the No. of the captured packet.

The screenshot shows the Capsa interface with a table of captured packets. The highlighted packet (No. 402) is an ARP request. The details pane shows the following information:

Field	Value
Packet Length	46
Captured Length	42
Timestamp	2013-04-09 17:59:07.616843
Ethernet Type II	[0/14]
Destination Address	FF:FF:FF:FF:FF:FF [0/6]
Source Address	B8:AC:6F:20:2B:68 [6/6]
Protocol	0x0806 (ARP) [12/2]
ARP - Address Resolution Protocol	[14/28]

Address Resolving Procedure Revealed by Capsa

Step 2. An **ARP Response** packet is answered by 00:9C:02:03:13:35 (with the asked IP: 10.15.60.22): “10.15.60.22 is at 00:9C:02:03:13:35”(interpretation by Capsa).

The screenshot shows the Colasoft Capsa 7 Free interface. The main window displays a table of captured packets. The selected packet is an ARP response. The packet details pane shows the Ethernet II header and ARP protocol fields.

No.	Absolute Time	Source	Destination	Protocol	Size	Summary
403	17:59:07.61...	00:9C:02:03:13:35	B8:AC:6F:20:2B:68	ARP	64	10.15.60.22 is at 00:9C:02:03:13:35
407	17:59:07.62...	08:00:09:8E:B8:91	B8:AC:6F:20:2B:68	ARP	64	10.15.60.241 is at 08:00:09:8E:B8:91
540	17:59:47.74...	00:19:B9:1D:FD:2D	B8:AC:6F:20:2B:68	ARP	64	10.15.60.67 is at 00:19:B9:1D:FD:2D
588	18:00:02.27...	00:25:64:39:4E:31	B8:AC:6F:20:2B:68	ARP	64	10.15.60.84 is at 00:25:64:39:4E:31
5475	18:03:41.88...	00:0F:90:2B:3C:BF	B8:AC:6F:20:2B:68	ARP	64	10.15.60.1 is at 00:0F:90:2B:3C:BF
5525	18:03:54.82...	00:25:64:39:22:00	B8:AC:6F:20:2B:68	ARP	64	10.15.60.201 is at 00:25:64:39:22:00
6128	18:05:29.77...	00:25:64:39:4E:31	B8:AC:6F:20:2B:68	ARP	64	10.15.60.84 is at 00:25:64:39:4E:31

The selected packet details are as follows:

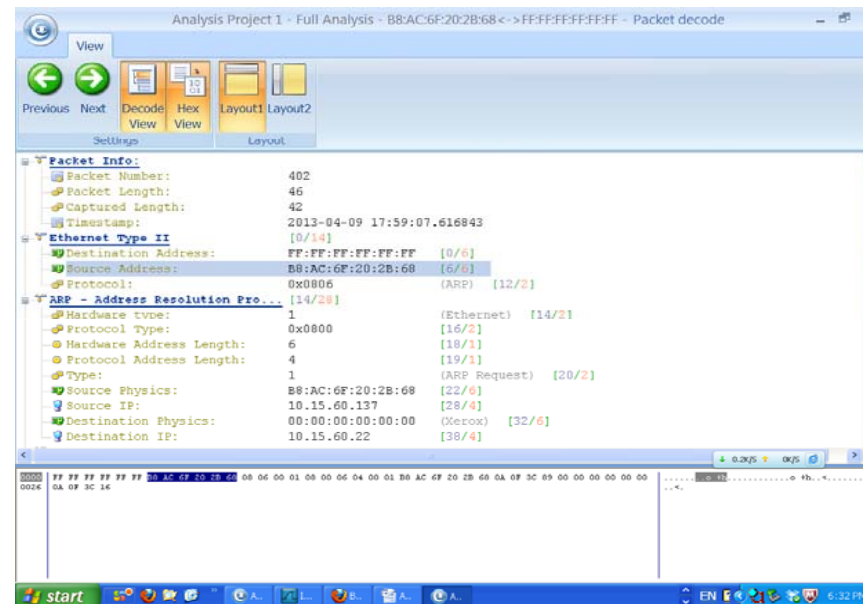
- Packet Length: 64
- Captured Length: 60
- Timestamp: 2013-04-09 17:59:07.617189
- Ethernet Type II: [0/14]
- Destination Address: B8:AC:6F:20:2B:68 [0/6]
- Source Address: 00:9C:02:03:13:35 [6/6]
- Protocol: 0x0806 (ARP) [12/2]
- ARP - Address Resolution Protocol [14/28]

ARP Packets Revealed by Capsa

- ARP Request Packet:
Sender: B8:AC:6F:20:
2B:68 (with IP: 10.15.60.137)
Destination: ???

- ARP Response Packet:
Sender: ???
Destination: ???

Lab 3. ARP: See lab handout for details



ARP Revealed by WireShark

Similar to the above

The screenshot shows the Wireshark interface with a list of network packets. The selected packet (No. 419) is an ARP request. The packet details pane shows the following information:

- Frame 419: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
- Ethernet II, Src: Dell_20:2b:68 (b8:ac:6f:20:2b:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Dell_20:2b:68 (b8:ac:6f:20:2b:68)
- Type: ARP (0x0806)
- Address Resolution Protocol (request)

The packet bytes pane shows the following hex and ASCII representation:

```
0000 ff ff ff ff ff ff b8 ac 6f 20 2b 68 08 06 00 01 ..... o +h....
0010 08 00 06 04 00 01 b8 ac 6f 20 2b 68 0a 0f 3c 89 ..... o +h..<.
0020 00 00 00 00 00 00 0a 0f 3c f1 ..... <.
```




Contents

- **Ch4.1. ICMP, IGMP and ARP**
- **Ch4.2. IP Addressing**
 - *See lecture notes*