

# Data-link layer

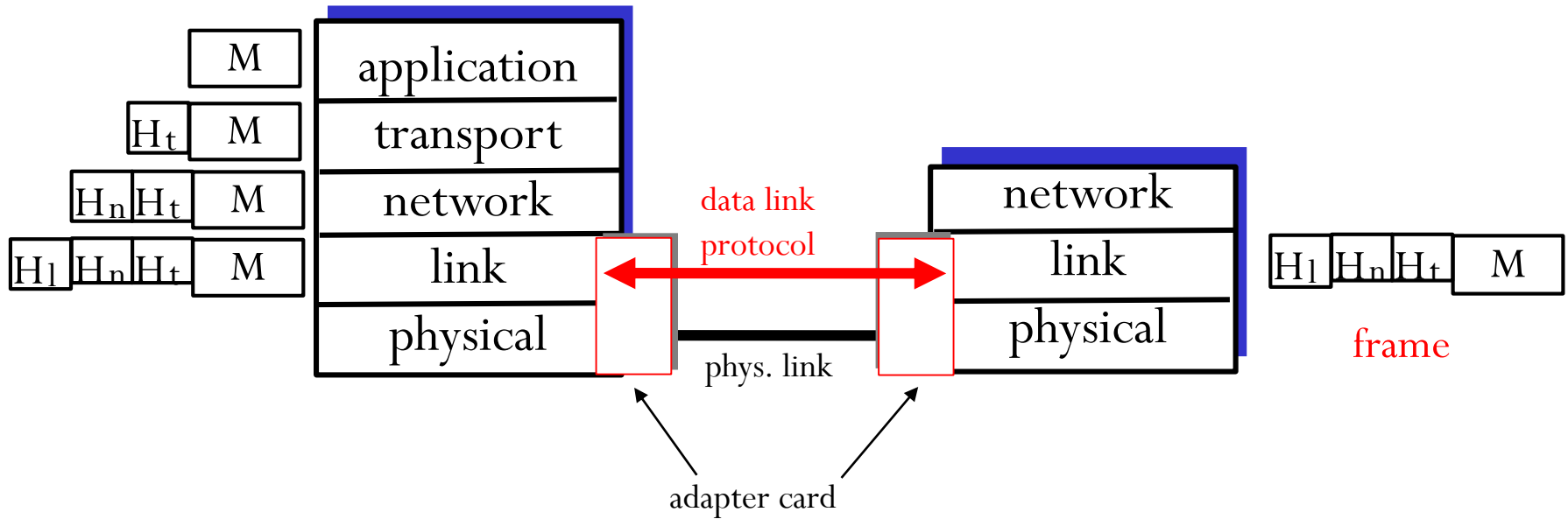


Portland State  
Computer Science

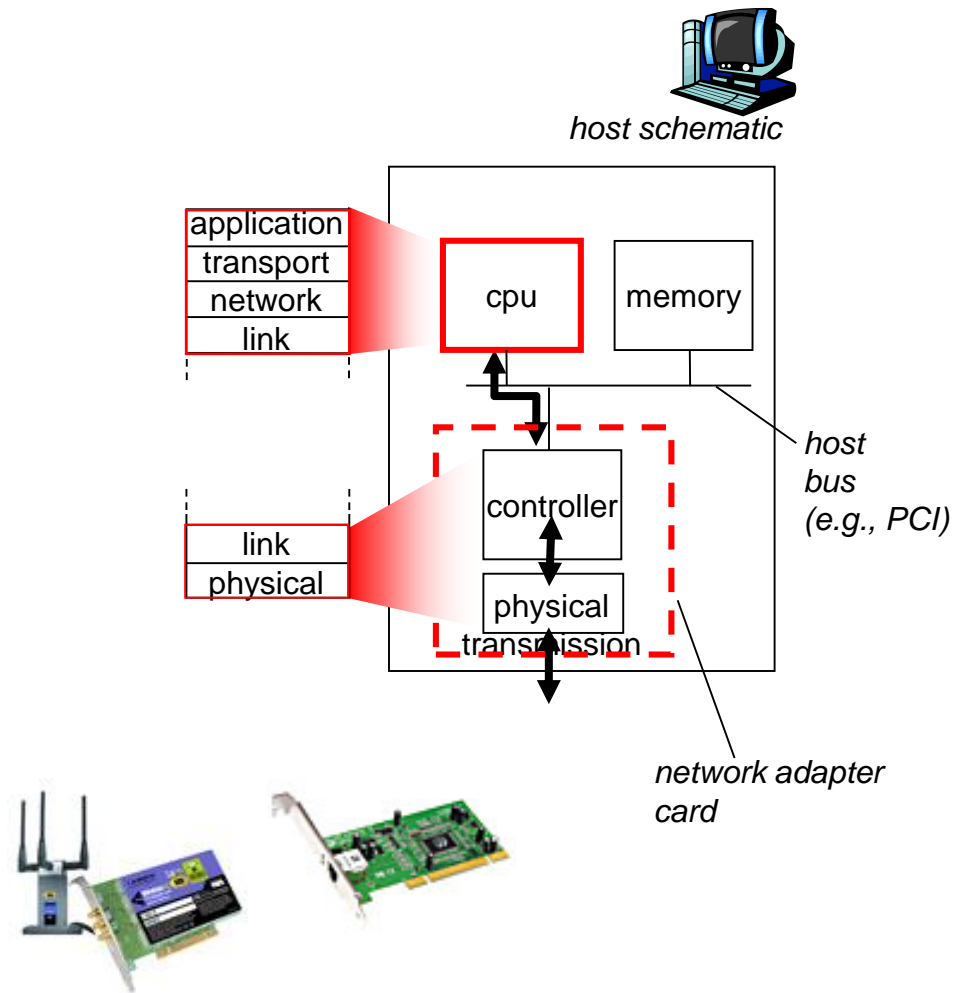
# Data-link layer

- Referred to as “layer 2”
  - Physical layer is “layer 1”
- Transferring datagram from one node to adjacent node over a physical link
  - wired links (Ethernet)
  - wireless links (802.11, Bluetooth)
- A layer-2 packet is called a **frame**

# Protocol stack picture



# Organization of stack on end-host



# Link Layer Functions

- Flow Control
  - Pacing between adjacent sending and receiving nodes
- Security
  - Mainly for broadcast data-link layers such as wireless LANs (e.g. WPA for 802.11)
  - End-to-end principle would suggest encryption at higher layers (e.g. TLS/HTTPS)
  - But ... see recent battle over metadata (Section 215)
    - Motivates encrypting headers \*and\* payloads for some...
- Error detection/correction using checksums/CRCs/FEC
- Medium access and quality of service
  - Channel access if shared medium

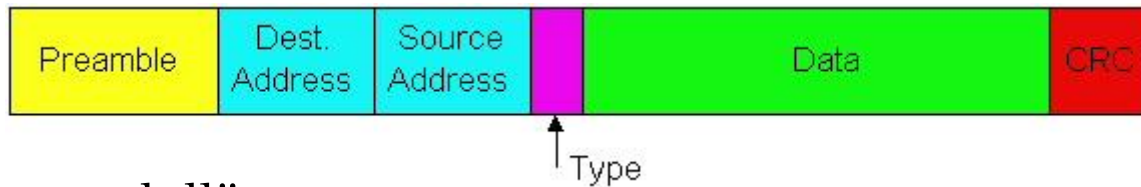
# Link Layer Functions

- Demux to upper protocol
  - Data-link layer can support any number of network layers
    - Type field in data-link header specifies network layer for packet
    - IP is one of many network layers
    - Other network layers (IPX, EtherTalk, SNA, etc) at
      - <https://en.wikipedia.org/wiki/EtherType>
  - Common Ethernet protocol types
    - 0800 DOD Internet Protocol (IP)
    - 0806 Address Resolution Protocol (ARP)
    - For network virtualization in the cloud (virtual private networks, virtual private clouds)
      - 8100 VLAN tagging
      - Virtual networks at L2 level

# Link Layer Functions

- Framing
  - Data encapsulated in link-layer frame before transmission over physical link, adding header/trailer
  - Physical addresses used in frame headers to identify source and destination (not IP)

# Example: Ethernet frame



- "Outermost doll"
- Preamble to synchronize network adapters for sender and receiver
- Type: indicates the higher layer protocol
  - mostly IP but others include Novell IPX and AppleTalk
- Data – 46 to 1500 bytes
  - Inner doll (e.g. IP/TCP/HTTP payload)
- CRC: 4 byte cyclic redundancy code (error detection)
- 6 byte (48-bit) hardware addresses
  - Different from IP address
  - Globally unique (allocated to manufacturers by IEEE)
    - Also known as media-access control or MAC addresses
  - Used to get from one interface to another physically-connected interface on same network
    - Identifies both source and destination of transmission



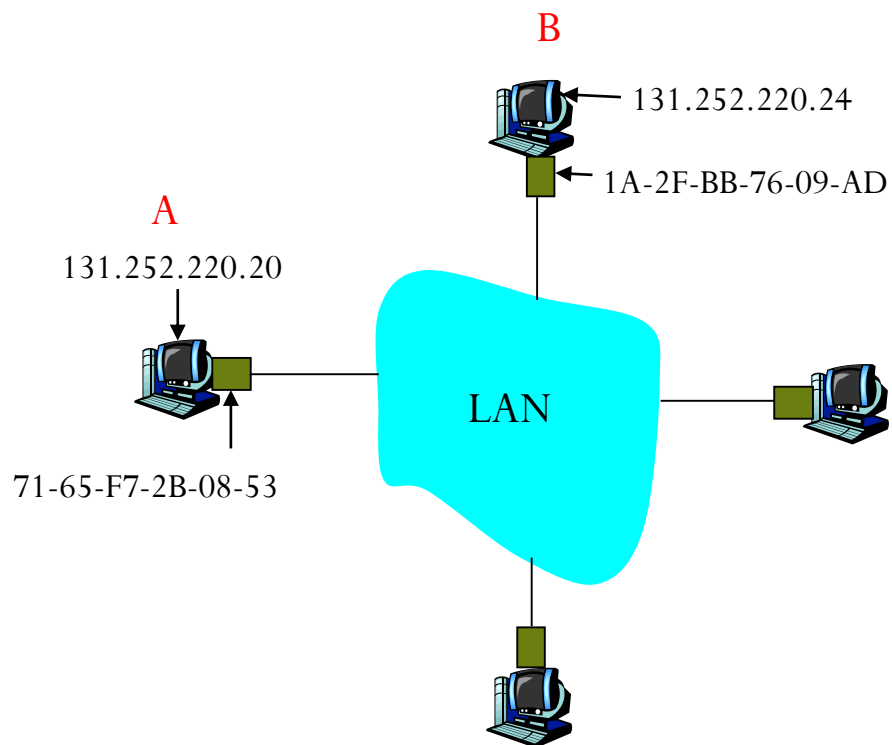
# MAC vs IP addressing

- MAC address
  - Flat (not hierarchical)
    - Like Social Security Numbers
    - Does not change when machine is moved (portable)
- IP addresses
  - Hierarchical
    - Like postal address
    - Depends on IP subnet that node is attached to
    - Must change when machine is moved (not portable)

ARP

# ARP: Address Resolution Protocol

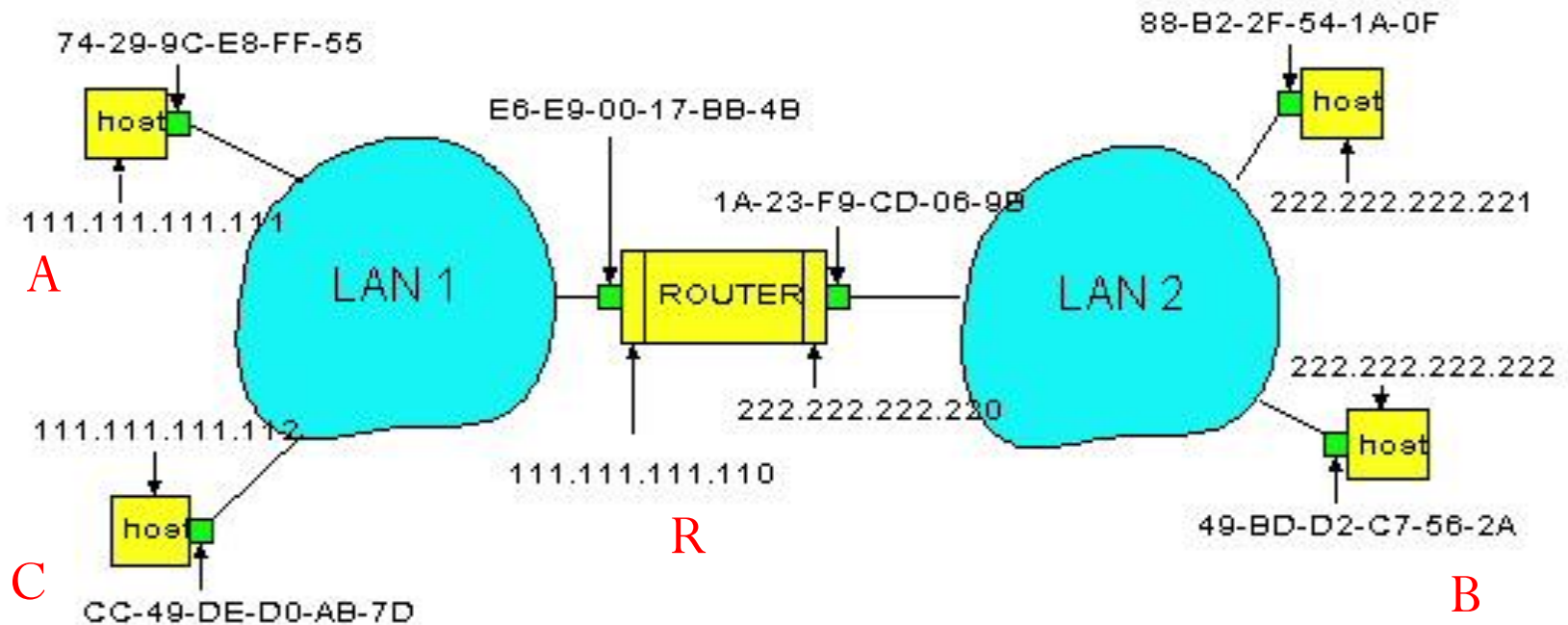
How does A determine MAC address of B given B's IP address?



- A broadcasts interest in B's MAC address
  - Dest MAC address = FF-FF-FF-FF-FF-FF
  - all machines on LAN receive ARP query
- B receives ARP packet, responds to A with its MAC address (1A-2F-...AD)
  - Frame sent to A's MAC address (71-65-...53)
- A caches IP-to-MAC address pair in its **ARP table**
  - "Soft state": Times out (goes away) unless refreshed
    - `< IP address; MAC address; TTL >`
  - TTL = Time To Live
- Accessed via
  - `arp -a`
  - `cat /proc/net/arp`

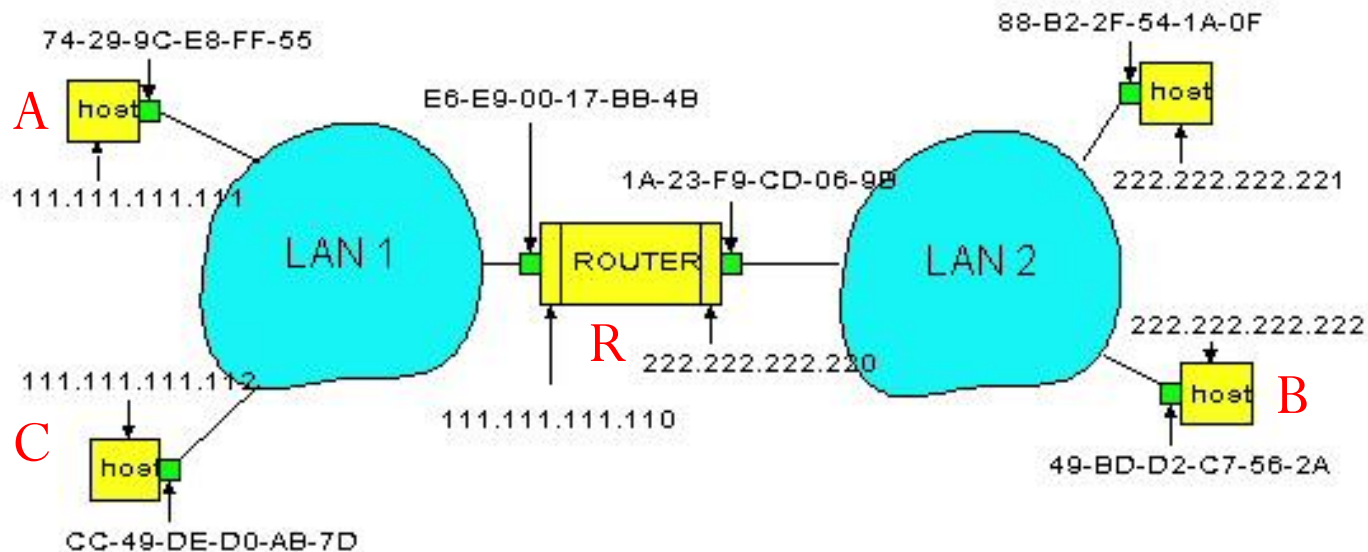
# Routing to another LAN

- What if A & B are on different networks?
  - Must **send datagram from A to B via router R**



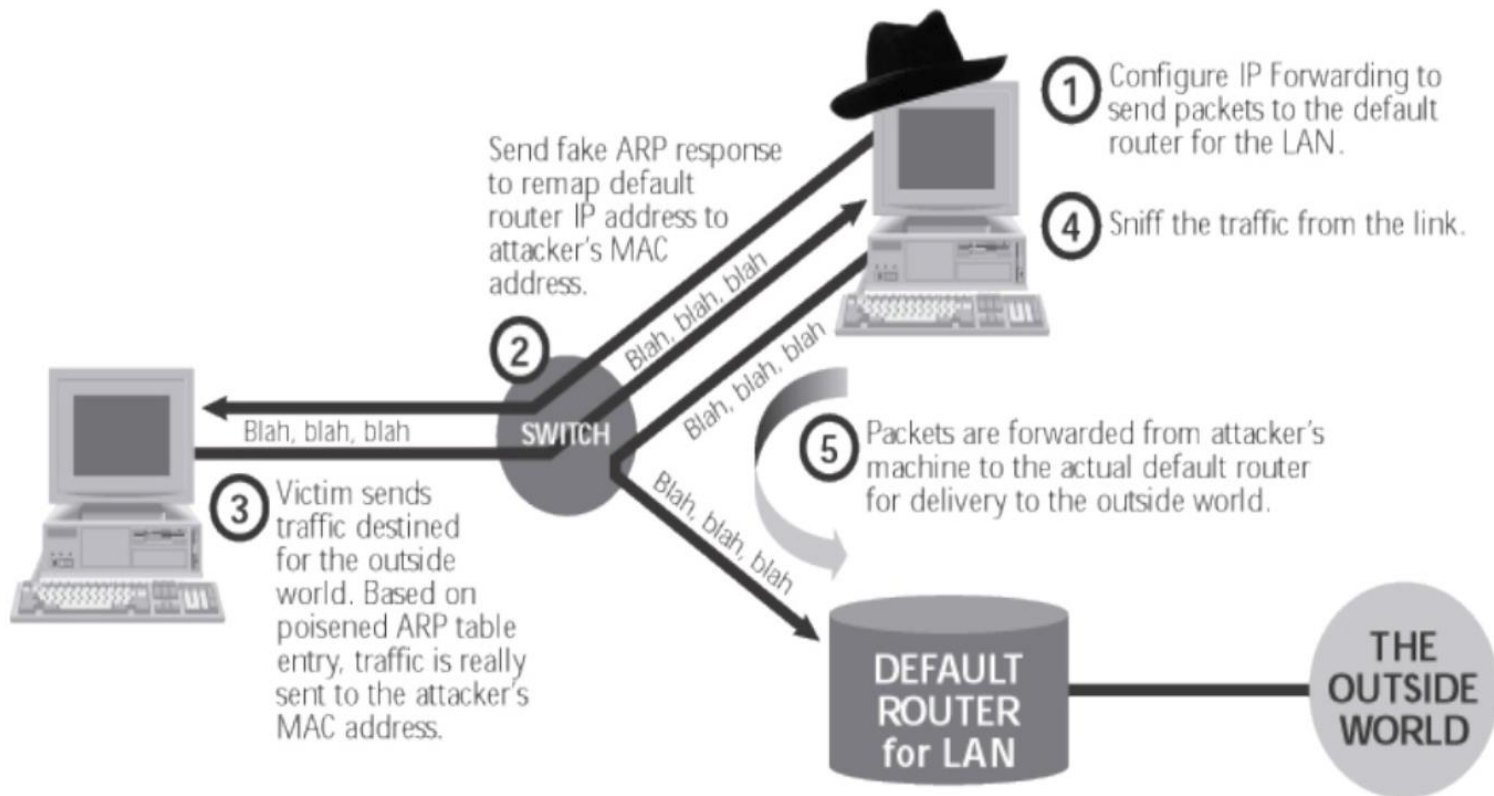
- Two ARP tables in router R, one for each interface/network
- In routing table at source A, default route 111.111.111.110
- A creates datagram with source A, destination B

- A checks route table to find B is not on its network
- A uses ARP to get R's MAC address (ARP for 111.111.111.110)
- A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram
- A's adapter sends frame
- R's adapter receives frame
- R removes IP datagram from Ethernet frame, sees its destined to B
- Looks up its route table and sees that B is directly attached to interface on LAN2
- R uses ARP on LAN2 to get B's MAC address
- R creates new frame containing A-to-B IP datagram sends to B
- What prevents C from responding to A's initial ARP request for R?



# ARP issues

- Not authenticated
- Subject to spoofing attacks (ARP poisoning)
  - dsniff, ettercap
  - Subterfuge credential harvesting toolkit
- Spoofing and man-in-the-middle attacks possible in many protocols



# DHCP

# DHCP

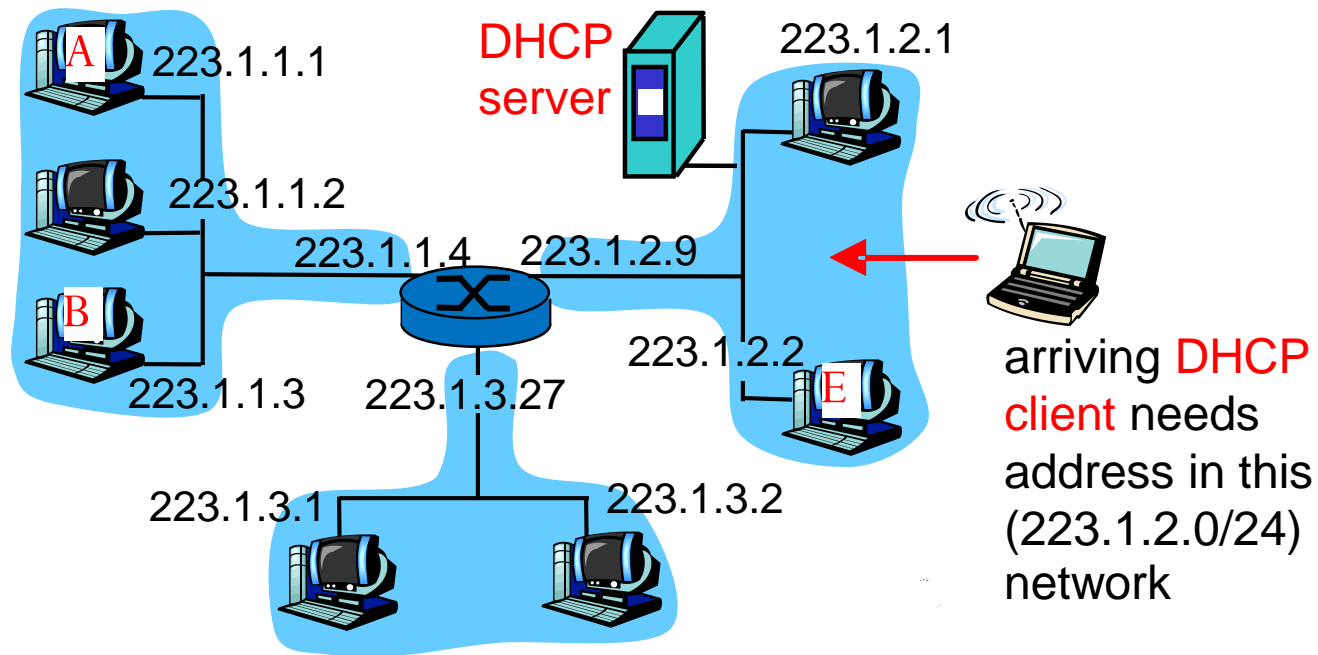
Q: How does host get an IP address on subnet?

- Hard-coded by system admin in a file
  - Windows
    - `control-panel->network->configuration->tcp/ip->properties`
  - Linux
    - `/etc/networks/interfaces`
- Dynamically ask network for one
  - DHCP: Dynamic Host Configuration Protocol
  - Typically used in wireless networks



# DHCP client-server scenario

- DHCP server on the network issues you an address



DHCP server: 131.252.220.5

### DHCP discover

src : 0.0.0.0, 68  
dest.: 255.255.255.255, 67  
yiaddr: 0.0.0.0  
transaction ID: 654

arriving  
client



### DHCP offer

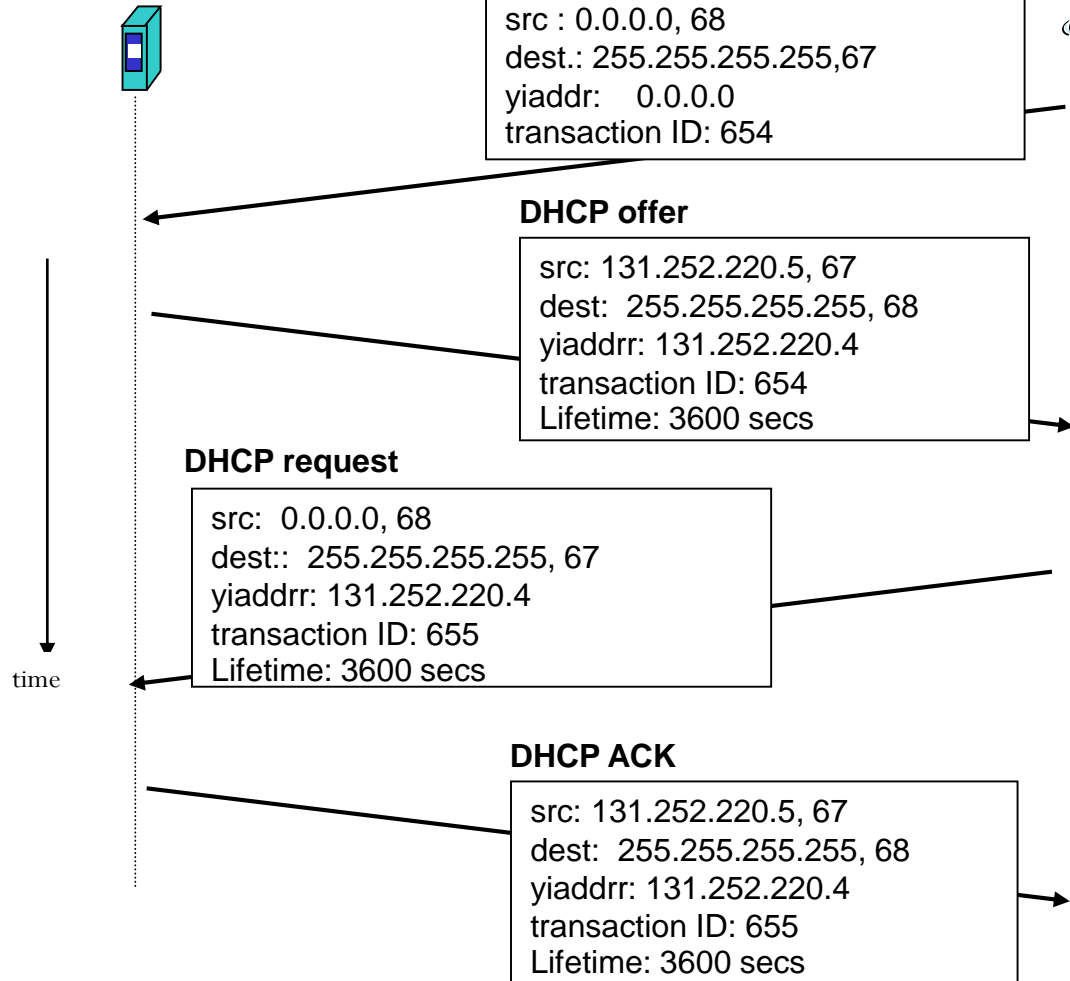
src: 131.252.220.5, 67  
dest: 255.255.255.255, 68  
yiaddr: 131.252.220.4  
transaction ID: 654  
Lifetime: 3600 secs

### DHCP request

src: 0.0.0.0, 68  
dest.: 255.255.255.255, 67  
yiaddr: 131.252.220.4  
transaction ID: 655  
Lifetime: 3600 secs

### DHCP ACK

src: 131.252.220.5, 67  
dest: 255.255.255.255, 68  
yiaddr: 131.252.220.4  
transaction ID: 655  
Lifetime: 3600 secs



- ARP: Give me the MAC address for an IP address
- DHCP: Give me an IP address given a MAC address

# DHCP: Dynamic Host Configuration Protocol

- Parameters typically configured
  - IP address
  - Default router : Where to send packets that are not local to network
  - Netmask (more later) : IP addresses associated with network
  - DNS server : IP address of server that resolves names (e.g. [www.google.com](http://www.google.com))
- Allows reuse of addresses
- Addresses only held while machine is connected and “on”
- What prevents someone from creating hundreds of virtual network interfaces and hogging all of the addresses to him/herself?

# Wireshark (for your lab)

# Wireshark

- Defacto tool for monitoring network activity
- Built on top of libpcap (packet capture library)
- Needs to be run with administrator privileges (`sudo`)
  - Supports promiscuous mode that sends *\*all\** frames up to host regardless of destination hardware address
  - How might one detect someone running in promiscuous mode on your network?
- Supports all major network protocols

# Link-layer

\*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf 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
703	40.6891080	131.252.220.66	10.0.2.15	TCP	60	80->50758 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
704	40.6891310	10.0.2.15	131.252.220.66	TCP	54	50758->80 [ACK] Seq=1 Ack=1 win=256960 Len=0
705	40.7123390	10.0.2.15	131.252.220.66	HTTP	429	GET / HTTP/1.1
706	40.7128190	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=1 Ack=376 win=65535 Len=0
707	40.7130890	131.252.220.66	10.0.2.15	HTTP	746	HTTP/1.1 200 OK (text/html)
708	40.9150500	10.0.2.15	131.252.220.66	TCP	54	50753->80 [ACK] Seq=376 Ack=693 win=254192 Len=0
709	42.6489380	10.0.2.15	131.252.220.66	HTTP	395	GET /favicon.ico HTTP/1.1
710	42.6490940	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=693 Ack=717 win=65535 Len=0
711	42.6492100	131.252.220.66	10.0.2.15	HTTP	1417	HTTP/1.1 200 OK (GIF89a)

Frame 705: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0

- Ethernet II, Src: CadmusCo\_cd:a5:97 (08:00:27:cd:a5:97), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 131.252.220.66 (131.252.220.66)
- Transmission Control Protocol, Src Port: 50753 (50753), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 375
- Hypertext Transfer Protocol

```

0000  52 54 00 12 35 02 08 00 27 cd a5 97 08 00 45 00  RT..5... ..E.
0010  01 9f 0f 5c 40 00 80 06 00 00 0a 00 02 0f 83 fc  ...@... ..
0020  dc 42 c6 41 00 50 7e 77 b4 ac e6 9f 6e 02 50 18  .B.A.P~w ....n.P.
0030  fa f0 6d df 00 00 47 45 54 20 2f 20 48 54 54 50  ..m...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 68 65 66  /1.1..Host: thef
0050  65 6e 67 73 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63  engs.com ..Connec
0060  74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65  tion: keep-alive
0070  0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75  ..Upgrade-Insecu
0080  72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a  re-Requests: 1..
0090  55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69  User-Agent: Mozi
00a0  6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73  lla/5.0 (windows
00b0  20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 29 20  NT 6.1; WOW64)
00c0  41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e  AppleWebKit/537.
00d0  33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20  36 (KHTML, like
00e0  47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 36 35  Gecko) Chrome/65
00f0  2e 30 2e 33 33 32 35 2e 31 36 32 20 53 61 66 61  .0.3325.162 Safa
0100  72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70  ri/537.36..Accep
0110  74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70  t: text/html,app
0120  6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78  lication/xhtml+x
0130  6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78  ml,application/x
0140  6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77  ml;q=0.9,image/w
0150  65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a  ebp,image/apng,*
0160  75 74 74 74 74 74 74 74 74 74 74 74 74 74 74  /%>0.8
  
```

# Network layer

\*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf 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
703	40.6891080	131.252.220.66	10.0.2.15	TCP	60	80->50758 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
704	40.6891310	10.0.2.15	131.252.220.66	TCP	54	50758->80 [ACK] Seq=1 Ack=1 win=256960 Len=0
705	40.7123390	10.0.2.15	131.252.220.66	HTTP	429	GET / HTTP/1.1
706	40.7128190	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=1 Ack=376 win=65535 Len=0
707	40.7130890	131.252.220.66	10.0.2.15	HTTP	746	HTTP/1.1 200 OK (text/html)
708	40.9150500	10.0.2.15	131.252.220.66	TCP	54	50753->80 [ACK] Seq=376 Ack=693 win=254192 Len=0
709	42.6489380	10.0.2.15	131.252.220.66	HTTP	395	GET /favicon.ico HTTP/1.1
710	42.6490940	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=693 Ack=717 win=65535 Len=0
711	42.6492100	131.252.220.66	10.0.2.15	HTTP	1417	HTTP/1.1 200 OK (JPEG)

Frame 705: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0

Ethernet II, Src: cadmusCo\_cd:a5:97 (08:00:27:cd:a5:97), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)

**Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 131.252.220.66 (131.252.220.66)**

Transmission Control Protocol, Src Port: 50753 (50753), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 375

Hypertext Transfer Protocol

```

0000 52 54 00 12 35 02 08 00 27 cd a5 97 08 00 45 00 RT..5... '.....E.
0010 01 9f 0f 5c 40 00 80 06 00 00 0a 00 02 0f 83 fc ...@.....
0020 dc 42 c6 41 00 50 7e 77 b4 ac e6 9f 6e 02 50 18 ..B.A.P~w ....n.P.
0030 fa f0 6d df 00 00 47 45 54 20 2f 20 48 54 54 50 ..m...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 68 65 66 /1.1..Host: thef
0050 65 6e 67 73 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 engs.com ..Connec
0060 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: keep-alive
0070 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..Upgrade-Insecu
0080 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Requests: 1..
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Agent: Mozi
00a0 6c 6c 61 2f 35 2e 30 20 28 5f 69 6e 64 6f 77 73 lla/5.0 (windows
00b0 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 29 20 NT 6.1; wow64)
00c0 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e AppleWebKit/537.
00d0 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 36 (KHTML, like
00e0 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 36 35 Gecko) Chrome/65
00f0 2e 30 2e 33 33 32 35 2e 31 36 32 20 53 61 66 61 .0.3325.162 Safa
0100 72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70 ri/537.36..Accep
0110 74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 t: text/html,app
0120 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 lication/xhtml+x
0130 6d 6c 2c 61 70 70 6f 6e 69 63 61 74 69 6f 6e 2f 78 ml,application/x
0140 6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77 ml;q=0.9,image/w
0150 65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a ebp,image/apng,*
0160 7f 7a 3b 71 3d 30 2e 39 0d 0a 41 63 63 65 70 74 /*q=0.8 Accept
  
```

# Transport layer

\*Local Area Connection [Wireshark 1.12.1 (v1.12.1-0-g01b65bf 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
703	40.6891080	131.252.220.66	10.0.2.15	TCP	60	80-50758 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=1460
704	40.6891310	10.0.2.15	131.252.220.66	TCP	54	50758->80 [ACK] Seq=1 Ack=1 win=256960 Len=0
705	40.7123390	10.0.2.15	131.252.220.66	HTTP	429	GET / HTTP/1.1
706	40.7128190	131.252.220.66	10.0.2.15	TCP	60	80-50753 [ACK] Seq=1 Ack=376 win=65535 Len=0
707	40.7130890	131.252.220.66	10.0.2.15	HTTP	746	HTTP/1.1 200 OK (text/html)
708	40.9150500	10.0.2.15	131.252.220.66	TCP	54	50753->80 [ACK] Seq=376 Ack=693 win=254192 Len=0
709	42.6489380	10.0.2.15	131.252.220.66	HTTP	395	GET /favicon.ico HTTP/1.1
710	42.6490940	131.252.220.66	10.0.2.15	TCP	60	80-50753 [ACK] Seq=693 Ack=717 win=65535 Len=0
711	42.6492100	131.252.220.66	10.0.2.15	HTTP	1417	HTTP/1.1 200 OK (text/css)

[+] Frame 705: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0  
 [+] Ethernet II, Src: CadmusCo\_cd:a5:97 (08:00:27:cd:a5:97), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
 [+] Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 131.252.220.66 (131.252.220.66)  
 [+] Transmission Control Protocol, Src Port: 50753 (50753), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 375  
 [+] Hypertext Transfer Protocol

```

0000  52 54 00 12 35 02 08 00 27 cd a5 97 08 00 45 00  RT..5... '.....E.
0010  01 9f 0f 5c 40 00 80 06 00 00 0a 00 02 0f 83 fc  ... \@... ..
0020  dc 42 c6 41 00 50 7e 77 b4 ac e6 9f 6e 02 50 18  .B.A.P~w ...n.P.
0030  fa f0 6d df 00 00 47 45 54 20 2f 20 48 54 54 50  ..m...GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 68 65 66  /1.1..Host: thef
0050  65 6e 67 73 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63  engs.com ..Connec
0060  74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65  tion: keep-alive
0070  0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75  ..Upgrade-Insecu
0080  72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a  re-Requests: 1..
0090  55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69  User-Agent: Mozil
00a0  6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73  lla/5.0 (windows
00b0  20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 29 20  NT 6.1; WOW64)
00c0  41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e  AppleWebKit/537.
00d0  33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20  36 (KHTML, like
00e0  47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 36 35  Gecko) Chrome/65
00f0  2e 30 2e 33 33 32 35 2e 31 36 32 20 53 61 66 61  .0.3325.162 Safa
0100  72 69 2f 35 33 37 2e 33 36 0d 0a 41 63 63 65 70  ri/537.36..Accep
0110  74 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70  t: text/html,app
0120  6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78  lication/xhtml+x
0130  6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78  ml,application/x
0140  6d 6c 3b 71 3d 30 2e 39 2c 69 6d 61 67 65 2f 77  ml;q=0.9,image/w
0150  65 62 70 2c 69 6d 61 67 65 2f 61 70 6e 67 2c 2a  ebp,image/png,*
0160  2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74  /*;q=0.8..Accept
0170  2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c  -Encoding: gzip,
  
```



# Application layer

The image shows a Wireshark capture of network traffic on a local area connection. The main pane displays a list of packets, with packet 705 selected. The packet list pane shows the following details:

No.	Time	Source	Destination	Protocol	Length	Info
703	40.6891080	131.252.220.66	10.0.2.15	TCP	60	80->50758 [ACK] Seq=1 Ack=1 win=65535 Len=0
704	40.6891310	10.0.2.15	131.252.220.66	TCP	54	50758->80 [ACK] Seq=1 Ack=1 win=256960 Len=0
705	40.7123390	10.0.2.15	131.252.220.66	HTTP	429	GET / HTTP/1.1
706	40.7128190	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=1 Ack=376 win=65535 Len=0
707	40.7130890	131.252.220.66	10.0.2.15	HTTP	746	HTTP/1.1 200 OK (text/html)
708	40.9150500	10.0.2.15	131.252.220.66	TCP	54	50753->80 [ACK] Seq=376 Ack=693 win=254192 Len=0
709	42.6489380	10.0.2.15	131.252.220.66	HTTP	395	GET /favicon.ico HTTP/1.1
710	42.6490940	131.252.220.66	10.0.2.15	TCP	60	80->50753 [ACK] Seq=693 Ack=717 win=65535 Len=0
711	42.6492100	131.252.220.66	10.0.2.15	HTTP	1417	HTTP/1.1 200 OK (JPEG)

The packet details pane for the selected packet (705) shows the following layers:

- Frame 705: 429 bytes on wire (3432 bits), 429 bytes captured (3432 bits) on interface 0
- Ethernet II, Src: cadmusCo\_cd:a5:97 (08:00:27:cd:a5:97), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)
- Internet Protocol Version 4, Src: 10.0.2.15 (10.0.2.15), Dst: 131.252.220.66 (131.252.220.66)
- Transmission Control Protocol, Src Port: 50753 (50753), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 375
- Hypertext Transfer Protocol**

The packet bytes pane shows the raw data of the HTTP GET request:

```
0000 52 54 00 12 35 02 08 00 27 cd a5 97 08 00 45 00 RT..5... '.....E.
0010 01 9f 0f 5c 40 00 80 06 00 00 0a 00 02 0f 83 fc ...\@... ..
0020 dc 42 c6 41 00 50 7e 77 b4 ac e6 9f 6e 02 50 18 ..B.A.P~w ....n.P.
0030 fa f0 6d df 00 00 47 45 54 20 2f 20 48 54 54 50 ..m...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 68 65 66 /1.1..Host: thef
0050 65 6e 67 73 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 engs.com ..Connec
0060 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 tion: keep-alive
0070 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 ..upgrade-Insecu
0080 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a re-Requests: 1.
0090 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 User-Agent: Mozi
00a0 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 lla/5.0 (windows
00b0 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 29 20 NT 6.1; WOW64)
00c0 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e AppleWebKit/537.
00d0 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 36 (KHTML, like
00e0 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 36 35 Gecko) Chrome/65
00f0 2e 30 2e 33 33 32 35 2e 31 36 32 20 53 61 66 61 .0.3325.162 Safa
```

# ARP Labs

---