Address Resolution Protocol

COMP30040

UCD School of Computer Science

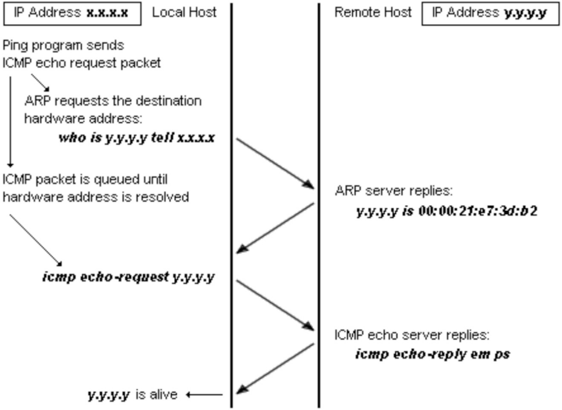
September 27, 2018

1. Address Resolution Protocol (ARP)

- Convert an IP address to a physical address, e.g., Ethernet address
- ARP is an Request/Reply communication protocol, communicated within the boundary of a single network and never routed across internetwork nodes.
- ARP is often described as residing between Layer 2 and 3 in **Open Systems Interconnection** (OSI) model, being encapsulated by Layer 2 protocols .
- A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network → The host on the network that has the IP address in the request then replies with its physical hardware address.

1. Address Resolution Protocol (ARP) - Cont

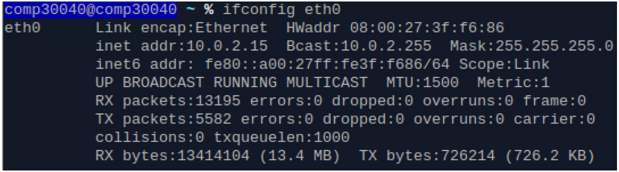
- Example of ARP: A user wants to `ping` another host computer on the same LAN (assume that no IP datagram has been received from that computer recently) → ARP is used to obtain the MAC address of the remote host.


IP Address **x.x.x.x**
Local Host
Remote Host
IP Address **y.y.y.y**
Ping program sends
ICMP echo request packet
ARP requests the destination
hardware address:
who is y.y.y.y tell x.x.x.x
ICMP packet is queued until
hardware address is resolved
ARP server replies:
y.y.y.y is 00:00:21:e7:3d:b2
icmp echo-request y.y.y.y
ICMP echo server replies:
icmp echo-reply em ps
y.y.y.y is alive

2. Linux Network tools

`ifconfig` - configure Network Interfaces

- View Network settings for a specific Network Interface



```
comp30040@comp30040 ~ % ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:3f:f6:86
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3f:f686/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5582 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13414104 (13.4 MB)  TX bytes:726214 (726.2 KB)
```

- Display details of all Interfaces including disabled Interfaces
  - `ifconfig -a`
- Enable/Disable an Interface
  - `ifconfig eth0 up`
  - `ifconfig eth0 down`
- Assign IP-address to an Interface
  - `ifconfig eth0 192.168.1.11`

2. Linux Network tools - Cont

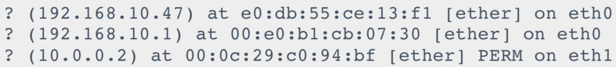
Potential problems with ARP:

- Host X does not receive ARP replies for a destination host Y with which it wishes to communicate
- ARP replies come in, but contain a MAC address associated with an incorrect host Z → **Traffic hijacking**: traffic should have been sent to Y but ends up arriving at host Z
- When dealing with such ARP-induced abnormal situations → it is useful to add static ARP entries manually on locally cached ARP tables ⇒ So, when a MAC address of a destination host Y is found in local ARP table, there is no need to send out ARP requests.

2. Linux Network tools - Cont

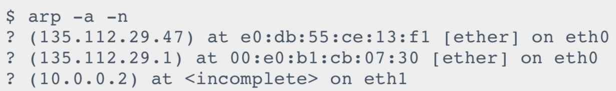
`arp` - manipulate the system ARP cache

1. **Add a static ARP entry to local ARP table**
   - `arp -s 10.0.0.2 00:0c:29:c0:94:bf` → Such command tells local ARP table that the host with IP address `10.0.0.2` has MAC address as `00:0c:29:c0:94:bf`
   - `arp -a -n` → to verify what you have just configured



```
? (192.168.10.47) at e0:db:55:ce:13:f1 [ether] on eth0
? (192.168.10.1) at 00:e0:b1:cb:07:30 [ether] on eth0
? (10.0.0.2) at 00:0c:29:c0:94:bf [ether] PERM on eth1
```

2. **Delete a static ARP entry from local ARP table**
   - `sudo arp -d 10.0.0.2`



```
$ arp -a -n
? (135.112.29.47) at e0:db:55:ce:13:f1 [ether] on eth0
? (135.112.29.1) at 00:e0:b1:cb:07:30 [ether] on eth0
? (10.0.0.2) at <incomplete> on eth1
```

2. Linux Network tools - Cont

Other commands

1. `arp-scan` - **ARP Scanner**
   - Before using `arp-scan` command, it is required to install it on your Linux virtual machine by typing: `sudo apt-get install arp-scan`
   - Type *man arp − scan* to open `man` page of the command → you should be able to obtain the necessary information to find the neighbors of a host in a LAN.
2. `ping` - **send ICMP ECHO_REQUEST to network hosts**
   - This command is used to send `ICMP ECHO_REQUEST` packets to network hosts.
   - A host receiving such request packets will echo them back to the sender → The bi-directional path between two hosts can be assessed.
   - `HINT`: Check `man` page of `ping` command to find out more information

ENJOY !!!