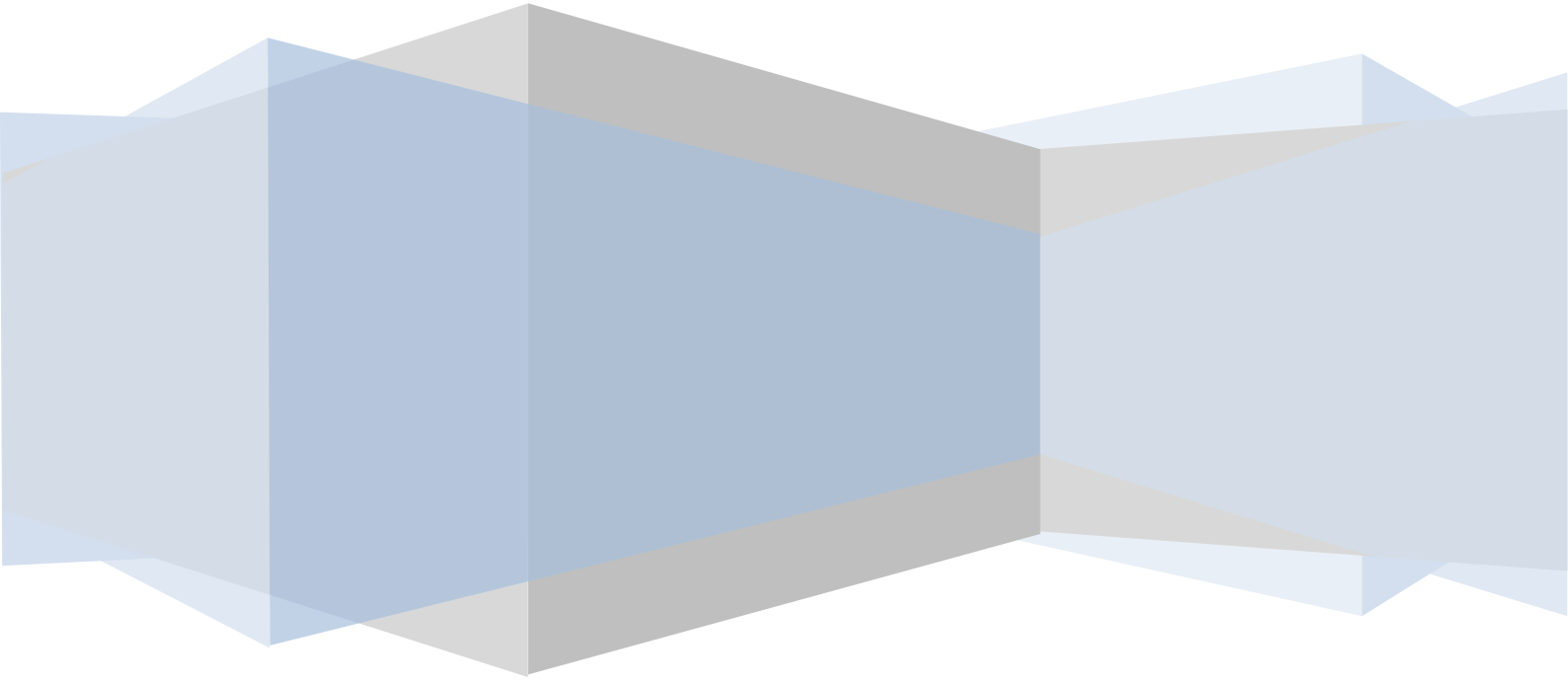
Institute of Computational Intelligence
Częstochowa University of Technology

ARP and DNS – address translation

Foundations of computer networks laboratory



The objective of the exercises

The aim of the exercise is to familiarize with translation between MAC, IP, and mnemonic addresses using ARP and DNS protocols.

Introduction

The TCP/IP computer networks use three levels of addressing:

- mnemonic (names),
- IP (network layer addresses),
- MAC (called also physical).

Additionally, services and session of clients are addressed by

- port numbers (TCP or UDP in transport layer).

MAC (media access control) addresses are assigned direct to each network interface, generally by manufacturer however can be changed by administrator. They are used to addressing nodes only in local network. Inside the frame build in data link layer there are at least two such addresses, i.e. addresses of recipient and sender. Such address consists of six bytes written as six hex pairs, e.g. 00-12-56-12-fe-c3.

IP addresses define the nodes in local communication and also between networks. It has been described in previous manuals.

Mnemonic addresses (names) allow indicating the node in network in more familiar way. The mnemonic addresses are easier to remember than IP addresses. In the Internet the names are organised in domain structure in form of tree. In such standard the full address contains of node name, local domain name and names of parent domains names. Al names are separated by dots, e.g. pc4.iisi.pcz.pl – address of computer with name pc4, which is located in iisi domain, which is the subdomain of pcz domain, which is the subdomain of pl domain.

In the most cases users prefer to apply the mnemonic addresses, so they should be translated to IP addresses and then to MAC addresses. The translation from mnemonic addresses to IP addresses is realised by DNS protocol and DNS servers using DNS queries. The reverse translation (from IP to mnemonic) is realised using RDNS queries. It can be also realised by other protocols, e.g. WINS and NetBEUI. The MAC addresses are determined using ARP (address resolution protocol). Note that translation of destination IP address to its MAC address is realised only in the destination network. In all other network on the path ARP is applied to determine MAC address of the next router (gateway) in current local network. The reverse translation is needed only during host auto configuration when the IP address should be assigned to interface with given MAC address. It could be realised by RARP (reverse address resolution protocol) but this protocol has been replaced by modern solutions as DHCP. DHCP has been described in previous manual.

To counter against multiple ARP and DSN queries each operating system stores the information obtained from ARP and DNS responses in ARP table and DNS resolver cache. To manage it we can use two commands – `arp` and `ipconfig` – as follows

```
>ipconfig /?

USAGE:
    ipconfig [/allcompartments] [/? | /all |
                                 /renew [adapter] | /release [adapter] |
                                 /renew6 [adapter] | /release6 [adapter] |
                                 /flushdns | /displaydns | /registerdns |
                                 /showclassid adapter |
                                 /setclassid adapter [classid] |
                                 /showclassid6 adapter |
                                 /setclassid6 adapter [classid] ]

where
    adapter             Connection name
```

```
                          (wildcard characters * and ? allowed, see examples)

        Options:
           /?               Display this help message
           /all             Display full configuration information.
           /release         Release the IPv4 address for the specified adapter.
           /release6        Release the IPv6 address for the specified adapter.
           /renew           Renew the IPv4 address for the specified adapter.
           /renew6          Renew the IPv6 address for the specified adapter.
           /flushdns        Purges the DNS Resolver cache.
           /registerdns     Refreshes all DHCP leases and re-registers DNS names
           /displaydns      Display the contents of the DNS Resolver Cache.
           /showclassid     Displays all the dhcp class IDs allowed for adapter.
           /setclassid      Modifies the dhcp class id.
           /showclassid6      Displays all the IPv6 DHCP class IDs allowed for
adapter.
           /setclassid6     Modifies the IPv6 DHCP class id.


    The default is to display only the IP address, subnet mask and
    default gateway for each adapter bound to TCP/IP.

    For Release and Renew, if no adapter name is specified, then the IP address
    leases for all adapters bound to TCP/IP will be released or renewed.

    For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is
removed.

    Examples:
        > ipconfig                       ... Show information
        > ipconfig /all                  ... Show detailed information
        > ipconfig /renew                ... renew all adapters
        > ipconfig /renew EL*            ... renew any connection that has its
                                             name starting with EL
        > ipconfig /release *Con*        ... release all matching connections,
                                             eg. "Wired Ethernet Connection 1" or
                                                 "Wired Ethernet Connection 2"
        > ipconfig /allcompartments      ... Show information about all
                                             compartments
        > ipconfig /allcompartments /all ... Show detailed information about all
                                             compartments

    C:\Users\Robert>ipconfig /?

    USAGE:
        ipconfig [/allcompartments] [/? | /all |
                                     /renew [adapter] | /release [adapter] |
                                     /renew6 [adapter] | /release6 [adapter] |
                                     /flushdns | /displaydns | /registerdns |
                                     /showclassid adapter |
                                     /setclassid adapter [classid] |
                                     /showclassid6 adapter |
                                     /setclassid6 adapter [classid] ]

    where
        adapter             Connection name
                           (wildcard characters * and ? allowed, see examples)

        Options:
           /?               Display this help message
           /all             Display full configuration information.
           /release         Release the IPv4 address for the specified adapter.
           /release6        Release the IPv6 address for the specified adapter.
           /renew           Renew the IPv4 address for the specified adapter.
           /renew6          Renew the IPv6 address for the specified adapter.
           /flushdns        Purges the DNS Resolver cache.
           /registerdns     Refreshes all DHCP leases and re-registers DNS names
           /displaydns      Display the contents of the DNS Resolver Cache.
```

```
           /showclassid     Displays all the dhcp class IDs allowed for adapter.
           /setclassid      Modifies the dhcp class id.
           /showclassid6       Displays  all  the  IPv6  DHCP  class  IDs  allowed  for
adapter.
           /setclassid6     Modifies the IPv6 DHCP class id.


    The default is to display only the IP address, subnet mask and
    default gateway for each adapter bound to TCP/IP.

    For Release and Renew, if no adapter name is specified, then the IP address
    leases for all adapters bound to TCP/IP will be released or renewed.

    For Setclassid and Setclassid6, if no ClassId is specified, then the ClassId is
removed.

    Examples:
        > ipconfig                       ... Show information
        > ipconfig /all                  ... Show detailed information
        > ipconfig /renew                ... renew all adapters
        > ipconfig /renew EL*            ... renew any connection that has its
                                             name starting with EL
        > ipconfig /release *Con*        ... release all matching connections,
                                             eg. "Wired Ethernet Connection 1" or
                                                 "Wired Ethernet Connection 2"
        > ipconfig /allcompartments      ... Show information about all
                                             compartments
        > ipconfig /allcompartments /all ... Show detailed information about all
                                             compartments
```

>arp /?

```
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Displays current ARP entries by interrogating the current
                protocol data.  If inet_addr is specified, the IP and Physical
                addresses for only the specified computer are displayed.  If
                more than one network interface uses ARP, entries for each ARP
                table are displayed.
  -g            Same as -a.
  -v            Displays current ARP entries in verbose mode.  All invalid
                entries and entries on the loop-back interface will be shown.
  inet_addr     Specifies an internet address.
  -N if_addr    Displays the ARP entries for the network interface specified
                by if_addr.
  -d            Deletes the host specified by inet_addr. inet_addr may be
                wildcarded with * to delete all hosts.
  -s            Adds the host and associates the Internet address inet_addr
                with the Physical address eth_addr.  The Physical address is
                given as 6 hexadecimal bytes separated by hyphens. The entry
                is permanent.
  eth_addr      Specifies a physical address.
  if_addr       If present, this specifies the Internet address of the
                interface whose address translation table should be modified.
                If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Adds a static entry.
  > arp -a                                    .... Displays the arp table.
```

A dialog with DNS servers can be realised also manually using `nslookup` application (in command line). Below the list of command available in `nslookup` is presented.

```
nslookup
```

```
Default Server:  dns.tpsa.pl
Address:  194.204.159.1

> help
Commands:   (identifiers are shown in uppercase, [] means optional)
NAME            - print info about the host/domain NAME using default server
NAME1 NAME2     - as above, but use NAME2 as server
help or ?       - print info on common commands
set OPTION      - set an option
    all                 - print options, current server and host
    [no]debug           - print debugging information
    [no]d2              - print exhaustive debugging information
    [no]defname         - append domain name to each query
    [no]recurse         - ask for recursive answer to query
    [no]search          - use domain search list
    [no]vc              - always use a virtual circuit
    domain=NAME         - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME           - set root server to NAME
    retry=X             - set number of retries to X
    timeout=X           - set initial time-out interval to X seconds
    type=X              - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,
SOA,SRV)
    querytype=X         - same as type
    class=X             - set query class (ex. IN (Internet), ANY)
    [no]msxfr           - use MS fast zone transfer
    ixfrver=X           - current version to use in IXFR transfer request
server NAME     - set default server to NAME, using current default server
lserver NAME    - set default server to NAME, using initial server
finger [USER]   - finger the optional NAME at the current default host
root            - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a          -  list canonical names and aliases
    -d          -  list all records
    -t TYPE     -  list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE           - sort an 'ls' output file and view it with pg
exit            - exit the program
```

Course of exercise

Clear both ARP table and DSN resolver cache using appropriate commands in command line. Then, initiate the network traffic with various nodes (computers servers, routers etc.) in local network and outside LAN. Check the records in ARP table and DSN resolver cache in each stage of the experiment. Comment the records connected with communication with nodes outside LAN.

Send various queries to default DNS server using `nslookup`. Then, change the DNS server and repeat the task. Follow teacher.

Repeat all above task capturing the traffic using wireshark. Annalise protocols.

The report

Students work in pairs or alone. The report should include the results obtained during exercises and conclusions.