

INSTRUKCJA 6 - ARP I DNS - TRANSLACJA ADRESÓW

6.1 Cel ćwiczenia

Celem ćwiczenia jest zaznajomienie rolą jakie pełnią protokoły ARP i DSN.

6.2 Wstęp

W sieciach komputerowych wykorzystujących stos protokołów **TCP/IP** używane są następujące poziomy adresowania urządzeń:

- adresy MAC,
- adresy IP,
- adresy mnemoniczne,

oraz adresowanie usług dostępnych na poszczególnych urządzeniach za pomocą **numerów portów**.

Adresy MAC są przypisane poszczególnym interfejsom sieciowym. Są wykorzystywane do adresowania urządzeń w sieci lokalnej. W nagłówkach ramek warstwy łącza danych (np. Ethernet, Token Ring, FDDI, WiFi) występuje co najmniej adres adresata oraz nadawcy ramki. Adres taki składa się sześciu bajtów zapisywanych zwyczajowo w postaci sześciu dwucyfrowych liczb szesnastkowych, np. 00-12-56-12-fe-c3.

Adresy IP, zasadniczo, również przypisuje się poszczególnym interfejsom sieciowym, choć możliwe jest również przypisanie wielu adresów do jednego interfejsu lub jednego adresu do grupy interfejsów (most). Wykorzystuje je warstwa sieciowa, która pozwala na komunikację zarówno w ramach sieci lokalnej, jak i pomiędzy sieciami. Adres IP składa się z 4 bajtów zapisywanych zwyczajowo w postaci czterech liczb, rozdzielonych kropką, np.: 217.45.22.17. W adresie IP występuje część określająca adres sieci oraz część określająca adres konkretnego urządzenia w danej sieci. Podział może być określony elastycznie w postaci maski lub odnosząc się do klas adresów:

Tabela 6.1: Klasy adresów IP

klasa	zakres adresów	rodzaj sieci	liczba sieci	identyfikacja
A	1.0.0.0 - 126.0.0.0	duże	127	pierwszy bit = 0
B	128.1.0.0 - 191.254.0.0	średnie	16.382	pierwsze dwa bity = 10
C	192.0.1.0 - 223.255.254.0	małe	2.097.150	pierwsze trzy bity = 110
D	224.0.0.0 - 239.255.255.254	trans. grupowej	dynamiczna	pierwsze cztery bity = 1110
E	240.0.0.0 - 255.255.255.255	IETF	dynamiczna	pierwsze cztery bity = 1111

Adresy mnemoniczne pozwalają na łatwe ich zapamiętanie i określają konkretne urządzenie w sieci. W sieci Internet stosuje się hierarchiczne nazewnictwo domenowe. Nazwa urządzenia składa się z części rozdzielonych kropkami, np. *pc4.iisi.pcz.pl*. Pierwszy element (w przykładzie *pc4*) to nazwa konkretnego urządzenia, który jest elementem domeny (w przykładzie *iisi*). Domena *iisi* jest z kolei częścią domeny nadrzędnej (w przykładzie *pcz*) itd.

Wszystkie trzy wymienione **rodzaje adresów** określają konkretne urządzenie w sieci. Użytkownik najczęściej posługuje się adresami mnemonicznymi, lecz te nie są przydatne w odnalezieniu urządzenia w sieci. Konieczne jest ich przetłumaczenie na adresy IP. Służy do tego usługa **DNS** (*Domain Name System*) oferowana przez serwery DNS. W odpowiedzi na zapytanie zawierające nazwę mnemoniczną przekazuje przypisany jej adres IP. Hierarchiczna (domenowa) organizacja nazewnictwa pozwoliła na rozproszenie baz danych przechowujących nazwy i przyporządkowane im adresy IP. Informacje o poszczególnych domenach są przechowywane na specjalizowanych serwerach. Np. serwer odpowiadający za domenę *pcz* przechowuje informację o wszystkich jej poddomenach oraz zarejestrowanych w nich urządzeniach. Na podstawie adresu IP można określić konkretną podsieć, w której znajduje się docelowe urządzenie. W sieci lokalnej konieczne jest wykorzystanie protokołu warstwy łącza danych oraz adresów **MAC** (*Media Access Control*). Adres IP musi zostać zatem przetłumaczony na adres MAC odpowiedniego interfejsu. Zadanie to realizuje protokół **ARP** (*Address Resolution Protocol*). Urządzenie poszukujące adresu MAC rozgłasza zapytanie „Kto posiada dany adres IP?”, a posiadacz odpowiada używając swojego adresu MAC.

Aby nie **powielać** zbędnych zapytań DNS i ARP, systemy operacyjne przechowują okresowo uzyskane informacje w **pamięci**. Do zarządzania nią służą polecenia **ipconfig** i **arp**. Innym omawianym przydatnym narzędziem jest **nslookup**.

6.2.1 IPCONFIG

Polecenie **ipconfig** posiada następujące możliwe przełączniki:

Tabela 6.2: Wybrane przełączniki programu ipconfig

przełącznik	parametr	opis
	/?	wyświetla ten komunikat pomocy
	/all	wyświetla pełne informacje o konfiguracji
/allcompartments		wyświetla informacje o wszystkich przedziałach
/release	[karta]	zwalnia adres IPv4 podanej karty
/release6	[karta]	zwalnia adres IPv6 podanej karty
/renew	[karta]	odnawia adres IPv4 podanej karty
/renew6	[karta]	odnawia adres IPv6 podanej karty
/displaydns		wyświetla zawartość buforu programu rozpoznawania nazw DNS
/flushdns		przeczyszcza bufor programu rozpoznawania nazw DNS
/registerdns		odświeża wszystkie dzierżawy DHCP i rejestruje ponownie nazwy DNS
/showclassid	karta	wyświetla wszystkie identyfikatory klas DHCP dozwolone dla karty
/setclassid	karta [id]	modyfikuje identyfikator klasy DHCP

Zachowanie domyślne to wyświetlanie tylko adresu IP, maski podsieci i bramy domyślnej dla każdej karty związanej z protokołem TCP/IP.

Jeśli dla przełączników `/release` i `/renew` nie zostanie określona nazwa karty, zwolnieniu lub odnowieniu ulegną dzierżawy adresów IP dla wszystkich kart związanych z protokołem TCP/IP.

Jeśli dla przełącznika `/setclassid` nie zostanie określony parametr identyfikator (`id`), to identyfikator zostanie usunięty.

Przykłady:

- ipconfig - Pokazuje informacje
- ipconfig /all - Pokazuje informacje szczegółowe
- ipconfig /renew - Odnowia adresy IP wszystkich kart
- ipconfig /renew EL* - Odnowia adresy IP połączeń o nazwach zaczynających się od EL
- ipconfig /release *lok* - Zwalnia adresy IP wszystkich pasujących połączeń, np. "Połączenie lokalne 1" lub "Połączenie lokalne 2"
- ipconfig /allcompartments - Pokazuje informacje o wszystkich przedziałach
- ipconfig /allcompartments /all - Pokazuje informacje szczegółowe o wszystkich przedziałach

```

Ethernet adapter Ethernet: Nazwa karty
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . : kik.pcz.pl
    Description . . . . . : Qualcomm Atheros AR8161 PCI-E Gigabit Ethernet Controller (NDIS 6.30)
    Physical Address. . . . . : B8-88-E3-82-E6-B2
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi: Nazwa karty

    Connection-specific DNS Suffix . . . . . : tel.pol.net.pl
    Description . . . . . : Intel(R) Centrino(R) Wireless-N 2200
    Physical Address. . . . . : 9C-4E-36-56-4B-44
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::ed6f:6356:6b5b:a93%3(Preferred)
    IPv4 Address. . . . . : 192.168.21.4(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained. . . . . : Tuesday, November 22, 2016 10:10:45
    Lease Expires . . . . . : Tuesday, November 22, 2016 11:10:45
    Default Gateway . . . . . : 192.168.21.1
    DHCP Server . . . . . : 192.168.21.1
    DHCPv6 IAID . . . . . : 60575286
    DHCPv6 Client DUID. . . . . : 00-01-00-01-1C-59-A9-D0-B8-88-E3-82-E6-B2

DNS Servers . . . . . : 192.168.200.250
    : 192.168.0.250
NetBIOS over Tcpip. . . . . : Enabled

C:\Windows\system32>

```

Rysunek 6.1: Wywołanie ipconfig /all

Serwery DNS zawierają różne typy rekordów, do najważniejszych z nich należą:

- **A** - rekord adresu, 32-bitowy adres IPv4.
- **AAAA** - rekord adresu, 128-bitowy adres IPv6.
- **CAA** - certyfikat autoryzacji dla danego hosta.
- **CNAME** - alias nazwy odwołujący się do dalszego poszukiwania.
- **DNAME** - alias nazw odwołujący się do dalszego poszukiwania.
- **LOC** - określa lokalizację geograficzną powiązaną z domeną.
- **NS** - określa serwery nazw DNS.
- **PTR** - wskaźnik do nazwy kanonicznej.

```

www.iisi.pcz.pl
-----
Record Name . . . . . : www.iisi.pcz.pl
Record Type . . . . . : 5
Time To Live . . . . . : 82500
Data Length . . . . . : 8
Section . . . . . : Answer
CNAME Record . . . . . : iisi.pcz.pl

Record Name . . . . . : iisi.pcz.pl
Record Type . . . . . : 1
Time To Live . . . . . : 82500
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . . : 212.87.228.2

plus.google.com
-----
Record Name . . . . . : plus.google.com
Record Type . . . . . : 28
Time To Live . . . . . : 117
Data Length . . . . . : 16
Section . . . . . : Answer
AAAA Record . . . . . : 2a00:1450:400d:803::200e

pcz.pl
-----
Record Name . . . . . : pcz.pl
Record Type . . . . . : 1
Time To Live . . . . . : 82471
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . . : 212.87.229.98

```

Rysunek 6.2: Wywołanie ipconfig /displaydns z zaznaczonymi typami rekordów DNS

6.2.2 ARP

ARP wyświetla i modyfikuje tabelę translacji adresów IP na adresy fizyczne, używane przez protokół rozróżniania adresów (ARP).

Istnieją 3 różne sposoby wywoływania polecenia ARP: Serwery DNS zawierają różne typy rekordów, do najważniejszych z nich należą:

- wyświetlenie bieżących wpisów: ARP -a [inet_addr] [-N if_addr] [-v]
- usunięcie określonego hosta: ARP -s inet_addr eth_addr [if_addr]
- dodanie określonego hosta: ARP -d inet_addr [if_addr]

Gdzie:

- inet_addr - oznacza **adres internetowy**,
- if_addr - oznacza **adres interfejsu**,
- eth_adds - oznacza **adres fizyczny**,
- -v - oznacza wyświetlenie adresów w trybie pełnym.

```

C:\Windows\system32>arp -a -v
Interface: 127.0.0.1 --- 0x1
Internet Address      Physical Address      Type
224.0.0.2             00-00-00-00-00-00    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.1.60            01-00-5e-00-01-3c    static
238.80.39.135         01-00-5e-50-27-87    static
239.255.255.250      ff-ff-ff-ff-ff-ff    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.21.4 --- 0x3
Internet Address      Physical Address      Type
192.168.21.1          c0-c6-87-5d-cf-60    dynamic
192.168.21.2          14-2d-27-19-c3-6d    dynamic
192.168.21.5          00-00-00-00-00-00    invalid
192.168.21.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.1.60            01-00-5e-00-01-3c    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 0.0.0.0 --- 0xffffffff
Internet Address      Physical Address      Type
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.1.60            01-00-5e-00-01-3c    static
238.80.39.135         01-00-5e-50-27-87    static

```

Rysunek 6.3: Wywołanie arp -a -v z zaznaczonymi rodzajami adresów

6.2.3 NSLOOKUP

Komunikację z usługami DNS można przeprowadzić za pomocą programu **nslookup**. Program ten po uruchomieniu pozwala na wywołanie następujących poleceń:

Tabela 6.3: Wybrane przełączniki programu nslookup

instrukcja	parametr	opis
	domena	wyświetlenie informacji o domenie
	domena [server]	wyświetlenie informacji o domenie z użyciem określonego serwera
help		wywołanie pomocy
set	all	wyświetlenie opcji programu
set	[no]opcja	ustawienie opcji binarnej
set	opcja=wartość	ustawienie opcji tekstowej
server	nazwa	ustawienie domyślnego serwera
root		ustawienie serwera na domyślny
ls	[opt] domena [> plik]	wyświetlenie listy adresów danej domeny
exit		zakończenie programu

Jedną z **ważniejszych** opcji nslookup jest opcja **określająca** jakie rodzaje rekordów DNS mają być zwracane dla danej domeny. Możliwe jest uzyskanie informacji o takich typach jak: A, AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV.

```
C:\Users\Krystian>nslookup
Default Server: UnKnown
Address: 192.168.200.250

> set type=A
> pcz.pl
Server: UnKnown
Address: 192.168.200.250

Non-authoritative answer:
Name:    pcz.pl.net.pl
Address: 212.91.7.33

> set type=AAAA
> pcz.pl
Server: UnKnown
Address: 192.168.200.250

*** No IPv6 address (AAAA) records available for pcz.pl
> exit
```

Rysunek 6.4: Użycie nslookup dla zwrócenia rekordów DNS serwera pcz.pl (typu A oraz AAAA).

6.3 Przebieg ćwiczenia

1. Wyświetlić pełne informacje o kartach sieciowych i połączeniach `ipconfig -all`.
2. Za pomocą polecenia **ipconfig** wyświetlić wszystkie serwery dns, zwolnić wszystkie adresy IP, ponownie wyświetlić wszystkie serwery dns, odnowić wszystkie adresy IP.
3. Przeglądając serwery dns `ipconfig /displaydns` **wyszukać kilka wpisów** o typie rekordu różnym od A (Host) i AAAA (np. CNAME, PTR). W celu szybszego wyszukiwania wyniki polecenia można zapisać do pliku lub zastosować wyszukiwanie: `ipconfig /displaydns | findstr /r /c:"Record[.]*:"`
W przypadku braku wpisów należy odwiedzić kilka różnych witryn internetowych.
4. Za pomocą polecenia **arp** wyświetlić wszystkie wpisy adresów w trybie pełnym. Następnie stosując podając odpowiednie **adresy** - `inet_addr` oraz `-N if_addr` wyświetlić tylko wybrane przez nas wpisy.
5. Za pomocą polecenia arp **spróbować** dodać i usunąć wpisy z tablicy wpisów.
6. Za pomocą polecenia **nslookup** pobrać adres IPv4 (type=A), IPv6 (type=AAAA) oraz nazwy serwerów dns (type=NS) dla kilku wybranych domen (m.in. pcz.pl, google.pl itp).
7. Za pomocą polecenia **nslookup** zmienić serwer domyślny na 1 z serwerów DNS uzyskany w ćwiczeniu 6. Spróbować pobrać dane na temat wybranych **przez siebie** domen.
8. Uruchomić ponownie nslookup, zmieniając typ rekordów DNS na: CNAME, MX, PTR, SOA, SRV spróbować pobrać informacje dla kilku wybranych domen (m.in. **www.pcz.pl**, google.pl, itp)

6.4 Sprawozdanie

Studenci pracują i przygotowują sprawozdania indywidualnie. W sprawozdaniu należy przedstawić przebieg przeprowadzonych eksperymentów, ich wyniki oraz wnioski.