

Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 3: Warstwa łącza danych. Działanie protokołu Ethernet, ARP i przełącznika

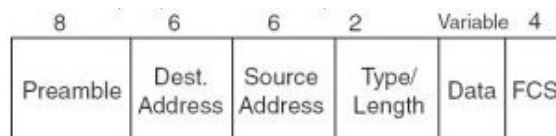
Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

03.2022

I. Wprowadzenie

Warstwa 2. modelu OSI — łącza danych — ma za zadanie doprowadzić do transmisji danych na poziomie lokalnym (nie wychodząc poza podsieć). Dbą o zapewnienie urządzeniom dostępu do medium transmisyjnego, przekazuje dane do wysłania warstwie fizycznej. Odbiera bity z warstwy fizycznej i organizuje je w **ramki**, a także wykrywa ewentualne błędy w ramach. Urządzenie źródłowe i docelowe identyfikowane są poprzez ich fizyczny **adres MAC**.

Jednym z najpopularniejszych obecnie protokołów działających na warstwie łącza danych jest protokół **Ethernet**, opisany standardem IEEE 802.3. Ramka budowana przez protokół Ethernet składa się z następujących pól:



- preamble — jest to ciąg naprzemiennie występujących po sobie 0 i 1, służy do synchronizacji komunikujących się ze sobą urządzeń. Ostatnie 2 bity mają postać 11 i oznaczają początek ramki,
- adresu docelowego — MAC urządzenia, które ma odebrać ramkę,

- adresu źródłowego — MAC urządzenia, które nadało ramkę,
- typu — typ protokołu, którego dane stanowią zawartość ramki, lub długość przesyłanych danych,
- danych — enkapsulowany w ramce pakiet z wyższej warstwy (właściwy ładunek),
- sumy kontrolnej — służy sprawdzeniu, czy w trakcie transmisji nie doszło do zaburzenia któregoś z bitów.

O ile urządzenie nadawcze dobrze zna swój własny adres MAC, o tyle w pierwszej chwili nie jest mu znany MAC urządzenia odbiorczego (znany jest co najwyżej adres sieciowy, który został sprecyzowany na wyższej warstwie). Aby poznać ten adres i móc dokończyć proces tworzenia ramki ethernetowej, wykorzystywany jest protokół **ARP** (ang. *Address Resolution Protocol*), który pozwala na utworzenie powiązań pomiędzy adresami fizycznymi i sieciowymi urządzeń. ARP wysyła do wszystkich urządzeń w ramach danej sieci zapytanie o to, które z nich posiada wskazany adres sieciowy, a urządzenie, które rozpozna w poszukiwanym adresie swój własny, przekaże do pytającego informację o swoim adresie MAC.

Wiele urządzeń (np. komputery) tworzą tablicę powiązań ARP, która może posiadać wpisy albo statyczne (wpisane „na sztywno” przez administratora), albo dynamicznie wyuczone w wyniku działania protokołu ARP. Wpis domyślnie jest usuwany z pamięci po upływie pewnego czasu (np. w systemie Windows po 2 minutach, chyba, że wpis był ponownie używany, wówczas po 10 minutach) — zachowany jest balans pomiędzy wysyłaniem zapytań ARP przy tworzeniu dosłownie każdej ramki, a pamiętaniem przez długi czas potencjalnie przestarzałych wpisów.

Urządzeniem sieciowym, które pracuje na 2. warstwie modelu OSI, jest **przełącznik**. Zadaniem przełącznika jest przekazywanie ramek pomiędzy swoimi portami (od portu, do którego podłączone jest urządzenie nadawcze, do portu, w którym podłączone jest urządzenie odbiorcze). Dzięki temu ramka przekazana jest tylko tam, gdzie powinna, a nie na wszystkie porty.

Aby wiedzieć, które urządzenie podłączone jest do którego portu, tj. do którego portu ma przekazać daną ramkę, przełącznik buduje tzw. **tablicę MAC adresów**, poprzez obserwowanie przepływającego ruchu sieciowego (dokładniej mówiąc, adresów źródłowych MAC w ramach pojawiających się na każdym z portów). Kiedy przełącznik nie znajduje docelowego MACa w tablicy, zachowuje się jak koncentrator i wysyła ramkę na wszystkie pozostałe porty. To samo może się wydarzyć, kiedy tablica MAC adresów przepełni się (czy to w wyniku normalnej pracy przełącznika, czy też ataku hakerskiego) i przełącznik nie jest w stanie zapamiętać nowych MACów na swoich portach.

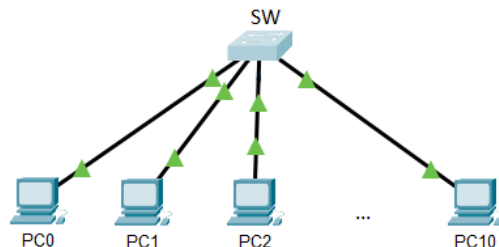
II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest zapoznanie się z funkcjonowaniem warstwy łącza danych modelu OSI w sieciach komputerowych, a w szczególności protokołu Ethernet i ARP, poprzez:

- przechwycenie w programie Wireshark ruchu sieciowego na 2. warstwie modelu OSI i zaobserwowanie, jak zbudowane są ramki ethernetowe,
- obserwację procesu tworzenia ramki ethernetowej dzięki protokołowi ARP,
- obserwację działania przełącznika sieciowego (urządzenia działającego na 2. warstwie modelu OSI) — przełączania ramek pomiędzy portami na podstawie adresów MAC dołączonych do niego urządzeń.

III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputerów klasy PC z zainstalowanym systemem Windows oraz oprogramowaniem Wireshark, połączonych w sieć za pomocą przełącznika sieciowego Cisco.



Przed przystąpieniem do ćwiczenia:

- Włącz komputer do lokalnej sieci laboratoryjnej, uruchamiając na nim kartę sieciową o nazwie *LAB*. Kliknij *Start* ⇒ *Ustawienia* ⇒ *Połączenia sieciowe*. Prawym klawiszem wybierz kartę sieciową *LAB* i kliknij *Włącz*, podobnie wybierz kartę sieciową *Internet* i wybierz *Wyłącz* (od tego momentu komputer straci połączenie z internetem na rzecz sieci laboratoryjnej).
- Ustaw statycznie adres IP według schematu:
IP: 172.16.1.*numer_Twojego_stanowiska*
Maska podsieci: 255.255.255.0

IV. Przebieg ćwiczenia

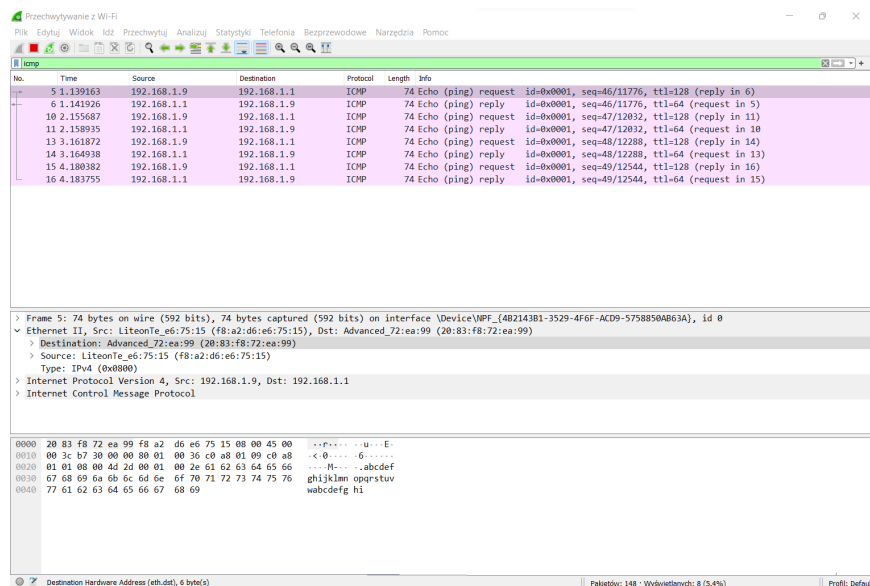
1 Analiza ramki Ethernet w programie Wireshark

1.1 Przechwycić ruch sieciowy pochodzący z prostej komunikacji sieciowej.

- Otwórz program Wireshark i rozpocznij przechwytywanie ruchu sieciowego na karcie sieciowej Realtek. Włącz filtrowanie przechwyconego ruchu, tak, by widoczne były tylko ramki z pakietami protokołu ICMP.
- Wygeneruj ruch sieciowy: poproś sąsiada o adres IP jego komputera i za pomocą Wiersza poleceń systemu Windows wyślij na ten adres ping (*Start* ⇒ *Uruchom* ⇒ *cmd* ⇒ *ping adres_IP*).
- Sprawdź, czy w programie Wireshark pojawiły się przechwycone ramki, po czym zatrzymaj przechwytywanie danych.

1.2 Przyjrzyj się strukturze ramki protokołu Ethernet.

- Zaznacz pierwszą przechwyconą ramkę (zawierającą wysłany od Ciebie *Echo (ping) request*) i rozwiń w środkowej części okna drugą sekcję — odpowiadającą nagłówkowi protokołu Ethernet.



- Możesz zauważyć, że Wireshark nie wyodrębnił preambuły.
- Porównaj docelowy adres MAC z adresem MAC komputera sąsiada (można go wyświetlić poleceniem *ipconfig/all* w Wierszu poleceń).

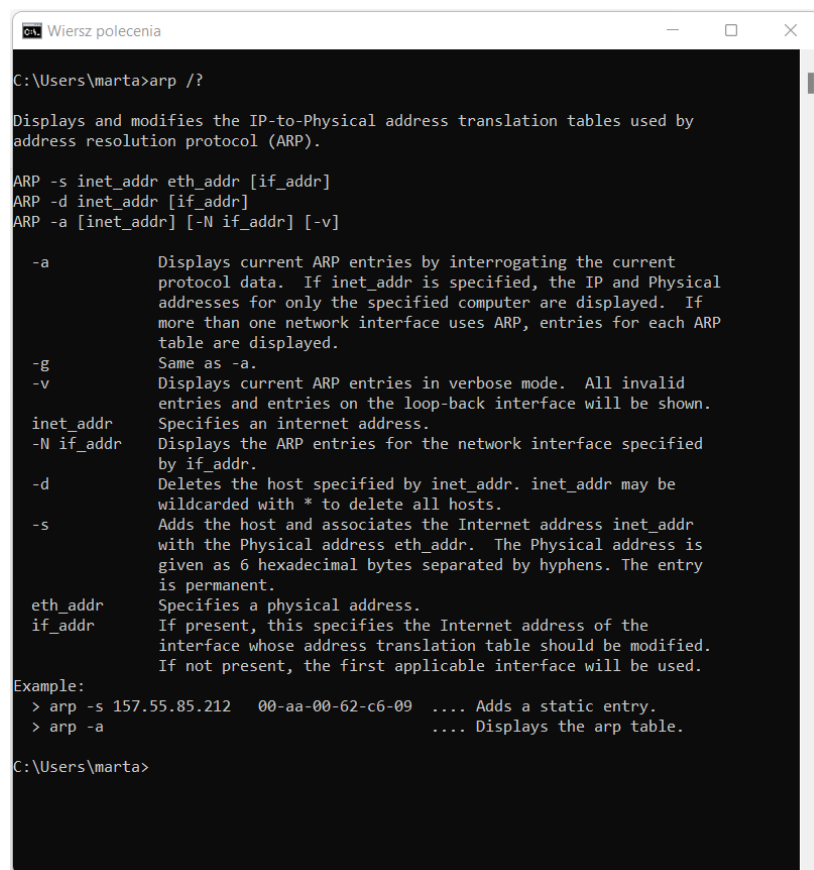
- Porównaj źródłowy adres MAC z adresem MAC swojego komputera.
 - Zidentyfikuj typ zawartości Twojej ramki (IP).
 - Zawartością Twojej ramki jest pakiet protokołu IP.
 - Wireshark nie wyświetla informacji o sumie kontrolnej.
- b) Zaznacz drugą przechwyconą ramkę (*Echo (ping) reply*, będącą odpowiedzią na Twojego requesta) i zaobserwuj, jak zmienił się adres źródłowy i docelowy.

2 Obserwacja działania protokołu ARP

2.1 Przyjrzyj się tablicy ARP na swoim komputerze.

- a) W Wierszu polecenia systemu Windows wydaj polecenie `arp /?`, dzięki któremu wyświetlisz wszystkie dostępne opcje komendy `arp` na Twoim komputerze.

`arp /?`



```

C:\Users\marta>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.

C:\Users\marta>
  
```

Zauważ, że możesz:

- wyświetlać tablicę powiązań ARP na Twoim komputerze poleceniem *arp -a*,
- usuwać wpisy z tablicy powiązań ARP poleceniem *arp -d IP*,
- dodawać statycznie wpisy do tablicy powiązań ARP poleceniem *arp -s IP MAC*.

b) Wyświetl tablicę powiązań ARP na Twoim komputerze, wydając polecenie *arp -a*.

```
arp -a
```

```
C:\>arp -a
Internet Address      Physical Address      Type
172.16.1.2            00d0.ffcd.e458        dynamic
```

Przyjrzyj się wpisom (jeśli żadnych nie ma w tablicy, wywołaj ruch sieciowy, wykonując ping na komputer sąsiada). Zaobserwuj, że w każdym z nich skojarzony jest adres sieciowy (*Internet Address*, w tym przypadku adres IP) z adresem fizycznym MAC (*Physical Address*).

2.2 Wyczyść tablicę ARP na swoim komputerze, aby wymusić ponowny przepływ zapytań ARP i przechwycić generowany wtedy ruch sieciowy.

- W programie Wireshark uruchom przechwytywanie ruchu (filtruj tak, aby wyświetlić jedynie ruch ARP).
- Wydadź polecenie *arp -d* z gwiazdką, co spowoduje wyczyszczenie całej tablicy ARP na Twoim komputerze.

```
arp -d *
```

Poleceniem *arp -a* upewnij się, że tablica została rzeczywiście wyczyszczona.

- Wyślij ping do komputera sąsiada. Zaobserwuj w programie Wireshark, jak pojawiają się wiadomości ARP wymienione podczas poszukiwania przez Twój komputer adresu MAC komputera sąsiada (ponieważ aby Twój komputer mógł złożyć pełną ethernetową ramkę z echo requestem, musi znać też adres MAC docelowego urządzenia, czyli komputera Twojego sąsiada, a nie posiada już odpowiedniego wpisu w pamięci).
- Przyjrzyj się pierwszej ramce (powinno to być zapytanie ARP wysłane przez Twój komputer: „*Who has IP_sąsiada? Tell Twój_MAC*”).
 - Jako adres docelowy, powinienien zaobserwować **adres rozgłoszeniowy** (skierowany do wszystkich urządzeń w sieci poza wysyłającym) warstwy 2: jest to MAC składający się binarnie z samych jedynek, a szesnastkowo z samych cyfr F: FF:FF:FF:FF:FF:FF.

- Jako adres źródłowy, powinieneś zobaczyć swój adres MAC.
 - Pole Type powinno wskazywać na to, że zawartość ramki stanowi wiadomość ARP (0x0806).
 - Po rozwinięciu zawartości (sekcji *Address Resolution Protocol*), zaobserwuj, jak dana, o którą pyta Twój komputer (*Target MAC Address*), zastąpiona jest zerami (00:00:00:00:00:00). Adres IP szukanego komputera widnieje jako *Target IP Address*. Twój komputer umieścił też informacje o sobie.
- e) Przyjrzyj się drugiej ramce (powinna to być odpowiedź na Twoje zapytanie ARP wysłane przez komputer sąsiada: „*IP_sąsiada is at MAC_sąsiada*”).
- Jako adres docelowy, powinieneś zaobserwować adres MAC Twojego komputera. Jest to już komunikacja jeden-do-jednego (unicast), a nie broadcast jak w poprzednim przypadku.
 - Jako adres źródłowy, powinieneś zobaczyć adres MAC komputera sąsiada.
 - Pole Type powinno wskazywać na to, że zawartość ramki stanowi wiadomość ARP (0x0806).
 - Po rozwinięciu zawartości (sekcji *Address Resolution Protocol*), zaobserwuj, jak dana, o którą pytał Twój komputer (*Sender MAC Address*), została uzupełniona przez „wywołane do tablicy” urządzenie, tj. komputer Twojego sąsiada.

3 Analiza tablicy MAC adresów na przełączniku firmy Cisco

3.1 Zaloguj się na laboratoryjny przełącznik Cisco.

- a) W wierszu polecenia wydaj polecenie *telnet* na adres IP przełącznika laboratoryjnego:

```
telnet 172.16.1.253
```

Telnet umożliwia uzyskanie dostępu do zdalnego urządzenia, np. w celu jego przekonfigurowania czy też sprawdzenia konfiguracji.

Pamiętaj! To, że przełącznik posiada skonfigurowany adres IP (3. warstwy), nie oznacza, że na 2. warstwie modelu OSI obsługiwane są adresy IP. Adres IP przypisany przełącznikowi służy jedynie temu, aby móc dostać się na niego i go przekonfigurować; nie ma wpływu na sam proces przełączania ramek, który to następuje na podstawie adresów MAC.

- b) Zaloguj się, używając hasła **cisco**.

3.2 Wyświetl tablicę MAC adresów na przełączniku.

- a) Przejdź do trybu umożliwiającego wyświetlanie większej części konfiguracji przełącznika (tzw. trybu uprzywilejowanego), wydając przełącznikowi polecenie *enable*:

```
Switch>enable
```

Ponownie podaj hasło *cisco*.

- b) Będąc w trybie uprzywilejowanym, wyświetl tablicę MAC adresów na przełączniku:

```
Switch#show mac address-table dynamic
```

```
Switch#show mac address-table dynamic
Mac Address Table
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	0000.0c3d.9d8c	DYNAMIC	Fa0/1
1	00d0.ffcd.e458	DYNAMIC	Fa0/3

- c) Zobacz, jak zbudowana jest tablica MAC adresów. Najbardziej interesują nas dwie kolumny: *Mac Address*, w której umieszczane są adresy MAC urządzeń widzianych przez przełącznik, oraz *Ports*, zawierająca informację o tym, na którym porcie widziany jest dany MAC.

3.3 Poszukaj portu, pod którym widoczny jest MAC Twojego komputera.

- a) Poleceniem *ipconfig/all* w Wierszu polecenia systemu Windows sprawdź adres fizyczny (MAC) swojego komputera.
- b) Poszukaj w tablicy MAC adresów przełącznika Cisco wpisu zawierającego MAC Twojego komputera. Zobacz, pod którym portem jest on wpięty (Fa0/X, gdzie Fa oznacza port w standardzie Fast Ethernet (100 Mb/s), a X — numer portu od 0 do 23). Jeśli nie możesz go znaleźć, wykonaj ping do sąsiada i sprawdź ponownie.
- c) Przekonaj się, że faktycznie Twój komputer jest wpięty do danego portu — podejdź do przełącznika laboratoryjnego w szafie i przy asyście prowadzącego, odepnij kabel od wyszukanego przez siebie portu. Na Twoim komputerze powinien pojawić się systemowy komunikat *Kabel sieciowy jest odłączony*. Włóż wtyczkę z powrotem do swojego portu.

3.4 Zaobserwuj proces uczenia się adresów MAC przez przełącznik.

- a) W porozumieniu z resztą grupy (po wykonaniu przez wszystkich powyższego ćwiczenia), wyczyść tablicę MAC adresów przełącznika laboratoryjnego, by zmusić go do ponownej nauki adresów MAC.

```
Switch#clear mac address-table dynamic
```

Upewnij się, że tablica rzeczywiście została wyczyszczona, ponownie ją wyświetlając poleceniem *show mac address-table dynamic*.

```
Switch#clear mac address-table dynamic
Switch#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
Switch#
```

- b) Uruchom przechwytywanie danych w programie Wireshark (ustaw filtrowanie na protokół ICMP).
- c) Razem z innymi osobami z grupy, stopniowo wysyłajcie do siebie ping.
- d) Po każdym pingu odświeżajcie tablicę MAC adresów na przełączniku (*show mac address-table dynamic*) i obserwujcie, jak przybywa w nim wpisów.
- e) Obserwujcie też, jak przełącznik, zanim nie pozna adresów MAC Waszych komputerów, wysyła ramki do Was adresowane na wszystkie porty (o czym możesz się przekonać, widząc przechwycone przez program Wireshark na Twoim komputerze ramki, które nie są do niego adresowane ani od niego nie pochodzą).

V. Pytania kontrolne

1. Z jakich pól składa się ramka ethernetowa?
2. Do czego służy protokół ARP?
3. Jak wygląda proces przełączania ramek przez przełącznik sieciowy?