**Politechnika Białostocka**

Wydział Elektryczny

Katedra Telekomunikacji i Aparatury Elektronicznej

Instrukcja do zajęć laboratoryjnych

Temat ćwiczenia: **Badanie protokołów rodziny TCP/IP**

Numer ćwiczenia: **6**

Laboratorium z przedmiotu: **Systemy i sieci telekomunikacyjne 1**

Kod przedmiotu: TS1D3019

Instrukcję opracował:
dr inż. Andrzej Zankiewicz

Białystok 2018

## 1. Ogólna charakterystyka ćwiczenia

Protokoły rodziny TCP/IP stanowią obecnie najczęściej stosowaną grupę protokołów warstw 3 i 4 modelu OSI. Grupa ta obejmuje podstawowy protokół warstwy 3, którym jest IP (*Internet Protocol)* oraz protokoły warstwy 4: TCP (*Transmission Control Protocol)* i UDP *(User Datagram Protocol)*, a także protokoły pomocnicze takie jak ARP (*Address Resolution Protocol)* i ICMP *(Internet Control Message Protocol*).

Protokoły te zostały zaprojektowane z myślą o odpornych na uszkodzenia sieciach przeznaczonych do celów wojskowych. Obecnie są one wykorzystywane powszechnie w ogólnoświatowej sieci Internet, a także w sieciach lokalnych nieprzyłączonych do Internetu.

Celem ćwiczenia jest poznanie właściwości protokołów rodziny TCP/IP poprzez obserwację i analizę pakietów transmitowanych w sieci wykorzystującej te protokoły.

## 2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- Całość niniejszej instrukcji
  - Opisy protokołów IP, TCP, UDP, ICMP oraz ARP zawarte np. w podręczniku „*Akademia sieci Cisco. CCNA Exploration. Semestr 1*” [1], rozdziały 4, 5, 6, 9.
- Opis programu *Wireshark*

Informacje zawarte w podanych powyżej źródłach stanowią minimum wiedzy teoretycznej **niezbędnej** do przystąpienia i prawidłowego wykonania ćwiczenia.

## 3. Podstawowe informacje o protokołach rodziny TCP/IP

W rodzinie protokołów TCP/IP podstawowym protokołem pracującym w warstwie 3 modelu OSI jest protokół IP stanowiący bezpołączeniowy protokół umożliwiający przesyłanie jednostek danych nazywanych pakietami. Do identyfikacji poszczególnych stacji protokół IP używa 32-bitowych liczb nazywanych adresami IP lub też adresami logicznymi. Adres IP składa się z dwóch części stanowiących odpowiednio adres sieci oraz adres hosta w tej sieci. O miejscu podziału adresu decyduje maska sieci podawana przy konfigurowaniu stacji.

W warstwie 4 modelu OSI może być użyty połączeniowy niezawodny protokół TCP lub prosty bezpołączeniowy protokół UDP, stosowany głównie w aplikacjach typu zapytanie-odpowiedź. Protokoły te umożliwiają jednoczesne tworzenie wielu połączeń transportowych w ramach jednego połączenia sieciowego (jednego

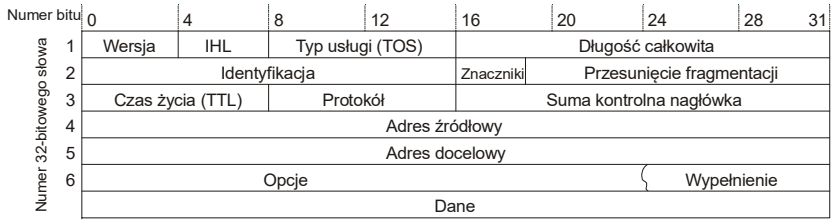
adresu IP). W celu rozróżnienia poszczególnych połączeń używają one 16-bitowych numerów portów.

Do celów kontrolnych oraz sygnalizacji błędów występujących w sieciach TCP/IP służy pomocniczy protokół ICMP stanowiący integralną część rodziny protokołów TCP/IP. Umożliwia on m.in. sprawdzenie dostępności danej stacji na poziomie warstwy 3 oraz informowanie o niedostępności stacji docelowych.

Stosowanie protokołów TCP/IP w sieciach lokalnych Ethernet umożliwia protokół pomocniczy ARP służący do wyznaczania adresów fizycznych (MAC) stacji na podstawie ich adresów logicznych (IP). Dzięki temu możliwe jest dostarczenie do stacji docelowej pakietu IP umieszczonego w ramce Ethernet.

## 4. Struktura pakietu protokołu IP

Poniżej przedstawiono strukturę pakietu protokołu IP oraz wyjaśnienie znaczenia informacji zawartych w poszczególnych polach tego pakietu.




Rys. 1. Struktura pakietu protokołu IP

**Wersja** – informacja o wersji protokołu IP (obecnie używana jest wersja 4).

**IHL (*Internet Header Length)*** – określa długość nagłówka w 32-bitowych słowach (minimum 5).

**Typ usługi (TOS – *Type Of Service)*** – wskazuje typ lub poziom wymaganych usług.

**Długość całkowita** – liczba bajtów całego pakietu (nagłówek + dane).

**Przesunięcie fragmentacji** –w przypadku fragmentacji pakietu zawartość tego pola wskazuje położenie danego fragmentu w początkowym pakiecie mierzone w jednostkach 8-bajtowych.

**Identyfikacja** – liczba całkowita identyfikująca pakiet. Po fragmentacji każdy fragment ma identyczną wartość tego pola.

**Znaczniki** – trzy bity: „nie fragmentuj", „dalsze fragmenty", „zarezerwowany".

**Czas życia (TTL – *Time To Live*)** – określa maksymalną liczbę węzłów sieci (routerów) przez które może jeszcze przejść dany pakiet. Każdy router przekazując pakiet zmniejsza wartość tego pola o jeden, a gdy TTL osiągnie zero pakiet jest usuwany z sieci.

**Protokół** –wskazuje protokół warstwy 4, którego informacje przenosi dany pakiet.

**Suma kontrolna nagłówka** – 16 bitowa suma kontrolna obejmująca nagłówek danego pakietu.

**Adresy źródłowy i docelowy** – 32 bitowe numery IP nadawcy i odbiorcy danego pakietu.

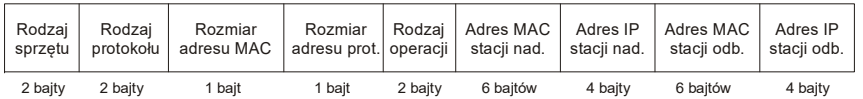
**Opcje** – pole o zmiennej długości umożliwiające np. wymuszenie przesyłania pakietu określoną trasą, rejestrację przebytej przez pakiet trasy oraz czasu lokalnego w poszczególnych węzłach sieci przez które przechodzi pakiet.

**Wypełnienie** – uzupełnia nagłówek zerami tak, aby jego długość była całkowitą wielokrotnością 32 bitów.

**Dane** – przesyłane przez pakiet dane z warstwy wyższej (np. segment TCP lub datagram UDP).

## 5. Struktura komunikatu protokołu ARP

Poniżej przedstawiono strukturę komunikatów zapytania i odpowiedzi protokołu ARP oraz wyjaśnienie znaczenia informacji zawartych w poszczególnych polach tych komunikatów.




Rys. 2. Struktura komunikatu protokołu ARP

**Rodzaj sprzętu** – określa rodzaj adresu używanego przez sprzęt. Dla sieci Ethernet wartość tego pola wynosi 1.

**Rodzaj protokołu** – określa protokół sieciowy (warstwy 3), którego adresy są mapowane z adresami sprzętowymi przy użyciu protokołu ARP. Dla protokołu IP wartość tego pola wynosi 0x0800.

**Rozmiar adresu MAC** – określa rozmiar adresu sprzętowego (MAC) znajdowanego przez protokół ARP na podstawie adresu protokołu sieciowego. Dla sieci Ethernet wartość tego pola wynosi 6.

**Rozmiar adresu protokołu** – określa rozmiar adresu protokołu sieciowego (3 warstwy) na podstawie którego protokół ARP znajduje adres sprzętowy. Dla sieci z protokołem IP v.4 wartość tego pola wynosi 4.

**Rodzaj operacji** – zawartość tego pola informuje czy dany komunikat jest zapytaniem ARP (wartość 1), odpowiedzią ARP (wartość 2), zapytaniem RARP (wartość 3), czy też odpowiedzią RARP (wartość 4).

**Adres MAC stacji nadawczej** – adres sprzętowy hosta wysyłającego dany komunikat. W przypadku odpowiedzi ARP, pole to zawiera znaleziony adres MAC.

**Adres IP stacji nadawczej** – adres sieciowy (IP) hosta wysyłającego dany komunikat.

**Adres MAC stacji odbiorczej** – adres sprzętowy hosta, dla którego przeznaczony jest dany komunikat ARP. W przypadku zapytania ARP w polu tym umieszczona jest wartość zerowa.

**Adres IP stacji nadawczej** – adres sieciowy (IP) hosta, dla którego przeznaczony jest dany komunikat ARP. W przypadku zapytania ARP pole to zawiera numer IP hosta którego adres MAC ma być znaleziony.

## 6. Plan wykonywania ćwiczenia laboratoryjnego

**Część 1**

1. Określić konfigurację sieciową komputera znajdującego się na stanowisku laboratoryjnym (adres IP, maska podsieci, adres bramy domyślnej). Wyznaczyć adres IP sieci do której przyłączony jest ten komputer.
2. Posługując się programem *Wireshark* prześledzić wymianę pakietów IP związaną z wykonaniem komendy *ping* pomiędzy dwoma komputerami znajdującymi się w tej samej sieci IP. Wskazane jest przy tym odpowiednie ustawienie filtrów w programie *Wireshark*, aby rejestrowane były jedynie ramki pochodzące z interesującej nas komunikacji. Zarejestrować i zinterpretować wartości zawarte w poszczególnych polach nagłówków protokołów IP oraz ICMP dla wysyłanych i odbieranych pakietów.
3. Posługując się programem *Wireshark* prześledzić wymianę pakietów IP związaną z wykonaniem programu *traceroute* do komputera wskazanego przez prowadzącego. Zarejestrować i zinterpretować wartości zawarte w poszczególnych polach nagłówków protokołów IP oraz ICMP. Szczegółowo opisać działanie programu *traceroute* posługując się danymi z zarejestrowanych pakietów.
4. Wysłać do wybranego komputera znajdującego się w tej samej sieci IP pojedyncze zapytanie *ping* z rozmiarem pakietu większym niż wynosi maksymalny rozmiar jednostki transmisyjnej (MTU) interfejsu danej stacji. W systemach rodziny Windows dla interfejsów Ethernet domyślna wartość MTU wynosi 1500 bajtów. Rozmiar pakietu wysyłanego poleceniem *ping* można ustalić poprzez opcję -l tego polecenia. Programem *Wireshark* zarejestrować ramki z wysłanym zapytaniem i odebraną odpowiedzią. Na podstawie analizy zawartości tych ramek opisać proces fragmentacji pakietu IP. W szczególności należy przy tym poprawnie zinterpretować zawartości pól „przesunięcie fragmentacji", „identyfikacja" oraz pola znaczników w nagłówkach wysyłanych i odbieranych pakietów IP.
5. Sprawdzić zachowanie sieci w przypadku wysłania pakietu IP z ustawionym znacznikiem DF („nie fragmentuj") i o rozmiarze większym niż wynosi najmniejsza wartość MTU na ścieżce połączenia. Do wysłania pakietu z ustawionym znacznikiem DF można użyć opcji –f polecenia *ping*.

**Część 2**

6. Zarejestrować i zanalizować komunikaty protokołu ARP wymieniane w czasie próby nawiązania połączenia (np. komendą *ping*) między dwoma komputerami w następujących sytuacjach:

- oba komputery znajdują się w tej samej sieci IP,
- jeden z komputerów pracuje w innej sieci IP.

Przed wykonaniem rejestracji należy wyzerować bufor protokołu ARP poprzez wykonanie komendy `arp - d *`.

Odczytać jaka wartość znajduje się w polu *Typ* ramek Ethernet zawierających zapytanie i odpowiedź protokołu ARP. Pod jakie adresy MAC wysyłane są te ramki?

7. Prześledzić wymianę datagramów UDP związaną z wykorzystaniem usługi DNS lub QUOTE. W tym celu można użyć np. programu *nslookup*. Zarejestrować i zinterpretować wartości zawarte w poszczególnych polach nagłówków wysyłanych i odbieranych datagramów protokołu UDP.

8. Zarejestrować przebieg połączeniowej sesji protokołu TCP przy korzystaniu z usługi WWW. Wskazane jest przy tym odpowiednie ustawienie filtrów w programie *Wireshark*. Aby rejestrowana sesja miała akceptowalną długość, należy skorzystać ze strony WWW specjalnie przygotowanej do tego ćwiczenia. Adres tej strony to http://bramka/test.asp, gdzie bramka jest numerem IP bramy domyślnej ustawionej w konfiguracji sieciowej używanego w ćwiczeniu komputera.

Sporządzić diagram przedstawiający zaobserwowany proces wymiany segmentów TCP uwzględniający zawartość pól „numer sekwencyjny", „numer potwierdzenia" oraz stan znaczników w nagłówku segmentu TCP. W szczególności na sporządzanym diagramie należy wyróżnić fazy nawiązania połączenia, wymiany informacji oraz zakończenia połączenia.

**Sprawozdanie**

W sprawozdaniu należy zamieścić wyniki uzyskane przy wykonywaniu poszczególnych części ćwiczenia poparte odpowiednimi danymi zarejestrowanymi programem *Wireshark*.

## 7. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

## 8. Literatura


1. Dye M. A., McDonald R., Rufi A. W.: Akademia sieci Cisco. CCNA Exploration. Semestr 1. Wydawnictwo PWN (MIKOM), Warszawa, 2008.
2. Kevin R. Fall, W. Richard Stevens: TCP/IP od środka. Protokoły. Wydawnictwo Helion, Gliwice 2013.
3. Dokumentacja poleceń *ping*, *traceroute*, *arp.*
4. Instrukcja obsługi programu *Wireshark* (www.wireshark.org).