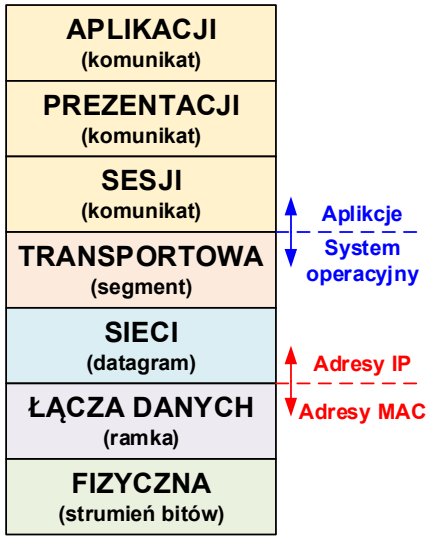
1. Model referencyjny OSI

Sieć komputerowa łączy komputery w celu współdzielenia zasobów, korzystania ze wspólnych danych, przesyłania komunikatów oraz korzystania z wielu innych usług.

Działanie sieci komputerowej opiera się na wykorzystaniu:
- komputerów i urządzeń sieciowych;
- mediów do transmisji danych;
- protokołów (zestawów reguł rządzących transmisją danych);
- oprogramowania umożliwiającego udostępnianie usług i korzystanie z tych usług.

Międzynarodowa Organizacja Normalizacyjna **ISO** (***I**nternational **O**rganization for **S**tandardization*) opracowała tzw. Model Referencyjny Połączonych Systemów Otwartych **OSI** (***O**pen **S**ystem **I**nterconnection*), nazywany w skrócie **ISO/OSI**. Model referencyjny opisuje działanie sieci komputerowych, dzieląc całą skomplikowaną strukturę sieci na 7 warstw (rys. 1). Pozwala on producentom różnych systemów połączyć wzajemnie ich produkty poprzez standardowy interfejs. Dzięki niemu możliwe jest scalenie zasobów programowych i sprzętowych oraz przenoszenie ich na różne systemy.

7. **Warstwa aplikacji** – oferuje usługi sieciowe użytkownikowi lub programom (HTTP, FTP, SSH, DNS, SMTP, POP3 i in.).
6. **Warstwa prezentacji** – interpretuje dane z punktu widzenia aplikacji, dokonuje konwersji danych, szyfrowania i deszyfrowania (JPG, MIDI, MPEG i in.).
5. **Warstwa sesji –** wyznacza ramy czasowe wymiany danych i synchronizuje ten proces.
4. **Warstwa transportowa** – zapewnia bezbłędną komunikację, dzieli dane na segmenty i kontroluje kolejność ich przesyłania (TCP, UDP, RTP i in.).
3. **Warstwa sieci** – ustala drogę transmisji datagramów i dostarcza je przez pośrednie węzły (IP, **ARP** i in.).
2. **Warstwa łącza danych** – przesyła ramki danych (ciągi bitów o ustalonej strukturze) i wykrywa błędy transmisji (**ARP**, Ethernet, Wi-Fi, PPP i in.).
1. **Warstwa fizyczna** – umożliwia szeregowe (bit po bicie) przesłanie strumienia bitów przez łącze fizyczne (modulacja, sposób fizycznej transmisji).

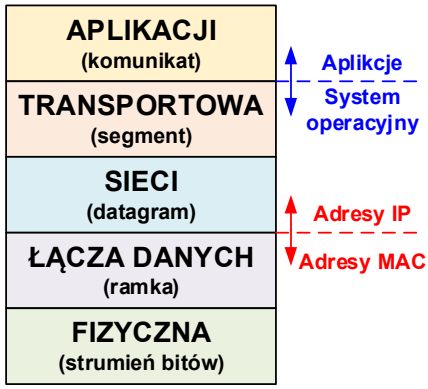


Rys. 1. Model referencyjny OSI

2. Stos protokołów internetowych

Model OSI ukształtowano w czasie, kiedy późniejsze protokoły internetowe dopiero powstawały (lata 70-te ubiegłego wieku). Po ich rozwoju, coraz większą rolę zaczął odgrywać model reprezentowany przez 5-cio warstwowy **stos protokołów internetowych**. Model ten wierniej od modelu OSI odzwierciedla procesy zachodzące podczas transmisji danych w Internecie.

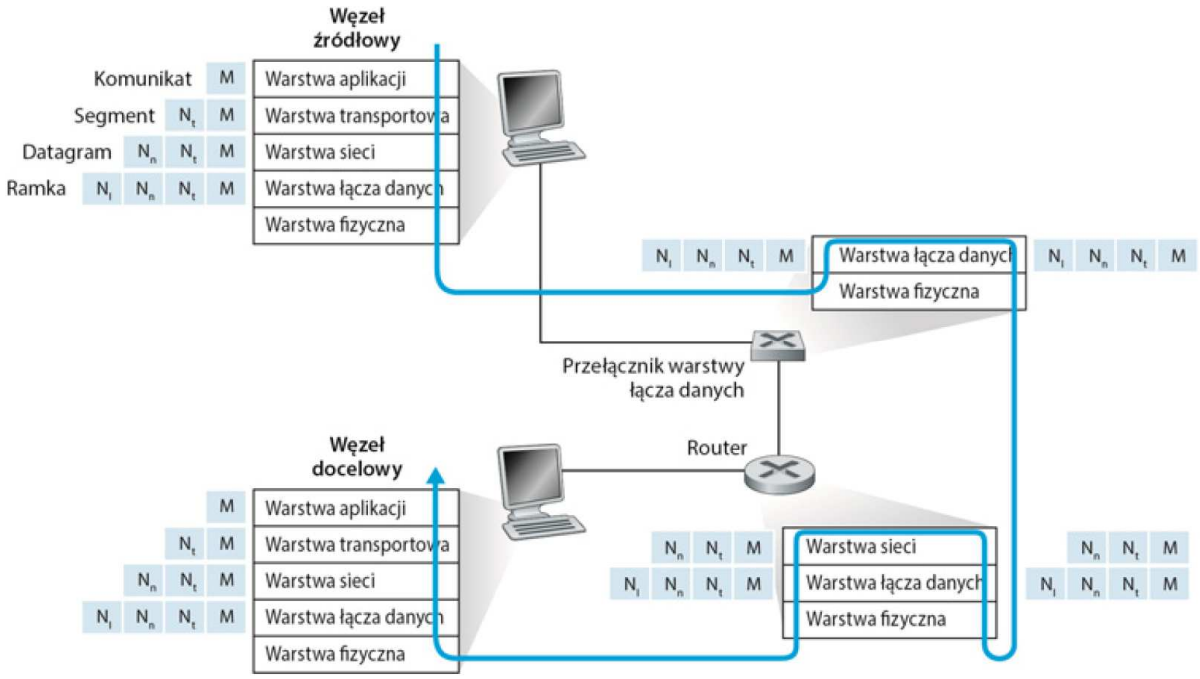
Zasadnicza różnica pomiędzy tymi modelami jest taka, że model internetowy nie obejmuje warstw **prezentacji** i **sesji** modelu OSI (rys. 2). W związku z tym, to autor aplikacji decyduje, czy usługi realizowane przez wspomniane warstwy mają znaczenie i czy aplikacja ich potrzebuje. Jeśli tak, programista musi wbudować w aplikację odpowiednie mechanizmy.



Rys. 2. Stos protokołów internetowych

3. Implementacja warstw protokołów przez urządzenia sieciowe i kapsułkowanie danych

Na rys. 3 zilustrowano fizyczną ścieżkę, jaką dane pokonują w dół stosu protokołów nadawczego systemu końcowego, w stosach protokołów pośrednich przełączników warstwy łącza danych i routerów, a następnie w górę stosu protokołów odbiorczego systemu końcowego. Urządzenia sieciowe (routery, przełączniki) zwykle nie implementują wszystkich warstw stosu protokołów, przeważnie obsługują tylko dolne warstwy. Na rys. 3 pokazano, że przełączniki warstwy łącza danych implementują warstwy pierwszą i drugą, a routery – warstwy od pierwszej do trzeciej. Oznacza to na przykład, że routery internetowe mogą implementować protokół IP (protokół warstwy trzeciej), natomiast przełączniki warstwy łącza danych tego nie potrafią. Obsługują jednak adresy warstwy drugiej, takie jak adresy ethernetowe. Zauważmy, że hosty implementują wszystkie 5 warstw.



Rys. 3. Hosty, routery i przełączniki warstwy łącza danych. Każdy z tych węzłów ma inny zestaw warstw, które są odzwierciedleniem ich różnego przeznaczenia

Kapsułkowanie danych przebiega w następujących etapach:

1. **Warstwa transportowa** pobiera **komunikat** z warstwy aplikacji (*M*), dodaje do niego swój nagłówek (N_t) i tworzy **segment**. Dodatkowe informacje w nagłówku są wykorzystywane przez warstwę transportową węzła odbiorczego. Dane te, np. **numery portów**, umożliwiają warstwie transportowej strony odbiorczej dostarczenie komunikatu do odpowiedniej aplikacji, pozwalają także na wykrywanie błędów, itp.
2. **Warstwa sieci** pobiera segment, dodaje własny nagłówek (N_n) i tworzy **datagram**. Dodany nagłówek zawiera, m.in. **adresy IP** źródłowego i docelowego systemu końcowego.
3. **Warstwa łącza danych** pobiera datagram, dołącza swój nagłówek i tworzy **ramkę danych**. W dołączonym nagłówku znajdują się, m.in. **adresy MAC** nadawcy i odbiorcy. Następnie, ramka przesyłana jest do warstwy fizycznej.

Po stronie odbiorczej, wszystkie procesy zachodzą w odwrotnej kolejności. Jak widać, efektem kapsułkowania jest to, że w każdej warstwie pakiet ma pola dwóch rodzajów – **nagłówkowe** i **danych**. Pole danych stanowi zwykle pakiet z wyższej warstwy.

4. Standard Ethernet

W zależności od wielkości, sieci dzielą się na lokalne, miejskie i rozległe. Przykładami standardów stosowanych w sieciach lokalnych są: Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), FDDI, WLAN (IEEE 802.11). Najpopularniejszym standardem stosowanym w sieciach lokalnych jest Ethernet. Bazuje on na idei węzłów podłączonych do wspólnego medium transmisyjnego oraz wysyłających

i odbierających za jego pomocą dane w postaci ramek. Kontrola dostępu do medium realizowana jest za pomocą metody **CSMA/CD**, a wszystkie węzły posiadają unikalny adres sprzętowy (**MAC**).

Specyfikacja standardu Ethernet obejmuje:

1. Media transmisyjne oraz przesyłane nimi sygnały.
2. Format ramek danych i protokoły z warstwy fizycznej i łącza danych (podwarstwy MAC).

5. Warstwa łącza danych

Warstwa łącza danych zapewnia adresowanie na poziomie sieci lokalnej (adresowanie w warstwie 2, adresowanie fizyczne) oraz przesyłanie ramek pomiędzy komunikującymi się urządzeniami.

Warstwa łącza danych składa się dwóch warstw:

1. **LLC** (***L**ogical **L**ink **C**ontrol*) – warstwa sterowania łączem logicznym.
   - Pobiera dane z warstwy sieciowej i dzieli je na ponumerowane ramki.
   - Steruje przepływem danych i kontroluje błędy transmisji.
2. **MAC** (***M**edia **A**ccess **C**ontrol*) – warstwa sterowania dostępem do medium.
   - Pobiera dane od warstwy LLC i współpracując z elementami fizycznymi przesyła je do medium.
   - Umożliwia węzłom współdzielenie jednego medium.
   - Generuje bity początku i końca ramki oraz bity detekcji błędów.
   - Dodaje informacje dotyczące kontroli dostępu oraz adresów MAC nadawcy i odbiorcy.

6. Format ramki Ethernetu

Preambuła	Adres MAC odbiorcy	Adres MAC nadawcy	Długość / typ ramki	Dane	CRC
8 bajtów	6 bajtów	6 bajtów	2 bajty	46-1500 bajtów	4 bajty

Rys. 4. Format ramki Ethernetu

Preambuła – składa się z 64 bitów (zer i jedynek na przemian), co ułatwia synchronizację nadawcy i odbiorcy. Sygnał ten informuje również węzły, że ma być nadesłana ramka i należy sprawdzić jej adres przeznaczenia.

Adres MAC odbiorcy – adres fizyczny (sprzętowy) interfejsu węzła przeznaczenia.

Adres MAC nadawcy – adres fizyczny (sprzętowy) interfejsu węzła źródłowego.

> **Adres MAC** (***M**edia **A**ccess **C**ontrol*) jest na stałe przypisanym przez producenta identyfikatorem urządzenia sieciowego (można go porównać do numeru PESEL). Jest on zazwyczaj definiowany za pomocą cyfr szesnastkowych, na przykład:
>
> `4C-31-22-10-F1-32  lub  4C31:2210:F132`
>
> Adres MAC składa się z 48 bitów, pierwsze 24 bity zawierają identyfikator producenta, a kolejne numer seryjny karty. Dzięki temu, zapewniona jest unikalność adresów MAC. **Adresy MAC zapewniają adresowanie ramek w ramach sieci lokalnej.** Obszar adresowy 48-bitowy pozwala na zakodowanie 2^{48} różnych adresów (lub w przybliżeniu 281 474 976 710 000 różnych adresów).

Długość / typ ramki – jeśli pole ma wartość mniejszą lub równą `1500`, określa liczbę bajtów w polu **Dane**. Jeśli wartość jest większa, niż `1536`, określa protokół, który ma przejąć ramkę (np. `ARP` – `0x0806`, `IPv4` – `0x0800`, itd.). System operacyjny, na podstawie typu ramki decyduje, do którego z modułów oprogramowania obsługi protokołów należy ją wówczas skierować.

Dane – informacja przesyłana przez ramkę. Jeśli danych jest więcej, niż ograniczenie górne, to są one dzielone na kilka ramek. Gdy danych jest mniej, niż ograniczenie dolne, dodawane są bity dodatkowe.

CRC (***C**yclic **R**edundancy **C**heck*) – pole 32-bitowe ułatwiające interfejsowi wykrywanie błędów transmisji. Nadawca oblicza CRC (zależy ono od danych znajdujących się w ramce), odbiorca również oblicza CRC i porównuje obie wartości, co umożliwia wykrycie przekłamań (w pewnym zakresie).

Ramka może zawierać do **1518 B** (bez preambuły i sygnału początku ramki).

7. Domena kolizji

Domena kolizji jest fizycznym segmentem sieci, w którym mogą wystąpić tzw. „kolizje”, jeśli dwa lub więcej komputerów podłączonych do niej będą nadawać „jednocześnie”. Efektem kolizji jest zniekształcenie nadawanego sygnału i w konsekwencji brak możliwości jego odbioru. Jeśli komputery połączone są za pomocą koncentratora (*hub*), tworzą pojedynczą domenę kolizji. Urządzenia takie jak most, przełącznik czy router tworzą oddzielne domeny kolizji na każdym ze swoich portów.

8. Interfejs sieciowy

Interfejs sieciowy komputera (karta sieciowa) analizuje ramki i określa, które z nich powinny trafić do danego komputera. Jeśli w domenie kolizji znajduje się kilka komputerów, każdy interfejs otrzymuje wszystkie ramki wysłane do sieci – także te adresowane do innych komputerów. Interfejs odfiltrowuje ramki, korzystając z pola adresu odbiorcy w ramce. Ignoruje on pakiety, które są adresowane do innych maszyn, przekazując do komputera tylko te, które są adresowane do niego. Mechanizm adresowania i **filtr sprzętowy** są konieczne, aby uniknąć przeciążenia komputera nadchodzącymi danymi.

Gdy interfejs komputera ma wysłać ramkę, wówczas sprawdza, czy w medium transmisyjnym są przesyłane dane (czyli sprawdza istnienie fali nośnej). Jeśli nie odbywa się żadna transmisja, interfejs zaczyna nadawanie. Czas trwania każdej transmisji jest ograniczony (gdyż jest określony maksymalny rozmiar ramki). Ponadto, sprzęt musi zapewniać minimalny czas jałowy między transmisjami, aby umożliwić również innym komputerom przesyłanie danych.

Po rozpoczęciu transmisji przez urządzenie nadawczo-odbiorcze (*transceiver*) interfejsu sieciowego, sygnał nie dociera do wszystkich węzłów sieci równocześnie. Rozchodzi się on w kablu sieciowym z prędkością równą 80% prędkości światła. Jest zatem możliwe, że dwa transceivery wykryją, że medium transmisyjne jest dostępne, i równocześnie zaczną nadawać. Dwa równocześnie nadawane sygnały zostaną zmieszane, co prowadzi do zakłóceń, które uniemożliwiają odbiór któregokolwiek z nich. Takie zdarzenia nazywamy właśnie **kolizjami**.

9. Kontrola dostępu do medium – CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*)

Każdy transceiver w czasie nadawania monitoruje kabel, aby wykryć, czy nie ma zakłóceń z powodu obcych sygnałów. Ten proces monitorowania jest określany jako **wykrywanie kolizji.** Po wykryciu kolizji, interfejs sieciowy komputera przerywa transmisję, czeka na zakończenie aktywności w sieci, a następnie próbuje ponownie wysłać informacje. Trzeba jednak wykluczyć w jakiś sposób sytuację, gdy wszystkie transceivery czekają na możliwość wysłania sygnału, a następnie wszystkie nadają równocześnie, powodując ciągłe kolizje. Aby uniknąć tego rodzaju sytuacji, Ethernet używa strategii wykładniczego wydłużania czasu odczekiwania. Oznacza to, że nadawca po pierwszej kolizji odczekuje przez okres o losowej długości (**10 ÷ 90 ms**). Jeśli druga próba spowoduje kolizję, to czeka dwa razy dłużej, jeśli przy trzeciej próbie nastąpi kolizja – cztery razy dłużej i tak dalej. Ta strategia jest umotywowana tym, że w rzadkich wypadkach, gdy kilka stacji zacznie nadawać równocześnie, może wystąpić poważny „korek”. Wówczas może się łatwo zdarzyć, że wybrane losowo wartości czasu oczekiwania kilku stacji będą się tylko nieznacznie różnić, prawdopodobieństwo następnej kolizji będzie więc duże. Podwajając opóźnienia, powoduje się coraz większe różnice czasów oczekiwania poszczególnych stacji, przez co prawdopodobieństwo dalszych kolizji staje się bardzo małe.

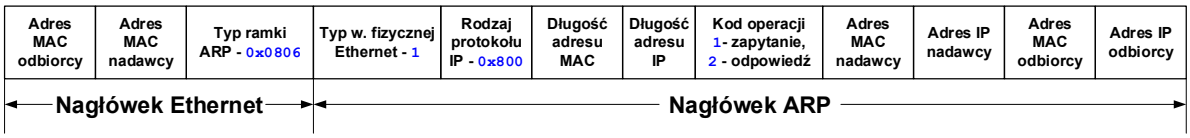
10. Protokół `ARP`

Protokół `ARP` funkcjonuje w dwóch warstwach – sieci i łącza danych. Zarządza on w komputerze tablicą odwzorowań adresów `IP` i `MAC`. Tablica `ARP` „pamięta”, jaki adres `MAC` jest związany z danym adresem `IP`. Dzięki temu, dwóm stacjom w sieci lokalnej nie zostanie przydzielony ten sam adres IP. Jeżeli tablica odwzorowań `ARP` nie zawiera adresu `MAC` urządzenia lokalnego, wówczas wysłana zostaje **rozgłoszeniowa** ramka ethernetowa (*broadcast*) z docelowym adresem `MAC` równym `FF-FF-FF-FF-FF-FF` (rys. 5).

Nagłówek Ethernet	Nagłówek ARP	Dane

Rys. 5. Miejsce nagłówka `ARP` w ramce ethernetowej

Na rys. 6 pokazano format nagłówka ARP. Przy operacji zapytania, pole **Adres MAC odbiorcy** jest wyzerowane (ten adres jest nieznany). W przypadku odpowiedzi, 4 ostatnie pola są wypełnione.

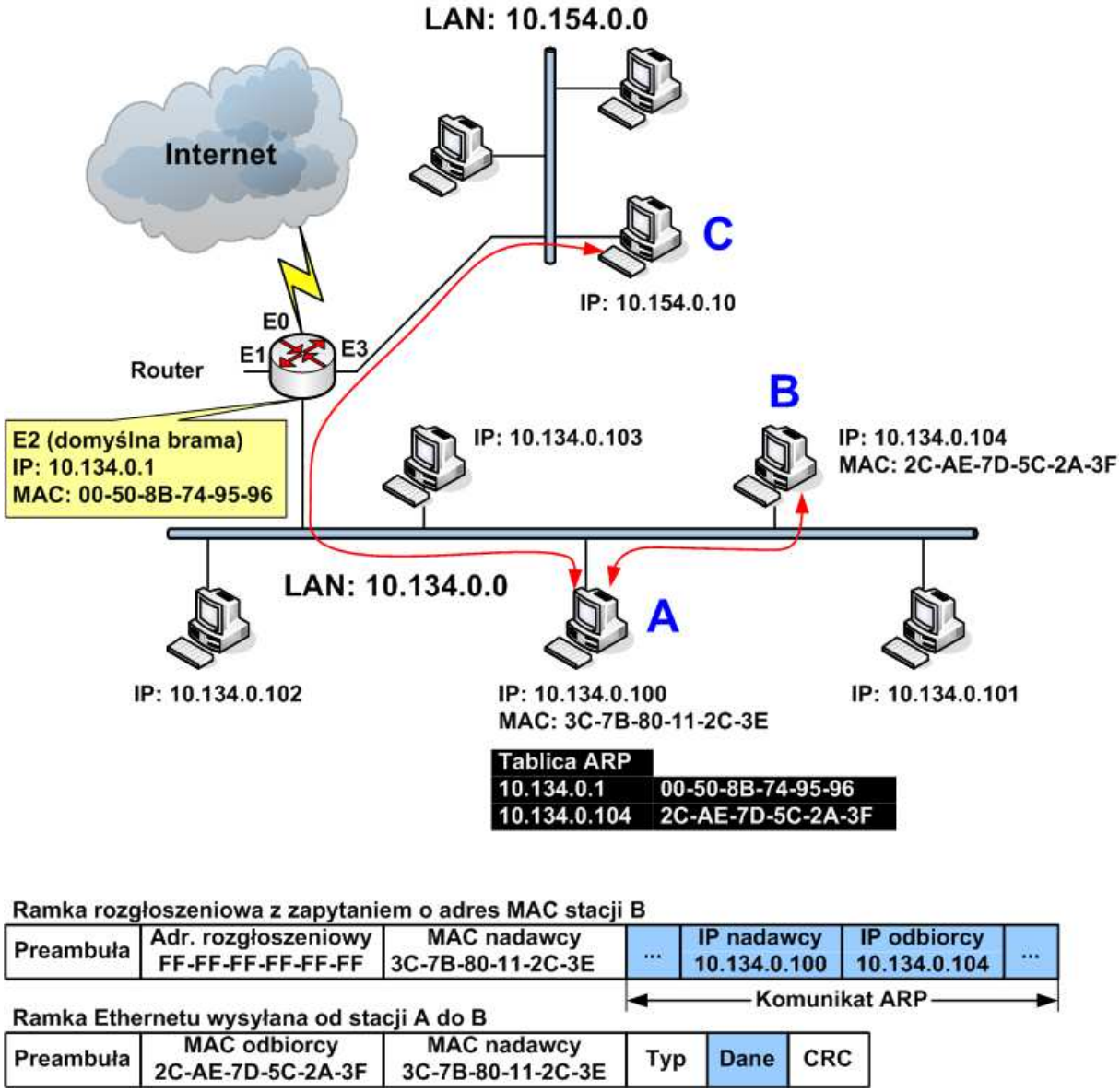


Rys. 6. Format nagłówka ARP

Ramkę rozgłoszeniową odbierają wszystkie komputery znajdujące się w tzw. **domenie rozgłoszeniowej** (logicznym segmencie sieci podłączonym do danego portu routera). Jeżeli ramkę tę odbierze komputer o poszukiwanym adresie IP, wysyła on odpowiedź, na podstawie której protokół ARP określa jego adres MAC. Powoduje to dodanie takiej pary adresów do tablicy ARP na komputerze, z którego zostało wysłane zapytanie.

Różnice pomiędzy zapytaniem ARP, a odpowiedzią są następujące:

- zmienia się kod operacji z **1** na **2**;
- informacje adresowe zostają zamienione miejscami – adresy IP i MAC nadawcy są teraz adresami IP i MAC odbiorcy;
- pakiet zawiera wszystkie informacje, m.in. szukany adres MAC komputera o znanym adresie IP.



Rys. 7. Ilustracja działania protokołu ARP

Jeżeli komputer w ciągu kilku minut nie otrzyma żadnych pakietów od danego adresu IP, wtedy adres ten, razem z odpowiadającym mu adresem MAC, zostaje usunięty z tablicy usługi ARP, ponieważ sytuacja taka oznacza, że urządzenie zostało wyłączone. Późniejsze próby użycia takiego adresu IP spowodują ponowne wysłanie ramki rozgłoszeniowej przez protokół ARP i zaktualizowanie tablicy.

Adresy MAC, a więc i protokół ARP, są używane jedynie wewnątrz sieci LAN. Podczas przygotowywania w komputerze pakietu do transmisji, następuje sprawdzenie, czy docelowy adres IP należy do sieci lokalnej. Polega to na skontrolowaniu, czy część adresu IP identyfikująca sieć jest taka sama, jak adres sieci lokalnej. Jeżeli tak, komputer przy pomocy usługi ARP pobiera adres MAC urządzenia docelowego. Znaleziony w ten sposób adres MAC służy jako adres docelowy dla pakietów z danymi.

Jeżeli docelowy adres IP nie jest adresem lokalnym, komputer musi znaleźć adres MAC bramy domyślnej. **Brama domyślna** to interfejs routera, do którego przyłączona jest sieć lokalna i który zapewnia łączność z innymi sieciami. Adres bramy jest przechowywany w konfiguracji lokalnego hosta. Adres MAC bramy jest potrzebny dlatego, że pakiety są przesyłane właśnie do niej, a router przesyła je dalej do sieci, dla której są przeznaczone.

Ćwiczenie 1.

Opisz działanie protokołu ARP.

Ćwiczenie wykonaj w oparciu o rys. 7, ilustrujący działanie protokołu ARP. Opisz dokładnie procesy zachodzące podczas komunikacji realizowanej według dwóch scenariuszy, które na rys. 7 są zaznaczone czerwonymi strzałkami:

a) stacja **A** wysyła dane do stacji **B**;

b) stacja **A** wysyła dane do stacji **C**.

Dla obu scenariuszy przyjmij założenie, że na początku, tablica ARP stacji **A** jest pusta. Dla każdego scenariusza podaj wartości pól (kod operacji, adresy MAC, adresy IP) zamieszczonych w nagłówku ARP podczas zapytania i odpowiedzi ARP. Podaj także zawartość nagłówka ethernetowego podczas wysyłania danych na pozyskany adres. W opisie, wykorzystaj format ramki Ethernet z rys. 4 oraz format nagłówka ARP z rys. 6.

Ćwiczenie 2.

Sprawdź konfigurację interfejsu sieciowego.

- Wyświetl i zanotuj konfigurację interfejsu sieciowego (łącznie z adresem fizycznym).

Ćwiczenie 3.

Wyświetl pomoc dla polecenia ARP.

- Wykonaj poniższe polecenie i zapoznaj się z opisem opcji polecenia arp.

```
arp /?
```

Ćwiczenie 4.

Wyświetl i usuń zawartość tablicy ARP.

- Wyświetl zawartość tablicy ARP poleceniem:

```
arp -a
```

Jeżeli pojawi się komunikat: Nie znaleziono wpisów ARP, oznacza to, że tablica ARP jest pusta.

- Dla każdego interfejsu sieciowego zanotuj jego adres **IP** oraz adres rozgłoszeniowy i przypisany mu adres fizyczny.
- Jeżeli zostaną wyświetlone adresy IP i przyporządkowane im adresy MAC, usuń całą zawartość tablicy poleceniem:

```
arp -d *          // Wymaga uprawnień administratora
```

- Wyświetl ponownie zawartość tablicy ARP. Czy są jakieś zmiany?
- Wyłącz kartę sieciową w oknie **Połączenia sieciowe**, a następnie włącz ją i ponownie wyświetl zawartość tablicy ARP. Co zauważyłeś?

Ćwiczenie 5.

Dodaj do tablicy ARP adres MAC komputera podłączonego do tej samej sieci lokalnej.

- Sprawdź adres IP innego komputera, który jest podłączony do tej samej sieci lokalnej.
- Wykasuj zawartość tablicy ARP.
- Wyślij pakiety ping na adres innego komputera.
- Sprawdź, czy tablica ARP została uzupełniona odpowiednim adresem MAC.

Uwaga: Jeżeli do Twojej sieci lokalnej nie jest podłączony inny komputer, wykonaj to ćwiczenie z wykorzystaniem dwóch systemów Linux Slax uruchomionych na odzielnych maszynach wirtualnych. W takiej sytuacji, dla drugiego systemu należy wykonać nową instalację, zgodnie z instrukcją dołączoną do materiałów z laboratorium nr 3. Każdy z tych systemów można traktować jako odrębny komputer podłączony do tej samej sieci lokalnej. Po instalacji, zapoznaj się z dokumentacją polecenia arp, wydając komendę `man arp`. Przed wysłaniem pakietów ping na adres drugiego komputera, najpierw usuń go z tablicy ARP, ponieważ został on tam dodany podczas uruchamiania systemu.

Ćwiczenie 6.

Dodaj konkretny wpis do bufora ARP.

- Załóżmy, że do sieci lokalnej podłączony jest komputer, którego adres IP w ostatnim oktecie jest o 1 większy od adresu IP Twojego interfejsu. Przypisz temu komputerowi adres MAC równy `0a-1b-2c-3d-4e-5f`.

Ćwiczenie 7.

Usuń konkretny wpis z bufora ARP.

- Usuń wpis z bufora ARP, który dodałeś w ćwiczeniu nr 6.

Ćwiczenie 8.

Sprawdź działanie protokołu ARP podczas wysyłania pakietów ping na wybrane adresy URL.

- Wykasuj zawartość tablicy ARP, a następnie wyślij pakiety ping na poniższe adresy URL i zanotuj odpowiadające im adresy IP.

```
onet.pl
allegro.pl
novell.com
```

- Porównaj statystyki dotyczące czasów RTT dla każdego przypadku.
- Wyświetl zawartość tablicy ARP i zanotuj adresy MAC każdego z powyższych serwerów obok ich adresów IP. Czy można to zrobić? Dlaczego tak sądzisz?
- Sprawdź, czy w tablicy ARP znajduje się adres IP domyślnej bramy, który zanotowałeś w ćwiczeniu pierwszym. Do czego potrzebny jest adres IP domyślnej bramy?
- Jaki adres MAC był używany przy przesyłaniu pakietów ping do serwerów określonych powyższymi adresami URL? Dlaczego?