

Sieci komputerowe

Wykład 5 — Warstwa sieciowa

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

03.2022

Plan prezentacji

1 Warstwa sieciowa modelu OSI

2 Protokół IP

- Cechy
- IPv4
- IPv6

3 Routing

- Definicja
- Tablica routingu
- Protokoły routingu
- Brama domyślna

4 Protokół ICMP

- Rola
- Rodzaje komunikatów
- ICMPv6

1. Warstwa sieciowa

Rola, protokoły i rodzaje transmisji

1. Warstwa sieciowa

Warstwa sieciowa — przypomnienie:

Rola

Zapewnienie komunikacji pomiędzy urządzeniami nawet z różnych sieci:

- trasowanie (routing),
- *load balancing*,
- adresowanie urządzeń sieciowych na poziomie globalnym.

Protokoły

- IP: IPv4, IPv6
- IPX
- także ICMP

Jednostka danych

Pakiet

1. Warstwa sieciowa

Rodzaje komunikacji:

- **Unicast** — komunikacja jeden do jednego
- **Broadcast** — komunikacja jeden do wszystkich (oprócz siebie)
- **Multicast** — komunikacja jeden do wielu (grupowa)
- **Anycast** — komunikacja do najbliższego sąsiada (tylko w IPv6)

2. Protokół IP

IPv4 vs IPv6

2.1 Protokół IP. Cechy

Cechy protokołu IP:

- **Bezpołączeniowość** — podczas transmisji pakietu nie jest tworzona sesja pomiędzy komunikującymi się urządzeniami
- **Działanie *best effort*** — nie ma zapewnienia bezstratnego dostarczenia pakietu
- **Niezależność od medium transmisyjnego** — protokołu IP nie interesuje, czy pakiet jest przesyłany przez medium przewodowe czy bezprzewodowe (tym zajmują się niższe warstwy)

Protokół IP jest zdecydowanie najbardziej popularnym protokołem na warstwie 3.

2.2 Protokół IP. IPv4

Nagłówek IPv4:

+	Bity 0 - 3	4 - 7	8 - 15	16 - 18	19 - 31
0	Wersja	Długość nagłówka	Typ usługi	Całkowita długość	
32	Numer identyfikacyjny			Flagi	Kontrola przesunięcia
64	Czas życia pakietu (TTL)		Protokół warstwy wyższej	Suma kontrolna nagłówka	
96	Adres źródłowy IP				
128	Adres docelowy IP				
160	Opcje IP			Uzupełnienie	
192	Dane				

Grafika: <https://www.soisk-me.pl/>

2.2 Protokół IP. IPv4

Nagłówek IPv4 — ważniejsze pola:

- **Wersja** — określa wersję protokołu — IPv4
- **Differentiated Services (DS)** (wcześniej: ToS, *Type of Service*) — określa priorytet pakietu,
- **Flagi** — informują o tym, czy dany pakiet może być/jest podzielony i wysłany w ramach kilku ramek ethernetowych (ramka ethernetowa może zawierać ładunek o wielkości maksymalnie 1500 bajtów, jeśli pakiet wyższej warstwy jest większy, musi zostać podzielony, o ile nie jest ustawiona flaga *Don't fragment*)

2.2 Protokół IP. IPv4

Nagłówek IPv4 — ważniejsze pola:

- **TTL** (ang. *Time to Live*) — czas życia, jaki pozostał pakietowi przed usunięciem go z sieci, innymi słowy maksymalna ilość przeskoków (routerów na trasie), które może jeszcze dokonać dany pakiet
- **Protokół warstwy wyższej** — informacja o zawartości pakietu (PDU jakiego protokołu enkapsulowany jest w ramach pakietu)
- **Adres źródłowy** — adres IPv4 urządzenia nadającego pakiet
- **Adres docelowy** — adres IPv4 urządzenia, ko którego adresowany jest pakiet

2.3 Protokół IP. IPv6

Przyczyny powstania IPv6:

- **Ograniczona ilość adresów IPv4** — przy rosnącej ilości urządzeń podłączonych do sieci, zaczynało brakować adresów, które można było stworzyć na 32 bitach
- **Konieczność dokonywania translacji adresów w IPv4** — z powodu małej ilości adresów IPv4, część adresów była „ukryta”, używana lokalnie i tłumaczona na adresy zewnętrzne, co czasem zaburzało komunikację

2.3 Protokół IP. IPv6

Różnice pomiędzy IPv6 a IPv4:

- **Zwiększona liczba bitów adresu IP** — z 32 bitów do 128 bitów
- **Znaczne uproszczenie nagłówka**
- **Brak ARP** — w to miejsce wymieniane są pakiety ND (*Neighbor Discovery*)
- **Brak ruchu typu broadcast** — zastąpiono go multiacastem na adresy link-local oraz transmisją anycast
- **Brak konieczności nadawania adresów statycznie lub przez DHCP** — zastąpiono to automatycznym rozgłaszaniem adresów SLAAC (ang. *StateLess Address AutoConfiguration*)

2.3 Protokół IP. IPv6

Nagłówek IPv6:

Bity	0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31
0	Wersja	Priorytet	Etykieta przepływu					
32	Długość danych			Następny nagłówek			Limit przeskoków	
64	Adres źródłowy (128 bitów)							
96								
128								
160								
192	Adres docelowy (128 bitów)							
224								
256								
288								

Grafika: <https://www.soisk-me.pl/>

2.3 Protokół IP. IPv6

Nagłówek IPv6 — ważniejsze pola:

- **Wersja** — określa wersję protokołu — IPv6
- **Priorytet** — odpowiednik pola DS w IPv4
- **Następny nagłówek** — odpowiednik pola Protokół warstwy wyższej w IPv4
- **Limit przeskoków** — odpowiednik pola TTL w IPv4
- **Adres źródłowy** — adres IPv6 urządzenia nadającego pakiet
- **Adres docelowy** — adres IPv6 urządzenia, ko którego adresowany jest pakiet

3. Routing

Definicja, rola tablicy routingu i bramy domyślnej, protokoły

3.1 Routing. Definicja

Definicja

Routing — proces kierowania pakietu w sieci taką optymalną drogą (tj. poprzez takie urządzenia), aby dotarł on do urządzenia docelowego.

- Urządzeniem wykonującym routing jest **router**
- Decyzje podejmowane są na podstawie **tablicy routingu**

3.1 Routing. Definicja

Proces routingu:

Urządzenie, po otrzymaniu pakietu, dokonuje dekapsulacji i sprawdza docelowy adres IP:

- Jeśli pakiet skierowany jest to tego urządzenia, przekazywany jest do wyższych warstw
- Jeśli pakiet ma być wysłany do innego urządzenia, sprawdzana jest tablica routingu — poszukiwany jest wpis zawierający informację o docelowej sieci, a pakiet wypuszczany jest wskazanym w tablicy routingu interfejsem
- Jeśli trasa docelowa nie jest znana, pakiet wysyłany jest **trasą ostatniej szansy** (o ile jest skonfigurowana)

3.2 Routing. Tablica routingu

Tablica routingu

```
61#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.6   to network 0.0.0.0

    10.0.0.0/30 is subnetted, 1 subnets
C      10.10.10.4   is directly connected, Serial0/1/0
    172.16.0.0/24 is subnetted, 1 subnets
C      172.16.1.0 is directly connected, FastEthernet0/1
S*    0.0.0.0/0 [1/0] via 10.10.10.6
```

- Zawiera informacje o znanych trasach, tj. dostępnych sieciach i którym interfejsem należy wypuścić pakiet, aby do niej dotarł
- Budowana zarówno przez komputery, jak i routery

3.2 Routing. Tablica routingu

Rodzaje tras w tablicy routingu routera:

- **Trasy statyczne (S)** — skonfigurowane ręcznie przez administratora
- **Trasy do sieci bezpośrednio dołączonych (C, *directly connected*)** — prowadzące do sieci zapiętych na interfejsach routera
- **Trasy dynamiczne** — otrzymane od sąsiednich routerów w wyniku działania **protokołu routingu**

3.3 Routing. Protokół routingu

Protokół routingu vs protokół routowany:

Protokoły routingu

Służą do przekazywania informacji pomiędzy routerami na temat tras do sieci przez nie znanych:

- wewnętrzne — RIP, EIGRP, OSPF, IS-IS
- zewnętrzne (używane pomiędzy sieciami różnych dostawców) — BGP

Protokoły routowane

Służą do przenoszenia danych w sieci za pomocą dostępnych tras:

- IP: IPv4, IPv6
- IPX

Nie mają wpływu na to, którą trasą zostanie przekazany pakiet, dbają jedynie o to, by dotarł do docelowego (wskazanego adresem sieciowym) urządzenia.

3.4 Routing. Brama domyślna

Definicja

Brama domyślna — urządzenie (najczęściej pierwszy router na trasie), które odbiera od hostów pakiety mające trafić do zdalnych sieci i jest w stanie je tam przekierować.

- Adres bramy domyślnej jest jedną z podstawowych (oprócz adresu IP i maski sieciowej) rzeczy do skonfigurowania na hoście
- Przy braku dostępu do bramy domyślnej (błędnej adresacji lub trasie, uszkodzonym urządzeniu) host nie będzie miał możliwości komunikowania się z zewnętrznymi hostami (poza swoją siecią)

3.4 Routing. Brama domyślna

Tablica routingu komputera:

```
c:\>route print
=====
Lista interfejsów
0x1 ..... MS TCP Loopback interface
0x10004 ...00 1a 92 3f a9 ..... Realtek RTL8168/8111 PCI-E Gigabit Ethernet
NIC - Sterownik miniport Harmonogramu pakiet"ów
=====
Aktywne trasy:
Miejsce docelowe w sieci      Maska sieci      Brama      Interfejs      Metryka
0.0.0.0      0.0.0.0      172.16.1.254  172.16.1.1      20
127.0.0.0    255.0.0.0    127.0.0.1    127.0.0.1      1
172.16.1.0   255.255.255.0 172.16.1.1   172.16.1.1      20
172.16.1.1   255.255.255.255 127.0.0.1    127.0.0.1      20
172.16.255.255 255.255.255.255 172.16.1.1   172.16.1.1      20
224.0.0.0    240.0.0.0    172.16.1.1   172.16.1.1      20
255.255.255.255 255.255.255.255 172.16.1.1   172.16.1.1      1
Domyślna brama: 172.16.1.254.
=====
Trasy trwałe:
Brak
```

Zawiera trasę domyślną (do bramy domyślnej), trasy do innych urządzeń w ramach sieci oraz do samego siebie

4. Protokół ICMP

Rola i rodzaje komunikatów

4.1 Protokół ICMP. Rola

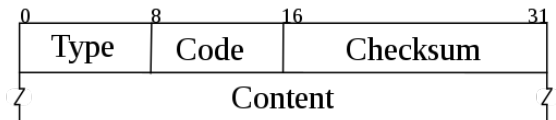
Definicja

Protokół ICMP (ang. *Internet Control Message Protocol*) — protokół wspomagający działanie warstwy sieciowej modelu OSI, pełniący funkcje kontrolne.

- Zadaniem ICMP jest przesyłanie komunikatów umożliwiających sprawdzenie poprawności komunikacji w sieci, np. dostępność urządzeń sieciowych.
- Wykorzystywany podczas wykonywania takich komend jak *ping* lub *tracert*.

4.2 Protokół ICMP. Rodzaje komunikatów

Nagłówek ICMP:



- Rodzaj wiadomości (czy jest to zapytanie, odpowiedź ICMP czy informacja o błędzie) przekazywana jest w polu **Type**
- Dokładniejsza informacja o źródle niepowodzenia transmisji umieszczona jest w polu **Code**

4.2 Protokół ICMP. Rodzaje komunikatów

Rodzaje komunikatów (wartości w polu Type):

- **Echo Request** (type 8) — żądanie echa (prośba o potwierdzenie poprawności komunikacji)
- **Echo Reply** (type 0) — odpowiedź na żądanie echa
- **Destination Unreachable** (type 3) — miejsce docelowe jest nieosiągalne, błąd w transmisji
- **Time Exceeded** (type 11) — przekroczono czas życia pakietu

4.2 Protokół ICMP. Rodzaje komunikatów

Rodzaje błędów (wartości w polu Code dla wiadomości typu 3 — Destination Unreachable):

- Sieć nieosiągalna (code 0)
- Host nieosiągalny (code 1)
- Protokół nieosiągalny (code 2)
- Port nieosiągalny (code 3)
- Zbyt duży pakiet, aby przesłać go bez fragmentacji (code 4)

4.2 Protokół ICMP. Rodzaje komunikatów

Wykonanie komendy ping – proste sprawdzenie komunikacji pomiędzy dwoma urządzeniami:

- Urządzenie wysyłające *ping* wysyła do urządzenia zdalnego (co do którego chce się przekonać, czy jest dostępne) tak naprawdę wiadomość ICMP o typie 8 — *echo request*
- Jeśli urządzenie zdalne jest dostępne, odsyła w odpowiedzi wiadomość ICMP typu 0 — *echo reply*
- Jeśli komunikacja nie doszła do skutku, wysyłany do drodze jest komunikat ICMP odpowiedniego typu, np. 3 — *Destination Unreachable*

4.2 Protokół ICMP. Rodzaje komunikatów

Wykonanie komendy `tracert` — sprawdzenie trasy do urządzenia docelowego:

- Urządzenie początkowe wysyła wiadomość ICMP *echo request* — ustawiając w nagłówku IP w polu TTL wartość 1
- Pierwszy router, który odbierze pakiet, musi zmniejszyć TTL o 1, jest on wówczas zerowany, przez co router musi odrzucić ten pakiet i odesłać nadawcy informację zwrotną o odrzuceniu (pakiet ICMP typu 11 — *Time to Live Exceeded*) — komputer początkowy czeka na pierwszy pakiet ICMP typu 11, jego nadawcą jest pierwszy router na trasie do urządzenia docelowego
- Następnie z komputera początkującego wysyłany jest pakiet o wyższym TTL (2) i oczekiwana jest odpowiedź od następnego routera na trasie (pierwszy router zmniejszy TTL z 2 na 1 i pakiet przepuści, drugi będzie musiał go odrzucić)
- Całość kontynuowana jest do momentu, w którym osiągnięte jest urządzenie docelowe — odebrany jest zwykły *echo reply*

4.3 Protokół ICMP. ICMPv6

Standardowe komunikaty informacyjne ICMPv6:

- **Echo Request** — żądanie echa (typ 128)
- **Echo Reply** — odpowiedź echa (typ 129)

Raporty błędów ICMPv6:

- **Destination Unreachable** — cel nieosiągalny (typ 1)
- **Packet Too Big** — za duży pakiet (typ 2)
- **Time Exceeded** — przekroczono czas (typ 3)
- **Parameter Problem** — problem z parametrami (typ 4)

4.3 Protokół ICMP. ICMPv6

Komunikaty ND (ang. *Neighbor Discovery*):

- **Neighbor Solicitation (NS)** — komunikat wywołania sąsiada, odpowiednik ARP request (typ 135)
- **Neighbor Advertisement (NA)** — komunikat rozgłoszenia sąsiada, odpowiednik ARP reply (typ 136)
- **Router Solicitation (RS)** — komunikat wywołania routera (typ 133)
- **Router Advertisement (RA)** — komunikat rozgłoszenia routera (typ 134)