Protokoły

IP

Protokół komunikacyjny przeznaczony dla Internetu (ang. Internet Protocol), jest protokołem wartstwy sieci modelu OSI, który stanowi podstawę struktury komunikacyjnej Internetu. Obecnie ciągle stosowany jest protokół w wersji 4 (IPv4), natomiast sukcesywnie wypierany jest przez swojego następcę, wersję 6 (IPv6). Długość nagłówka IPv4 wynosi od 20 do 60 bajtów.

<table>
<tr><th>0-3</th><th>4-7</th><th>8-13</th><th>14-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>Wersja</td><td>Długość nagłówka</td><td>Usługi zróżnicowane</td><td>ECN</td><td colspan="2">Całkowita długość</td></tr>
<tr><td colspan="4">Numer identyfikacyjny</td><td>Flagi</td><td>Przesunięcie</td></tr>
<tr><td colspan="2">Czas życia</td><td colspan="2">Protokół warstwy wyższej</td><td colspan="2">Suma kontrolna nagłówka</td></tr>
<tr><td colspan="6">Adres źródłowy IP</td></tr>
<tr><td colspan="6">Adres docelowy IP</td></tr>
<tr><td colspan="5">Opcje IP</td><td>Wypełnienie</td></tr>
<tr><td colspan="6">Dane</td></tr>
</table>

Budowa nagłówka IPv4

- **Wersja** – pole opisujące wersję protokołu.
- **Długość nagłówka** – długość nagłówka IP wyrażona w 32-bitowych słowach; minimalna długość nagłówka to 5.
- **Usługi zróżnicowane** – Pierwsze trzy bity pola Usługi zróżnicowane informują o priorytecie (111 to najwyższy, a 000 - zwyczajny priorytet). Kolejne trzy bity, oznaczają ważność poszczególnych parametrów: D - małe opóźnienie (ang. delay), T - duża przepustowość (ang. throughput) i R - wysoka niezawodność (ang. reliability).
- **ECN** – jeśli ustawiony na wartość 1, informuje o przeciążeniu bufora
- **Całkowita długość pakietu** – długość całego datagramu IP (nagłówek oraz dane); minimalna długość to 576 bajtów, natomiast maksymalna to 65535 bajty.
- **Numer identyfikacyjny** – numer identyfikacyjny, wykorzystywany podczas fragmentacji do określenia przynależności pofragmentowanych datagramów.
- **Flagi** – flagi wykorzystywane podczas fragmentacji datagramów.
- **Przesunięcie** – w przypadku fragmentu większego datagramu pole to określa miejsce danych w oryginalnym datagramie;
- **Czas życia** – czas życia datagramu. Zgodnie ze standardem liczba przeskoków przez jaką datagram znajduje się w obiegu.
- **Protokół warstwy wyższej** – informacja o protokole warstwy wyższej, który jest przenoszony w polu danych datagramu IP.
- **Suma kontrolna nagłówka** – suma kontrolna nagłówka pakietu, pozwalająca stwierdzić czy został on poprawnie przesłany, sprawdzana i aktualizowana przy każdym przetwarzaniu nagłówka.

- **Adres źródłowy i adres docelowy** – pola adresów nadawcy i odbiorcy datagramu IP.
- **Opcje** – niewymagane pole opcji, opisujące dodatkowe zachowanie pakietów IP
- **Wypełnienie** – opcjonalne pole wypełniające nagłówek do wielkości będącej wielokrotnościa 32.

TCP

Protokół kontroli transmisji (ang. Transmission Control Protocol), jest to połączeniowy i niezawodny protokół komunikacyjny warstwy transportowej modelu OSI. Stanowi część powszechnie stosowanego stosu TCP/IP. Nagłówek TCP składa się conajmniej z pięciu 32 bitowych słów, co łącznie daje 160 bitów. Dodatkowo zawierać może pole Opcje o zmiennej długości będącej wielokrotnością 8 bitów.

0-3	4-9	10-15	16-31
Port źródłowy			Port docelowy
Numer sekwencji			
Numer potwierdzenia (jeśli flaga ACK jest ustawiona)			
Długość nagłówka	Zarezerwowane	Flagi	Szerokość okna
Suma kontrolna			Wskaźnik priorytetu (jeśli URG jest ustawiona)
Opcje			

Budowa nagłówka TCP

Najważniejsze cechy protokołu:

- działa w trybie klient-serwer
- wykorzystuje procedury do nawiązania i zakończenia połączenia
- połączenie sterowane jest przy pomocy flag
- gwarantuje dostarczenie wszystkich pakietów z zachowaniem kolejności, bez duplikatów

Flagi:

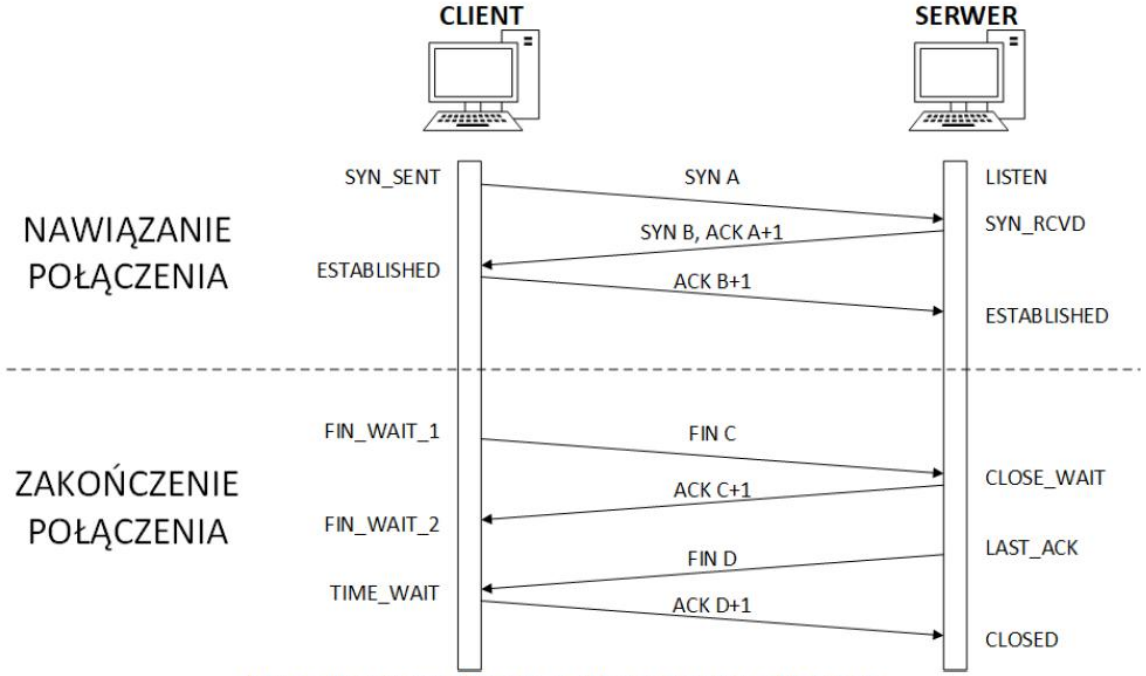
- NS – (ang. Nonce Sum) jednobitowa suma wartości flag ECN (ECN Echo, Congestion Window Reduced, Nonce Sum) weryfikująca ich integralność
- CWR – (ang. Congestion Window Reduced) flaga potwierdzająca odebranie powiadomienia przez nadawcę, umożliwia odbiorcy zaprzestanie wysyłania echa
- ECE – (ang. ECN-Echo) flaga ustawiana przez odbiorcę w momencie otrzymania pakietu z ustawioną flagą CE
- URG – informuje o istotności pola "Priorytet"
- ACK – informuje o istotności pola "Numer potwierdzenia"
- PSH – wymusza przesłanie pakietu
- RST – resetuje połączenie (wymagane ponowne uzgodnienie sekwencji)
- SYN – synchronizuje kolejne numery sekwencyjne
- FIN – oznacza zakończenie przekazu danych

Nawiązanie połączenia TCP

Jedną z najważniejszych cech protokołu sterowania transmisją jest obecność mechanizmów nawiązania i zakończenia połączenia. Nawiązanie połączenia jest oparte o procedurę zwaną *three-way handshake*.

Ustanowienia połączenia wygląda następująco:

1. Klient wysyła segment SYN wraz z inicjującym numerem sekwencji np. liczbą 100 (symbol A)
2. Serwer odpowiada wysyłając segment SYN ze swoim numerem sekwencji (symbol B), a także potwierdza otrzymanie segmentu od klienta wysyłając ACK z numerem A+1.
3. Klient wysyła potwierdzenie ACK z numerem B+1 odebrania segmentu SYN od serwera.



Procedury nawiązania i zakończenia połączenia

UDP

Protokół pakietów użytkownika (ang. User Datagram Protocol) jest bezpołączeniowym protokołem komunikacyjnym warstwy transportowej modelu OSI. W przeciwieństwie do protokołu TCP nie gwarantuje dostarczenia wszystkich pakietów, ani zachowania kolejności. W zamian za to oferuje szybszą transmisję oraz mniejszy narzut danych. Nagłówek UDP składa się z 4 pól po 16 bitów.

0-15	16-31
Port źródłowy	Port docelowy
Długość datagramu	Suma kontrolna

Budowa nagłówka UDP

ICMP

Internetowy protokół komunikatów kontrolnych (ang. Internet Control Message Protocol) jest protokołem warstwy sieciowej modelu OSI wykorzystywanym w diagnostyce sieci oraz trasowaniu. Umożliwia on przesyłanie między urządzeniami sieciowymi informacji o błędach w funkcjonowaniu sieci IP. Protokół ICMP jest wykorzystywany przez takie programy jak ping, czy traceroute.

0-7	8-15	16-23	24-31
Typ	Kod	Suma kontrolna	
Dane (opcjonalnie)			

Budowa pakietu ICMP

Wybrane typy wiadomości:
0 – Echo Reply (odpowiedź na ping)
3 – Destintation Unreachable
8 – Echo Request (ping)
9 – Router Advertisement
11 – Time Exceeded
17 – Address Mask Request (żądanie maski adresowej)
18 – Address Mask Reply (zwrot maski adresowej)
30 – Traceroute

0-7	8-15	16-23	24-31
Typ	Kod	Suma kontrolna	
Identyfikator		Numer sekwencji	
Dane (opcjonalnie)			

Budowa pakietu ICMP Echo Request i Echo Reply

W przypadku pakietów ICMP Echo Request i Echo Reply w sekcji Dane dodatkowo pojawiają się dodatkowe wartość: identyfikator (16 bitów) i numer sekwencji (16 bitów). Służą one do oznaczania żądań w przypadku, gdy nadawca wysyła kilka pakietów Echo Request.

DNS

System nazw domenowych (ang. Domain Name System) wykorzystuje do wymiany danych z systemem serwerów dedykowany protokół warstwy aplikacji. Jest on transportowany przeważnie w pakietach UDP.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
ID															
QR	OPCODE				AA	TC	RD	RA	Z			RCODE			
QDCOUNT															
ANCOUNT															
NSCOUNT															
ARCOUNT															

Format nagłówka wiadomości DNS

- **ID** –identyfikator tworzony przez program wysyłający zapytanie; serwer przepisuje ten identyfikator do swojej odpowiedzi, dzięki czemu możliwe jest jednoznaczne powiązanie zapytania i odpowiedzi
- **QR** – określa, czy komunikat jest zapytaniem (0) czy odpowiedzią (1)
- **OPCODE** – określa rodzaj zapytania wysyłanego od klienta, jest przypisywany przez serwer do odpowiedzi. Wartości: 0 – QUERY (standardowe zapytanie); 1 – IQUERY (zapytanie zwrotne); 2 – STATUS (pytanie o stan serwera).
- **AA** – oznacza, że odpowiedź jest autorytatywna.
- **TC** – oznacza, że odpowiedź nie zmieściła się w jednym pakiecie UDP i została obcięta.
- **RD** – oznacza, że klient żąda rekurencji – pole to jest kopiowane do odpowiedzi
- **RA** – bit oznaczający, że serwer obsługuje zapytania rekurencyjne
- **Z** – zarezerwowane do przyszłego wykorzystania.
- **RCODE** –od odpowiedzi. Przyjmuje wartości:
  - 0 – brak błędu,
  - 1 – błąd formatu – serwer nie potrafił zinterpretować zapytania,
  - 2 – błąd serwera – wewnętrzny błąd serwera,
  - 3 – błąd nazwy – nazwa domenowa podana w zapytaniu nie istnieje,
  - 4 – nie zaimplementowano – serwer nie obsługuje typu otrzymanego zapytania,
  - 5 – odrzucono – serwer odmawia wykonania określonej operacji, np. transferu strefy,

- **QDCOUNT** – określa liczbę wpisów w sekcji zapytania
- **ANCOUNT** – określa liczbę rekordów zasobów w sekcji odpowiedzi
- **NSCOUNT** – określa liczbę rekordów serwera w sekcji zwierzchności
- **ARCOUNT** – określa liczbę rekordów zasobów w sekcji dodatkowej