

Protokół TCP/IP (część 3)

Ponadto TCP zapewnia kontrolę przepływu. Każdy z końców połączenia TCP ma przestrzeń buforową o skończonej wielkości. Strona odbierająca TCP pozwala stronie nadającej na wysłanie tylko takiej ilości danych, która może być umieszczona w buforze odbiorcy. Taki mechanizm zapobiega przeładowaniu bufora w hoście wolnym przez datagramy wysyłane z hosta szybszego.

2.4.1. Nagłówek TCP

Dane TCP umieszczane są w datagramach IP w sposób pokazany na rysunku 2.7.

nagłówekIP dane TCP nagłówekTCP datagram IP segment TCP 20 bajtów 20 bajtów nagłówekIP dane TCP nagłówekTCP datagram IP segment TCP 20 bajtów 20 bajtów

Rysunek 2.7. Enkapsulacja danych TCP w datagramie IP

URG ACK PSH RST SYN FIN 0 opcje Numer potwierdzenia Numer sekwencji Port docelowy 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity Port źródłowy Rozmiar okna Znacznik pilności Suma kontrolna Dane Długość nagłówka Zarezerwowane 6 Flag 1-bitowych URG ACK PSH RST SYN FIN 0 opcje Numer potwierdzenia Numer sekwencji Port docelowy 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity Port źródłowy Rozmiar okna Znacznik pilności Suma kontrolna Dane Długość nagłówka Zarezerwowane 6 Flag 1-bitowych

Rysunek 2.8. Format nagłówka TCP

Znaczenie poszczególnych pól jest następujące[3]:

Numer portu źródłowego, docelowego

Pola te identyfikują aplikacje wysyłającą i odbierającą dane. Te dwie wielkości wraz adresami IP źródła i przeznaczenia

umieszczonymi w nagłówku IP, jednoznacznie identyfikują każde połączenie. Kombinacja IP i numeru portu jest czasem nazywana gniazdem.

Numer sekwencyjny

Pole to zawiera numer sekwencyjny pierwszego bajtu danych w segmencie. Ta wartość określa pozycję segmentu w strumieniu bajtów. Podczas ustanawiania połączenia, jeśli bit SYN w polu znaczniki jest ustawiony na 1, w tym polu zawarty jest inicjujący numer sekwencyjny INS, od którego rozpoczyna numerację bajtów w połączeniu. Zatem pierwszy wysyłany bajt ma numer $INS+1$.

Numer potwierdzenia

Zawiera numer sekwencyjny następnego oczekiwanego bajtu po stronie odbiorczej. Jednocześnie jest to potwierdzenie poprawnego odbioru bajtów o numerach sekwencyjnych mniejszych od zawartego w tym polu. Potwierdzenia mówią nadawcy, ile bajtów danych zostało już poprawnie odebranych.

Długość nagłówka

Określa liczbę 32 bitowych słów w nagłówku segmentu TCP. Tym samym określone zostaje miejsce, w którym rozpoczynają się dane. Pole to ma określone znaczenie tylko wtedy, gdy bit $ACK=1$.

Bity znaczników

Pole to zawiera 6 flag 1 – bitowych :

URG – wskaźnik ważności pola wskaźnika przynaglającego;

ACK – wskaźnik ważności pola numer potwierdzenia;

PSH – odbiorca powinien jak najszybciej przesłać dane do aplikacji;

RST – restart połączenia;

SYN – synchronizacja numerów sekwencyjnych w celu inicjalizacji połączenia;

FIN – zakończenie wysyłania danych.

Rozmiar okna

Określa liczbę bajtów, jaką może jeszcze zaakceptować odbiorczy moduł TCP.

Suma kontrolna

Pole to jest 16 bitowym jedynkowym uzupełnieniem jedynkowo uzupełnionej sumy wszystkich 16 bitowych słów w segmencie. Ta suma kontrolna obejmuje zarówno nagłówki jak i dane.

Wskaźnik ważności

Brany pod uwagę przy ustawieniu bitu URG. Pole to zawiera numer sekwencyjny bajtu następującego po pilnych danych.

Opcje

Pole to ma długość zmienną będącą wielokrotnością 8 bitów. Dla protokołu TCP zdefiniowano trzy opcje: 0 – koniec listy opcji, 1 – brak działania, 2 – maksymalna długość segmentu.

Zagadnienie jakości usług (Quality of Service) w sieciach IP stanowi obecnie jeden z najbardziej kluczowych aspektów ewolucji współczesnych technologii teleinformatycznych. Gwałtowny rozwój aplikacji wymagających przesyłania danych w czasie rzeczywistym, takich jak Voice over IP (VoIP), wideokonferencje czy zaawansowane usługi strumieniowania multimedialnych, wymusił na inżynierach poszukiwanie zupełnie nowych, wysoce efektywnych rozwiązań w dziedzinie niezawodności i optymalizacji. Protokół internetowy, który od początku swojego istnienia zorientowany był przede wszystkim na przesyłanie informacji tekstowych w standardzie 'best-effort', musiał ulec głębokiej transformacji. Przekształcenia te nie mogły ograniczyć się jedynie do powierzchownych

ulepszeń; konieczne stało się opracowanie i zintegrowanie skomplikowanych mechanizmów kontroli i priorytetyzacji, zdolnych zarządzać ogromnym natężeniem zróżnicowanych typów transmisji. Oczekuje się, że nowoczesne środowiska sieciowe będą w pełni przewidywalne i zagwarantują stabilną przepustowość w każdych warunkach obciążenia, co jest fundamentem współczesnej telekomunikacji.

Równolegle z rozwojem standardów QoS obserwuje się rosnące zapotrzebowanie rynkowe na kompleksowe wdrażanie rozwiązań hybrydowych. Konwergencja różnych standardów transmisji umożliwia współdzielenie zasobów w sposób niespotykany dotąd na rynku operatorskim. Oznacza to również ewolucję samej architektury sprzętowej – nowoczesne przełączniki (switche) oraz routery szkieletowe muszą dzisiaj charakteryzować się ogromną mocą obliczeniową, by na bieżąco analizować i kierować ruchem pakietowym zgodnie z rygorystycznymi wymogami opóźnień (delay) i zmienności opóźnień (jitter). Dostawcy usług (Service Providers) mierzą się z wyzwaniem utrzymania wysokiej konkurencyjności poprzez oferowanie pakietów usług (SLA) ściśle dostosowanych do indywidualnych, biznesowych uwarunkowań klientów. Konieczne stało się nie tylko gwarantowanie określonego wolumenu transferu, ale przede wszystkim stuprocentowej niezawodności strumieni danych poddanych priorytetyzacji. Wykorzystanie w tym kontekście ustandaryzowanych miar wydajności pozwala precyzyjniej kontrolować poprawność funkcjonowania całego łańcucha transmisyjnego na linii dostawca-odbiorca.

Kluczową rolę w utrzymaniu odpowiedniego poziomu usługi odgrywa odpowiednio zaplanowany system monitoringu i kontroli. Nie da się efektywnie zarządzać parametrami, których uprzednio dokładnie się nie zmierzyło i nie przeanalizowało. Implementacja aktywnych i pasywnych sond pomiarowych w krytycznych węzłach infrastruktury sieciowej pozwala na bieżące zbieranie danych analitycznych. Dane te, nierzadko gromadzone i przetwarzane za pomocą potężnych systemów

informatycznych w tzw. jednostkach post-processingu, dostarczają precyzyjnych informacji o potencjalnych zatorach, miejscach gubienia pakietów czy degradacji łącz. Dzięki tak zaawansowanej teledetrii operatorzy mogą proaktywnie reagować na wszelkie zakłócenia, często jeszcze zanim zostaną one odnotowane przez samego abonenta. Odpowiednie procedury alarmowania, wspierane mechanizmami histerezy, zapobiegają przy tym nadmiernej fali fałszywych ostrzeżeń (tzw. alarm flooding), co w efekcie znacznie usprawnia pracę administratorów systemów informatycznych.

Warto również zwrócić uwagę na sam aspekt bezpieczeństwa i enkapsulacji protokołów w zintegrowanych sieciach danych. W miarę wdrażania technologii zorientowanych na QoS, coraz większego znaczenia nabierają kwestie zapewnienia integralności strumieni zarządzających i samej sygnalizacji. Hakerzy oraz cyberprzestępcy nierzadko wykorzystują luki w zarządzaniu pasmem, by poprzez ataki typu Denial of Service zakłócać priorytetyzację i paraliżować ważne kanały komunikacyjne (np. dla służb ratunkowych korzystających z sieci IP). Dlatego współczesne modele wdrożeniowe, uwzględniając mechanizmy takie jak uwierzytelnianie, podpisywanie nagłówków pakietów kontrolnych czy rygorystyczna izolacja ruchu, gwarantują, że odpowiedni standard (np. DiffServ lub IntServ) zadziała bezbłędnie nawet w obliczu celowych przeciążeń lub zakłóceń wywołanych w niekontrolowanym obszarze globalnego Internetu. To nowatorskie podejście powoli staje się powszechnym wymogiem regulacyjnym na rynkach międzynarodowych.

Nie można również zapominać o perspektywach i przyszłości, jakie stwarza implementacja najnowszego protokołu internetowego, czyli IPv6. Choć w dużej mierze proces jego adaptacji i wdrażania jest powolny, to właśnie on został zaprojektowany z myślą o natywnym wsparciu dla zaawansowanych mechanizmów kontroli ruchu, co widać już na poziomie struktury jego nagłówka i zastosowania innowacyjnych etykiet potoków

(flow labels). Ta standaryzacja, eliminując konieczność przeprowadzania skomplikowanych i obciążających analiz na niższych warstwach modelu sieciowego, pozwoli odciążyć sprzęt brzegowy i zmniejszyć stałe opóźnienia. Docelowo uważa się, że synergia między nowymi technologiami przesyłowymi, ogromną dostępnością światłowodów i pełnym przejściem na IP w wersji 6., naturalnie wyeliminuje większość dzisiejszych barier wydajnościowych. Mimo to, precyzyjne mechanizmy przydzielania gwarantowanego pasma pozostaną filarem, bez którego komercyjne dostarczanie najwyższej jakości serwisów komunikacyjnych byłoby absolutnie niemożliwe do zrealizowania.

Co więcej, wysoce wyspecjalizowane zastosowania, takie jak telemedycyna czy zdalne sterowanie procesami przemysłowymi w czasie rzeczywistym, stawiają systemom sieciowym jeszcze bardziej drastyczne wymagania. W tych dziedzinach nawet mikrosekundowe opóźnienia (latency) czy zagubienie minimalnej części pakietu mogą skutkować katastrofalnymi w skutkach błędami. Oznacza to, że tradycyjne metryki wydajnościowe muszą podlegać rygorystycznemu rygorowi, a inżynieria ruchu (Traffic Engineering) opierać się na zaawansowanej predykcji. Nowe, oparte na sztucznej inteligencji algorytmy przewidywania kongestii zaczynają powoli wspierać ludzkich administratorów, analizując w czasie rzeczywistym wzorce obciążeń we wszystkich dostępnych w regionie autonomicznych systemach. Mamy więc do czynienia z erą, w której same parametry i konfiguracje sieci adaptują się i ewoluują bez bezpośredniej interwencji człowieka, dynamicznie przesuwając strumienie o najwyższym priorytecie poza zagrożone przeciążeniem rewiry infrastruktury.

Zagadnienie jakości usług (Quality of Service) w sieciach IP stanowi obecnie jeden z najbardziej kluczowych aspektów ewolucji współczesnych technologii teleinformatycznych. Gwałtowny rozwój aplikacji wymagających przesyłania danych w czasie rzeczywistym, takich jak Voice over IP (VoIP), wideokonferencje czy zaawansowane usługi strumieniowania

multimediów, wymusił na inżynierach poszukiwanie zupełnie nowych, wysoce efektywnych rozwiązań w dziedzinie niezawodności i optymalizacji. Protokół internetowy, który od początku swojego istnienia zorientowany był przede wszystkim na przesyłanie informacji tekstowych w standardzie 'best-effort', musiał ulec głębokiej transformacji. Przekształcenia te nie mogły ograniczyć się jedynie do powierzchownych ulepszeń; konieczne stało się opracowanie i zintegrowanie skomplikowanych mechanizmów kontroli i priorytetyzacji, zdolnych zarządzać ogromnym natężeniem zróżnicowanych typów transmisji. Oczekuje się, że nowoczesne środowiska sieciowe będą w pełni przewidywalne i zagwarantują stabilną przepustowość w każdych warunkach obciążenia, co jest fundamentem współczesnej telekomunikacji.

Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę [pisanie prac](#) - profesjonalna pomoc w pisaniu prac w granicach prawa.