Definicje i podział parametrów jakości (część 2)

Traffic Conditioning Specification (TCS) jest to zbiór parametrów o określonych wartościach, który jednoznacznie określa profil ruchu oraz reguły klasyfikowania pakietów [11]. TCS jest pojęciem ściśle technicznym, podczas gdy TCA jest pojęciem szerszym, obejmującym oprócz TCS definicje poszczególnych usług i uzgodnienia z klientem. TCS jest integralną częścią SLS.

3.2. Wielkości opisujące QoS w IP

W środowisku IP jakość QoS może być scharakteryzowana między innymi przez następujący zbiór parametrów [15]:

Pojemność transmisyjna

Parametr ten opisuje, ile czasu potrzebuje sieć na przesłanie zadanej porcji informacji, z pominięciem zagadnienia opóźnień. Tak zdefiniowany wskaźnik opisuje medium transmisyjne, z którego korzysta IP. Ponieważ sieć IP może być zbudowana z wykorzystaniem różnych technologii w warstwie łącza danych i różnych fizycznych łączy, pojemność transmisyjna jest różna w każdym kierunku. Dla każdych dwu sąsiadujących ze sobą węzłów w sieci oczkowej, jaką jest sieć IP, pojemność transmisyjna oferowana przez sieć pomiędzy tymi punktami jest równa szerokości pasma w łączu pomiędzy tymi węzłami. Oczywiste jest, że łącze 2 Mbit/s, zbudowane w oparciu o łączność satelitarną, kanał cyfrowy (SDH, PDH, itp.) czy linie miedziane wyposażone w modemy (HDSL), ma jednakową pojemność transmisyjna. Jednakże dla ścieżki łączącej dwa niesąsiadujące ze sobą węzły sieci określenie pojemności transmisyjnej jest znacznie bardziej złożone ze względu na współdzielenie łączy przez różne ścieżki. Ponieważ współdzielenie jest oparte na multipleksacji statystycznej, pojemność transmisyjna ścieżki

nie jest wartością stałą. Jeżeli przyjąć założenie, że żadne łącze, z którego korzysta ścieżka, nie jest współdzielone, można powiedzieć, że pojemność transmisyjna jest równa najmniejszej pojemności transmisyjnej łącza składowego. Niektóre nowoczesne technologie wykorzystywane do budowy rozległych sieci IP, takie jak Frame Relay czy ATM, charakteryzują się pojemnością transmisyjną zmienną w czasie. Wynika to z zastosowania multipleksacji statystycznej w sieciach FR czy ATM. Łącze w którejś z tych technologii pomiędzy dwoma sąsiednimi węzłami sieci IP jest tak naprawdę ścieżką, wykorzystującą wiele łączy fizycznych pomiędzy węzłami sieci FR czy ATM. W bardzo wczesnej fazie istnienia sieci IP pojemność transmisyjna była podstawowym parametrem. Systemy podłączone do sieci pracowały w trybie wsadowym, a więc ważne było jedynie wydajne przesyłanie zadań i rozwiązań – nie istniał problem interakcji z systemem zdalnym. Pojemność transmisyjna nie jest zależna od urządzeń w węzłach sieci IP – ruterów.

Wraz z pojawieniem się możliwości zdalnego interaktywnego dostępu powstał następny parametr:

Opóźnienie

Jest to czas, potrzebny na dostarczenie pakietu z jednego węzła w sieci IP do drugiego.

Parametr ten jest złożony z kilku składowych i nie jest równy dla różnych kierunków w sieci.

Nie jest on również stały w czasie, choć niektóre jego składowe są stałe. Na opóźnienie składają się następujące czynniki:

Czas serializacji pakietu przy opuszczaniu każdego węzła sieci. Parametr ten jest stały w czasie. Opisuje go poniższy wzór:

; (3.1.)

gdzie:

T – czas serializacji,

L – długość pakietu w bitach,

AR – Access Rate, czyli szybkość interfejsu w bitach na sekundę.

AR jest oczywistym i jednoznacznym parametrem dla kanałów cyfrowych w strukturze łączy analogowych. Dla FR i ATM szybkość przyłączenia AR oznacza szybkość interfejsu przyłączającego do sieci, a nie parametr kanału wirtualnego i jest ograniczeniem fizycznym każdej implementacji.

Czas Propagacji w każdym z łączy na ścieżce. Jest on stały i niezmienny w czasie dla danego łącza, ale zależny od technologii, ośrodka i długości łącza. Dla łącza satelitarnego czas propagacji jest większy niż naziemnego kanału cyfrowego czy łącza modemowego. Czas propagacji dla łącza światłowodowego jest jeszcze krótszy. Oba powyższe efekty maja charakter ograniczeń fizycznych i nie mogą być poprawione poprzez technologię związaną z IP. Chcąc ograniczyć te czynniki opóźnienia, należy budować sieć IP w oparciu o szerokopasmowe łącza z małym czasem propagacji sygnału w medium transmisyjnym.

Czas obróbki pakietu w każdym węźle pośrednim. Ten czas zależy od sprzętu i oprogramowania węzła i może być różny dla różnych węzłów, a nawet dla różnych pakietów w tym samym węźle. Czas obróbki zmienia się, ze względu na zmiany obciążenia CPU. Ograniczenie wartości tego czynnika jest możliwe przez stosowanie lepszych algorytmów przełączania i wydajniejszego sprzętu.

Jako przykłady można tu przytoczyć mechanizmy:

route-cache – ostatnio używane pozycje tablicy rutingu są przechowywane w szybkiej pamięci podręcznej CPU,

MPLS,

distributed switching – inteligentne karty liniowe ruterów.

Opóźnienia w buforach wyjściowych w węzłach pośrednich. Ten czynnik jest zmienny w czasie, ze względu na następujące zjawiska:

w czasie dt wpływa dP informacji do tej samej sieci.

ruter musi je wysyłać łączem o pojemności transmisyjnej PT podanej poniższym wzorem:

; (3.2.)

gdzie:

PT – pojemność transmisyjna łącza,

dL – ilość informacji,

dt – czas.

Ponieważ dl < dP, a ponadto dP może się składać z wielu pakietów, które należy wysłać sekwencyjnie, jedyne, co można zrobić, to założyć, że w następnej chwili czasowej dt wartość dl < dP i zbuforować dane wejściowe, a następnie wysłać z szybkością łącza PT. Taka technika wprowadza jednak opóźnienie. Ograniczenie tych zjawisk jest możliwe poprzez strategie obsługi kolejek bardziej wyrafinowane niż FIFO.

Ponieważ szybkość łącza jest stała, nie jest możliwe wysyłanie wszystkich danych z bufora szybciej, można jednak pakiety danych określonego typu wysłać częściej niż inne lub przed innymi. Prowadzi to do minimalizacji opóźnienia danych danego typu, kosztem wzrostu opóźnienia danych innego typu.

Jitter

Zmienność opóźnień w czasie jest znana pod angielską nazwą jitter i dla klasycznych usług transmisji danych wartość tego

parametru nie ma większego znaczenia. Opóźnienia rzędu dziesiątków milisekund nie są zauważalne dla użytkowników usługi Telnet czy RSH. Nowe usługi szerokopasmowe z rodziny multimediów są jednak wrażliwe na ten parametr. Minimalizację efektu zmiennego opóźnienia można uzyskać poprzez inteligentne algorytmy mechanizmów kolejkowania.

Straty

Straty we współczesnych sieciach IP mogą mieć dwie przyczyny:

Przepełnienie buforów wyjściowych w routerach IP, czyli zjawisko przeciążenia (congestion). Aby zminimalizować prawdopodobieństwo wystąpienia przeciążenia należy doprowadzić do spowolnienia pracy nadajnika. Protokół IP nie przewiduje takich mechanizmów, możliwe jest jedynie pośrednie wpłynięcie na tempo nadawania danych w sesji TCP, poprzez odrzucenie pakietów tej sesji;

Przekroczenie kontraktu, zawartego z operatorem FR lub ATM, pod warunkiem,że technologie te zostały użyte do przenoszenia IP. Optymalizację pracy na takim łączu można uzyskać stosując odpowiednie mechanizmy sterowania przepływem poprzez ograniczenie prędkości nadajnika w zależności od możliwości transmisyjnych kanału wirtualnego FR lub ATM.

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 telemetrii 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.

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.

Definicje i podział parametrów jakości (część 1)

Obecna generacja sieci Internet bazuje na protokole IPv.4 i realizuje przekaz pakietów na zasadzie best-effort (najlepszego osiągnięcia) bez gwarancji jakości usługi. Sieć ta nie realizuje żadnej polityki przyjmowania / odrzucania nowych połączeń, zaś sterowanie liczbą pakietów napływających do sieci jest przeniesione do użytkownika. De facto, mechanizmy zaimplementowane w protokole TCP (takie jak mechanizm wolnego startu oraz unikania przeciążenia) mają na celu jedynie dostosowanie szybkości wysyłania pakietów do sieci do aktualnie obserwowanych warunków ruchowych.

Rozszerzenie sieci IP na sieć wielousługową gwarantującą odpowiednią jakość przekazu pakietów, tzw. sieć QoS IP (Quality of Service Internet Protocol), wymaga zdefiniowania nowych usług sieciowych, w pewnym sensie wzorowanych na usługach oferowanych w sieciach ATM. Ogólnie, usługi te

powinny różnić się pomiędzy sobą możliwością zapewnienia różnych poziomów strat pakietów czy też dopuszczalnymi oferowanymi wartościami opóźnienia przekazu danych.

Zapewnienie odpowiedniej jakości przekazu przez sieć IP wymaga, podobnie jak to uczyniono w sieci ATM, zdefiniowania odpowiednich funkcji realizujących QoS. Postępując w tym duchu należy:

Zdefiniować klasy usług sieciowych wraz z mechanizmami zapewniającymi sterowanie ruchem; ogólnie mechanizmy takie mogą być zaimplementowane w każdym węźle (w tym przypadku w ruterze IP);

Określić zasoby sieci przynależne danej usłudze sieciowej; w przypadku sieci pakietowej należy dla danej usługi sieciowej przydzielić odpowiednią przepustowość na każdym łączu wyjściowym wraz z buforem dla gromadzenia pakietów powodujących chwilowe przeciążenia;

W ruterze IP powinny być również zaimplementowane mechanizmy pozwalające rozróżniać pakiety według ich przynależności do danej usługi sieciowej;

Zdefiniować dla każdej z usług sieciowych tzw. parametry QoS, określającą jakość obsługi odbieraną na poziomie wywołania i na poziomie pakietów;

Zdefiniować funkcję realizującą przyjmowanie / odrzucanie nowych wywołań;

Zdefiniować parametry połączenia, zgłaszane w fazie zestawiania połączenia i dotyczące charakterystyki oferowanego ruchu; zwykle są one podawane w formie parametrów tzw. Token-Bucket’u;

Nie dopuszczać do sieci ruchu, który nie jest zgodny z kontraktem ruchowym.

W sieci QoS IP powyższe mechanizmy muszą być zdefiniowane.

Należy nadmienić, iż implementacja efektywnych mechanizmów QoS w sieci IP jest szczególnie trudna, co wynika z faktu, iż sieć ta nie realizuje połączeń wirtualnych (jak to ma miejsce w sieci ATM) oraz długość przesyłanych pakietów jest zmienna.

Rozdział ten omawia obecny stan zaawansowania prac w kierunku stworzenia nowej generacji sieci Internet, tj. sieci z zaimplementowanymi mechanizmami QoS.

3.1. Terminologia

Najczęściej używane terminy związane z jakością usług to:

- QoS (Ouality of Service) – jakość usługi;
- CoS (Class of Service) – klasa usług;
- GoS (Grade of Service) – kategoria usług;
- SLA (Service Level Agreement) – kontrakt pomiędzy użytkownikiem a operatorem;
- SLS (Service Level Specificafion) – uzgodniony pomiędzy operatorem a klientem zbiór parametrów sieciowych i ich wartości związany ze świadczoną usługą;
- TCA (Traffic Conditioning Agreement) – porozumienie określające reguły klasyfikowania pakietów oraz profile ruchu;
- TCS (Traffic Conditioning Specification) – określony zbiór parametrów technicznych i ich wartości związanych z TCA.

Niestety pojęcia te są często mylone i używane niewłaściwie. Konieczne, więc wydaje się ich uporządkowanie.

Najwięcej nieporozumień wiąże się z pojęciem jakości usług (QoS). Termin ten jest używany w różnym znaczeniu, w zależności od kontekstu. Często zapewnienie jakości usługi jest nie słusznie utożsamiane przez użytkownika jedynie z uzyskaniem zadowalającej jakości obrazu, dźwięku czy krótkiego czasu przesyłania danych, co jest dużym uproszczeniem. Jednak takimi kryteriami posługuje się zwykle odbiorca usługi. Z

drugiej strony dla jej dostawcy istotne jest uzyskanie wysokiej oceny użytkownika. W tym celu dostawca musi zapewnić kanał transmisyjny spełniający określone wymagania, które bezpośrednio przekładają się na zbiór parametrów sieciowych. W każdym z tych dwóch podejść jest trochę racji. Konieczne jest jednak ustalenie spójnej terminologii obejmującej oba podejścia. W książce [5] poświęconej jakości usług wyróżniono trzy podstawowe pojęcia:

- zadana jakość usług (intrinsic QoS),
- postrzegana jakość usług (perceived QoS),
- oceniana jakość usług (assessed QoS).

Przez zadaną jakość usługi rozumie się jej cechy ściśle związane z aspektami technicznymi, począwszy od zastosowanego łącza fizycznego, skończywszy na protokołach transmisyjnych i zastosowanych mechanizmach zapewniających określoną jakość. W tym kontekście jakość usługi (QoS) oznacza zbiór wymagań związanych z daną usługą. Powinny one być spełnione podczas przesyłania przez sieć strumienia danych w ramach tej usługi [6]. W praktyce jest to zbiór parametrów sieciowych, wymaganych do przesyłania strumienia danych. Przez zapewnienie jakości usługi (zapewnienie QoS) należy rozumieć przesłanie strumienia danych z zapewnieniem określonych wartości tych parametrów w relacji od końca do końca (od dostawcy do odbiorcy usługi). W zależności od rodzaju usługi dostawca definiuje wartości tych parametrów.

Z postrzeganą jakością usługi mamy do czynienia wtedy, gdy użytkownik korzysta z tej usługi. Na wrażenia, jakie on odnosi, mają wpływ jego oczekiwania, doświadczenia z podobną usługą świadczoną przez innego operatora, opinie innych użytkowników czy też środowisko, w którym się znajduje. W związku z tym zapewnienie wysokiej wrodzonej jakości usługi nie daje jeszcze gwarancji, że będzie on usatysfakcjonowany. Samo zapewnienie parametrów sieciowych może być niewystarczające. Jeżeli bowiem korzystanie z usługi będzie niewygodne z powodu innych czynników, użytkownik odczuje

niezadowolenie.

Z ocenianą jakością usługi mamy do czynienia w chwili, gdy użytkownik podejmuje decyzję, czy chce z niej korzystać, czy zrezygnować. Wpływ na to może mieć między innymi sposób, w jaki dostawca usługi reaguje na problemy i reklamacje użytkownika.

Podsumowując można stwierdzić, że zadana jakość usługi jest tym, co czyni ją atrakcyjną dla potencjalnego użytkownika. Postrzegana jakość usługi determinuje, czy użytkownik uzna ją za satysfakcjonującą, zaś oceniana jej jakość decyduje o ewentualnej kontynuacji bądź rezygnacji z korzystania z tej usługi. Łatwo zauważyć, że bezpośredni związek z projektowaniem sieci ma zadana jakość usług. Pozostałe dwa pojęcia są raczej związane z polityką marketingową operatora, a zapewnienie wysokiej jakości usług na tych poziomach należy do zadań marketingu, projektantów usług czy obsługi technicznej.

Pojęcie jakości usługi QoS jest często mylone z klasą usług (CoS). Klasa usług jest terminem bardziej ogólnym, opisującym zbiór cech charakterystycznych i właściwości określonej usługi lub zbioru usług [7]. Usługi należące do określonej klasy charakteryzują się gwarancją wybranych parametrów QoS. Zwykle określa się tylko, jakie parametry są gwarantowane w ramach danej klasy, bez określania ich konkretnych wartości. Przykładem mogą być, omówione dalszej części pracy, klasy usług w modelach IntServ i DiffServ. W literaturze spotyka się również termin poziom usług LoS (Level of Service). Jest on zwykle utożsamiany z klasą usług. Terminy te są stosowane zamiennie.

Kategoria usług GoS (Grade of Service) jest pojęciem szerszym niż QoS. Podział usług na kategorie – oprócz parametrów transmisyjnych – może uwzględniać wiele wymagań wysokiego poziomu, takich jak bezpieczeństwo, protekcja czy prawdopodobieństwo mechanicznego uszkodzenia łącza [8], [9].

Przykładowo, w dokumencie [10] zdefiniowano cztery kategorie usług: standardową, średniego poziomu bezpieczeństwa, wysokiego poziomu bezpieczeństwa oraz najwyższego poziomu bezpieczeństwa. Rozróżnienie uwzględnia możliwość stałego utrzymywania rozłącznej ścieżki zapasowej oraz poprowadzenie ścieżki podstawowej przez obszary o małym prawdopodobieństwie mechanicznego uszkodzenia łącza (np. obszary, na których nie występują trzęsienia ziemi). Omawiane kategorie usług zestawiono w tabeli 3.1.

Tabela 3.1. Przykładowe kategorie usług

Poziom bezpieczeństwa

| Utrzymanie stałej ścieżki zapasowej

| Ścieżka podstawowa poprowadzona przez łącza o małym prawdopodobieństwie uszkodzenia fizycznego

Standardowy

| –

| –

Średni

| –

| +

Wysoki

| +

| –

Najwyższy

| +

| +

Service Level Agreement (SLA) jest to porozumienie pomiędzy klientem a dostawcą usługi. SLA musi określać w sposób zrozumiały dla klienta, czego może on oczekiwać w ramach danej usługi. Kontrakt taki powinien zawierać jasno określone sposoby oceny jakości otrzymywanej usługi, a więc zgodności dostarczonej usługi z zawartym kontraktem. Z drugiej strony konieczne jest kontrolowanie klienta, czy dotrzymuje warunków umowy oraz ustalenie zakresu odpowiedzialności za jej złamanie przez każdą ze stron. Ponadto SLA powinno definiować:

- klasę dostarczanej usługi (CoS) lub wartości gwarantowanych parametrów jakościowych usługi (QoS),
- dostępność usługi,
- zakres gwarantowanej obsługi technicznej,
- zasady naliczania i pobierania opłat.

Porozumienie SLA może również obejmować zbiór reguł wymuszania charakterystyk ruchu klienta w ramach świadczonej usługi (TCA). Na SLA składają się, więc zarówno parametry techniczne (sieciowe) danej usługi, jak również aspekty prawne, kwestie naliczania opłat, obsługa techniczna itp.

Service Level Specification (SLS) jest to zbiór parametrów technicznych o określonych wartościach, z jakimi będzie przesyłany przez sieć strumień pakietów związanych z daną usługą [11]. SLS obejmuje również zbiór reguł niezbędnych do zdefiniowania różnorodnych usług opartego na różnych parametrach i ich wartości. SLS jest techniczną częścią kontraktu SLA pomiędzy klientem a dostawcą usługi. Specyfikuje wartości parametrów sieciowych dostarczanej usługi. SLS wraz z aspektami prawnymi, ustaleniami dotyczącymi naliczania opłat czy obsługi technicznej składa się na SLA. Pojęcie SLS zostało wprowadzone w celu wyodrębnienia z SLA, będącego pojęciem szerokim, informacji ściśle technicznych.

W ramach IETF są prowadzone prace mające na celu precyzyjne zdefiniowanie SLS. Dyskutowane są dwie koncepcje. Jedna zakłada możliwość dynamicznego negocjowania parametrów SLS

pomiędzy klientem i operatorem [12], druga zaś przewiduje opracowanie predefiniowanych typów SLS i zasad posługiwania się nimi, obowiązujących wszystkich operatorów [13]. Takie podejście ma na celu ułatwienie świadczenia usług za pośrednictwem kilku operatorów, uproszczenie procedur zarządzania i ułatwienie realizacji mechanizmów agregacji strumieni.

Traffic Conditioning Agreement (TCA) jest to porozumienie określające reguły klasyfikowania pakietów oraz profile ruchu odpowiednie dla różnych strumieni ruchu. TCA definiuje zasady oznaczania pakietów (marking), odrzucania pakietów (dropping), kształtowania ruchu (shaping) oraz wykonywania pomiarów ruchu (metering). Zbiór reguł formowania ruchu zdefiniowany w ramach TCA może stanowić część SLA [14]. Porozumienie TCA nakłada na klienta obowiązek dostosowania generowanego ruchu do uzgodnionego profilu ruchu. Określa również, w jaki sposób będą traktowane pakiety klienta zarówno w przypadku zgodności z profilem ruchu, jak i w przypadku naruszenia warunków umowy.

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.

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.

nagłówekIPdane TCPnagłówekTCPdatagram IPsegment TCP20 bajtów20 bajtównagłówekIPdane TCPnagłówekTCPdatagram IPsegment TCP20 bajtów20 bajtów

Rysunek 2.7. Enkapsulacja danych TCP w datagramie IP

URGACKPSHRSTSYNFINOpcjeNumer potwierdzeniaNumer sekwencjiPort docelowy 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bityPort źródłowyRozmiar oknaZnacznik pilnościSuma kontrolnaDaneDługość nagłówkaZarezerwowane6 Flag 1-bitowychURGACKPSHRSTSYNFINOpcjeNumer potwierdzeniaNumer sekwencjiPort docelowy 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bity 4 bityPort źródłowyRozmiar oknaZnacznik pilnościSuma kontrolnaDaneDługość nagłówkaZarezerwowane6 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 zwiera 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 nagłówek 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 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.

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 telemetrii 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.

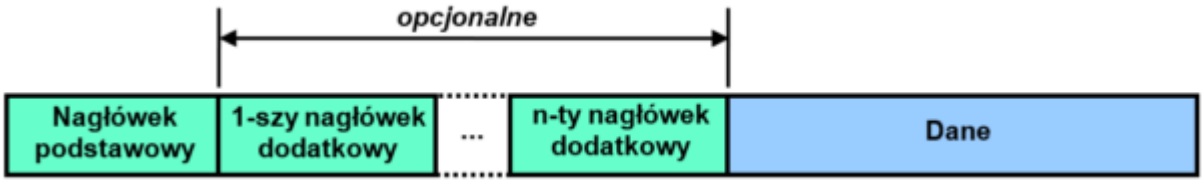
Protokół TCP/IP (część 2)

Nagłówek IPv6

Proponowany protokół IPv6 zachowuje wiele cech, które przyczyniły się do sukcesu IPv4. W rzeczywistości konstruktorzy scharakteryzowali IPv6 jako IPv4 z kilkoma modyfikacjami.

Jak widać na rysunku 2.4. datagram IP ma nagłówek podstawowy o ustalonym rozmiarze, po którym następuje zero lub więcej nagłówków dodatkowych poprzedzających dane [38].

Rysunek 2.4. Ogólna postać datagramu IPv6 z wieloma nagłówkami



Format nagłówka podstawowego

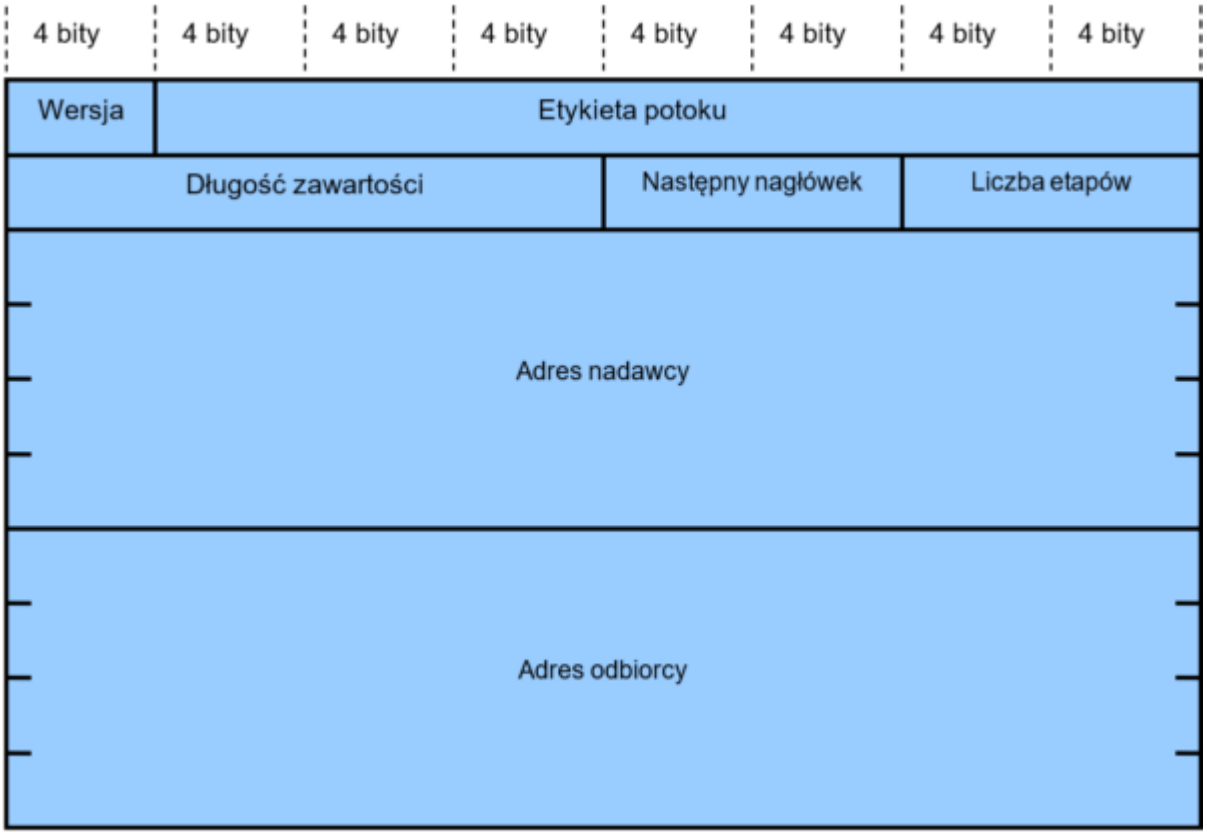
Pomimo tego, że nagłówek podstawowy IPv6 musi obsługiwać większe adresy, to zawiera on mniej informacji niż nagłówek datagramu IPv4. Opcje i niektóre z ustalonych pól, które pojawiają się w nagłówku datagramu IPv4, zostały w IPv6 przeniesione do nagłówków dodatkowych. W ogólności zmiany w

nagłówku datagramu odpowiadają zmianom w samym protokole [38]:

- wyrównywanie do 32-bitów zostało zmienione na wyrównywanie do 64-bitów,
- pole długości nagłówka zostało wyeliminowane, a pole długości datagramu zastąpiono polem długość zawartości,
- rozmiar pól adresów nadawcy i odbiorcy został zwiększony do 16 oktetów,
- informacje o fragmentacji zostały przeniesione z pól stałych w nagłówku podstawowym do nagłówka dodatkowego,
- pole czas życia zostało zastąpione polem liczba etapów,
- pole typ obsługi zastąpiono polem etykiety potoku,
- pole protokół zostało zastąpione polem, które określa typ następnego nagłówka.

Na rysunku 2.5. są pokazane zawartość i format nagłówka podstawowego IPv6. Kilka pól tego nagłówka odpowiada bezpośrednio polom w nagłówku IPv4. Tak jak w IPv4, początkowe 4-bitowe pole wersja służy do określenia wersji protokołu w datagramie IPv6, zawiera ono zawsze 6. Podobnie jak w IPv4 pola adres nadawcy i adres odbiorcy zawierają adresy wysyłającego i odbierającego. Jednak w IPv6 na każdy z tych adresów zużywa się 16 oktetów. Pole liczba etapów odpowiada polu czas życia w IPv4. Inaczej niż IPv4, które traktuje czas życia jak kombinację liczby etapów oraz maksymalnego czasu podróży, IPv6 interpretuje tę wartość jako ścisłe ograniczenie maksymalnej liczby etapów, jaką może datagram wykonać zanim zostanie usunięty.

Rysunek 2.5. Format 40-oktetowego nagłówka podstawowego IPv6. Każdy datagram IPv6 rozpoczyna się od takiego nagłówka



IPv6 używa nowego sposobu specyfikacji długości datagramu. Po pierwsze, ponieważ rozmiar nagłówka podstawowego wynosi 40 oktetów, nie zawiera on pola odpowiedzialnego za długość nagłówka. Po drugie w IPv6 pole długości datagramu jest zastąpione 16-bitowym polem długość zawartości, które służy do określenia liczby oktetów przenoszonych w datagramie, nie licząc oktetów nagłówka. Dzięki temu datagram może zawierać 64 kilo-otetów danych.

IPv6 oferuje nowy mechanizm, który umożliwia rezerwację zasobów i pozwala ruterowi na wiązanie każdego datagramu z podaną rezerwacją zasobów. Wykorzystywane jest do tego pojęcie potoku oznaczające ścieżkę poprzez intersieć, na której pośrednie rutery gwarantują określoną jakość obsługi. Przykładowo dwa programy, które chcą przesyłać obrazy mogą ustanowić potok, w ramach, którego są gwarantowane określona przepustowość i opóźnienie. Alternatywnie usługodawca sieciowy może wymagać od swojego klienta, aby ten określił potrzebną mu jakość usługi, a następnie używać potoków do ograniczania ruchu generowanego przez dany komputer czy program użytkowy.

Pole etykieta potoku w nagłówku podstawowym zawiera informacje, których rutery używają do wiązania datagramu z odpowiednim potokiem informacji oraz priorytetem. Pole to jest podzielone na dwa podpola, które widać na rysunku 2.6.

Identyfikator potokuKlasa ruchu4 bity 24 bity Identyfikator potokuKlasa ruchu4 bity 24 bity

Rysunek 2.6. Dwa podpola pola ”etykieta potoku”. Każdy datagram IPv6 zawiera etykietę potoku, która może być używana do wiązania datagramu z określonym rodzajem obsługi

W etykiecie potoku 4-bitowe pole klasa ruchu służy do określenia, jaką klasą ma podróżować datagram. Wartości od 0 do 7 są używane do określania wrażliwości na czasy dla ruchu kontrolowanego potokami, a wartości od 8 do 15 określają priorytet ruchu poza nimi. Pozostałe 24 bity zawierają identyfikator potoku.

Podsumowując, datagram IPv6 zaczyna się od 40-oktetowego nagłówka podstawowego, który zawiera pola adresów nadawcy i odbiorcy, maksymalnej liczby etapów, etykiety potoku oraz typu następnego nagłówka. Wobec tego datagram IPv6 oprócz danych musi zawierać, co najmniej 40 oktetów.

Protokół TCP (Transmission Control Protocol)

TCP jest protokołem działającym w warstwie transportowej, wykorzystując warstwę sieci IP dostarcza usług aplikacjom. Obecna wersja TCP jest oficjalnie zdefiniowana w RFC 793 [3], od tego czasu dodano wiele rozszerzeń, które udokumentowano w odpowiednich dokumentach RFC.

TCP zapewnia zorientowaną połączeniowo, niezawodną obsługę ciągów przesyłanych bajtów. Połączeniowość oznacza, że dwie aplikacje używające tego protokołu muszą przed rozpoczęciem wymiany danych nawiązać ze sobą połączenie [1].

Protokół TCP zapewnia niezawodność poprzez:

Dane przekazywane przez aplikację są dzielone na fragmenty, które według TCP mają najlepszy do przesłania rozmiar. Jest to podejście całkowicie inne niż w UDP, w którym datagram generowany był na podstawie przekazanego przez aplikację komunikatu. Jednostka informacji przekazywana przez TCP do IP nazywana jest segmentem.

Kiedy TCP wysyła segment, to jednocześnie uruchamia zegar, który rozpoczyna oczekiwanie na potwierdzenie odebrania segmentu przez drugą stronę. Jeśli potwierdzenie nie nadejdzie w określonym czasie, segment wysyłany jest powtórnie.

Kiedy TCP odbiera dane nadesłane przez drugą stronę połączenia, wysyła wtedy potwierdzenie odbioru. Potwierdzenie to nie jest wysyłane natychmiast, tylko po odczekaniu zwykle kilku sekund.

TCP posługuje się sumami kontrolnymi nagłówka datagramu i danych. Jest to suma typu end-to-end, której zadaniem jest wykrycie każdej modyfikacji danych w czasie ich przesyłania. Jeśli segment zostanie nadesłany z niepoprawną sumą kontrolną, TCP odrzuca go i nie potwierdza odbioru. (Spodziewa się, że wysyłający prześle go po raz kolejny, po odczekaniu założonego czasu).

Ponieważ segmenty TCP są przesyłane jako datagramy IP, które mogą być nadsyłane w dowolnej kolejności, to segmenty TCP również mogą nadchodzić w innej kolejności niż zostały wysłane. Strona odbierająca segmenty TCP porządkuje je, jeśli zachodzi taka konieczność, i przekazuje do aplikacji.

Ponieważ datagramy IP mogą być powielane, odbiorca TCP musi umieć odrzucić zdublowane dane.

Jedną z podstawowych cech protokołu TCP jest zapewnienie aplikacjom logicznego, uporządkowanego strumienia bajtów. Aplikacja korzystająca z TCP nie musi samodzielnie zajmować

się numerowaniem kolejnych fragmentów przesyłanych danych, wykrywaniem ich utraty czy ustawianiem we właściwej kolejności. Funkcje te realizuje warstwa transportowa. Z punktu widzenia programu dane mogą być więc traktowane jako ciąg bajtów przesyłanych pomiędzy dwoma końcami ustanowionego połączenia.

TCP jest protokołem pełnodupleksowym. Oznacza to, że po ustanowieniu połączenia dane mogą być przesyłane równocześnie w obu kierunkach. Każda ze stron jest jednocześnie nadawcą i odbiorcą oraz posiada własną przestrzeń numerów sekwencyjnych. Rozwiązanie takie jest potrzebne na przykład podczas komunikacji klienta z serwerem, gdzie klient wysyła żądania, a serwer przekazuje odpowiedzi, lecz obie strony mogą przesyłać także dodatkowe informacje związane z obsługą połączenia.

Porty i identyfikacja połączenia TCP

Samo podanie adresu IP komputera nie wystarcza do określenia aplikacji, do której mają zostać dostarczone dane. Na jednym urządzeniu może jednocześnie działać wiele programów korzystających z sieci. TCP wykorzystuje więc numery portów, dzięki którym system operacyjny może skierować przychodzące dane do właściwego procesu.

Połączenie TCP można określić przy użyciu adresów IP oraz numerów portów obu stron. Dzięki temu ten sam serwer może jednocześnie obsługiwać wiele połączeń pochodzących od różnych klientów. Każde z nich jest rozpoznawane jako oddzielny strumień komunikacyjny i posiada własny stan, numery sekwencyjne, parametry sterowania przepływem oraz inne informacje potrzebne do niezawodnego przesyłania danych.

Numery portów są wartościami 16-bitowymi. Część z nich jest tradycyjnie związana z określonymi usługami sieciowymi, natomiast aplikacje klienckie mogą korzystać z portów przydzielanych dynamicznie przez system operacyjny. Mechanizm portów umożliwia więc multipleksowanie wielu połączeń

transportowych przy użyciu jednego interfejsu sieciowego.

Nagłówek segmentu TCP

Każdy segment TCP posiada nagłówek zawierający informacje niezbędne do prawidłowej obsługi połączenia. Znajdują się w nim między innymi numery portów źródłowego i docelowego, numer sekwencyjny, numer potwierdzenia, informacje o długości nagłówka, pola sterujące, wielkość okna odbiorczego oraz suma kontrolna. Nagłówek może również zawierać opcje rozszerzające podstawowe możliwości protokołu.

Numer sekwencyjny odgrywa podstawową rolę w zapewnieniu właściwej kolejności danych. TCP numeruje bajty przesyłanego strumienia. Odbiorca może dzięki temu określić, które fragmenty danych już otrzymał, których jeszcze brakuje oraz czy pojawiły się dane przesłane ponownie. Pozwala to odtworzyć prawidłowy strumień nawet wtedy, gdy poszczególne segmenty docierają różnymi drogami i w innej kolejności niż zostały wysłane.

Numer potwierdzenia informuje natomiast drugą stronę, którego bajtu oczekuje odbiorca w następnej kolejności. Potwierdzenia TCP mają charakter kumulacyjny. Jeśli odbiorca potwierdza określony numer, oznacza to zasadniczo, że otrzymał poprawnie wszystkie wcześniejsze bajty należące do ciągłego fragmentu strumienia.

Takie rozwiązanie ogranicza liczbę informacji, które muszą być wymieniane pomiędzy stronami. Nie jest konieczne wysyłanie oddzielnego potwierdzenia dla każdego pojedynczego bajtu ani nawet każdego segmentu. Mechanizmy TCP mogą agregować potwierdzenia, zachowując jednocześnie możliwość wykrywania brakujących fragmentów.

Nawiązywanie połączenia

Przed rozpoczęciem właściwej transmisji danych strony muszą

ustanowić połączenie. W klasycznym przypadku wykorzystywany jest mechanizm określany jako trójfazowe uzgadnianie, czyli three-way handshake. Pozwala on obu stronom potwierdzić gotowość do komunikacji oraz uzgodnić początkowe numery sekwencyjne.

Klient rozpoczynający połączenie wysyła segment z ustawioną flagą SYN. Serwer odpowiada segmentem zawierającym SYN oraz ACK, potwierdzając tym samym odebranie żądania i przekazując własne informacje potrzebne do rozpoczęcia transmisji. Klient wysyła następnie potwierdzenie ACK. Po zakończeniu tej wymiany połączenie może przejść do stanu umożliwiającego przesyłanie danych.

Mechanizm ten jest ważny między innymi dlatego, że obie strony muszą zsynchronizować swoje przestrzenie numerów sekwencyjnych. Chroni on również przed pomyleniem nowego połączenia z opóźnionymi segmentami pochodzącymi z wcześniejszej komunikacji pomiędzy tymi samymi urządzeniami.

Podczas ustanawiania połączenia mogą być również wymieniane niektóre opcje TCP. Przykładem jest parametr MSS, określający największy segment danych TCP, jaki druga strona jest gotowa odbierać. Dzięki temu nadawca może odpowiednio dobierać wielkość przekazywanych fragmentów i ograniczać ryzyko niepotrzebnej fragmentacji na poziomie IP.

Sterowanie przepływem

Sama niezawodność dostarczania danych nie wystarcza, jeżeli nadawca przekazuje je szybciej, niż odbiorca jest w stanie przetwarzać. TCP posiada więc mechanizm sterowania przepływem. Jego zadaniem jest dostosowanie ilości danych znajdujących się w drodze do możliwości odbiorcy.

Odbierający posiada bufor, w którym przechowywane są dane przed przekazaniem ich aplikacji. W nagłówkach TCP informuje nadawcę, ile miejsca jest aktualnie dostępne. Informacja ta

określana jest jako okno odbiorcze. Nadawca powinien respektować jego wielkość i nie przesyłać niepotwierdzonych danych w ilości przekraczającej możliwości odbiorcy.

Wykorzystuje się tutaj ideę przesuwnego okna. Nadawca może wysłać pewną ilość danych bez oczekiwania na potwierdzenie każdego pojedynczego segmentu. W miarę otrzymywania potwierdzeń okno przesuwa się, dzięki czemu mogą być wysyłane kolejne fragmenty. Rozwiązanie takie jest znacznie wydajniejsze niż system wymagający oczekiwania na potwierdzenie po każdym segmencie.

Gdy aplikacja odbiorcza przetwarza zgromadzone dane, w buforze ponownie pojawia się wolne miejsce. Odbiorca może wtedy zwiększyć reklamowane okno, umożliwiając nadawcy kontynuowanie transmisji. Mechanizm ten pozwala na automatyczne dostosowywanie szybkości komunikacji do możliwości końcowego urządzenia i aplikacji.

Sterowanie przeciążeniem sieci

Sterowanie przepływem nie powinno być mylone ze sterowaniem przeciążeniem. Pierwszy mechanizm chroni przede wszystkim odbiorcę przed nadmiarem danych. Drugi służy ograniczeniu przeciążenia samej sieci znajdującej się pomiędzy nadawcą i odbiorcą.

Nawet bardzo szybki odbiorca nie rozwiąże problemu, jeżeli pośrednie łącza i rutery nie są w stanie obsłużyć całego generowanego ruchu. Nadmierna liczba pakietów może prowadzić do przepełnienia kolejek, odrzucania danych oraz gwałtownego pogorszenia wydajności. TCP wykorzystuje więc mechanizmy pozwalające stopniowo dostosowywać intensywność transmisji do obserwowanych warunków sieciowych.

Jednym z klasycznych mechanizmów jest slow start, czyli powolny start. Nazwa może być nieco myląca, ponieważ wzrost szybkości w tej fazie może następować stosunkowo dynamicznie.

Istotą jest jednak to, że nowo ustanowione połączenie nie rozpoczyna od natychmiastowego wysłania bardzo dużej ilości danych. Wielkość ruchu jest początkowo ograniczona, a następnie zwiększana w miarę otrzymywania potwierdzeń.

TCP wykorzystuje również okno przeciążenia. Jego wielkość jest ustalana przez nadawcę na podstawie informacji o zachowaniu sieci. W praktyce ilość danych możliwych do wysłania bez potwierdzenia zależy zarówno od możliwości odbiorcy, jak i od oszacowanych możliwości sieci. Pozwala to na stosunkowo efektywne wykorzystanie dostępnej przepustowości bez całkowitego ignorowania ryzyka przeciążenia.

Utrata segmentów może być interpretowana jako sygnał pogorszenia warunków transmisji. W zależności od zastosowanych mechanizmów nadawca może ograniczyć tempo wysyłania danych i następnie ponownie stopniowo je zwiększać. Współczesne implementacje TCP korzystają z różnych algorytmów sterowania przeciążeniem, jednak ich wspólnym celem pozostaje dostosowywanie transmisji do aktualnych właściwości sieci.

Retransmisja utraconych danych

W sieci IP nie istnieje gwarancja, że każdy wysłany pakiet dotrze do odbiorcy. Może on zostać utracony między innymi z powodu przeciążenia, błędów transmisji lub problemów urządzeń pośredniczących. TCP musi więc wykrywać brak danych i w razie potrzeby przesyłać je ponownie.

Jednym z podstawowych mechanizmów jest zegar retransmisji. Po wysłaniu danych nadawca oczekuje przez określony czas na ich potwierdzenie. Jeżeli odpowiednie potwierdzenie nie pojawi się, dane mogą zostać wysłane ponownie. Czas oczekiwania nie powinien być jednak stały dla wszystkich połączeń.

TCP dokonuje pomiarów czasu potrzebnego na przesłanie informacji do drugiej strony i powrót potwierdzenia. Na podstawie obserwacji może dostosowywać wartość limitu

retransmisji. Jest to konieczne, ponieważ zupełnie inne opóźnienia mogą występować w szybkiej sieci lokalnej, a inne w połączeniu przebiegającym przez dużą liczbę urządzeń i rozległą sieć.

Utratę segmentu można w pewnych sytuacjach wykryć również wcześniej, bez oczekiwania na wygaśnięcie całego czasu retransmisji. Powtarzające się potwierdzenia wskazujące na brak określonego fragmentu mogą być sygnałem, że segment został utracony, podczas gdy późniejsze dane dotarły prawidłowo. Mechanizmy szybkiej retransmisji pozwalają wtedy przyspieszyć naprawienie strumienia danych.

Suma kontrolna TCP

TCP wykorzystuje sumę kontrolną do wykrywania uszkodzeń powstałych podczas transmisji. Obejmuje ona nagłówek TCP oraz przesyłane dane, a przy jej obliczaniu uwzględniany jest również tak zwany pseudo-nagłówek zawierający wybrane informacje z warstwy IP. Pozwala to wykrywać nie tylko zmiany bitów w samym segmencie, lecz również niektóre błędy związane z jego dostarczeniem.

Jeżeli odbiorca stwierdzi niezgodność sumy kontrolnej, segment nie może zostać potraktowany jako poprawny. TCP opiera się następnie na mechanizmach niezawodnej transmisji, które prowadzą do ponownego przekazania brakujących danych. Dzięki temu aplikacja nie powinna otrzymać uszkodzonego fragmentu jako prawidłowej części strumienia.

Porządkowanie danych i usuwanie duplikatów

Warstwa IP może dostarczyć pakiety w innej kolejności niż kolejność ich wysłania. TCP wykorzystuje numery sekwencyjne do prawidłowego uporządkowania danych. Jeżeli segment dotyczący późniejszej części strumienia przyjdzie przed wcześniejszym, odbiorca może odpowiednio przechować otrzymane informacje do

momentu uzupełnienia brakującego fragmentu.

Podobny mechanizm pozwala wykrywać dane zdublowane. Duplikat może pojawić się na przykład wtedy, gdy nadawca ponowił transmisję, ponieważ wcześniejsze potwierdzenie zostało utracone, mimo że sam segment danych dotarł prawidłowo. Odbiorca, korzystając z numerów sekwencyjnych, rozpoznaje, że określone bajty zostały już odebrane, i nie przekazuje ich aplikacji po raz drugi.

Dzięki temu aplikacja otrzymuje uporządkowany strumień danych niezależnie od części problemów występujących na niższych warstwach sieci. Jest to jedna z głównych przyczyn, dla których TCP przez wiele lat był wykorzystywany przez bardzo dużą liczbę protokołów aplikacyjnych.

Zamykanie połączenia

Po zakończeniu transmisji połączenie TCP powinno zostać prawidłowo zamknięte. Ponieważ komunikacja jest pełnodupleksowa, zakończenie wysyłania danych w jednym kierunku nie musi automatycznie oznaczać, że druga strona również zakończyła transmisję. Proces zamykania może więc wymagać osobnego zakończenia obu kierunków.

Do normalnego zamykania połączenia wykorzystywana jest flaga FIN. Strona informuje za jej pomocą, że nie będzie już wysyłała nowych danych. Druga strona potwierdza otrzymanie tego sygnału. Jeżeli również zakończyła swoją transmisję, przesyła własny FIN, który następnie także zostaje potwierdzony.

Inną funkcję pełni flaga RST. Jest ona wykorzystywana do resetowania połączenia, na przykład wtedy, gdy wystąpi sytuacja uniemożliwiająca jego normalne kontynuowanie albo gdy segment odnosi się do połączenia, które nie istnieje. Reset oznacza bardziej nagłe zakończenie komunikacji niż standardowa procedura z użyciem FIN.

TCP a UDP

TCP i UDP działają w tej samej warstwie modelu komunikacyjnego, ale oferują aplikacjom odmienne usługi. TCP zapewnia połączenie, uporządkowany strumień danych, retransmisję utraconych fragmentów oraz mechanizmy sterowania przepływem. Kosztem tych właściwości jest większa złożoność i dodatkowy narzut związany między innymi z ustanawianiem oraz utrzymywaniem stanu połączenia.

UDP jest znacznie prostszy. Nie ustanawia połączenia w znaczeniu charakterystycznym dla TCP i nie zapewnia automatycznego odzyskiwania utraconych datagramów ani ich porządkowania. W zastosowaniach, w których ważniejsza jest minimalizacja opóźnień niż bezwzględne dostarczenie każdego fragmentu, takie zachowanie może być korzystne. W innych przypadkach ewentualne mechanizmy niezawodności muszą zostać zrealizowane przez aplikację lub protokół wyższej warstwy.

Nie można więc powiedzieć, że TCP jest zawsze lepszy od UDP. Wybór zależy od wymagań aplikacji. Przesyłanie pliku wymaga przede wszystkim poprawności i kompletności danych, dlatego utrata nawet niewielkiego fragmentu musi zostać naprawiona. W komunikacji czasu rzeczywistego retransmisja bardzo starego fragmentu może natomiast nie mieć już wartości, ponieważ ważniejsza jest aktualność kolejnych danych.

TCP w stosie TCP/IP

TCP nie funkcjonuje samodzielnie. Korzysta z usług warstwy IP, która odpowiada za przesyłanie pakietów pomiędzy urządzeniami znajdującymi się w różnych sieciach. IP nie zapewnia jednak TCP informacji o tym, czy pakiet rzeczywiście dotarł do celu. Właśnie dlatego niezawodność musi zostać zrealizowana w warstwie transportowej.

TCP może współpracować zarówno z IPv4, jak i IPv6. Z punktu widzenia aplikacji podstawowy charakter świadczonej usługi

pozostaje podobny. Różnice dotyczą natomiast warstwy sieciowej, formatów adresów i sposobu budowania odpowiednich pakietów.

Połączenie funkcji IP i TCP dobrze pokazuje podstawową zasadę warstwowej architektury sieci. IP zajmuje się przede wszystkim przekazywaniem pakietów pomiędzy hostami, nie gwarantując ich dostarczenia. TCP wykorzystuje tę usługę i tworzy na jej podstawie znacznie bardziej niezawodny kanał komunikacyjny widziany przez aplikacje.

Niezawodność TCP nie oznacza oczywiście, że połączenie nie może zostać przerwane. Jeżeli przez odpowiednio długi czas komunikacja z drugą stroną jest niemożliwa, protokół nie może zagwarantować dostarczenia danych. Jego zadaniem jest wykrywanie strat i ich naprawianie tak długo, jak istnieją warunki pozwalające utrzymać połączenie.

TCP jest zatem przykładem protokołu, w którym wiele mechanizmów współdziała w celu zapewnienia aplikacji spójnego strumienia danych. Numery sekwencyjne pozwalają uporządkować informacje, potwierdzenia informują o skutecznym odbiorze, retransmisje uzupełniają straty, okno odbiorcze zapobiega przeciążeniu odbiorcy, a mechanizmy sterowania przeciążeniem dostosowują transmisję do sytuacji w sieci.

Dzięki takiemu rozwiązaniu program korzystający z TCP nie musi samodzielnie rozwiązywać większości problemów wynikających z zawodności sieci IP. Może przekazywać ciąg danych do warstwy transportowej, która zajmuje się jego podziałem, wysyłaniem, potwierdzaniem, ewentualnym ponawianiem oraz ponownym składaniem po stronie odbiorcy. Właśnie połączenie tej funkcjonalności z uniwersalnością IP było jednym z najważniejszych czynników umożliwiających rozwój sieci opartych na rodzinie protokołów TCP/IP.

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.

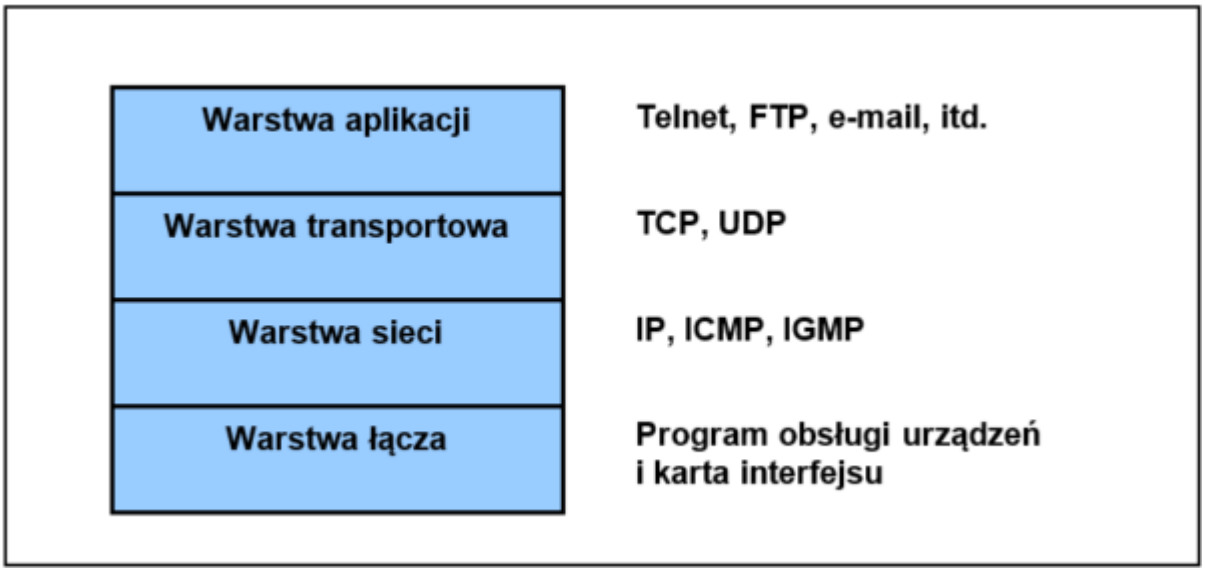
Protokół TCP/IP (część 1)

Zestaw protokołów TCP/IP pozwala na komunikowanie się komputerów różnej mocy obliczeniowej, pochodzących od różnych producentów i pracujących pod kontrolą różnych systemów operacyjnych. Jest to zdumiewające zjawisko, ponieważ wykorzystanie TCP/IP znacznie przekroczyło zakładany na początku zakres zastosowań. To, co pod koniec lat 60 rozpoczęto jako finansowany przez rząd projekt badawczy zmierzający do opracowania sieci pakietowej, w latach 90 zmieniło się w powszechnie używaną formę sieci łączącej miliony komputerów. Jest to naprawdę system otwarty, ponieważ zestaw protokołów i jego kolejne implementacje są w prawie niezmienionej formie powszechnie dostępne w sieci, bezpłatnie lub za niewielką opłatą. Podstawą tego, co powszechnie nazywane jest światowym Internetem lub po prostu Internetem, jest globalna sieć WAN (Wide Area Network), w której pracują miliony komputerów.

Warstwy sieci

Protokoły sieciowe opracowywane są zwykle z uwzględnieniem warstwowego modelu sieci, w którym kolejne warstwy odpowiedzialne są za różne aspekty komunikacji. Zestaw protokołów, taki jak TCP/IP, jest kombinacją różnych protokołów działających w kilku warstwach. Zestaw protokołów TCP/IP rozważa się zwykle jako system czterowarstwowy, jak pokazano na rysunku 2.1. [1].

Rysunek 2.1. Cztery warstwy protokołów TCP/IP



Każda z tych warstw odpowiedzialna jest, za co innego:

Warstwa łącza, nazywana czasami warstwą łącza danych lub warstwą dostępu do sieci, zawiera zwykle programy obsługi urządzeń wchodzące w skład systemu operacyjnego i odpowiadające im karty interfejsów sieciowych w komputerze. Razem tworzą one zestaw obsługujący wszystkie sprzętowe szczegóły związane z fizycznym dołączeniem komputera do kabla sieciowego (lub innych mediów, jakie zostały użyte do budowy sieci komputerowej).

Warstwa sieci nazywana czasami warstwą Internetu obsługuje ruch pakietów w sieci. W tym miejscu następuje na przykład ruting pakietów. W zestawie protokołów TCP/IP warstwę tę tworzą: IP (Internet Protocol), ICMP (Internet Control Message Protocol) i IGMP (Internet Group Management Protocol).

Warstwa transportowa zapewnia przepływ danych pomiędzy dwoma hostami, obsługując znajdującą się nad nią warstwę aplikacji. W skład TCP/IP wchodzą dwa całkowicie różne protokoły warstwy transportowej: TCP (Transmission Control Protocol) i UDP (User Datagram Protocol). Protokół TCP zapewnia niezawodny przepływ danych pomiędzy dwoma hostami. Zajmuje się takimi funkcjami, jak dzielenie danych przekazywanych mu przez aplikacje na kawałki wielkości odpowiadającej warstwie sieci znajdującej się poniżej. Ponadto potwierdza on odebranie pakietów, określa

czasy pozwalające hostowi, z którym następuje wymiana danych, na potwierdzenie ich odbioru i tak dalej. Ponieważ warstwa transportowa zapewnia niezawodny przepływ danych, warstwa aplikacji nie musi już się tym zajmować. Z drugiej strony, protokół UDP umożliwia znacznie prostsze usługi dla warstwy aplikacji. Przesyła między hostami pakiety danych, zwane datagramami, nie gwarantując jednak, że dotrą one do punktu przeznaczenia. W tym przypadku, jeśli żądany jest jakiś poziom niezawodności przesyłania danych, to musi go zapewnić warstwa aplikacji.

Warstwa aplikacji obsługuje funkcje związane z określoną aplikacją korzystającą z sieci. Istnieje wiele aplikacji TCP/IP, które dostępne są w prawie każdej implementacji:

Telnet pozwalający na zdalne zalogowanie się do systemu,

FTP (File Transfer Protocol) protokół transmisji plików,

SMTP (Simple Mail Transfer Protocol) protokół obsługujący pocztę elektroniczną,

SNMP (Simple Network Management Protocol) protokół zarządzania siecią.

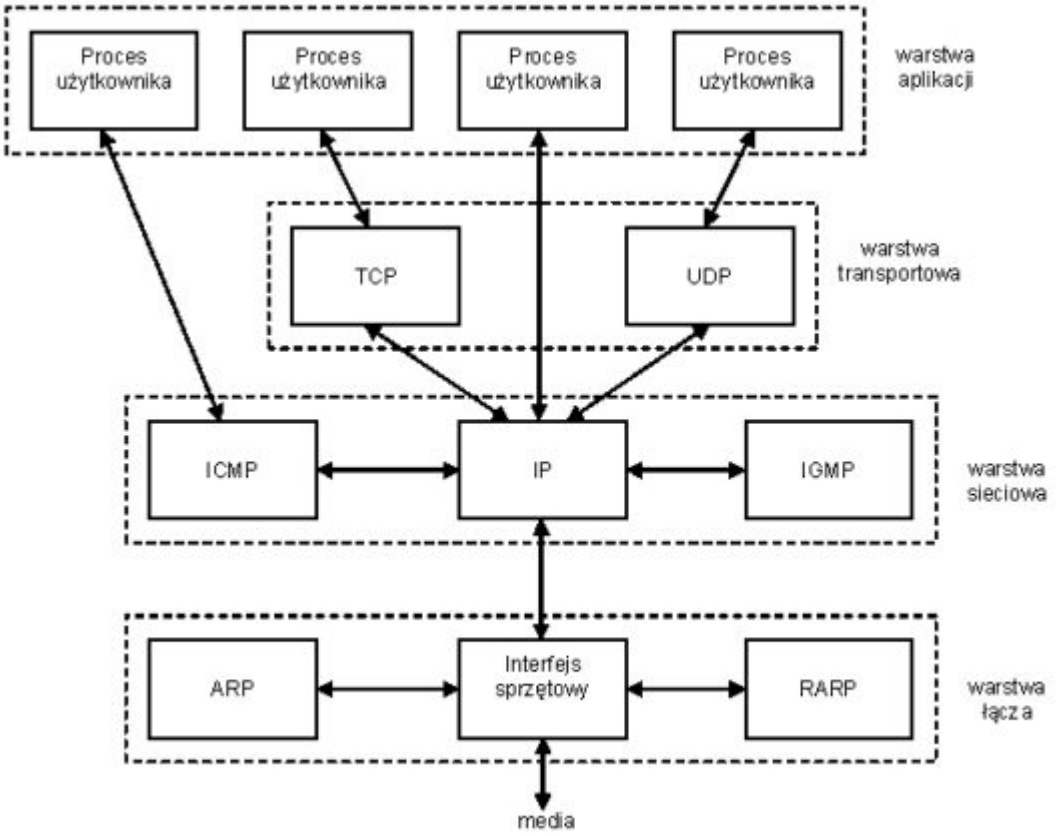
Skład TCP/IP

W zestawie protokołów TCP/IP jest wiele innych protokołów poza tymi, które występują w nazwie. Na rysunku 2.2. przedstawiono kilka innych protokołów wchodzących w skład TCP/IP [1].

TCP (Transmission Control Protocol) i UDP (User Datagram Protocol) są dwoma dominującymi protokołami warstwy transportowej. Obydwa używają IP jako protokołu warstwy sieci. TCP zapewnia niezawodne usługi warstwy transportowej, chociaż posługuje się IP, który nie gwarantuje niezawodności. UDP wysyła i odbiera datagramy przekazywane z aplikacji. Datagram jest jednostką informacji (tzn. określoną przez wysyłającego liczbą bajtów informacji), która przesyłana jest od nadawcy do

odbiorcy. Jednakże w przeciwieństwie do TCP, UDP nie jest usługą niezawodną. Nie ma żadnej gwarancji, że wysłany datagram kiedykolwiek dotrze do celu.

Rysunek 2.2. Różne protokoły wchodzące w skład TCP/IP z podziałem na warstwy, w których pracują



IP jest podstawowym protokołem warstwy sieci. Używany jest on zarówno przez TCP, jak i przez UDP. Każdy segment danych TCP i UDP, który przysyłany jest przez sieć, musi przejść przez warstwę IP zarówno w systemach końcowych, jak i w ruterach pośrednich. Na rysunku 2.2. pokazana jest również aplikacja mająca bezpośredni dostęp do IP. Jest to rozwiązanie możliwe do zrealizowania, choć rzadko stosowane.

ICMP jest protokołem dodatkowym dla IP. Używany jest przez warstwę IP do wymiany komunikatów o błędach i innych ważnych informacji z warstwą IP na innym hoście lub ruterze. Choć ICMP używany jest głównie przez IP, to możliwe jest posługiwanie się nim z poziomu aplikacji (programy diagnostyczne Ping i

Traceroute).

Protokół IGMP (Internet Group Management Protocol) jest używany przy multicastingu: wysyłaniu datagramów UDP do wielu hostów równocześnie.

ARP (Address Resolution Protocol) i RARP (Reverse Address Resolution Protocol) są specjalizowanymi protokołami, używanymi tylko z niektórymi rodzajami interfejsów sieciowych (takimi jak Ethernet i token ring), zapewniającymi konwersję pomiędzy adresami warstwy IP a adresami interfejsu sieciowego.

Protokół IP (Internet Protocol)

IP jest podstawowym protokołem w zestawie TCP/IP. Wszystkie dane z TCP, UDP, ICMP i IGMP przesyłane są przez datagramy IP rysunek 2.3. IP świadczy zawodne, bezpołączeniowe usługi dostarczania pakietów.

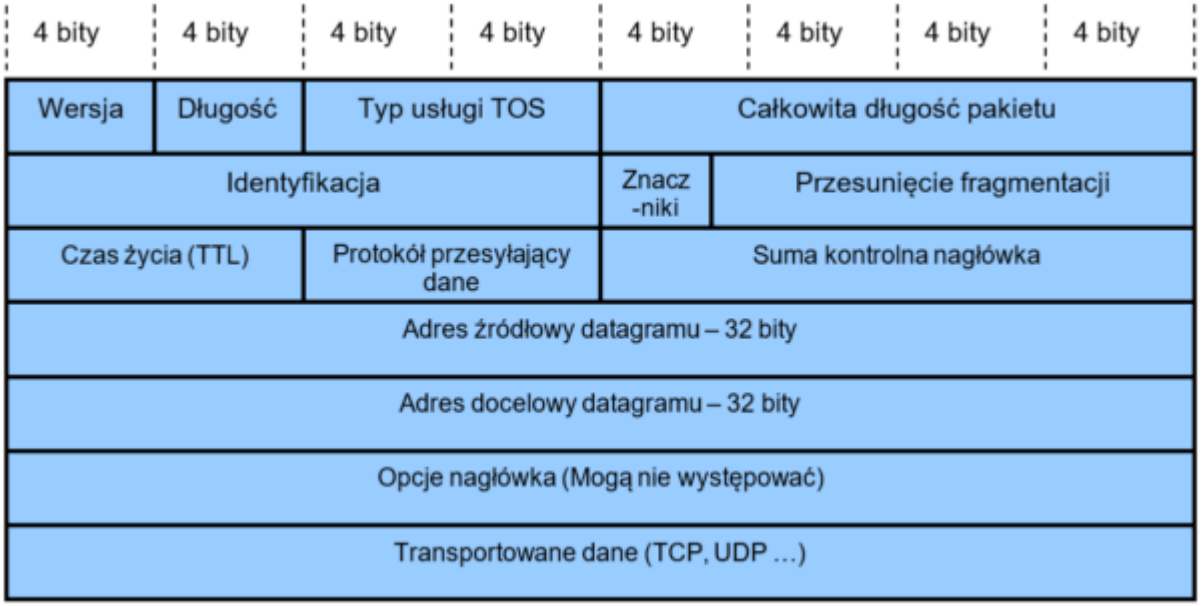
Poprzez słowo zawodne (unreliable) rozumiemy to, że nie ma żadnej gwarancji na pomyślne dostarczenie datagramu IP do punktu przeznaczenia. IP stara się jedynie dobrze przesłać datagramy. Kiedy jednak coś się nie uda, na przykład wystąpi przepełnienie buforów rutera, IP uruchamia bardzo prosty algorytm obsługi błędów: usuwa datagram i próbuje wysłać do źródła wiadomość ICMP. Wszelkie wymagane mechanizmy niezawodności transmisji muszą być zapewnia ne przez wyższe warstwy (np. TCP).

Określenie bezpołączeniowy oznacza, że IP nie zachowuje żadnej informacji o datagramach, które zostały przesłane pomyślnie. Każdy datagram obsługiwany jest niezależnie od pozostałych. Oznacza to również, że datagramy IP mogą docierać do punktu przeznaczenia w innej kolejności niż zostały wysłane. Jeśli nadawca wysyła dwa kolejne datagramy (najpierw A, potem B) do tego samego punktu przeznaczenia, każdy z nich rutowany jest niezależnie i może być przesłany inną trasą, w wyniku czego B może dotrzeć przed A.

Nagłówek IPv4

Obecnie używaną wersją protokołu jest wersja 4, dlatego czasem IP nazywany jest IPv4. Oficjalną specyfikacją IP jest dokument [4]. Na rysunku 2.3. pokazano format datagramu IP. Typowym rozmiarem nagłówka IP jest 20 bajtów, chyba, że umieszczone są w nim dodatkowe opcje.

Rysunek 2.3. Datagram IPv4 z uwzględnieniem pól tworzących nagłówek IP



Przedstawienie cech, możliwości i sposobu działania protokołu IP najłatwiej przedstawić omawiając kolejno znaczenie i zastosowanie poszczególnych elementów struktury danych, jaką stanowi nagłówek protokołu.

Adres źródłowy i docelowy

Wszystkie urządzenia pracujące wewnątrz sieci IP identyfikowane są poprzez unikatowy 32 bitowy adres IP. Wysyłając datagram nadawca umieszcza we właściwych polach adresy IP: swój i odbiorcy oraz dysponując wiedzą z tabeli rutingu wysyła datagram do rutera najwłaściwszego z punktu widzenia lokalizacji adresu odbiorcy. W przypadku sieci lokalnej typu ethernet datagram o adresie docelowym IP „lokalnym” dla danej sieci jest wysyłany bezpośrednio do

żądanego komputera, zaś datagramy o innych adresach docelowych są kierowane do rutera – bramki. Zawartość obu pól adresowych nie jest zmieniana w trakcie przesyłania informacji. Sprawia to, że kolejny router wie, kto jest nadawcą informacji oraz gdzie powinna ona dotrzeć, lecz nieznana jest mu dotychczasowa trasa pakietu w sieci (adresy ruterów, które przesyłały datagram). W ten sposób informacja o sposobie dobierania trasy jest silnie rozproszona. Pole adres źródłowy nie odgrywa w procesie dostarczania datagramu istotnej roli, wykorzystywane jest dopiero przez odbiorcę do identyfikowania nadawcy wiadomości.

Czas życia datagramu (TTL)

Ponieważ jak opisano powyżej proces wybierania trasy datagramu zależy w dużej mierze od sprawności działania wszystkich węzłów pośredniczących, możliwe jest, że w sytuacjach awaryjnych pakiet będzie krążył pomiędzy ruterami bardzo długo, lub wręcz trasa jego przesyłania zostanie zapętlona. Pole TTL (Time-To-Live) zapobiega takiej sytuacji – jego zawartość jest wstępnie inicjowana przez nadawcę i dekrementowana przez każdy z węzłów, który przesyła datagram. Gdy jego wartość wyniesie 0, datagram zostaje usunięty, a do nadawcy wysyłany jest komunikat ICMP o błędzie.

Protokół przesyłający dane

Immanentną cechą enkapsulacji danych przez protokoły warstwowe jest fakt, iż najważniejszym zadaniem protokołu warstwy niższej jest dostarczanie danych dla warstwy wyższej. Choć powszechnie używa się akronimu TCP/IP, protokół sieciowy IP, oprócz danych warstwy TCP przenosi również dane protokołu transportowego UDP oraz dane sygnalizacyjne protokołów ICMP i IGMP (które uznane są za element protokołu IP choć stanowią de facto warstwę wyższą). Aby rozróżnić rodzaj przesyłanych w datagramie informacji nadawca umieszcza w tym polu nagłówka liczbę reprezentującą zestandaryzowane oznaczenie protokołu

przesyłanych informacji. Pole to może zostać również użyte przez rutery do traktowania z wyższym priorytetem wiadomości sygnalizacyjnych ICMP.

Suma kontrolna nagłówka

Pole to zabezpiecza integralność informacji przesyłanych tylko w nagłówku datagramu. Z reguły jednak warstwy łącza danych (np. MAC w ethernecie, PPP w połączeniu modemowym) sprawdzają poprawność całej przesyłanej informacji, dodatkowo zaś dane mogą być jeszcze zabezpieczane przed przekłamaniem przez warstwy wyższe.

Identyfikacja

Pole to jest unikalnym numerem, który identyfikuje w sposób jednoznaczny datagram wysyłany z danego hosta. Szesnastobitowa wartość tego pola (65 536 możliwości) w połączeniu z mechanizmem TTL gwarantują, że w danej chwili w sieci nie będą nigdy istniały dwa identyczne pakiety.

Wersja protokołu

Pole to oznacza wprost numer używanego protokołu IP obecnie używana wersja to 4, w przyszłości zastąpi ją IPv6.

Długość nagłówka

Liczba 32-bitowych słów umieszczonych w nagłówku wraz z opcjami tworzy długość nagłówka. Typowa (minimalna) długość nagłówka wynosi 5. Liczba ta informuje komputer odbierający, kiedy ma zakończyć czytanie nagłówka i rozpocząć czytanie danych.

Całkowita długość pakietu

Wielkość ta, pomniejszona o rozmiar nagłówka wyznacza rozmiar pola danych enkanpsulowanych przez datagram. Jego teoretyczny rozmiar sięga, co prawda wartości 64kB, jednak w praktyce ze względu na ograniczenia interfejsów fizycznych długość

datagramu nigdy nie przekracza wartości tzw. MTU (*Maximum Transmission Unit*), zaś w wielu przypadkach ze względu na różnice w wielkości największego dopuszczalnego pakietu konieczna jest segmentacja datagramu (podział na kilka pakietów).

Typ usługi TOS

W założeniach, protokół IP posiadać miał pewne elementy mechanizmów sterowania przepływem, których celem jest zapewnienie gradacji poziomu jakości usługi sieciowej (QoS). W tym celu pole TOS zawiera 3 bitowy wskaźnik priorytetu przesyłania pakietu oraz trzy flagi zalecanego doboru trasy, które mogą być używane do określania parametrów pierwszeństwa, opóźnienia, przepustowości i niezawodności tego pakietu. Niestety, obecne implementacje nie używają żadnego z tych pól (tzn. pola te są z reguły ustawiane, lecz elementy komutacyjne sieci – rutery ignorują je). Ponieważ transmitowanie informacji przez sieć odbywa się na poziomie sieciowym, utracono w ten sposób możliwość efektywnego i zestandardyzowanego sterowania przepływem na poziomie IP. Istniejące rozwiązania posługują się na ogół informacjami zasięgniętymi z nagłówka TCP w celu rozpoznania rodzaju przesyłanej usługi.

Znaczniki

Pole zawiera 3 bity. Pierwszy jest zawsze zerem. Drugi bit określa czy można (wartość 1), czy też nie można (wartość 0) fragmentować datagram. Natomiast ostatni bit służy do identyfikacji ostatniego fragmentu składającego się na pierwotny datagram. Wartość 0 określa ostatni, a wartość 1 oznacza kolejny fragment.

Przesunięcie fragmentacji

Pole to zawiera 13 bitów, wskazuje, którą częścią całości pierwotnego datagramu jest dany fragment. Poszczególne fragmenty mają pola danych o długości będącej wielokrotnością

8 bitów. Wyjątkiem jest ostatni fragment, którego długość wynika z długości pierwotnego datagramu. W polu tym podaje się o ile zawartość fragmentu jest przesunięta w stosunku do początku pola danych pierwotnego datagramu.

Opcje

To pole nagłówka o zmiennej długości w zamierzeniach autorów umożliwiało uzyskanie między innymi następujących funkcji:

- ograniczenia dotyczące bezpieczeństwa;
- zapisu trasy podróży przez sieć;
- zapisu czasu wyjścia datagramu z danego węzła sieci (router);
- ustalenie swobodnej trasy rutowania – lista węzłów przez które datagram musi przejść (pomiędzy nimi droga może być wybierana dowolnie);
- ustalenie dokładnej trasy rutowania – datagram nie może przejść inną drogą niż wskazaną na liście.

Możliwości pola *opcje* otwierają pewną drogę do wsparcia zastosowań wymagających utrzymywania w miarę stałych i powtarzalnych parametrów opóźnień i przepustowości sieci. W praktyce jednak ze względu na powszechne ignorowanie tej opcji przez rutery oraz zbyt małą dopuszczalną długość tego pola w stosunku do ilości punktów przeskoku na typowej trasie połączenia internetowego, nie można wpływać na sposób przesyłania informacji.

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.

Technika ślepych podpisów

Ślepe podpisy są jedną z podstawowych technik współczesnej kryptografii. Dzięki nim osoba podpisująca dokument nie widzi jego treści. Jeżeli więc klient banku sam utworzył banknot z niepowtarzalnym numerem seryjnym, to bank otrzymuje ten banknot do podpisu zgodnie z protokołem ślepych podpisów. Nie widzi więc numeru seryjnego banknotu i nie jest później w stanie przyporządkować klientowi jego wydatków.

Do generowania ślepych podpisów w dużej mierze wykorzystuje się asymetryczny algorytm RSA, który służy do tworzenia zwykłych podpisów cyfrowych. Dzięki wykorzystaniu własności arytmetyki modularnej bank podpisuje ciąg, który dopiero przy znajomości pewnego klucza może zostać przetworzony na oryginalną, podpisywaną wiadomość. Algorytm został tak utworzony, aby przy podpisywaniu zamaskowanego ciągu podpis był jednocześnie prawdziwy dla oryginalnej wiadomości.

Banknoty cyfrowe tym różnią się od prawdziwych, że mogą opiewać praktycznie na dowolną sumę i nie są uzależnione od ściśle określonych nominałów. Może się więc zdarzyć, że klient podsunie bankowi do podpisu banknot opiewający na sumę 1000 zł, a powie, że przysyła banknot na 100 zł. Ponieważ bank zgodnie z protokołem ślepych podpisów nie widzi treści banknotu, nie może sprawdzić prawdziwości danych podanych przez klienta.

Problem ten ma dwa popularne rozwiązania. Firma realizująca system eCash wybrała rozwiązanie prostsze, polegające na wystawianiu jedynie monet elektronicznych, czyli banknotów o ściśle określonej sumie, np. 1 dolar. System ten jest mało wydajny, bo przy zakupach za 1000 dolarów trzeba zaopatrzyć się w 1000 monet. Zważywszy że szyfrowanie asymetryczne nie jest szybkie, a używane liczby są duże, zarówno przesyłanie danych, jak i wykonywanie obliczeń jest czasochłonne.

Bardziej wyrafinowany sposób rozwiązania tego problemu umożliwia generowanie banknotów o dowolnym nominale. W tym celu klient generuje aż 100 banknotów o tym samym nominale. Wszystkie wysyłane są do banku zakryte, jak w protokole ślepych podpisów. Bank wybiera jeden z nich i nie odkrywając go, żąda ujawnienia pozostałych. Jeżeli wszystkie odkryte banknoty faktycznie opiewają na podaną sumę, bank może z dużym prawdopodobieństwem założyć, że wybrany banknot ma również odpowiedni nominał. Może go więc podpisać, mając praktycznie pewność, że klient nie oszukuje.

Podstawową cechą ślepego podpisu jest więc rozdzielenie dwóch czynności, które w przypadku zwykłego podpisu cyfrowego występują razem. Podmiot podpisujący potwierdza autentyczność określonego obiektu kryptograficznego, ale nie poznaje informacji, którą ostatecznie swoim podpisem uwierzytelnia. Po zakończeniu procedury odbiorca dysponuje prawidłowym podpisem możliwym do zweryfikowania przy użyciu klucza publicznego podpisującego. Jednocześnie podpisujący nie powinien być w stanie powiązać później przedstawionego dokumentu z konkretną operacją jego podpisania. To właśnie ta cecha sprawia, że ślepe podpisy znalazły zastosowanie przede wszystkim w rozwiązaniach, w których trzeba pogodzić możliwość potwierdzenia autentyczności z ochroną anonimowości użytkownika.

W klasycznym rozwiązaniu opartym na RSA klient rozpoczyna od przygotowania wiadomości, która ma zostać podpisana. Może nią być na przykład ciąg danych reprezentujący monetę elektroniczną wraz z jej numerem seryjnym. Następnie wybiera losową wartość, określaną jako czynnik zaślepiający. Przy użyciu klucza publicznego banku oraz działań wykonywanych modulo liczba stanowiąca moduł RSA klient tworzy z wiadomości postać zamaskowaną. Z punktu widzenia banku otrzymany ciąg nie ujawnia treści właściwej wiadomości.

Bank wykonuje na zamaskowanym ciągu operację przy użyciu swojego klucza prywatnego. Rezultat przekazuje klientowi.

Klient wykorzystuje następnie znany tylko sobie czynnik zaślepiający, a dokładniej jego odwrotność modularną, dzięki czemu usuwa maskowanie. Wynikiem jest podpis odnoszący się już do właściwej wiadomości, mimo że bank podczas operacji podpisywania nie poznał jej treści. Współczesne konstrukcje RSA blind signatures zachowują właśnie ten ogólny schemat: przygotowanie wiadomości, jej zaślepienie, wykonanie podpisu przez serwer oraz finalizację polegającą na odślepieniu i sprawdzeniu poprawności podpisu.

Najważniejszą własnością takiego protokołu jest ślepość, czyli niemożność ustalenia przez podpisującego, którą z później przedstawionych wiadomości podpisał podczas konkretnej interakcji z klientem. W elektronicznej gotówce pozwala to odtworzyć jedną z podstawowych cech tradycyjnej gotówki. Bank może potwierdzić, że moneta elektroniczna została przez niego prawidłowo wystawiona, ale nie powinien móc stwierdzić, który klient później się nią posłużył. Jeżeli użytkownik wypłaca elektroniczną monetę, a następnie płaci nią sprzedawcy, bank otrzymujący tę monetę do rozliczenia nie powinien być w stanie połączyć jej z wcześniejszą operacją wypłaty.

Właściwość ta różni elektroniczną gotówkę od wielu typowych systemów płatniczych. W przypadku zwykłej płatności elektronicznej operator systemu posiada zazwyczaj dane pozwalające powiązać płatnika, odbiorcę, kwotę i moment transakcji. Ślepy podpis umożliwia natomiast zaprojektowanie systemu, w którym bank potwierdza ważność środka płatniczego, nie otrzymując jednocześnie kompletnej informacji pozwalającej śledzić sposób jego późniejszego wykorzystania.

Anonimowość nie może jednak prowadzić do możliwości samodzielnego tworzenia pieniędzy przez klienta. Drugą podstawową własnością bezpiecznego systemu ślepych podpisów jest więc odporność na fałszowanie. Użytkownik, który uzyskał od banku podpis pod jedną określoną liczbą monet, nie powinien być w stanie wykorzystać przeprowadzonych operacji do utworzenia większej liczby prawidłowych podpisów. W

nowoczesnych analizach bezpieczeństwa ślepych podpisów zwraca się zatem uwagę nie tylko na samą ślepość, ale również na odporność na uzyskiwanie dodatkowych podpisów poza tymi, do których użytkownik był uprawniony.

Jednym z problemów wynikających bezpośrednio ze ślepoty jest właśnie kontrolowanie treści podpisywanej wiadomości. Bank nie może bezkrytycznie wykonywać operacji prywatnym kluczem na dowolnych danych przekazywanych przez klienta. W przeciwnym wypadku klient mógłby próbować wykorzystać bank jako tak zwaną wyrocznię podpisującą i uzyskiwać podpisy pod nieprawidłowo skonstruowanymi obiektami. Dlatego protokół musi zapewniać nie tylko ukrycie treści, ale również możliwość sprawdzenia, że podpisywany obiekt posiada właściwą strukturę.

Klasyczną odpowiedzią na ten problem jest metoda *cut-and-choose*. Jej logika jest stosunkowo prosta. Klient nie tworzy jednego kandydata do podpisania, lecz wiele równoważnych kandydatów. Wszystkie zostają zamaskowane i przesłane bankowi. Bank wybiera losowo jeden z nich, natomiast w odniesieniu do pozostałych żąda ujawnienia danych potrzebnych do sprawdzenia ich prawidłowości. Jeżeli sprawdzone egzemplarze zostały przygotowane zgodnie z regułami, zwiększa się prawdopodobieństwo, że również pozostawiony w ukryciu egzemplarz jest prawidłowy.

Jeżeli przykładowo klient przygotował sto obiektów, a bank losowo wybrał jeden i polecił otworzyć pozostałe dziewięćdziesiąt dziewięć, próba oszustwa polegająca na przygotowaniu tylko jednego nieprawidłowego egzemplarza ma niewielką szansę powodzenia. Oszust musi liczyć na to, że właśnie wadliwy egzemplarz będzie tym jedynym, którego bank nie każe ujawnić. Im większa liczba kandydatów podlegających losowemu sprawdzeniu, tym mniejsze prawdopodobieństwo skutecznego oszustwa. Ceną za zwiększenie bezpieczeństwa jest jednak większa liczba obliczeń i większa ilość przesyłanych danych.

Właśnie z tego powodu technika *cut-and-choose*, mimo swojej przejrzystości, nie jest rozwiązaniem idealnym dla dużych i wydajnych systemów. Generowanie wielu obiektów tylko po to, aby zdecydowana większość została następnie odrzucona, powoduje znaczny narzut obliczeniowy i komunikacyjny. W literaturze dotyczącej elektronicznej gotówki wielokrotnie wskazywano nieefektywność systemów opartych na rozbudowanych procedurach tego rodzaju. Późniejsze konstrukcje kryptograficzne poszukiwały więc sposobów zapewnienia podobnych gwarancji przy mniejszej liczbie operacji.

Jednym z takich rozwinięć są podpisy częściowo ślepe. W klasycznym ślepym podpisie podpisujący nie powinien znać treści podpisywanej wiadomości. W podpisie częściowo ślepym strony mogą natomiast uzgodnić, że pewna część informacji pozostanie jawna. Pozwala to na przykład bankowi znać nominał elektronicznej monety albo termin jej ważności, podczas gdy niepowtarzalny numer służący do identyfikacji samej monety pozostaje ukryty. Rozwiązanie takie może znacznie ułatwić projektowanie praktycznego systemu płatności.

W przypadku nominału możliwe są również inne rozwiązania. Bank może na przykład stosować różne klucze podpisujące dla różnych wartości monet. Jeden klucz służy wówczas do wystawiania monet o wartości jednego złotego, inny monet dziesięciozłotowych, a jeszcze inny monet o większej wartości. Sam fakt wykorzystania określonego klucza pozwala określić nominał, natomiast ukryta pozostaje pozostała treść monety. Takie podejście eliminuje możliwość przedstawienia bankowi monety o większej wartości jako monety o wartości mniejszej, choć równocześnie komplikuje zarządzanie większą liczbą kluczy. Literatura dotycząca elektronicznej gotówki wskazuje właśnie stosowanie różnych kluczy dla poszczególnych nominałów jako jedno z klasycznych rozwiązań tego problemu.

Odrębnym i bardzo ważnym problemem elektronicznej gotówki jest możliwość wielokrotnego wydania tej samej monety. Fizycznego banknotu po przekazaniu sprzedawcy nie posiada już kupujący.

Dane cyfrowe można natomiast kopiować praktycznie bez ograniczeń. Osoba posiadająca plik reprezentujący monetę elektroniczną może więc próbować przesłać identyczny plik kilku sprzedawcom.

Najprostszy sposób zapobiegania takiemu zjawisku polega na wykorzystaniu unikalnego numeru seryjnego każdej monety. Kiedy sprzedawca otrzymuje elektroniczną gotówkę, bank sprawdza, czy dany numer nie znajduje się już w bazie monet wykorzystanych. Jeżeli numer pojawia się po raz pierwszy, płatność może zostać zaakceptowana i numer trafia do bazy. Jeżeli ten sam numer został już wcześniej przedstawiony do rozliczenia, bank stwierdza próbę ponownego wydania tej samej monety.

Takie rozwiązanie wymaga jednak kontaktu z bankiem podczas każdej transakcji albo przynajmniej przed jej ostatecznym zaakceptowaniem. Jest to system typu *online*. Zapewnia stosunkowo prostą ochronę przed podwójnym wydawaniem, ale powoduje konieczność stałej dostępności infrastruktury bankowej. Rozwiązania typu *offline* próbowały pozwolić sprzedawcy przyjąć monetę bez natychmiastowego połączenia z bankiem. W takim przypadku nie zawsze da się zapobiec podwójnemu wydaniu w chwili transakcji, dlatego mechanizmy kryptograficzne projektowano tak, aby możliwe było późniejsze wykrycie oszustwa i w określonych konstrukcjach ustalenie tożsamości osoby, która wykorzystała tę samą monetę więcej niż raz. Klasyczne systemy e-cash wykorzystujące *cut-and-choose* stosowały tę technikę właśnie również w mechanizmach związanych z wykrywaniem podwójnego wydawania.

Istotą dobrze zaprojektowanego systemu jest pogodzenie dwóch z pozoru sprzecznych celów. Uczciwy użytkownik powinien zachować anonimowość, a bank nie powinien mieć możliwości odtworzenia historii jego zakupów. Jednocześnie system nie może zapewniać pełnej bezkarności osobie próbującej wielokrotnie wykorzystać tę samą monetę. W niektórych konstrukcjach informacje identyfikujące właściciela są więc kryptograficznie zakodowane w monecie w taki sposób, że pojedyncza prawidłowa transakcja

ich nie ujawnia, natomiast zestawienie danych pochodzących z dwóch różnych prób wydania tej samej monety pozwala wykryć oszusta.

Ślepe podpisy mają zastosowania znacznie szersze niż sama elektroniczna gotówka. Podobny problem pojawia się na przykład w elektronicznym głosowaniu. System powinien potwierdzić, że osoba oddająca głos jest uprawniona do udziału w wyborach i nie głosuje wielokrotnie, ale jednocześnie nie powinien umożliwiać powiązania konkretnego głosu z konkretnym wyborcą. W takim modelu odpowiednia instytucja może potwierdzić uprawnienie do głosowania bez poznawania treści później wykorzystanej karty wyborczej.

Technika ta może być używana również w systemach anonimowych poświadczeń, tokenów dostępowych i innych mechanizmach ochrony prywatności. Współczesne specyfikacje wskazują zastosowania ślepych podpisów nie tylko w płatnościach, ale także w mechanizmach uwierzytelniania i rozwiązaniach pozwalających oddzielić proces przyznania określonego uprawnienia od jego późniejszego wykorzystania.

Warto jednocześnie zauważyć, że współczesne implementacje nie powinny wykorzystywać wprost najprostszego „podręcznikowego” RSA. Historyczny opis ślepego podpisu jest bardzo przydatny do zrozumienia mechanizmu algebraicznego, ale praktyczne protokoły wymagają odpowiedniego kodowania wiadomości, bezpiecznego generowania liczb losowych oraz ochrony przed atakami wynikającymi z błędnej implementacji. W aktualnej specyfikacji RSA Blind Signatures wykorzystywany jest między innymi mechanizm RSA-PSS, a końcowy podpis może zostać zweryfikowany przy użyciu standardowej procedury weryfikacji RSA-PSS.

Bardzo ważna jest jakość losowego czynnika zaślepiającego. Jeżeli wartości losowe są przewidywalne, wielokrotnie używane albo generowane w niewłaściwy sposób, anonimowość użytkownika może zostać osłabiona. Bezpieczeństwo ślepego podpisu zależy

więc nie tylko od matematycznych własności RSA, lecz również od prawidłowej implementacji całego protokołu. Podobnie jak w innych rozwiązaniach kryptograficznych, silny algorytm może okazać się nieskuteczny, jeżeli zostanie niewłaściwie zastosowany.

Trzeba również pamiętać, że anonimowość zapewniana przez sam podpis nie rozwiązuje wszystkich problemów prywatności. Nawet jeżeli bank nie potrafi matematycznie powiązać podpisanej monety z operacją jej wypłaty, użytkownik może zostać rozpoznany na podstawie innych informacji, na przykład adresu sieciowego, czasu wykonania transakcji, sposobu komunikowania się z systemem czy danych przekazanych sprzedawcy. Pełny system anonimowych płatności musi więc chronić nie tylko treść kryptograficzną transakcji, ale również informacje dodatkowe powstające podczas komunikacji.

Technika ślepych podpisów jest zatem interesującym przykładem rozwiązania kryptograficznego, które umożliwia jednoczesne potwierdzenie autentyczności i ograniczenie wiedzy podmiotu dokonującego podpisu. Bank może zagwarantować, że określony cyfrowy obiekt jest przez niego autoryzowany, nie uzyskując przy tym informacji pozwalających śledzić jego późniejsze wykorzystanie. W tradycyjnym podpisie cyfrowym podpisujący zna dokument, który zatwierdza. W podpisie ślepym relacja ta zostaje celowo przerwana.

Największą trudnością nie jest więc samo wykonanie podpisu, lecz stworzenie całego protokołu gwarantującego, że anonimowość nie będzie wykorzystywana do oszustwa. Konieczne jest kontrolowanie poprawności podpisywanych obiektów, uniemożliwienie tworzenia nieautoryzowanych monet oraz rozwiązanie problemu podwójnego wydawania. Techniki *cut-and-choose*, różne klucze dla różnych nominałów, podpisy częściowo ślepe oraz bardziej zaawansowane protokoły kryptograficzne są różnymi sposobami rozwiązania tych problemów.

Ślepy podpis pokazuje tym samym jedną z najważniejszych

właściwości współczesnej kryptografii: możliwość udowodnienia określonego faktu bez ujawniania wszystkich informacji związanych z tym faktem. Użytkownik może otrzymać potwierdzenie banku, nie pokazując bankowi danych, które pozwoliłyby później śledzić jego transakcję. Z tego względu koncepcja zaproponowana pierwotnie dla anonimowej elektronicznej gotówki stała się podstawą znacznie szerszej grupy rozwiązań służących ochronie prywatności w systemach informatycznych.

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.

Media transmisyjne sieci LAN

Skrętka nieekranowana (UTP – Unshielded Twisted Pair)

Kabel typu UTP składa się ze skręconych ze sobą par przewodów, tworząc linię zrównoważoną (symetryczną). Skręcenie przewodów w stosunku 1 zwój na 6–10 cm chroni transmisję przed zakłóceniami elektromagnetycznymi i interferencjami otoczenia. Ten rodzaj kabla jest powszechnie stosowany w sieciach komputerowych oraz telefonicznych. Istnieje wiele technologii splotu, a poszczególne skrętki mogą różnić się gęstością i sposobem skręcenia przewodów.

Do przesyłania sygnałów w sieciach komputerowych wykorzystuje się skrętki kategorii 3 (10 Mb/s) oraz kategorii 5 (100 Mb/s), przy czym w praktyce powszechnie stosuje się głównie kategorię 5. Skrętki UTP są uniwersalne, stosunkowo tanie i łatwe w

instalacji, co czyni je najpopularniejszym medium transmisyjnym w sieciach lokalnych.

Skrętka foliowana (FTP – Foiled Twisted Pair)

Skrętka FTP jest ekranowana folią z przewodem uziemiającym, co zapewnia dodatkową ochronę przed zakłóceniami elektromagnetycznymi. Jest przeznaczona głównie do budowy sieci komputerowych w środowiskach o dużym poziomie interferencji. Tego typu kabel jest stosowany także w sieciach Gigabit Ethernet (1 Gb/s), przy wykorzystaniu wszystkich czterech par przewodów.

Skrętka ekranowana (STP – Shielded Twisted Pair)

STP różni się od FTP tym, że ekran stanowi oplot otaczający przewody oraz dodatkowa zewnętrzna koszulka ochronna. W związku z rosnącymi wymaganiami europejskich norm EMC dotyczących emisji zakłóceń elektromagnetycznych (EMI), zastosowanie skrętek ekranowanych STP staje się coraz bardziej istotne w nowych instalacjach.

Hybrydowe rozwiązania:
FFTP – każda para przewodów otoczona jest osobnym ekranem z folii, a cały kabel dodatkowo pokryty jest folią.
SFTP – każda para przewodów posiada własny ekran z folii, a cały kabel jest dodatkowo pokryty oplotem. Takie hybrydy łączą zalety różnych typów ekranowania, zwiększając odporność na zakłócenia.

Kategorie skrętek miedzianych

Kategorie kabli miedzianych określono w specyfikacji EIA/TIA. Przydatność kabla do transmisji określa się w MHz:
Kategoria 1 – tradycyjna nieekranowana skrętka telefoniczna,

przeznaczona do przesyłania głosu, nie nadaje się do transmisji danych.
Kategoria 2 – nieekranowana skrętka o szybkości transmisji do 4 MHz, z dwoma parami skręconych przewodów.
Kategoria 3 – skrętka o szybkości transmisji do 10 MHz, stosowana w sieciach Token Ring (4 Mb/s) oraz Ethernet 10Base-T (10 Mb/s), z czterema parami przewodów.
Kategoria 4 – skrętka działająca z prędkością do 16 MHz, zbudowana z czterech par przewodów.
Kategoria 5 – skrętka z dopasowaniem rezystancyjnym, umożliwiająca transmisję danych z prędkością 100 MHz na odległość do 100 m, przy prawidłowej instalacji zgodnie z wymaganiami okablowania strukturalnego.
Kategoria 5e (enhanced) – ulepszona wersja kategorii 5, zalecana w przypadku nowych instalacji, zapewniająca lepszą jakość transmisji i większą odporność na przesłuchy.
Kategoria 6 – skrętka umożliwiająca transmisję z częstotliwością do 200 MHz, odpowiednia dla nowoczesnych sieci Ethernet 1 Gb/s i 10 Gb/s w krótkim zasięgu.
Kategoria 7 – kabel o przepustowości do 600 MHz, wymagający nowych typów złączy, a każda para przewodów jest ekranowana oddzielnie.

Skrętki produkowane są w znormalizowanych średnicach, podawanych w jednostkach AWG, oraz mogą zawierać różną liczbę par. W sieciach komputerowych standardem są skrętki czteroparowe. Ze względu na fakt, że kategoria 6 nie jest jeszcze w pełni zatwierdzona normami międzynarodowymi, oraz w obliczu rosnącej dostępności i spadającego kosztu łączy światłowodowych, istnieje perspektywa, że w niedalekiej przyszłości struktury oparte na światłowodach mogą być bardziej opłacalne niż instalacje z kabli miedzianych kategorii 6.

Kabel współosiowy (koncentryczny)

Kabel koncentryczny składa się z dwóch przewodów umieszczonych

jeden wewnątrz drugiego, co zwiększa odporność na zakłócenia i poprawia jakość transmisji. Wewnętrzny przewód, wykonany z drutu lub linki miedzianej, stanowi rdzeń (przewód gorący), natomiast zewnętrzny przewód pełni funkcję ekranu w postaci oplotu.

Stosuje się kable koncentryczne o impedancji falowej 50 i 75 Ohm. Kable 50 Ohm wykorzystuje się m.in. w sieciach komputerowych.
Cienki Ethernet (Thin Ethernet, 10Base-2) – kabel RG-58 o średnicy ½" i maksymalnej długości segmentu 185 m. Stosowany tam, gdzie wymagane są połączenia dłuższe niż 100 m.
Gruby Ethernet (Thick Ethernet, 10Base-5) – kable RG-8 i RG-11 o średnicy ¼" i długości segmentu do 500 m. Obecnie rzadko spotykany, wykorzystywany jedynie w bardzo starych sieciach.

Zalety kabli współosiowych: wysoka odporność na zakłócenia i szumy, możliwość przesyłania sygnałów szerokopasmowych, niższy koszt w porównaniu z ekranowanymi skrętkami. Obecnie stosowane głównie w małych sieciach do 3–4 komputerów, przy czym ich wadą jest większa awaryjność instalacji w porównaniu do skrętek.

Kabel światłowodowy

Transmisja światłowodowa polega na prowadzeniu promieni świetlnych przez włókno szklane, generowanych przez laserowe źródło światła. Dzięki minimalnym stratom i odporności na pola elektromagnetyczne, światłowód jest obecnie najbardziej wydajnym medium transmisyjnym.

Kabel światłowodowy może zawierać od jednego do kilkudziesięciu włókien. Rdzeń wykonany jest zwykle z domieszkowanego dwutlenku krzemu, otoczony płaszczem ze szkła czystego (SiO_2) i zabezpieczony osłoną buforową. Włókno zapewnia całkowite wewnętrzne odbicie promieni świetlnych dzięki różnicy współczynnika załamania światła między rdzeniem a płaszczem. Zewnętrzna warstwa buforowa wykonana z akrylonu

poprawia elastyczność i chroni włókno przed uszkodzeniami, nie wpływając na właściwości transmisyjne.

Światłowody dzielą się na jedno- i wielomodowe. Jednomodowe oferują większe pasmo przenoszenia i większy zasięg, ale są droższe. W transmisji full-duplex zwykle stosuje się dwa włókna do przesyłania sygnałów w obie strony, choć istnieją rozwiązania umożliwiające transmisję dwukierunkową jednym włóknem.

Zalety światłowodów obejmują większą przepustowość w porównaniu do kabli miedzianych, małe straty sygnału, odporność na zakłócenia elektromagnetyczne, brak przesłuchów międzykablowych, niewielką masę i rozmiary, wysoką niezawodność oraz relatywnie niski koszt, który ciągle spada.

Kabel światłowodowy, jako nowoczesne medium transmisyjne, cechuje się nie tylko wysoką przepustowością, ale również wyjątkową odpornością na zakłócenia elektromagnetyczne. Światłowody są obecnie wykorzystywane zarówno w sieciach lokalnych, jak i w sieciach dalekiego zasięgu, w tym w sieciach telekomunikacyjnych i centrach danych. Jednym z podstawowych parametrów włókna światłowodowego jest jego konstrukcja, która decyduje o rodzaju transmisji. Włókna dzielą się na jednomodowe (single-mode, SMF) oraz wielomodowe (multi-mode, MMF). Włókna jednomodowe charakteryzują się bardzo małym rdzeniem o średnicy około 8–10 µm, co pozwala na przesyłanie jednego promienia świetlnego wzdłuż włókna, minimalizując zjawisko dyspersji modalnej. Dzięki temu światłowody jednomodowe oferują transmisję na odległości rzędu kilkudziesięciu, a nawet kilkuset kilometrów bez potrzeby stosowania wzmacniaczy sygnału. Z kolei włókna wielomodowe mają większy rdzeń, zazwyczaj o średnicy 50 lub 62,5 µm, co umożliwia przesyłanie wielu modów światła równocześnie. Transmisja w światłowodach wielomodowych jest jednak ograniczona z powodu dyspersji, co zmniejsza maksymalną odległość przesyłania danych, ale pozwala na niższy koszt okablowania i prostsze źródła światła, takie jak diody LED.

Ważnym parametrem światłowodu jest jego tłumienie, wyrażane w decybelach na kilometr (dB/km). Tłumienie określa, jak dużo energii sygnału optycznego jest tracone na każdym kilometrze włókna. Dla włókien jednomodowych w zakresie długości fali 1310–1550 nm tłumienie wynosi zwykle około 0,2–0,35 dB/km, co pozwala na przesyłanie danych na bardzo duże odległości bez znacznej degradacji sygnału. W przypadku włókien wielomodowych tłumienie jest wyższe, około 0,5–3 dB/km, co ogranicza ich zastosowanie do sieci lokalnych i kampusowych.

Kabel światłowodowy składa się z kilku warstw ochronnych. Rdzeń i płaszcz tworzą zasadnicze włókno, natomiast kolejne warstwy obejmują warstwę buforową, aramidowy wzmacniacz (np. kevlar), oraz powłokę zewnętrzną wykonaną z tworzywa sztucznego odpornego na ścieranie, promieniowanie UV i czynniki atmosferyczne. Niektóre kable są dodatkowo wypełnione żelem lub wyposażone w rurki żelowe, co zapewnia ochronę przed wilgocią. Kable światłowodowe mogą być jedno- lub wielowłóknowe, a ich liczba może sięgać nawet kilkudziesięciu włókien w jednym przewodzie, co pozwala na budowę sieci o bardzo dużej przepustowości.

Metody transmisji w światłowodach obejmują systemy oparte na modulacji amplitudy, fazy lub częstotliwości światła, jak również bardziej zaawansowane techniki, takie jak WDM (Wavelength Division Multiplexing), czyli multipleksacja falowa. Dzięki WDM możliwe jest przesyłanie wielu niezależnych kanałów światła wzdłuż tego samego włókna, co zwiększa całkowitą przepustowość łącza nawet kilkudziesięciokrotnie w porównaniu do tradycyjnych metod transmisji. W sieciach nowej generacji stosuje się także DWDM (Dense Wavelength Division Multiplexing), pozwalający na bardzo gęste upakowanie kanałów, co umożliwia przesyłanie setek terabitów danych na godzinę na jednym włóknie.

Światłowody są również praktyczne w kontekście instalacji. Mogą być układane w rurkach kanalizacyjnych, na liniach napowietrznych, w kanałach kablowych czy w tunelach

podziemnych. Instalacja wymaga jednak precyzyjnego traktowania włókien, ponieważ nawet niewielkie zgięcie może powodować straty sygnału lub złamanie włókna. Dlatego kable światłowodowe posiadają określony promień gięcia minimalnego, którego nie wolno przekraczać podczas montażu. W celu łączenia włókien stosuje się spawanie optyczne lub złącza mechaniczne, które muszą zapewniać minimalne straty sygnału i zachować parametry transmisyjne.

Światłowody znajdują zastosowanie nie tylko w sieciach telekomunikacyjnych i internetowych, ale także w medycynie, systemach monitoringu, przemyśle energetycznym oraz systemach automatyki przemysłowej. Dzięki niewielkim rozmiarom i masie, a także wysokiej odporności na zakłócenia elektromagnetyczne, światłowody są idealnym medium do przesyłania dużych ilości danych w trudnych warunkach środowiskowych.

Kabel światłowodowy stanowi obecnie najbardziej wydajne i przyszłościowe medium transmisyjne, łącząc wysoką przepustowość, niskie straty, odporność na zakłócenia oraz możliwość budowy sieci dalekosiężnych i lokalnych. Dzięki rozwojowi technologii modulacji i multipleksacji, a także spadającemu kosztowi instalacji, światłowody stają się standardem w nowoczesnych sieciach informatycznych i telekomunikacyjnych.

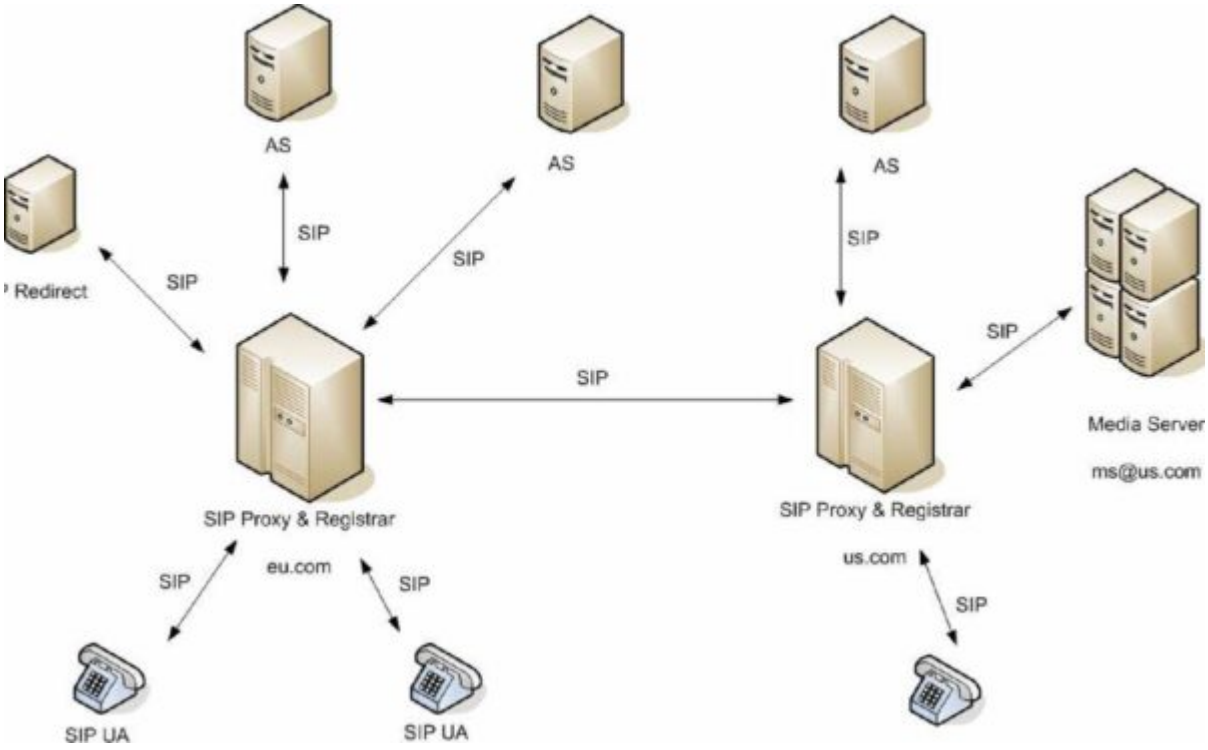
Jeśli szukają Państwo pomocy w napisaniu własnej pracy - potrzebują Państwo fachowych konsultacji to polecamy stronę pisanie prac - profesjonalna pomoc w pisaniu prac w granicach prawa.

Sieć VOIP wg architektury

zdefiniowanej dla protokołu SIP

Najprostszy typ sieci VOIP stanowi architektura zdefiniowana w specyfikacji protokołu SIP. Wzbogacając ją o elementy takie jak serwery aplikacji oraz serwer mediów, można w jej ramach realizować szeroki zbiór usług telekomunikacyjnych.

Architekturę tej sieci zilustrowano na poniższym rysunku:



Rys. 3 Przykładowa sieć VOIP oparta na architekturze zdefiniowanej dla protokołu SIP

Rola, jaką pełnią dodatkowe elementy, jest następująca:

- Serwer Aplikacji (AS) – jest to blok funkcjonalny, który przechowuje logikę usług telekomunikacyjnych zaimplementowaną w postaci aplikacji usługowych. Logika aplikacji określa, w jaki sposób AS przetwarza wiadomości SIP. AS zawiera blok funkcjonalny B2BUA.
- Serwer mediów – blok odpowiedzialny za operacje na

strumieniach audio i video,

Przyjęcie założenia, że każdy element zilustrowanej na powyższym rysunku sieci jest postrzegany przez inne elementy jako agent użytkownika SIP UA (którego logika przetwarzania wiadomości SIP wynika z pełnionej funkcji), upraszcza integrowanie wprowadzanych do sieci kolejnych elementów funkcjonalnych, uczestniczących w procesie sterowania sesjami (np. bramy medialne – Media Gateways).

Rozszerzalność powyższej sieci VOIP wynika również z faktu, iż terminale użytkownika, implementujące agentów SIP, to często aplikacje działające na maszynach typu PC podłączonych do sieci Internetu. W związku z tym serwery aplikacji mogą integrować funkcje SIP UA z funkcjami serwerów HTTP, WWW, FTP etc. Poszerza to znacząco spektrum możliwych do zrealizowania usług telekomunikacyjnych.

Sieć VoIP zbudowana zgodnie z architekturą protokołu SIP opiera się na fundamentalnym rozdzieleniu płaszczyzny sygnalizacyjnej i płaszczyzny mediów. SIP odpowiada za zestawienie, modyfikację i zakończenie połączeń, natomiast sama transmisja głosu odbywa się strumieniowo w RTP z nadzorem jakości przez RTCP. Ten podział pozwala skalować system, niezależnie dobierać kodeki, stosować różne mechanizmy zapewnienia jakości usług oraz wprowadzać zaawansowane funkcje, od przekierowań i forkingu po konferencje wielostronne. Kluczowe jest to, że SIP jest protokołem tekstowym, transakcyjnym i rozszerzalnym, co ułatwia jego analizę, debugowanie i integrację z innymi usługami czasu rzeczywistego.

Podstawowymi elementami architektury są użytkownicy końcowi, czyli User Agents, które działają jako User Agent Client i User Agent Server w zależności od kierunku komunikacji. Urządzenia te, czy to telefony IP, softphony, czy bramki ATA, rejestrują się w domenie SIP, publikując swój aktualny adres kontaktowy w serwerze rejestracji. Proces rejestracji

realizowany jest komunikatami REGISTER i powoduje aktualizację bazy lokalizacyjnej, zwykle określanej jako location service. Dzięki temu, gdy do abonenta kierowane jest wywołanie, serwer pośredniczący ma wiedzę, dokąd przekazać sygnalizację. Ta logika umożliwia mobilność użytkownika, jego wielopunktową dostępność oraz równoczesne dzwonienie wielu urządzeń przypisanych do jednego identyfikatora.

Ruch sygnalizacyjny przechodzi przez serwery proxy, które mogą działać w trybie bezstanowym lub z utrzymywaniem stanu transakcji, a w bardziej złożonych wdrożeniach w postaci B2BUA, czyli Back-to-Back User Agent. O ile proxy pośredniczy i przekazuje komunikaty, o tyle B2BUA kończy dialog od strony jednego abonenta i inicjuje nowy od strony drugiego, co pozwala na dogłębną kontrolę wywołania, wstrzykiwanie polityk, nagrywanie lub rozliczanie bez ujawniania topologii. Uzupełnieniem są serwery przekierowań, które nie pośredniczą w strumieniu sygnalizacyjnym, lecz informują inicjatora, dokąd wysłać kolejne żądanie. W sferze operatorów i granic sieci działa Session Border Controller, który realizuje **topology hiding**, inspekcję sygnalizacji, translację adresów i portów, egzekwowanie polityk bezpieczeństwa oraz ochronę przed atakami na warstwę SIP i RTP.

Zestawienie połączenia odbywa się zwykle sekwencją INVITE, 1xx odpowiedzi wstępnych, 200 OK z opisem sesji i ACK potwierdzającym parametry. Negocjacja mediów zachodzi przez SDP, gdzie strony uzgadniają kodeki, kierunki strumieni, porty i ewentualnie zabezpieczenia. SIP umożliwia **early media**, czyli przesył dźwięku zanim nastąpi finalne 200 OK, co jest użyteczne dla zapowiedzi i sygnałów sieciowych. W sytuacjach wymagających niezawodnego potwierdzania odpowiedzi wstępnych stosuje się rozszerzenie 100rel i komunikaty PRACK. Rozbudowane scenariusze połączeń wykorzystują REFER do przekazywania rozmów, SUBSCRIBE/NOTIFY dla obecności i monitoringu stanu, a INFO lub RFC 4733 do sygnalizacji DTMF, gdy konieczne jest zdalne sterowanie IVR lub bramką płatniczą.

W warstwie mediów wybór kodeków determinuje opóźnienie, przepływność i odporność na straty. G.711 zapewnia prostotę i wysoką wierność kosztem przepływności, G.729 redukuje pasmo kosztem licencji i artefaktów, a współczesne rozwiązania chętnie sięgają po **Opus** z adaptacyjnym bitrate i dobrą odpornością na jitter. Niezależnie od kodeka końcowe wrażenia użytkownika poprawiają bufor jittera, eliminacja echa, PLC naprawiający straty ramek oraz odpowiednia priorytetyzacja pakietów w sieci. Parametry jakości ocenia się modelami E-model (R-factor) i MOS, przy czym na percepcję wpływa nie tylko opóźnienie end-to-end i jitter, ale także zmienność trasy, kolejkowanie i korekcje błędów.

Skuteczne wdrożenie VoIP w oparciu o SIP wymaga świadomego zaprojektowania DNS. Domena telefoniczna publikuje rekordy NAPTR i SRV, wskazując preferencje względem transportu (UDP, TCP, TLS) i priorytety serwerów. Pozwala to na przełączanie awaryjne i równoważenie obciążenia bez ingerencji w konfigurację użytkowników. W środowiskach o wysokiej dostępności klastrowane rejestratory współdzielą stan, a serwery proxy korzystają z mechanizmów hashujących dialogi, aby utrzymać spójność transakcji. Przy połączeniach międzydomenowych często stosuje się federację przez SBC, a w rozwiązaniach operatorskich integrację z IMS, gdzie SIP pozostaje rdzeniem, ale jest obudowany funkcjami P-CSCF, S-CSCF i HSS.

Trwałym wyzwaniem w architekturze SIP jest translacja NAT i zapory. Ponieważ media płyną bezpośrednio między końcami, a adresy i porty są negocjowane w SDP, mechanizmy NAT potrafią zerwać sesję, jeśli nie zastosuje się odpowiednich rozwiązań. Standardowy zestaw obejmuje **STUN** do odkrywania publicznych mapowań, **TURN** dla relaying’u mediów, gdy NATy są symetryczne, oraz **ICE**, który automatycznie wybiera najlepszą ścieżkę kandydatów. Na granicach sieci często dodatkowo działa ALG modyfikujący SIP w locie, lecz bywa on źródłem problemów i kolizji z ICE; dojrzałe wdrożenia preferują wyłączenie ALG i

poleganie na SBC oraz mechanizmach klienta.

Bezpieczeństwo warstwy sygnalizacji i mediów wymaga odrębnej uwagi. Szyfrowanie sygnalizacji realizowane jest przez **TLS** na porcie 5061 lub kanał SIPS, natomiast media zabezpiecza **SRTP** z wymianą kluczy przez SDES, DTLS-SRTP albo MIKEY. To ostatnie ma znaczenie w środowiskach o podwyższonych wymaganiach poufności, takich jak opieka zdrowotna czy sektor finansowy. Ochrona przed nadużyciami obejmuje limity transakcji, listy reputacyjne, przeciwdziałanie nadużyciom typu toll fraud, a także uwierzytelnianie digest z politykami haseł i, coraz częściej, integrację z **OAuth** lub certyfikatami klienta. W domenie publicznej telefonii IP wdraża się podpisy wywołań (np. STIR/SHAKEN), aby ograniczyć spoofing numerów i robocalling.

Na brzegu między VoIP a siecią PSTN pracują bramy medialne łączące SIP z ISDN PRI, SS7 lub SIP-I. To w tym miejscu wykonywane są mapowania planów numeracyjnych, translacja sygnalizacji, transkodowanie kodeków i obsługa usług analogowych, takich jak fax przez **T.38** lub fallback do G.711 pass-through. Z punktu widzenia przedsiębiorstwa popularnym wzorcem jest „hosted PBX” lub „SIP trunking”, gdzie centrala IP-PBX komunikuje się z operatorem przez bezpieczny trunk TLS/SRTP, a polityki wyjściowe definiują routing po prefiksach, kosztach i jakości. W centrach kontaktowych do architektury dołącza się serwery kolejkowania, IVR z ASR/TTS, nagrywanie zgodne z reżimami prawnymi oraz integrację z CRM przez webhooki SIP i zdarzenia CTI.

SIP nie ogranicza się do rozmów głosowych. Z tym samym szkieletem działa **presence i instant messaging** w ramach SIMPLE, wideokonferencje z centralnym „focus”, współdzielenie treści z BFCP, a w systemach hybrydowych czat i transfer plików może przejmować **MSRP**. Dzięki temu jeden mechanizm rejestracji, autoryzacji i routingu obsługuje wielokanałową komunikację, co ma znaczenie w środowiskach zdalnej pracy i w aplikacjach klientowskich, gdzie użytkownik płynnie przełącza

się między urządzeniami.

Jakość w trakcie eksploatacji utrzymuje się przez zarządzanie QoS w warstwie IP. Pakiety RTP są znakowane DSCP na poziomie AF/EF, a sieć szkieletowa wymusza odpowiednie kolejki i bufory. W łączach wąskopasmowych pomocne są techniki kształtowania ruchu i policery, które chronią rozmowy przed zakłóceniami spowodowanymi przez bursty danych. Dostępność usług VOIP poprawia się przez georedundancję, anycast DNS, aktywne monitorowanie ścieżek oraz automatyczny **re-INVITE** lub **UPDATE** w razie zmiany parametrów mediów. Dobrą praktyką jest też stosowanie krótkich czasów keep-alive na UDP oraz mechanizmów SIP Outbound w mobilnych i niestabilnych sieciach.

Z punktu widzenia operacyjnego nie do przecenienia są narzędzia obserwowalności. Analiza drabinek SIP, korelacja Call-ID i tagów dialogu, inspekcja SDP i znaczników CSeq pozwalają szybko diagnozować przyczyny 4xx i 5xx, pętle routingu czy błędy autoryzacji. Na warstwie RTP ocenia się jednolicie jitter, straty, opóźnienie i MOS, wykorzystując RTCP XR, raporty QoE oraz dane z buforów jittera w endpointach. Testy obciążeniowe z generatorami SIP i mediów, profile ruchowe z forkingiem oraz scenariusze failoveru są niezbędne, by potwierdzić, że architektura wytrzyma realne warunki, w tym szczyty ruchowe i nagłe fluktuacje dostępności.

Wreszcie, architektura zgodna z SIP powinna uwzględniać wymagania prawne i krytyczne scenariusze biznesowe. Obsługa połączeń alarmowych wymaga mapowania lokalizacji abonenta i przekazywania jej do odpowiedniego centrum, co bywa realizowane przez bazy LIS i protokoły HELD w środowiskach korporacyjnych. Retencja metadanych i zgodność z RODO lub innymi reżimami prywatności wpływają na to, jakie informacje są logowane i jak długo. Mechanizmy nagrywania muszą uwzględniać przepisy lokalne oraz szyfrowanie w spoczynku i w tranzycie, a polityki zgodności wymuszają granularne role i audyt działań administratorów.

Tak zarysowana sieć VoIP w architekturze SIP łączy elastyczność protokołu tekstowego, modularność komponentów i dojrzałe mechanizmy sieciowe. Projektując ją, warto zaczynać od czytelnego DNS i planu numeracyjnego, dbać o bezpieczne granice dzięki SBC i TLS/SRTP, zapewnić wielościeżkowość dzięki SRV/NAPTR i klastrom registrarów, a w warstwie mediów świadomie zarządzać kodekami, QoS i NAT-traversalem przez ICE. To połączenie dobrych praktyk sygnalizacji, inżynierii IP i bezpieczeństwa sprawia, że SIP pozostaje uniwersalnym szkieletem współczesnej telefonii i usług czasu rzeczywistego.

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.

Gry sieciowe

Jako, że praca ta traktuje o klanach graczy komputerowych należy podać definicję gier sieciowych. Klany graczy komputerowych mogą tworzyć się tylko wokół gier, które posiadają opcję gry przez Internet lub sieć lokalną LAN.

„Gra sieciowa (gra internetowa, gra wieloosobowa, multiplayer, sieciówka, tryb sieciowy, tryb wielu graczy) – bardzo ogólne określenie na gry, które umożliwiają dwóm lub więcej graczom na rywalizację lub współpracę za pośrednictwem sieci komputerowej; każdy z graczy grających w *grę sieciową* ma do dyspozycji własny komputer; jeden z komputerów, przeważnie posiadający największą moc służy jako serwer gry, czyli w praktyce gra toczy się właśnie na nim, czyniąc z pozostałych komputerów jedynie odbiorców i nadawców informacji o poczynaniach poszczególnych graczy.”[1]

Należy zaznaczyć, że grą sieciową może być każda gra

posiadająca opcję rozgrywania potyczek przez wielu graczy jednocześnie w czasie rzeczywistym – zarówno gra zdefiniowana wcześniej jako zręcznościowa (FPS – first person shooter), strategiczna (RTS – real time strategy) czy RPG (roleplaying game).

Co miesiąc w świecie komputerów ukazuje się od kilkunastu do kilkudziesięciu nowych gier. Ogromna większość z nich daje możliwość zabawy z innymi graczami przez Internet. W sieci popularne są niemal wszystkie rodzaje gier: strzelanki, strzelanki taktyczne, RTS i RPG (strategiczne i role-playing), symulacje i gry sportowe:

„**Strzelanki** są pisane głównie z myślą o grze w Internecie, stąd też cieszą się w Sieci największą popularnością. W klasycznych trójwymiarowych strzelankach (takich jak „Quake", „Unreal Tournament" czy „Half-Life") najbardziej wciągająca jest bardzo szybka akcja: wymiany ognia są niezwykle dynamiczne, a od gracza wymagana jest zręczność i doskonała orientacja w trójwymiarowej przestrzeni gry. Każda z tych gier wymaga trochę innego stylu walki. Niewielki asortyment bardzo konfrontacyjnych broni w Quake'u powoduje, że w tej grze najważniejsza jest zręczność i refleks. Unreal Tournament zawiera znacznie bardziej rozbudowany zestaw broni, stąd rozgrywka staje się mniej zręcznościowa, a bardziej taktyczna. Ciekawostką w tym gronie jest „Alien vs Predator", w której to grze można wcielić się w postać Obcego. Nie dość, że Obcy może biegać po suficie, to jeszcze nie potrafi atakować na odległość – musi zaczaić się w ciemnym rogu i czekać, aż przeciwnik podejdzie blisko. W Polsce najbardziej rozpowszechnionymi grami są „Quake" i „Unreal Tournament". Zwolennicy tych gier mogą liczyć w każdej chwili na możliwość zabawy na kilkudziesięciu serwerach."[2]

Odrębną kategorię gier internetowych stanowią **strzelaniny taktyczne**, symulujące operacje przeprowadzane przez wojskowe lub policyjne oddziały specjalne. Tu niekwestionowany prym wiedzie dodatek do „Half-Life'a" – „Counter-Strike".

Praktycznie nie ma kafejki internetowej, w której by nie istniał jakiś klan graczy specjalizujący się w tej grze. Mniej popularne są „Rainbow Six” oraz dwa dodatki do „Unreal Tournament”: „Strike Force” i „Tactical Ops”. O ile liczbę serwerów CS w Polsce można liczyć w dziesiątkach i setkach, miłośnicy SF i TO muszą się zadowolić zaledwie kilkoma. Wszystkie strzelanki taktyczne osadzone są w podobnych realiach: rozgrywkę prowadzą dwa zespoły, z których jeden reprezentuje siły porządku (wojsko, policja), a drugi tzw. chaosu (terroryści, spiskowcy itp.). Do dyspozycji jest zawsze dość duży arsenał, na który składają się wirtualne kopie rzeczywistych broni. Używa się więc pistoletów, pistoletów maszynowych, karabinów i karabinów snajperskich, a magazynki potrafią się kończyć w najmniej odpowiednich momentach. Dodatkowo można wykorzystywać różnego rodzaju granaty: od zwykłych przez oślepiające na dymnych skończywszy. Rozgrywka opiera się wyłącznie na ostrożnej, przemyślanej grze zespołowej (każdy gracz ma tylko jedno wirtualne życie). Przykładowo, aby przejść przez drzwi, często wymagana jest współpraca trzech osób: dwie asekurują boki, trzecia przechodzi. Nie ma miejsca na bohaterów – wirtualne cmentarze są ich pełne.[3]

Gry strategiczne i role-playing cieszą się w Internecie wielką popularnością. Ich największą atrakcją jest różnorodność partnerów (przeciwników), a o tych w globalnej sieci nietrudno. Do najpopularniejszych sieciowych RPG w Polsce należy zaliczyć „Diablo” oraz „Ultima Online”. Realia gier tego typu są różne, od czysto baśniowych krain, wypełnionych magami i monstrami, do światów technologicznie zaawansowanych (np. gra „Star Wars Galaxies” osadzona w realiach filmów z serii „Gwiezdne Wojny”). Wszędzie idea jest jednak taka sama: tworzy się swoją postać (lub postaci), których cechy stopniowo rozwijane są w czasie gry. Do tego dochodzi kwestia wyposażenia, które trzeba znaleźć, zdobyć, kupić lub wymienić. Można śmiało założyć, że o dowolnej porze dnia i nocy w Polsce gra przynajmniej kilkadziesiąt, a w szczytowych momentach

nawet kilkaset osób. Nie mniej jest miłośników strategii – tu dużą popularnością cieszą się starsze, lecz doskonałe tytuły: „Warcraft III”, „Starcraft” itp.[4]

„Ciekawą odmianą gier internetowych są **gry symulacyjne i sportowe**. Pierwsze pozwalają na wirtualne loty samolotami (tu godne polecenia są: doskonała symulacja Su-27 – Flanker 2.0 oraz darmowy symulator lotniczy Warbirds) czy różnego rodzaju wyścigi samochodowe, drugie – umożliwiają wirtualną grę w piłkę nożną bądź koszykówkę (przykładem może być legendarna seria FIFA). Niestety, gry te są znacznie mniej popularne i znalezienie dobrego serwera, najlepiej polskiego, może być kłopotliwe. W większości przypadków pojedynki internetowe toczą się w tej grupie gier między dwoma graczami, którzy „odnaleźli” się w sieci dzięki serwisom WWW związanym z daną grą.”[5]

Gry sieciowe jest to więc kategoria gier komputerowych, w których gracze mogą rywalizować lub współpracować ze sobą za pośrednictwem internetu lub sieci lokalnej. Stanowią istotny element współczesnej rozrywki cyfrowej i są popularne wśród osób w różnym wieku.

Cechy gier sieciowych:

- **Interakcja społeczna**: gracze mogą komunikować się za pomocą czatów, głosowych lub wizualnych form kontaktu.
- **Aktualizacje i rozwój**: twórcy gier często wprowadzają nowe funkcje, postacie, mapy i wydarzenia.
- **Rywalizacja i współpraca**: gry sieciowe oferują tryby kooperacyjne, rywalizacyjne lub hybrydowe.
- **Turnieje i e-sport**: wiele tytułów jest podstawą profesjonalnych rozgrywek, z ogromnymi nagrodami pieniężnymi i szeroką widownią.

Zalety:

- Budowanie umiejętności pracy zespołowej i strategii.

- Możliwość rywalizacji z graczami z całego świata.
- Rozwijanie refleksu i zdolności szybkiego podejmowania decyzji.

Wady:

- Możliwość uzależnienia od gry.
- Wysokie wymagania sprzętowe i konieczność stałego dostępu do internetu.
- Zagrożenia związane z toksyczną społecznością lub oszustwami (tzw. „cheaty”).

Gry sieciowe pozostają jednym z najbardziej dynamicznie rozwijających się segmentów branży gier, wpływając na kulturę, technologie i sposób, w jaki ludzie nawiązują relacje w cyfrowym świecie.

---

[1] Słownik Gracza – Gry Online http://www.gry-online.pl/slownik_gracza.asp

[2] Gry Online – Gazeta.pl http://www2.gazeta.pl/gry/1,32238,380036.html

[3] Gry Online – Gazeta.pl http://www2.gazeta.pl/gry/1,32238,380036.html

[4] Gry Online – Gazeta.pl http://www2.gazeta.pl/gry/1,32238,380036.html

[5] Gry Online – Gazeta.pl http://www2.gazeta.pl/gry/1,32238,380036.html

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.