LABORATORIUM SIECI WIELOUSŁUGOWYCH

# Architektura DiffServ

**POLITECHNIKA WARSZAWSKA**

INSTYTUT TELEKOMUNIKACJI

Warszawa, 2015

# 1 Wstęp

Wymaganie zapewnienia zróżnicowanej jakości przekazu pakietów w sieciach opartych na technice IP (Internet Protocol) jest bezpośrednio związane z przyjętą koncepcją ewolucji sieci IP w kierunku tzw. sieci wielo-usługowej (Multi-service Network), czyli sieci umożliwiającej przekaz ruchu generowanego przez różne typy aplikacji (np. mowa, dane, wideo) i, w związku z tym, wymagającego różnych gwarancji dotyczących przekazu pakietów. Gwarancje te są określane przez tzw. parametry jakościowe (Quality of Service - QoS), nazywane w dalszej części parametrami QoS, które dotyczą np. charakterystyk opóźnień przekazu pakietów (np. średni czas przekazu pakietu, maksymalny dopuszczalny czas przekazu pakietu, itd.), dopuszczalnego poziomu strat pakietów, średniej szybkości przekazu pakietów, itp. Sieć IP zapewniającą zróżnicowanie jakości przekazu pakietów nazywamy siecią IP QoS.

Obecnie eksploatowana sieć IP nie ma zaimplementowanych mechanizmów różnicowania jakości przekazu pakietów, a zatem pakiety generowane przez różne typy aplikacji są przesyłane w sieci wg takich samych zasad, korzystając z jedynej dostępnej usługi sieciowej nazywanej usługą best effort (w wolnym tłumaczeniu nazywanej „usługą największego wysiłku sieci", czy po prostu „usługą standardową"). Oznacza to, iż przykładowo, pakiety generowane przez aplikację wymagającą określonych gwarancji na dopuszczalny czas przekazu (np. maksymalny czas przekazu 150 ms dla aplikacji VoIP – Voice over IP) są obsługiwane w każdym węźle komutacyjnym (ruterze IP) przez tą samą kolejkę z dyscypliną obsługi FIFO (First In First Out), jak pakiety generowane przez aplikacje nie wrażliwe lub mało wrażliwe na opóźnienia przekazu pakietów (np. e-mail, FTP – File Transfer Protocol). Powyższe praktycznie uniemożliwia użytkownikom sieci na korzystanie z aplikacji wymagających jakości przekazu pakietów.

Sieci klasy IP QoS dzielimy na te, które zapewniają ściśle określone gwarancje jakości przekazu pakietów i te, które jedynie zapewniają potencjalnie lepszą jakość przekazu dla wybranych strumieni pakietów. W pierwszym przypadku sieci te określamy jako sieci oferujące ścisłe gwarancje QoS (strict-QoS), zaś w drugim przypadku jako sieci oferujące względne gwarancje QoS (relative-QoS). Zapewnienie ścisłych gwarancji QoS wymaga ograniczenia obciążenia ruchowego sieci, co jest realizowane przez zastosowanie funkcji przyjmowania nowych wywołań (Admisssion Control - AC). Funkcjonalność ta nie jest konieczna dla zapewnienia względnych gwarancji QoS. Jednakże, w obu dyskutowanych klasach sieci IP QoS muszą być

zaimplementowane odpowiednie metody dla zapewnienia zróżnicowania jakości przekazu pakietów.

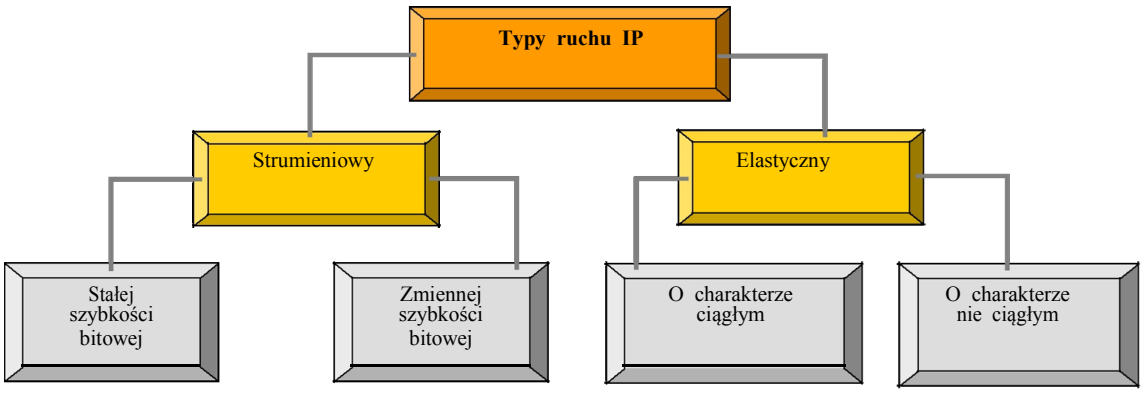
Zastosowane metody różnicowania jakości przekazu pakietów w istotny sposób są związane z przyjętą architekturą sieci oraz założonymi usługami sieciowymi (Network Services). Dla realizacji sieci IP QoS, poza prostymi rozszerzeniami obecnej architektury sieci IP, wypracowano dwie nowe architektury, architekturę dla integracji usług sieciowych (Integrated Services - IntServ) oraz architekturę dla zróżnicowania jakości przekazu pakietów w ramach dostępnych usług sieciowych (Differentiated Services - DiffServ). Dla każdej z wymienionych architektur sieciowych zdefiniowano podstawowe mechanizmy pozwalające na różnicowanie przekazu pakietów w węzłach sieci. W odróżnieniu do architektury DiffServ, architektura IntServ wymaga zastosowania sygnalizacji dla zestawienia i utrzymania każdego połączenia w sieci. Z tego powodu, architektura IntServ została uznana jako architektura charakteryzująca się słabymi własnościami skalowalności i nie jest rozwijana. Zatem, architektura DiffServ jest obecnie uważana jako jedyna pozwalająca na zapewnienie ścisłych gwarancji QoS w sieci IP. Jednakże, wzbogacenie obecnej sieci IP jedynie o wspomniane wyżej mechanizmy dla zróżnicowania przekazu pakietów nie zapewnia, że sieć ma możliwości dla oferowania ścisłych gwarancji QoS.

Celem ćwiczenia jest zapoznanie studentów z mechanizmami QoS dla sieci IP QoS działającymi w oparciu o architekturę DiffServ. W szczególność studenci zbadają wpływ zastsowania mechanizmów na poziomie pakietów, takich jak machanizm klasyfikacji pakietów, szeregowania pakietów, odrzucania pakietów. Ćwiczenie jest wykonywane za pomocą narzędzia symulacyjnego RIVERBED.

# 2 Typy ruchu i wymagania na jakość przekazu w sieciach IP QoS

W sieciach IP QoS wyróżnia się dwa typy ruchu, tj. ruch strumieniowy i ruch elastyczny. Następnie, w ramach ruchu strumieniowego, mamy strumienie pakietów generowane ze stałą szybkością bitową (*Constant Bit Rate - CBR*) lub ze zmienną szybkością bitową (*Variable Bit Rate - VBR*). Źródłem ruchu strumieniowego, niezależnie od tego czy jest on typu CBR czy też VBR, są aplikacje działające w reżimie czasu rzeczywistego. Przykładem aplikacji generującej ruch CBR jest telefonia IP, zaś ruch VBR jest wideo-konferencja. Dla zapewnienia przekazu przez sieć strumienia pakietów w reżimie czasu rzeczywistego wymaga się, aby opóźnienia przekazu poszczególnych pakietów nie przekraczały założonych wartości progowych przy jednoczesnym zachowaniu ich małej zmienności. Dodatkowo, dopuszczalny poziom straty pakietów w sieci również nie powinien być większy niż założony jako dopuszczalny dla danej aplikacji. Tak postawione wymagania wiążą się z koniecznością zagwarantowania właściwej dla danej aplikacji szybkości przekazu pakietów przez sieć. Ruch strumieniowy, w warstwie transportowej, może być obsługiwany np. przez protokół UDP (*User Datagram Protocol*) [RFC0768], bądź też inne protokoły o charakterze bezpołączeniowym. Protokół UDP nie dopuszcza retransmisji utraconych pakietów.

W odróżnieniu do ruchu strumieniowego, ruch elastyczny jest generowany przez źródła posiadające właściwość adaptowania szybkości wysyłania danych w zależności od aktualnych warunków panujących w sieci. Przykładem takiego źródła jest aplikacja korzystająca z protokołu TCP [RFC0793, RFC3168], w dalszej części nazywana źródłem TCP. W przypadku ruchu elastycznego możemy wyróżnić dwa typy ruchu: (1) generowany przez tzw. źródła TCP typu zachłannego (greedy sources), np. aplikację FTP, (2) generowany przez tzw. źródła TCP typu nie zachłannego (non-greedy sources), np. aplikacje TELNET, HTTP, czyli przeglądarki WWW (Word Wide Web), SMTP – poczta elektroniczna, gry interaktywne lub aplikacje realizujące zdalne operacje bankowe. Ruch generowany przez źródła TCP typu zachłannego ma charakter ruchu ciągłego co oznacza, iż aplikacja w ramach połączenia ma zawsze dane do wysłania. Natomiast, ruch generowany przez źródła TCP typu nie zachłannego ma charakter nie ciągły, co oznacza że aplikacja nie zawsze ma dane do wysłania co jest charakterystyczne dla interaktywnych aplikacji elastycznych. Rysunek 2-1 podsumowuje przedstawioną klasyfikację typów ruchu występujących w sieciach IP QoS.




*Rysunek 2-1. Typy ruchu w sieciach IP QoS*

### 2.1. Wymagania na jakość obsługi

Dla sieci IP QoS oferującej ścisłe gwarancje jakości obsługi, wymagania na jakość przekazu pakietów bezpośrednio wynikają z danego typu aplikacji i profilu generowanego przez nią ruchu. W przypadku ruchu CBR, są to wymagania na obsługę w tzw. reżimie czasu rzeczywistego, czyli obsługa powinna gwarantować: bardzo małe opóźnienia pakietów i bardzo małą zmienność opóźnienia (*jitter*), bardzo małe straty pakietów oraz odpowiednią szybkość bitową obsługi pojedynczego strumienia (zgodną z szybkością generowania pakietów przez aplikację). Dla ruchu VBR wymagania na jakość obsługi są podobne jak dla ruchu CBR. W przypadku ruchu elastycznego oczekiwania od sieci są różne w zależności od tego czy dane połączenie dotyczy źródła typu zachłannego czy też nie zachłannego. Dla źródeł TCP typu zachłannego wymaga się, aby dla danego połączenia sieć gwarantowała określoną *a priori* minimalną szybkość bitową. W szczególności, dla przekazu zbioru o danej wielkości, można w ten sposób określić maksymalny czas jego przesłania przez sieć. Dla źródeł TCP typu nie zachłannego zwykle wymaga się, aby poziom strat pakietów był na możliwie niskim poziomie, co w konsekwencji zapobiega niepożądanym retransmisjom pakietów i zatem pozwala na minimalizację opóźnienia przy przekazie krótkich wiadomości przez sieć. Należy przypomnieć, iż takie własności sieci są pożądane w przypadku krótkich wiadomości ale z krytycznymi wymaganiami na czas ich przekazu. Dla sieci IP QoS oferującej jedynie względną jakość przekazu pakietów, użytkownicy nie mogą się spodziewać dotrzymania ścisłych gwarancji jakości przekazu a jedynie ich zróżnicowania, w zależności od przyjętych kryteriów uprzywilejowania dla wybranych strumieni pakietów.

Podsumowując, występowanie różnych typów ruchu w sieciach IP QoS i ich różne wymagania dotyczące jakości przekazu w istotny sposób rzutują na projektowanie usług sieciowych

(usług telekomunikacyjnych). Każdy z typów ruchu wymaga odrębnego podejścia do jego opisu, co jest zwłaszcza konieczne przy monitorowaniu parametrów ruchu i przy podejmowaniu decyzji o przyjęciu/nie przyjęciu nowych wywołań. Odnośnie zróżnicowania wymagań na jakość przekazu pakietów dla różnych strumieni ruchu nakazuje konieczność wprowadzenia do sieci mechanizmów zapewniających zróżnicowanie obsługi pakietów w poszczególnych węzłach sieci.

# 3 Mechanizmy QoS dla sieci IP

Rozdział ten zawiera przegląd mechanizmów, zwanych mechanizmami QoS, wspierających zapewnienie jakości obsługi w sieciach IP QoS. Mechanizmy QoS można podzielić na dwie główne grupy [Bur00]: (1) mechanizmy działające na poziomie pakietów (*packet level mechanisms*) oraz (2) mechanizmy działające na poziomie wywołań (*admission level mechanisms*). Do pierwszej grupy zalicza się następujące mechanizmy: (1) dla klasyfikacji pakietów (*classifier*), (2) dla monitorowania (*meter*), oznaczania (*marker*), kształtowania (*shaper*) oraz odrzucania pakietów (*dropper*), określane wspólną nazwą jako mechanizmy dla profilowania ruchu (*traffic conditioners*), oraz (3) dla szeregowania pakietów (*scheduler*). Powyższe mechanizmy są przewidziane do implementacji w poszczególnych węzłach (ruterach) sieci IP QoS.

Mechanizm QoS odnoszący się do poziomu wywołań realizuje funkcję przyjmowania/odrzucania nowych wywołań (*admission control - AC*), a tym samym odpowiedzialną za regulowanie wielkości ruchu w sieci do poziomu nie przekraczającego zadany poziom dopuszczalny. Zatem, funkcja AC zapobiega również stanom przeciążenia w sieci. Należy podkreślić, iż funkcja AC jest niezbędna w sieci IP oferującej ścisłe gwarancje QoS.

Na potrzeby niniejszego ćwiczenia skupimy się tylko na mechanizmach QoS na poziomie pakietów.

## 3.1. Poziom pakietów

Z punktu widzenia jakości obsługi w sieciach IP QoS, mechanizmy QoS działające na poziomie pakietów powinny zapewnić przekaz pakietów na zadanym poziomie QoS. Mechanizmy te są zaimplementowane w węzłach sieci i odnoszą się do sposobu obsługi poszczególnych pakietów w danym węźle, a więc ich działanie odbywa się w skali czasowej co najwyżej milisekund. Mechanizmy te powinny zapewnić spełnienie takich wymagań QoS jak dopuszczalne opóźnienie przekazu pakietów przez sieć, dopuszczalna zmienność tego opóźnienia, dopuszczalne prawdopodobieństwo utraty pakietów wynikające z chwilowego przeciążenia sieci, czy też zapewnienie danej średniej szybkości bitowej przekazu pakietów.

W dalszej części rozdziału zostaną przedstawione własności oraz algorytmy dostępnych mechanizmów QoS dla przekazu pakietów IP przez sieć.

### 3.1.1. Mechanizmy klasyfikacji pakietów

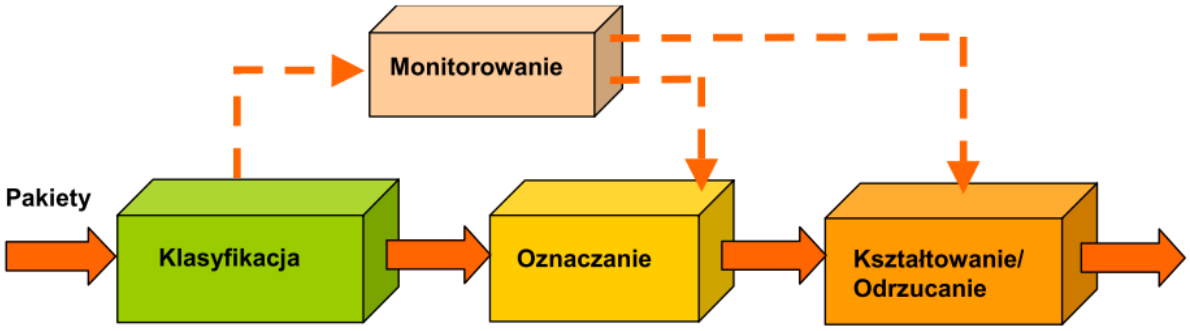
Mechanizmy klasyfikacji pakietów składają się z klasyfikatorów, które dokonują filtrowania pakietów przychodzących do danego węzła. Klasyfikatory służą np. do klasyfikacji napływających pakietów do poszczególnych usług sieciowych na podstawie wartości przyjętych pól nagłówka IP. Odpowiednie elementy filtrujące dzielą pakiety na dopasowane i nie dopasowane do przyjętego modelu filtra. W oparciu o dokonaną selekcję, pakiety są przekazywane dalej, czyli na właściwą ścieżkę przekazu (*datapath*) w węźle. Klasyfikator za pomocą filtrów może dokonywać rozdzielenia pojedynczego napływającego strumienia ruchu na wiele strumieni. Liczba możliwych strumieni ruchu, wychodzących z klasyfikatora, zależy od liczby przyjętych filtrów. Najprostszym modelem klasyfikatora jest taki klasyfikator, który uznaje wszystkie przychodzące pakiety za dopasowane i wówczas strumień wyjściowy pakietów jest po prostu strumieniem wejściowym. Filtry mogą działać np. w oparciu o wartości wybranego pola nagłówka pakietu, bądź też kilku pól. Przykładowo, Tabela 3-1 przedstawia możliwe ustawienia filtrów dla klasyfikatora odpowiedzialnego za przyporządkowanie napływających do danego węzła strumieni pakietów do uprzednio zdefiniowanych klas ruchu, czyli klasyfikatora typu BA (*Behaviour Aggregate*) zdefiniowanego dla architektury DiffServ [RFC3290]. Dla tego przypadku, klasyfikacja pakietów jest przeprowadzana na podstawie wartości pola DSCP (*Differantiated Services Code Point*) nagłówka pakietu IPv4. Innym przykładem jest klasyfikator, który może być zastosowany np. w ruterach brzegowych, nazywanym klasyfikatorem MF (*Multi-Field*), który działa na podstawie wartości kilku pól nagłówka IPv4, np.: adresu źródłowego, adresu docelowego, źródłowego portu TCP, docelowego portu TCP. Klasyfikator taki jest niezbędny przy klasyfikacji pakietów należących do pojedynczego strumienia, które dalej mają podlegać działaniu mechanizmów profilowania ruchu.

*Tabela 3-1. Przykład klasyfikatora BA z trzema filtrami*

| Filtr | DSCP |
|---|---|
| Filtr1 | 101010 |
| Filtr2 | 111111 |
| Filtr3 | Pozostałe |

### 3.1.2. Mechanizmy profilowania ruchu

Jak powyżej wspomniano, mechanizmy profilowania ruchu realizują [RFC2475]: monitorowanie ruchu, kształtowanie ruchu, oznaczanie pakietów, oraz odrzucanie pakietów. Rysunek 3-1 przedstawia schemat blokowy logicznych powiązań między mechanizmami dla klasyfikacji pakietów i profilowania ruchu [RFC2475]. Należy zauważyć, iż mechanizmy profilowania ruchu zastosowane dla konkretnej usługi sieciowej, nie muszą zawierać wszystkich czterech realizowanych funkcji. Wybór zestawu funkcji zależy np. od sposobu realizacji danej usługi w sieci.




*Rysunek 3-1. Logiczne połączenie mechanizmów klasyfikacji pakietów oraz profilowania ruchu w węźle sieci*

#### *3.1.2.1. Monitorowanie i kształtowanie ruchu*

Monitorowanie ruchu ma na celu sprawdzenie, czy dany strumień pakietów ma profil zgodny, czy niezgodny z założonym. Monitorowanie ruchu odbywa się za pomocą elementów, które w oparciu o przyjęte profile ruchu oraz poziomy zgodności, dzielą pojedynczy strumień wejściowy pakietów na wiele strumieni wyjściowych. Liczba strumieni wyjściowych zależy od liczby przyjętych poziomów zgodności [RFC3290]. Najczęściej stosowany mechanizm monitorowania ruchu to mechanizm „*token bucket*". *Token bucket* jest opisany dwoma parametrami (R, B), gdzie R oznacza stałą szybkość napływu tokenów do puli, zaś B maksymalny rozmiar puli tokenów.

#### *3.1.2.2. Oznaczanie pakietów*

Oznaczanie pakietów w węźle sieci może odbywać się bezpośrednio po przejściu pakietu przez mechanizm klasyfikacji, bądź też po przejściu przez mechanizm monitorowania ruchu. Oznaczanie pakietów polega na ustawianiu odpowiedniej wartości pól nagłówka pakietu, które są przewidziane do tego celu. Przykładowo, w przypadku architektury DiffServ oznaczanie pakietów polega na ustawianiu odpowiedniej wartości pól DSCP w nagłówku pakietu. W przypadku przejścia pakietu przez mechanizm monitorowania, wartości pól zależą od przyporządkowania pakietu do odpowiedniego poziomu zgodności. Przykładowo pakiety zgodne z założonym profilem ruchu

mogą być oznaczane inaczej niż pakiety niezgodne. Oznaczanie pakietów pozwala na ich odpowiednią obsługę przez kolejne mechanizmy na ścieżce przekazu w danym węźle. Dzięki oznaczaniu pakietów, można m.in. różnicować pakiety w ramach strumienia, na te które powinny być obsłużone np. w procesie kolejkowania z wyższym lub niższym priorytetem, bądź też na te które powinny być przekazane do dalszej obsługi lub powinny zostać odrzucone w pierwszej kolejności w razie przeciążenia w danym węźle sieci.

*3.1.2.3. Odrzucanie pakietów*

Mechanizmy odrzucania pakietów pozwalają na usuwanie z sieci pakietów, które bądź to są niezgodne z deklarowanym profilem ruchu (reakcyjne regulowanie ruchu), bądź ich odrzucenie może zmienić ruch generowany przez źródło z którego pochodzą pakiety (prewencyjne regulowanie ruchu). W obu przypadkach usuwanie pakietów, powinno wspierać obsługę ruchu, zgodnie z założonymi dla danej usługi sieciowej wymaganiami QoS.

Odrzucanie pakietów może się odbywać na zasadzie bezwzględnego lub selektywnego odrzucania. Bezwzględne odrzucanie polega na tym, iż wszystkie pakiety napływające do elementu odrzucającego są po prostu usuwane. Taki element odrzucający nie przekazuje pakietów dalej, dlatego nie musi posiadać elementu wyjściowego.

W przypadku mechanizmu z selektywnym odrzucaniem pakietów, pakiety napływające do elementu odrzucającego są usuwane selektywnie, zgodnie z przyjętym algorytmem usuwania. Dlatego też, taki element odrzucający pakiety posiada zarówno wejście, jak i wyjście. Algorytm selektywnego odrzucania pakietów może być skojarzony z kolejką o dyscyplinie obsługi FIFO. Dla takiego przypadku można wymienić dwa typowe algorytmy odrzucania: (1) odrzucany jest pakiet, który miałby zostać umieszczony w ogonie kolejki FIFO (*Tail Dropper*). W tym przypadku, element wyjściowy urządzenia odrzucającego jest połączony z elementem wejściowym kolejki, lub (2) odrzucany jest pakiet, który znajduje się na samym początku kolejki (*Head Dropper*). W przypadku 2., element wejściowy urządzenia odrzucającego jest połączony z elementem wyjściowym kolejki.

### 3.1.4. Mechanizmy szeregowania pakietów

Zastosowanie odpowiednich metod szeregowania pakietów w węzłach sieci może wspierać zapewnienie zróżnicowania jakości przekazu pakietów w ramach różnych strumieni. Ogólnie, metoda szeregowania pakietów przydziela różnym pakietom różną jakość obsługi przez wybór, który z oczekujących pakietów jest obsłużony jako pierwszy oraz przez wybór które pakiety są

tracone. W konsekwencji możemy mówić o dwóch parametrach przekazu pakietów, są to: poziom straty pakietów oraz opóźnienie pakietów.

Prawo zachowania

Najprostsza metoda szeregowania pakietów jest oparta na zasadzie pierwszy przybył pierwszy zostaje obsłużony (funkcjonują dwie nazwy tej metody: FCFS - First Come First Served lub FIFO – First In First Out). W metodzie tej pakiety są obsługiwane w kolejności ich napływu. Tracone są te pakiety, które zastają kolejkę zapełnioną. Wadą tej metody jest to, że nie pozwala ona na różnicowanie obsługi pakietów w ramach wybranych strumieniu ruchu.

Dla mechanizmów szeregowania pakietów obowiązuje tak zwane prawo zachowania (conservation law) [Kesh97], które mówi, iż suma średnich opóźnień w kolejce, których doznają pakiety nie zależy od zastosowanego mechanizmu szeregowania pakietów. Pewne mechanizmy mogą redukować opóźnienia w ramach wybranych strumieni, w porównaniu z opóźnieniami doznanymi w kolejce obsługiwanej zgodnie z metodą FIFO. Jest to jednak możliwe tylko poprzez zwiększenie opóźnienia pakietów z innych strumieni. Definicja prawa zachowania jest następująca [Kesh97]: jeżeli mechanizm szeregowania jest typu work conserving, czyli nie obsługuje pakietów tylko wtedy, gdy kolejka jest pusta, wówczas spełniona jest następująca zależność:

$$\sum_{i=1}^{N} \rho_i W_i = \text{Constant} \qquad \text{eq. 3-1}$$

Przy założeniach, że do kolejki napływa N niezależnych strumieni pakietów, średnia szybkość strumienia-i wynosi li, średni czas obsługi pakietu wynosi $1/\mu_i$, $\rho_i=\lambda_i/\mu_i$ oznacza średnie obciążenie łącza przez ruch ze strumienia-i, zaś $W_i$ jest średnim opóźnieniem, którego doznają pakiety należące do strumienia-i w wyniku oczekiwania w kolejce. Prawo to nie jest spełnione dla mechanizmów szeregowania pakietów typu non-work conserving. Wówczas średnie opóźnienie, jakiego doznają pakiety w kolejce może być większe niż w przypadku metody FIFO.

Wymagania

W zależności od typu obsługiwanego ruchu oraz wymagań QoS, metodom szeregowania pakietów stawiane są następujące wymagania:

- Łatwość implementacji (dla wszystkich usług sieciowych)

- Sprawiedliwość i zapewnienie obsługi (dla usług z wymaganiami na sprawiedliwy podział zasobów)
- Zapewnienie QoS (dla usług ze ścisłą gwarancją QoS)
- Możliwość implementacji łatwego i efektywnego algorytmu AC (dla usług ze ścisłą gwarancją QoS).

Należy zwrócić uwagę, iż każdy mechanizm szeregowania pakietów może się cechować różnymi zależności pomiędzy wymienionymi wymaganiami, zaś niektóre z wymagań wykluczają się wzajemnie. Dlatego też, w zależności od wymagań QoS, które powinna realizować dana sieć, pewne wymagania wobec metod szeregowania mogą stać się ważniejsze od innych.

Mechanizm priorytetów bez wywłaszczania (non-preemptive priority)

W metodzie szeregowania z priorytetami, każdy strumień jest skojarzony z pewnym priorytetem. Jeżeli założymy *n* poziomów priorytetów i wyższy numer poziomu odpowiada strumieniowi z wyższym priorytetem, mechanizm szeregowania pobiera do obsługi pakiety ze strumienia skojarzonego z poziomem *k* tylko wówczas, jeżeli nie ma pakietów oczekujących do obsługi ze strumieni skojarzonych z poziomami priorytetów *k+1, k+2, ..., n*. Priorytety pozwalają pakietom skojarzonym z wyższym priorytetem na krótszy czas oczekiwania na obsługę w stosunku do pakietów o niższym priorytecie.

Mechanizm WFQ (Weighted Fair Queuing)

Mechanizm WFQ stanowi aproksymację idealnej metody szeregowania GPS (Generalized Processor Sharing). Metoda GPS zapewnia sprawiedliwy podział zasobów (fair share allocation), jednak nie jest możliwa do zaimplementowania, ponieważ zakłada że w każdym cyklu serwer obsługuje nieskończenie małą część danych z każdej niepustej kolejki. Metoda WFQ symuluje działanie GPS i nie wymaga dzielenia pakietów na nieskończenie małe porcje.

W metodzie WFQ dla każdego pakietu obliczany jest znacznik czasowy, który wyraża czas po którym pakiet opuściłby serwer gdyby obsługa polegała na zasadzie GPS. Pakiety pobierane są do obsługi przez serwer w kolejności obliczonych znaczników czasowych. Jeśli kolejki posiadają wagi obsługi, wtedy są obsługiwane w proporcji do przydzielonych wag.

Metoda WFQ nie wymaga znajomości średniego rozmiaru pakietów w ramach obsługiwanych połączeń oraz spełnia wymagania na sprawiedliwą alokację pasma (fair share allocation) w krótkich odcinkach czasu.

Na potrzeby niniejszego ćwiczenia zajmiemy się tylko mechanizmami szeregowania FIFO oraz mechanizmem z priorytetami. Przegląd pozostałych mechanizmów szeregowania pakietów, które są obecnie stosowane w sieciach IP QoS można znaleźć np. w [Kesh97].

# 4. Metody różnicowania jakości obsługi w wielo-usługowych sieciach IP

## 4.1. Technika IP

Technika IP jest oparta na komutacji pakietów. W odróżnieniu do techniki ATM, w przypadku IP, pakiety mogą przyjmować zmienną długość. Powszechnie stosowaną wersją protokołu IP jest wersja 4 (IPv4). Opis standardu dla IPv4 został zawarty w dokumencie [RFC0791]. Format nagłówka pakietu IPv4 przedstawia Rysunek 4-1. Pola nagłówka pakietu obejmują 20 bajtów, od pola „wersji" do pola „adresu przeznaczenia" włącznie, oraz od 4 do 40 bajtów w zależności od długości pola opcji, które może przyjmować zmienną długość. Ostatecznie, maksymalna długość nagłówka IPv4 może wynieść 60 bajtów.


*Rysunek 4-1. Format nagłówka pakietu IPv4 [RFC0791]*

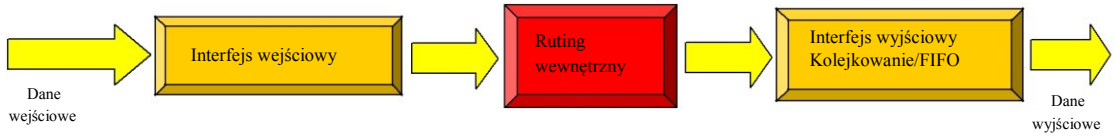
## 4.2. Sieć Internet

Obecna sieć Internet działa w oparciu o protokół IPv4. Jest to sieć niezorientowana na oferowanie jakości obsługi pakietów. Sieć oferuje tylko jedną usługę, usługę standardową (*best effort*).

### 4.2.1. Usługa standardowa

W przypadku usługi standardowej, dostęp nowych strumieni ruchu do sieci nie jest ograniczany przez mechanizmy sieciowe, zaś w węzłach sieci pakiety są obsługiwane wg kolejności napływu. Ponieważ sieć Internet powstała przede wszystkim dla przekazu danych, aplikacje działające w tej sieci, nazywane aplikacjami standardowymi (patrz rozdział 2), korzystają głównie z protokołu TCP, który odpowiada za sterowanie ruchem danych w ramach połączenia. TCP posiada mechanizmy, które pozwalają na dostosowanie transmisji pakietów do warunków panujących w sieci. Aplikacje obsługiwane przez ten protokół są określane jako aplikacje elastyczne. Jak wspomniano w rozdziale 2, w wyniku rozwoju powstały nowe aplikacje, które w odróżnieniu od aplikacji elastycznych, wymagają obsługi z reżimem czasu rzeczywistego. Niestety, sieć Internet nie posiada mechanizmów QoS dla różnicowania jakości przekazu pakietów ze względu na takie

wymagania QoS. Rysunek 4-2 przedstawia poglądowy model ścieżki pakietów w ruterze sieci Internet jedynie z usługą standardową. Model ten nie posiada żadnych mechanizmów QoS.




*Rysunek 4-2. Model ścieżki pakietów w ruterze sieci Internet*

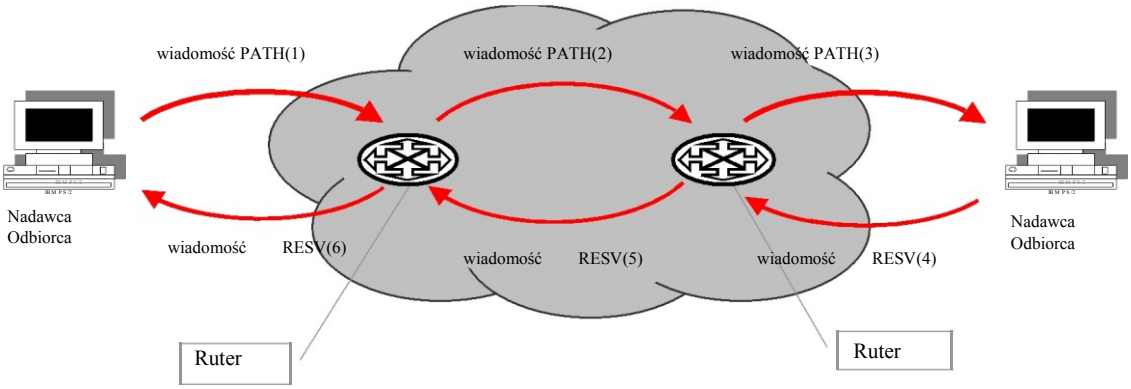
W kolejnych punktach zostaną przedstawione architektury sieci IP zorientowane na oferowanie oraz różnicowanie jakości obsługi.

### 4.3. Architektury zorientowane na oferowanie jakości obsługi

Obserwując brak aplikacji wykorzystujących usługi telekomunikacyjne oferowane przez technikę ATM oraz jednoczesny gwałtowny wzrost liczby użytkowników sieci Internet, projektanci nowych architektur zorientowanych na oferowanie QoS wnioskują, iż architektury te powinny być oparte na technice IP, ze względu na jej szerokie zastosowanie [RFC1633].

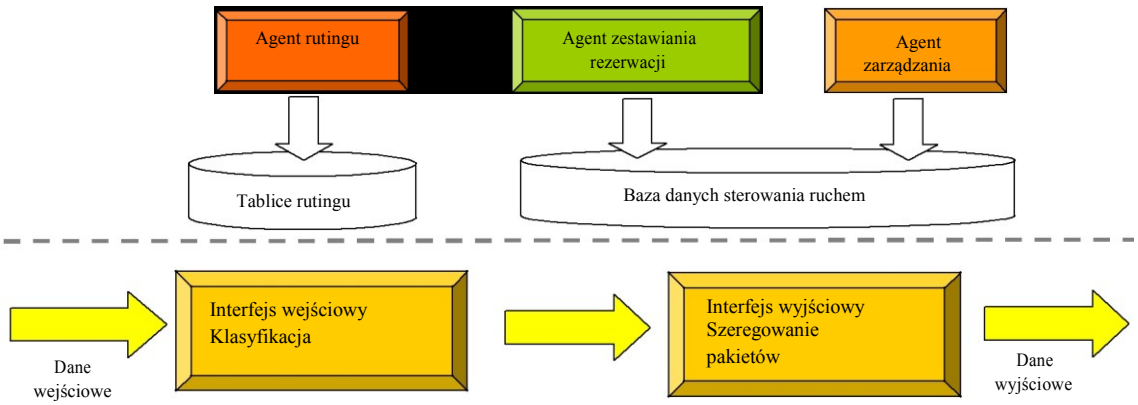
#### 4.3.1. Architektura IntServ

Architektura IntServ [RFC1633] stanowi rozszerzenie architektury sieci Internet o model usług zintegrowanych. W szczególności, w architekturze IntServ zakłada się, iż dostęp do zasobów sieci jest sterowany za pomocą mechanizmu AC (patrz rozdział 3). W celu zapewnienia QoS odpowiednie zasoby sieci (bufory, pasmo) są rezerwowane w każdym węźle i łączu wzdłuż drogi połączenia. Rezerwacje mogą być realizowane dla pojedynczego strumienia pakietów lub dla strumieni zbiorczych.




*Rysunek 4-3. Przepływ wiadomości sygnalizacyjnych w protokole RSVP*

W związku z potrzebą rezerwacji zasobów, istnieje konieczność zastosowania odpowiedniego protokołu sygnalizacyjnego, dla zestawiania połączenia w sieci. W tym celu został zdefiniowany protokół *Resource ReSerVation Protocol* (RSVP) [RFC2205, RFC2210]. Przykładowy przepływ wiadomości sygnalizacyjnych w protokole RSVP przedstawia Rysunek 4-3. Żądanie rezerwacji zasobów jest inicjowane przez stronę nadawczą, która wysyła wiadomość typu PATH. Wiadomość ta zawiera informacje o generowanym profilu ruchowym. W oparciu o te dane są określane wymagania na pasmo oraz wielkość bufora dla zapewnienia QoS w poszczególnych węzłach sieci. Wiadomość PATH jest wysyłana od stacji nadawczej do stacji odbiorczej, realizując konieczne rezerwacje w każdym węźle wzdłuż drogi połączeniowej. Strona odbiorcza po otrzymaniu wiadomości PATH, wysyła wiadomość RESV, której zadaniem jest rezerwacja zasobów w kierunku od stacji odbiorczej do stacji nadawczej. Wiadomość RESV jest przesyłana tą samą drogą jak wiadomość PATH. W przypadku, kiedy sieć dysponuje zasobami, algorytm AC akceptuje przyjęcie wywołania w każdym węźle na drodze połączeniowej. Dokonana rezerwacja musi być okresowo odnawiana (*soft reservation*). Rezerwacja zasobów na całej drodze połączeniowej wymaga również, aby w każdym węźle była przechowywana informacja o profilach ruchowych dla obsługiwanych strumieni ruchu, co z kolei ogranicza skalowalność tego rozwiązania. Oprócz mechanizmów AC oraz sygnalizacji RSVP, mechanizmami QoS, które wspierają jakość obsługi w sieci IntServ są klasyfikatory pakietów stosowane w interfejsach wejściowych ruterów oraz mechanizmy szeregowania pakietów, ulokowane w interfejsach wyjściowych. Model odniesienia, dla implementacji rutera w sieci IntServ przedstawia Rysunek 4-4. W modelu tym możemy wyróżnić dwie warstwy logiczne. „Dolna część" modelu przedstawia warstwę przekazu danych z urządzeniami do klasyfikacji i szeregowania pakietów, zaś „górna część" stanowi warstwę rezerwacji oraz sterowania zasobami, odpowiednio z agentami rutingu, zestawiania rezerwacji oraz zarządzania.




*Rysunek 4-4. Model ścieżki pakietów w ruterze dla sieci IntServ*

W ramach architektury IntServ zaproponowano dwie usługi sieciowe oferujące QoS:

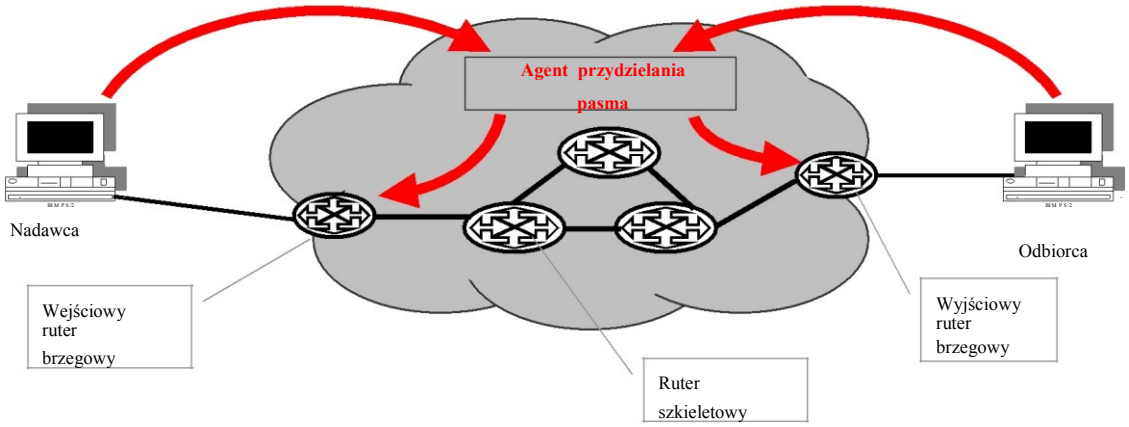
- Usługę, która powinna oferować ścisłe gwarancje QoS - *Guaranteed Service* [RFC2212]. Usługa ta została zaprojektowana dla aplikacji wymagających obsługi w rezimie czasu rzeczywistego i powinna zapewnić, aby maksymalne wartości opóźnień, których doznają pakiety przekazywane przez sieć, nie przekraczały założonych wartości granicznych.
- Usługę, która powinna zapewniać pewną jakość obsługi dla elastycznych aplikacji standardowych - *Controlled-load Service* [RFC2211]. Usługa powinna zapewniać bardzo małe średnie opóźnienia pakietów, a także bardzo małe straty pakietów, w skalach czasowych większych, niż czas obsługi paczki pakietów.

Dla obu wymienionych usług, aby zagwarantować założone wymagania QoS należy zdefiniować odpowiednią metodę AC. Zastosowanie konkretnego algorytmu AC zależy od implementacji danej usługi i pozostaje w gestii operatora sieci. Dodatkowo, w ramach architektury IntServ, przewidziano trzecią usługę, którą może być np. usługa standardowa.

Pomimo dużych nadziei, jakie wiązano z zastosowaniem architektury IntServ, problem skalowalności rozwiązania stanowi istotny czynnik hamujący rozwój tego podejścia. Dlatego też, dalsze prace nad architekturą sieci opartej na protokole IP, która wspierałaby gwarancje QoS, zostały ukierunkowane na takie podejścia, które rozwiązałyby problem skalowalności. Taką architekturą jest architektura DiffServ.

### 4.3.2. Architektura DiffServ

Architektura DiffServ dzięki zastosowaniu właściwych mechanizmów QoS ma pozwolić operatorom sieci na świadczenie usług różniących się oferowaną jakością obsługi. Różnicowanie jakość obsługi może odbywać się ze względu na różnicowanie jakości obsługi w ramach różnych klas abonentów lub różnych klas ruchu [RFC2475, RFC3260, RFC3290].




*Rysunek 4-5. Ogólna architektura DiffServ*

Rysunek 4-5 przedstawia ogólną architekturę DiffServ. W architekturze tej wyróżniamy rutery brzegowe, usytuowane na wejściu i wyjściu z sieci szkieletowej oraz rutery szkieletowe. Jak już wspomniano jednym z warunków, który ma być spełniony przez architekturę DiffServ, jest skalowalność rozwiązania.

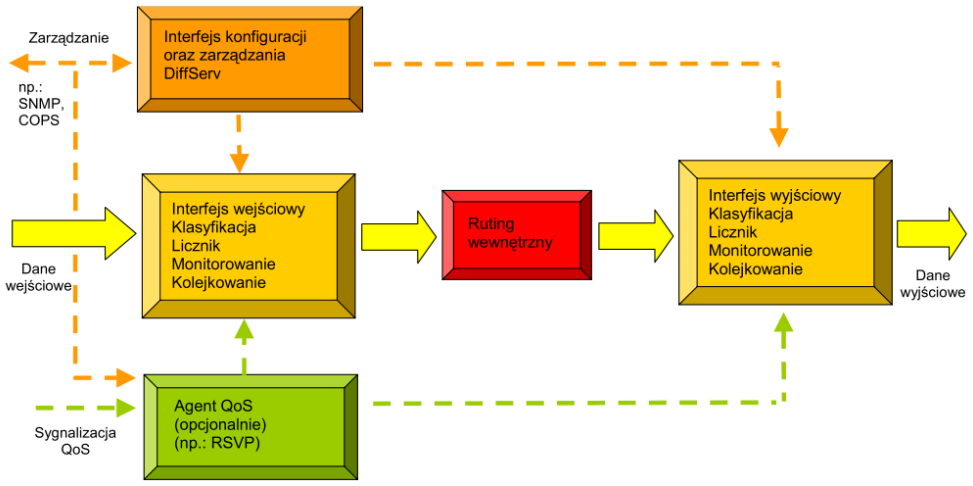
Elementem wyróżniającym architekturę DiffServ, od wcześniej przedstawionej architektury IntServ, jest zastosowanie tzw. agenta przydzielania pasma (*Bandwidth Broker*). Agent ten odpowiada za realizację funkcji AC, zarządzanie zasobami sieci oraz za funkcje związane z konfiguracją ruterów brzegowych. Wymienione funkcje są realizowane tylko w węzłach brzegowych sieci. Zakłada się, iż sieć szkieletowa jest odpowiednio przewymiarowana, aby nie stanowić ograniczenia dla przekazu pakietów.

Główna koncepcja DiffServ polega na tym, iż rutery brzegowe obsługują pojedyncze strumienie pakietów, natomiast w sieci szkieletowej obsługa odbywa się na podstawie strumieni zbiorczych. Dlatego też funkcje profilowania ruchu (patrz rozdział 3) są realizowane jedynie w węzłach brzegowych sieci. Natomiast, obsługa ruchu zbiorczego (klas ruchu) przez sieć powinna

odbywać się zgodnie z przyjętymi modelami przekazu pakietów, określanymi jako *Per-Hop-Behaviour* (PHB). PHB określają, w jaki sposób ruch w ramach danej klasy ruchu ma być przekazywany między poszczególnymi węzłami sieci. Pakiety, obsługiwane wg tego samego PHB są rozpoznawane w ruterach dzięki odpowiedniemu ustawieniu pola DSCP, nagłówka pakietu IP. Odpowiednie definicje dla wartości pól nagłówków pakietów zarówno dla IPv4 oraz IPv6 przedstawiono w dokumencie [RFC2474].

W ramach architektury DiffServ zdefiniowano dwie główne grupy PHB, *Expedited Forwarding* (EF) [RFC3246] i *Assured Forwarding* (AF) [RFC2597]. Grupa EF PHB została zdefiniowana dla przekazu pakietów wymagających obsługi w reżimie czasu rzeczywistego, natomiast grupa AF PHB odpowiada za przekaz pakietów w ramach wielu klas ruchu elastycznego. W przypadku obu grup PHB, zdefiniowane mechanizmy QoS powinny zapewnić jakość przekazu pakietów zgodnie z wymaganiami QoS przyjętymi dla danej klasy ruchu oraz zapewnić różnicowanie jakości między poszczególnymi klasami ruchu. Dlatego też, w celu gwarancji QoS przy przekazie pakietów przez sieć, w każdym węźle sieci (ruterze), powinny być utworzone tzw. bloki dla regulowania ruchu (*Traffic Conditioning Blocks - TCB*) [RFC3290], które stanowią zestaw wybranych mechanizmów QoS dla regulowania ruchu w ramach danej usługi sieciowej. Zestaw mechanizmów QoS w ramach bloków TCB zależy od typu rutera. Bloki TCB dla ruterów brzegowych będą zawierały mechanizmy QoS dla obsługi pojedynczych strumieni ruchu, zaś bloki ruterów szkieletowych tylko mechanizmy QoS dla obsługi strumieni zbiorczych. Przykładowo, mechanizmy monitorowania ruchu dedykowane do obsługi pojedynczych strumieni ruchu są stosowane jedynie w ruterach brzegowych sieci. Również funkcje związane z sygnalizacją QoS oraz metodami AC, a w konsekwencji konfiguracją parametrów urządzeń monitorujących ruch, powinny być realizowane jedynie na wejściu do sieci szkieletowej oraz na jej wyjściu.

Główne elementy funkcjonalne rutera w architekturze DiffServ przedstawia Rysunek 4-6.




*Rysunek 4-6. Główne elementy funkcjonalne rutera DiffServ*

Jak wynika z definicji architektury DiffServ, architektura ta powinna wspierać różnicowanie jakości obsługi np. różnych klas abonentów lub różnych klas ruchu. W pracy rozważane są jedynie aspekty różnicowania jakości obsługi z punktu widzenia różnych klas ruchu, a zwłaszcza ze względu na stawiane tym klasom wymagania QoS. Różnicowanie jakości obsługi wymaga zastosowania odpowiednich mechanizmów. Najprostszym mechanizmem dla zróżnicowania QoS jest nadanie strumieniom poszczególnych klas ruchu różnych priorytetów obsługi. Jednak zastosowanie jedynie prostego mechanizmu priorytetów w ruterach szkieletowych sieci bez zastosowanie właściwych metod AC na dostępie do sieci nie wystarczy dla zapewnienia ścisłych gwarancji QoS, gdyż niekontrolowany ruch w ramach klas o wyższym priorytecie obsługi mógłby wpływać na pogorszenie lub całkowitą blokadę przekazu pakietów z klas o niższym priorytecie.

W ramach architektury DiffServ można oprócz usług oferujących ścisłe gwarancje QoS zaprojektować również usługi, które będą oferować względne gwarancje QoS. Usługi takie nie wymagają zastosowania mechanizmów AC. W ramach IETF, w oparciu o EF PHB, zaproponowano realizację usługi Premium [RFC2638], dla aplikacji generujących ruch o stałej szybkości bitowej. Usługa Premium realizuję emulację łącza o stałej szybkości (na poziomie pakietów). Wymagania QoS dla usługi Premium są następująca. Usługa powinna gwarantować bardzo małe opóźnienia przekazu pakietów, małą zmienność tych opóźnień oraz małe strat pakietów. Zakłada się, iż pakiety w ramach usługi Premium będą obsługiwane z najwyższym priorytetem z zastosowaniem odpowiedniej metody AC. W tym przypadku proponuje się zastosowanie metody AC typu REM z alokacją pasma na podstawie szczytowej szybkości bitowej (peak rate allocation scheme), jak to

przedstawiono w rozdziale 3. W celu jest konieczne uprzednie uzgodnienie tzw. „kontraktu ruchowego" między użytkownikiem a siecią. Kontrakt taki jest określany jako *Service Level Agreement* (SLA) i jest zawierany na podstawie parametrów mechanizmu *token bucket*, tj. szczytowej szybkości bitowej oraz maksymalnego rozmiaru paczki pakietów. Dodatkowo, w ruterach brzegowych sieci DiffServ ruch, w ramach pojedynczych strumieni, podlega procesowi kształtowania, aby był zgodny z zawartym kontraktem ruchowych na wejściu do sieci szkieletowej i na jej wyjściu. Usługa *Premium* jest jedną z propozycji realizacji usługi w ramach architektury DiffServ. Przewiduje się, iż jednocześnie sieć może oferować także inne usługi QoS.

## 5. Literatura dodatkowa


[Taras04] H. Tarasiuk, "Metody różnicowania jakości obsługi w sieciach z komutacją pakietów", Rozprawa doktorska, Politechnika Warszawska, Warszawa 2004.

[Kesh97] S. Keshav, "An engineering approach to computer networking", chapter 9: "Scheduling", Addison-Wesley, 1997, pp. 209-263.

[RFC0768] J. Postel, „User Datagram Protocol", Internet RFC 0768, August 1980.

[RFC0791] J. Postel, „Internet Protocol", Internet RFC 0791, September 1981.

[RFC0793] J. Postel (ed.), et al., „Transmission Control Protocol", Information Sciences Institute, University of Southern California, Internet RFC 0793, September 1981.

[RFC1633] R. Braden, D. Clark, S. Shenker, „Integrated Services in the Internet Architecture: an Overview", Internet RFC 1633, June 1994.

[RFC2205] R. Braden (ed.), et al., „Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification", Internet RFC 2205, September 1997.

[RFC2210] J. Wroclawski, „The Use of RSVP with IETF Integrated Services", Internet RFC 2210, September 1997.

[RFC2211] J. Wroclawski, „Specification of the Controlled-Load Network Element Service", Internet RFC 2211, September 1997.

[RFC2212] S. Shenker, C. Patridge, R. Guerin, „Specification of Guaranteed Quality of Service", Internet RFC2212, September 1997.

[RFC2474] K. Nichols, et al., „ Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", Internet RFC 2474, December 1998.

[RFC2475] S. Blake, et al., "An Architecture for Differentiated Services", Internet RFC 2475, December 1998.

[RFC2597] J. Heinanen, et al., „Assured Forwarding PHB Group", Internet RFC 2597, June 1999.

[RFC2638] K. Nichols, et al., „A Two-bit Differentiated Services Architecture for the Internet", Internet RFC 2638, July 1999.

[RFC3246] B. Davie, et al., „An Expedited Forwarding PHB (Per-Hop-Behavior)", Internet RFC 3246, March 2002.

[RFC3260] D. Grossman, „New Terminology and Clarifications for Diffserv", Internet RFC 3260, April 2002.

[RFC3290] Y. Bernet, et al., „An Informal Management Model for Diffserv Routers", Internet RFC 3290, May 2002.

# 4 Przykładowe pytania na kolokwium

1. Podaj rodzaje ruchu w sieciach IP
2. Podaj wymagania na jakość przekazu pakietów w sieciach IP QoS dla poszczególnych typów ruchu.
3. Jak jest różnica między relatywnym i ścisłym zapewnieniem QoS w sieciach IP ?
4. Wymień mechanizmy QoS na poziomie pakietów stosowane w sieciach IP QoS, które z tych mechanizmów stosowane są w portach wejściowych, a które w portach wyjściowych ruterów.
5. Podaj podstawowe różnice w funkcjonalności ruterów brzegowych i szkieletowych w architekturze DiffServ (chodzi o wykonywane zadania i zaimplementowane w tych ruterach mechanizmy QoS).
6. W jaki sposób ruter brzegowy zgodny z architekturą DiffServ identyfikuje pakiety należące do danego pojedynczego strumienia?
7. W jaki sposób ruter zgodny z architekturą DiffServ identyfikuje pakiety należące do różnych usług sieciowych?

# 6. Zadania

## 6.1. Obsługa pojedynczego strumienia VoIP z wyższą wagą

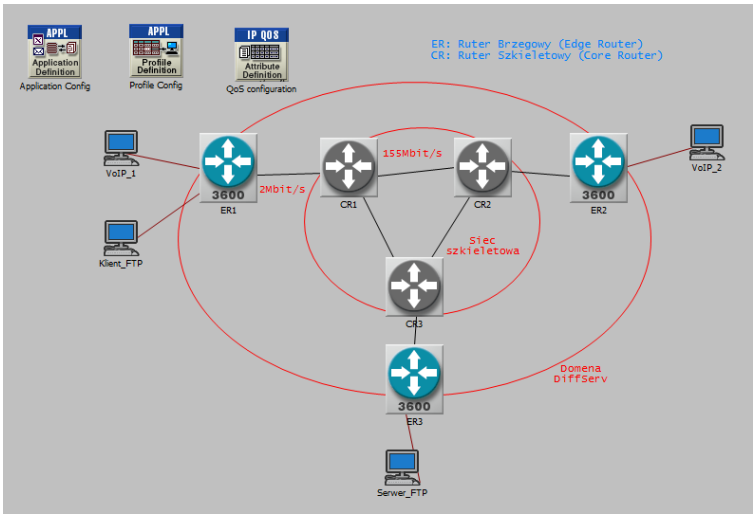
Celem ćwiczenia jest zapoznanie się z funkcjonalnością, konfiguracją i działaniem mechanizmów QoS w sieci IP opartej o architekturę Differentiated Services.

Ćwiczenie należy wykonać korzystając z symulatora RIVERBED. Po uruchomieniu programu należy wczytać projekt *„STIN_DS1_2”*. Scenariusz symulacji potrzebny do wykonania zadania to (*„Scenarios->Switch to scenario”*): *„VoIP”*.

Topologia testowa (Rysunek 6-1) składa się z trzech ruterów szkieletowych (CR), połączonych ze sobą łączami o przepływności 155 Mbit/s, oraz trzech ruterów brzegowych (ER), podłączonych do sieci szkieletowej za pomocą łączy o przepływności 2 Mbit/s. Łącze pomiędzy ruterami ER1 i CR1 stanowi wąskie gardło w sieci, gdyż sumaryczny ruch oferowany od klientów VoIP_1 i Klient_FTP przekracza 2Mbit/s.

Generowane są dwa typy ruchu:

- Ruch związany z aplikacją głosową (VoIP), uruchomioną pomiędzy komputerami VoIP_1 i VoIP_2. Wykorzystuje ona kodek PCM, który generuje strumień pakietów o stałej długości 160B, w równych odstępach 20ms. Szybkość bitowa strumienia jest stała i wynosi 64 kbit/s.
- Ruch generowany przez klienta Klient_FTP, który przesyła do serwera Serwer_FTP pliki o długości 300kB, z czasem pomiędzy kolejnymi sesjami losowanym zgodnie z rozkładem wykładniczym, z wartością średnią 1s.




- *Rysunek 6-1. Topologia testowa dla realizacji ćwiczenia: CR – ruter szkieletowy; ER – ruter brzegowy*

Rutery w rozważanej sieci potrafią obsługiwać pakiety zgodnie z regułami EF PHB. Na ich portach wyjściowych, skonfigurowany jest mechanizm priorytetów, który obsługuje pakiety oznaczone kodem TOS=4 (co odpowiada Precedence=128), z wyższą wagą niż pozostałe pakiety.

1) Zadaniem wykonującego ćwiczenie jest takie ustawienie parametrów mechanizmów QoS związanych z klasyfikacją, monitorowaniem i odrzucaniem pakietów należących do sesji aplikacji VoIP ustanowionej pomiędzy komputerami VoIP_1 i VoIP_2, aby były one przesyłane w sieci DiffServ z odpowiednią jakością przekazu. Zatem, na odpowiednim porcie rutera ER1 należy:
Skonfigurować parametry mechanizmu TB, w sposób odpowiedni dla profilu ruchu związanego z rozważaną aplikacją VoIP,
Skonfigurować odpowiednio mechanizm klasyfikacji pakietów na wejściu do sieci,
Skonfigurować mechanizmy oznaczania i odrzucania pakietów tak, aby pakiety uznane za zgodne z kontraktem były oznaczane odpowiednią wartością TOS i natychmiast wpuszczane do sieci, a pakiety niezgodne były odrzucane.

Prawidłowe ustawienie parametrów należy udokumentować poprzez wykonanie symulacji i podanie osiąganych wartości następujących parametrów QoS:

- Poziomu strat pakietów,
- Minimalnego, maksymalnego i średniego opóźnienia przesłania pakietów w sieci.

### 6.2. Obsługa dwóch strumieni ruchu VoIP i FTP z tym samym priorytetem

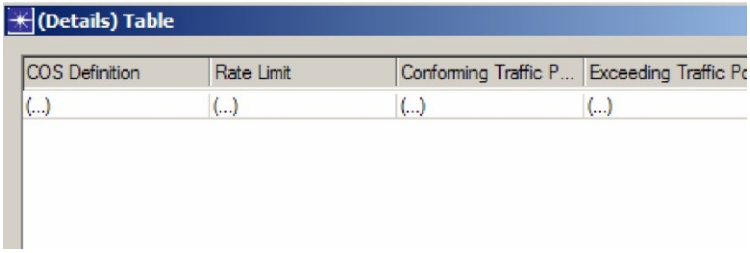
Zakładamy, iż w sieci mamy dwa typy ruch, tj. ruch generowany przez pojedynczą aplikację VoIP oraz klienta FTP. Należy w podobny sposób, jak w zadaniu pierwszym skonfigurować odpowiednie mechanizmy dla komputera Klient_FTP, aby generowany przez niego ruch także był przesyłany w sieci z wyższym priorytetem. Ponownie odczytać i podać wartości parametrów QoS określające jakość przekazu ruchu związanego z sesją VoIP.

# 7. Skrócona instrukcja obsługi programu RIVERBED

## 7.1. Konfiguracja parametrów mechanizmu monitorowania, oznaczania i odrzucania pakietów

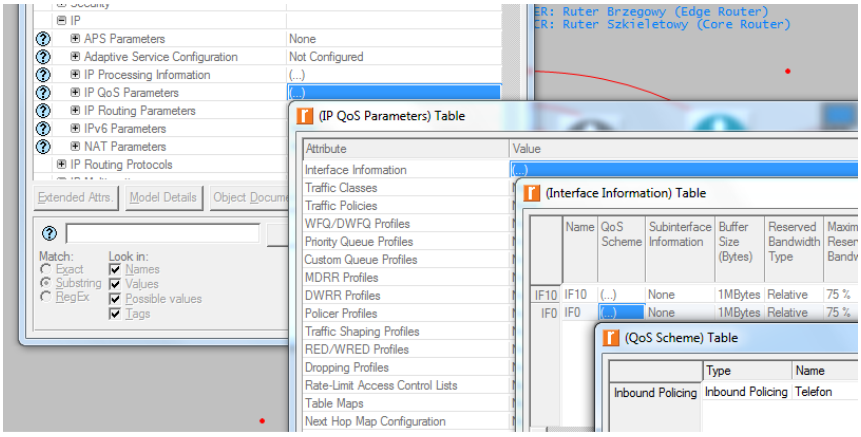
W programie RIVERBED, mechanizmy monitorowania kontraktu, oznaczania i odrzucania pakietów są określane wspólną nazwą mechanizmu CAR (*ang. Commited Access Rate*). Jego parametry konfiguruje się w oknie atrybutów obiektu „*QoS configuration*". Tam, należy przejść do okna konfiguracji profili CAR (*CAR Profiles->Edit*) i kliknąć pole „Edit" odpowiadające odpowiedniemu profilowi CAR. W ten sposób, przechodzimy do okna parametrów CAR (Rysunek 7-1), w którym można ustawić:

- Parametry klasyfikatora pakietów („*COS Definitions"*). Uwaga: w ćwiczeniu wystarczy ustawić wartości wszystkich parametrów klasyfikatora jako „*Any*". Wtedy, każdy przychodzący pakiet był traktowany jako należący do rozważanego strumienia.
- Parametry mechanizmu token bucket ("*Rate Limit"*). Uwaga: wartość parametru "*Excess burst size*" powinna być równa wartości parametru „*Normal burst size*".
- Rodzaj akcji podejmowanej w przypadku, kiedy pakiet jest uznany jako zgodny („*Conforming Traffic Policy*").
- Rodzaj akcji podejmowanej w przypadku, kiedy pakiet jest uznany jako niezgodny („*Exceeding Traffic Policy"*).




Rysunek 7-1. Konfiguracja parametrów profilu CAR

Następnie, zdefiniowany w ten sposób profil CAR należy ustawić na odpowiednim porcie rutera. W tym celu, należy przejść do okna atrybutów rutera i rozwinąć kolejno (Rysunek 7-2): „*IP->IP QoS Parameters->Interface Information->Row X->QoS Scheme*" (*Type InboundPolicing*), gdzie *X* odpowiada numerowi odpowiedniego interfejsu. Tam, należy ustawić odpowiedni profil dla pakietów wchodzących (*incoming*) lub wychodzących (*outgoing*) z rutera na danym interfejsie.




*Rysunek 7-2. Ustawienie uprzednio zdefiniowanego profilu CAR na odpowiednim porcie rutera*

## 7.2. Oliczanie poziomu straty pakietów

Obliczenie tej wartości jest nieco skomplikowane i wymaga wykonania następujących czynności:

- **Odczytanie liczby pakietów IP wysłanych po stronie VoIP_1**

  Należy ją obliczyć w następujący sposób: najpierw, należy odczytać wykres *„Network->VoIP_1->Voice Application->Traffic Sent (packets/sec)”*. Z tak otrzymanego wykresu (*STIN_DS1_2-VoIP-DES1*) należy obliczyć wartość średnią (*„sample mean”*), klikając prawym przyciskiem na krawędzi wykresu i wybierając *„Show statistic data”*. Po przemnożeniu przez czas symulacji (120sek) otrzymujemy ***liczbę wysłanych pakietów IP***.

- **Odczytanie liczby pakietów IP odebranych po stronie VoIP_2**

  Należy ją obliczyć w następujący sposób: najpierw, należy odczytać wykres *„Network->VoIP_2->Voice Application ->Traffic Receicved (packets/sec)”*. Z tak otrzymanego wykresu (*STIN_DS1_2-VoIP-DES1*) należy obliczyć wartość średnią (*„sample mean”*), klikając prawym przyciskiem na krawędzi wykresu i wybierając *„Show statistic data”*. Po przemnożeniu przez czas symulacji (120sek) otrzymujemy ***liczbę odebranych pakietów IP***.

- **Obliczenie poziomu straty pakietów** zgodnie ze wzorem:

$$p = \frac{liczba\_pakietów\_wysłanych - liczba\_pakietów\_odebranych}{liczba\_pakietów\_wysłancyh}$$

### 7.3. Odczytanie wartości parametrów związanych z opóźnieniem przesłania pakietów w sieci

Opóźnienie przekazu pakietów VoIP można odczytać korzystając ze statystyki „*Network->VoIP_2->Voice Application->Packet End-to-End Delay (sec)"* (*STIN_DS1_2-VoIP-DES1*). Wartość minimalną, maksymalną i średnią można odczytać w oknie „*Show statistic data*" (*vertical min, max*)

### 7.4. Odczytanie czasu oczekiwania i poziomu straty pakietów na łączu wyjciowym rutera

Dla sprawdzenia poprawności konfiguracji mechanizmów QoS, czasem pomocne jest odczytanie, jaki był poziom strat i opóźnienia pakietów należących do określonej usługi sieciowej, na danym porcie wyjściowym rutera. Można wtedy przekonać się, że np. pakiety należące do danej usługi rzeczywiście są obsługiwane na tym łączu z wyższą wagą.

Wartości tych statystyk można odczytać na wykresach dostępnych w: „*Network->X->IP Interface*" (*STIN_DS1_2-VoIP-DES1*), gdzie *X* oznacza nazwę określonego rutera. Parametry dotyczące różnych łączy wychodzących z danego rutera i różnych usług sieciowych są oznaczane jako „*IFx Qy*", gdzie *x* oznacza numer interfejsu rutera, a *y* numer kolejki.