**Metody gwarantowania jakości usług w sieciach IP**

**6.1 QoS (Quality of Service)**

Teoretycznie nic nie stoi na przeszkodzie, aby głos zamieniony na pakiety można było transmitować przez globalną sieć Internetu dzięki aplikacji VoIP, ale jak dotąd problemem jest nieprzewidywalna jakość transmisji w globalnej sieci IP. W przypadku przekazu "czystych" danych komputerowych niska jakość tej sieci ma stosunkowo niewielkie znaczenie, gdyż pakiety danych odebrane w niewłaściwej kolejności, mogą być odpowiednio uszeregowane, fragmenty uszkodzone bądź stracone, przesłane powtórnie, a na pakiety opóźnione można przez pewien czas poczekać. Inaczej wygląda sytuacja w przypadku transmisji głosu czy obrazu, gdzie jakość sieci przesyłowej ma zasadnicze znaczenie. Uszkodzonych lub straconych pakietów głosowych zwykle nie można retransmitować, na poprawne kolejkowanie też nie ma czasu, a nadmierne opóźnienia pakietów czynią cały przekaz głosowy nieużytecznym.   
Wraz z pojawieniem się w sieciach IP aplikacji czasu rzeczywistego, stały się ważne parametry, na które nie zwracano uwagi gdy przez sieć wędrowały tylko dane nie związane z tego typu ruchem. Gwarantowana jakość usług (Quality of Service) jest jedną z najważniejszych charakterystyk wymaganych dziś w Internecie. Definiuje się ją, jako zbiór technologii, które pozwalają użytkownikom otrzymywać od sieci przewidywalny poziom usług w kontekście przepustowości (bandwith), opóźnienia (delay) i zmienności opóźnienia (jitter) [10]. Oryginalna architektura TCP/IP nie zapewnia gwarantowania jakości usług, w związku z powyższym stosuje się także określenie QoIP (Quality over IP), które informuje o nowej dodatkowej funkcjonalności sieci. Obecne możliwości w zakresie gwarantowanej jakości usług w Internecie oraz innych sieciach z protokołem IP są niewielkie. Zagadnienie jakości w telefonii IP, jak również wszędzie tam, gdzie wymaga się działalności w czasie rzeczywistym jest bardzo skomplikowane. Quality of Service to zespół czynników wpływających na jakość usługi ocenianych na podstawie zadowolenia z niej użytkownika. W telefonii internetowej najważniejsza jest jakość odbieranego głosu i opóźnienia w dwustronnej konwersacji. Sytuację komplikuje po części fakt, że te parametry są ze sobą powiązane, ponieważ lepsza jakość głosu wymaga większego strumienia bitów, a większy strumień bitów wprowadza większe opóźnienia. W celu zapewnienia wymaganej jakości należy znać przyczyny powstawania niekorzystnych zjawisk podczas transmisji pakietów. Następnie do rozległych sieci pakietowych należy wprowadzić mechanizmy, pozwalające poprawić istniejącą obecnie sytuację.

**6.2. Parametry sieci pakietowych**

**6.2.1. Pojemność transmisyjna**

Parametr ten opisuje ile czasu potrzeba do przesłania informacji gdy pominie się opóźnienia [10]. Dla każdych dwóch sąsiadujących ze sobą węzłów, pojemność transmisyjna jest równa szerokości dostępnego pasma w łączu. Tak zdefiniowany wskaźnik opisuje medium transmisyjne, z którego korzysta sieć IP. W warstwie transportowej sieć taka może korzystać z wielu różnych technologii oraz różnych łącz. Ze względu na taką budowę pojemność transmisyjna w każdym z kierunków może być inna. Sprawa komplikuje się, gdy rozpatrujemy pojemność transmisyjną węzłów nie sąsiadujących ze sobą. Jest to trudne ze względu na współdzielenie łączy przez różne ścieżki. Ponieważ to współdzielenie jest oparte na multipleksacji statystycznej, pojemność transmisyjna nie charakteryzuje się stałą wartością. Gdyby przyjąć, że żadne łącze nie jest współdzielone to pojemność transmisyjna między węzłami nie sąsiadującymi ze sobą jest równa najmniejszej pojemności łącza pomiędzy sąsiadującymi węzłami należącymi do łącza składowego.

**6.2.2. Straty**

Straty występują we wszystkich typach sieci, podobne są mechanizmy ich powstawania różne jednak możliwości ich ograniczania. Do podstawowych źródeł strat zaliczamy [10]:

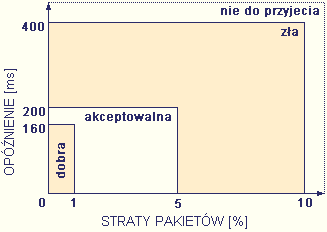
* Straty wynikające z błędów transmisyjnych w sieci. Powstają w sieciach o złej jakości, w momencie uszkodzenia sieci oraz w wyniku dostania się do sieci transmisyjnej niepożądanych sygnałów. Ogranicza się je poprzez stosowanie łączy wysokiej jakości.
* Przepełnienie buforów wyjściowych w węzłach sieci IP. Jest to zjawisko nazywane spiętrzeniem (congestion). Ograniczać je można przez zmniejszenie prędkości nadawania sygnałów ze źródła. Niestety protokół IP nie przewiduje takiego mechanizmu, w związku z tym nadmiarowe pakiety w kolejce są odrzucane.
* Przekroczenie możliwości kanału transmisyjnego sieci Frame Relay lub ATM. Jeżeli do przenoszenia ruchu związanego z IP są wykorzystywane sieci ATM i/lub Frame Relay to można optymalizować pracę na tym łączu poprzez wykorzystanie możliwości sterowania przepływem sieci i ograniczania prędkości nadajnika w zależności od możliwości transmisyjnych kanału wirtualnego. W celu wykorzystania tych możliwości konieczne jest zainstalowanie odpowiednich urządzeń wraz z oprogramowaniem w węzłach IP.

**6.2.3. Opóźnienia**

Opóźnienie jest to czas potrzebny na dostarczenie pakietu z jednego węzła sieci IP do drugiego. Czas ten zmienia się w trakcie trwania transmisji i może się różnić dla różnych kierunków w sieci. Na jego sumaryczną wartość, składają się:

* Czas propagacji w każdym z łączy na ścieżce - parametr stały w czasie, zależny od ośrodka i zastosowanej technologii.
* Czas serializacji pakietu przy opuszczaniu węzła sieci - opisany zależnością: czas serializacji = długość pakietu w bitach / prędkość interfejsu w bitach na sekundę.
* Czas obróbki pakietu w węźle sieci - zależny od sprzętu, oprogramowania i obciążenia procesora w węźle.
* Opóźnienia w buforach wyjściowych w węzłach sieci - zależne od ilości napływającej informacji do węzła w danej chwili i od szybkości łącza wychodzącego.

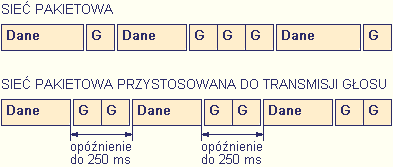
Pierwsze dwa parametry mają charakter ograniczeń fizycznych i ich poprawianie przez zastosowanie nowych technologii IP jest niemożliwe. Co najwyżej można ograniczyć ich wpływ przez budowanie sieci szerokopasmowych z małym czasem propagacji sygnału w łączu. Trzeci parametr można ograniczać poprzez stosowanie wydajniejszych algorytmów przetwarzania danych oraz wydajniejszych urządzeń. Parametr czwarty można ograniczyć przez zmianę mechanizmów kolejkowania z FIFO (First In First Out), na bardziej zaawansowane. Ze względu na stałą prędkość łącza nie jest możliwe wysyłanie danych z bufora z różną prędkością. Można jednak pewne dane wysyłać wcześniej od innych. Spowoduje to oczywiście zmniejszenie opóźnień pewnego typu danych np. audio i wideo, a wzrost opóźnień dla pozostałych danych, mniej wrażliwych na wielkość opóźnień.   
Przybliżone wartości dopuszczalnych opóźnień i strat pakietów oraz ich wpływ na jakość sygnału mowy przesyłanego w sieci pakietowej, przedstawiono na rys 6.1 [3]. Wielkości te mają charakter orientacyjny i ich spełnienie nie gwarantuje jeszcze zapewnienia odpowiedniej jakości usługi.



Rys. 6.1. Jakość rozmowy telefonicznej w zależności od parametrów sieci pakietowej

**6.2.4. Zmienność opóźnień w czasie - jitter**

Parametr na który szczególnie są wrażliwe sygnały pochodzące od aplikacji czasu rzeczywistego. Zmiany w opóźnieniu wprowadzane są w wyniku zmiennych w czasie warunków transmisji oraz przez buforowanie danych. Wielkość tych zmian jest rzędu dziesiątków milisekund, zatem dla użytkowników innych aplikacji jest zazwyczaj niezauważalna. Chcąc jednak aby sieć IP była przygotowana do transmisji głosu i sygnałów wideo należy ten parametr ograniczać. Możliwe jest to przez zastosowanie zaawansowanych metod kolejkowania uwzględniających zawartość pakietu, a także przez fragmentację pakietów.



Rys. 6.2. Opóźnienia przy przesyłaniu głosu w sieciach pakietowych

Rozmieszczenie pakietów zawierających dane i głos pokazano rys. 6.2. W górnym wierszu przedstawiono sytuację jaka panuje w sieciach nieprzystosowanych do transmisji głosu, poniżej zaś sytuację oczekiwaną w sieciach nowoczesnych.

**6.3. Mechanizmy kolejkowania i obsługi danych nadmiarowych**

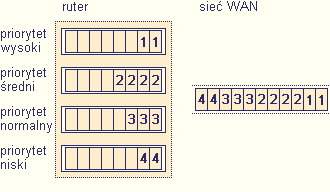
QoS wymaga utrzymywania w ruterach informacji o dotyczących stanu każdego przepływu, wpływających na normalne mechanizmy sygnalizacji i kolejkowania. Wszystkie hosty, rutery i inne elementy infrastruktury sieciowej leżące pomiędzy systemem źródłowym a docelowym, muszą mieć zaimplementowane mechanizmy obsługi funkcji QoS. Każde z tych urządzeń musi także mieć możliwość rezerwowania na ten cel zasobów, tzn. pasma, mocy obliczeniowej i pamięci operacyjnej. W chwili obecnej prowadzi się prace standaryzacyjne mające na celu zapewnienie jakości usług IP. Z krótkiej analizy obecnej sytuacji wynika, że standardy ciągle się rozwijają, protokoły nie zostały jeszcze należycie przetestowane, a produkty dopiero osiągną fazę dojrzałą. W rzeczywistości sieci uwarunkowane regułami podziału zasobów zaczną dopiero powstawać. Nie mniej należy jednak zauważyć, że w pewnych obszarach pojawiły się dość dobre rozwiązania zasługujące na krótkie omówienie. Są to między innymi mechanizmy związane z zachowaniem się węzłów w sytuacji gdy nastąpiło przeciążenie.  
W momentach gdy następują krótkie spiętrzenia danych, w celu uchronienia pakietów przed utratą, stosuje się mechanizmy kolejkowania i obsługi danych nadmiarowych. Strategia ta daje dobre rezultaty jeśli spiętrzenie jest na tyle krótkie, że możliwe jest opróżnienie buforów. Poniżej opisano kilka współcześnie stosowanych metod kolejkowania uwzględniających charakter ruchu istniejącego obecnie w sieciach IP.

**6.3.1. FIFO (First In First Out)**

Strategia stosowana powszechnie we współczesnych sieciach. Dane nadmiarowe są umieszczane w pamięci buforowej i opóźniane do momentu możliwości ich wysłania, mając nadzieję, że nie nadejdzie na tyle duża ilość danych, że bufory się przepełnią. Widać, że bez względu na zawartość pakietów, umieszczane są one w szeregu w kolejności w jakiej przybyły i w takiej samej kolejności są one też wysyłane dalej. Strategii tej nie można jednak zaliczyć do mechanizmów QoS, a jedynie do metod zapobiegających odrzucaniu pakietów.

**6.3.2. PQ (Priority Queuing)**

Metoda polegająca na podziale pamięci buforowej na kolejki o czterech różnych priorytetach, tzn. wysokim (High), średnim (Medium), normalnym (Normal) i niskim (Low). Schemat tak skonstruowanej pamięci buforowej przedstawiono na rys. 6.3.



Rys. 6.3. Podział pamięci buforowej na kolejki o różnych priorytetach

W momencie opróżniania buforów najwcześniej pobierane są dane z kolejki o priorytecie wysokim, w chwili gdy jest ona pusta przechodzi się do obsługi kolejki o priorytecie średnim. Po pobraniu z niej pakietu sprawdza się znów kolejkę o priorytecie wysokim. Jeżeli są w niej pakiety, to się je pobiera a jeżeli nie ma, to pobiera się pakiet z kolejki o najwyższym w danej chwili priorytecie, sprawdzając po tym kolejki o priorytetach wyższych. Postępuje się w ten sposób aż do opróżnienia wszystkich kolejek.   
Rozdzielanie pakietów na kolejki o różnych priorytetach odbywa się według reguł, które ustala administrator w każdym węźle sieci. Zasoby muszą być rozdzielane wśród klientów sieci którymi mogą być użytkownicy, aplikacje lub hosty. Same kolejki mogą być przydzielane na podstawie takich czynników, jak zawartość pól nagłówka IP i nagłówków TCP i UDP, zależeć mogą także od drogi, którą pakiet dotarł do rutera, czyli od interfejsu wejściowego. Możliwa jest klasyfikacja uwzględniająca zawartość pola Type of Service protokołu IP (IP Precedence), adresów źródłowego i docelowego IP jak i portu źródłowego i docelowego TCP i UDP. Możliwe jest także uwzględnianie rodzaju protokołu warstwy 5, dając wyższy priorytet protokołom czasu rzeczywistego takim jak RTP i RTCP (opisanymi w dalszej części pracy). Wadami mechanizmu Priority Queuing są:

* Zawłaszczanie pasma przez ruch o wyższym priorytecie.
* Zawłaszczanie kolejki przez jeden przepływ (flow), czyli sekwencję pakietów wysyłanych z określonego adresu IP i portu warstwy 4, do określonego adresu IP i portu warstwy 4.
* Brak możliwości współpracy z protokołem RSVP o którym będzie mowa w jednym z kolejnych rozdziałów, ponieważ mechanizm Priority Queuing wymaga jawnego i statycznego skonfigurowania i określenia reguł, według których będzie pracował proces klasyfikatora.

**6.3.3. PFPQ (Per Flow Priority Queuing)**

Jest to zmodyfikowany mechanizm Priority Queuing, gdzie usunięto wadę zawłaszczania kolejek przez jeden przepływ o nieproporcjonalnej liczbie pakietów, względem pozostałych przepływów o tym samym priorytecie. Utworzono tutaj tysiące kolejek, z których każda jest przeznaczona na pakiety należące do jednego przepływu. Pozostał także podział na kolejki o priorytetach wysokim (High), średnim (Medium), normalnym (Normal) i niskim (Low). Kolejki o jednakowym priorytecie są obsługiwane według ustalonego wcześniej algorytmu zapewniającego równouprawnienie wszystkich przepływów tego samego poziomu. Podobnie jak w mechanizmie Priority Queuing, kolejki o niższym priorytecie obsługiwane są w momencie gdy w kolejkach o priorytetach wyższych nie znajdują się żadne pakiety.

**6.3.4. CQ (Custom Queuing)**

W przypadku mechanizmu Custom Queuing, pamięć buforową związaną z interfejsem, dzieli się na kilkanaście niezależnie nazwanych kolejek, którym przypisuje się względny udział w dostępnym na interfejsie paśmie. Klasyfikacja odbywa się na podstawie takich samych reguł jakie stosowano w mechanizmie Priority Queuing. Pobieranie pakietów z kolejek odbywa się po oszacowaniu względnego udziału kolejek w paśmie. Udział w paśmie można definiować na dwa sposoby, na podstawie liczby pakietów lub na podstawie liczby bajtów jakie pobiera się w jednym cyklu z kolejki. Pierwsza metoda nie daje precyzyjnego podziału, między danymi pochodzącymi z różnych kolejek, ze względu na możliwe różne długości pakietów. Pozwala jednak na kontrolę nad czasem obsługi poszczególnych kolejek, co jest szczególnie ważne dla pakietów wrażliwych na opóźnienia. Druga metoda pozwala na bardziej precyzyjne rozdzielenie pasma pomiędzy pakietami pochodzącymi z różnych kolejek, jednak posiada także kilka wad. Jedną z nich jest konieczność stosowania dużych liczb bajtów do pobierania w jednym cyklu, aby dopasować limit bajtów do wielkości pakietów i aby pakiety nie przekraczały swą długością dopuszczalnego limitu bajtów aby mogły być w ogóle wysłane. Ze względu na stosowanie dużych parametrów, powstają duże opóźnienia związane z czasem obsługi kolejek. Istotną zaletą tegoż mechanizmu jest eliminacja zjawiska zawłaszczania łącza przez jeden rodzaj ruchu. Mechanizmy Custom Queuing i Priority Queuing nie współpracują z protokołem rezerwacji zasobów sieci RSVP, ze względu na konieczność statycznego skonfigurowania i określenia reguł, według których ma się odbywać klasyfikacja.

**6.3.5. WFQ (Weighted Fair Queuing)**

Mechanizm kolejkowania polegający na podziale pamięci buforowej na tysiące niezależnych kolejek, z których każda jest przeznaczona na pakiety należące do jednego przepływu. Na jeden przepływ składają się pakiety, które mają jednakowe wartości w polach definiujących porty w nagłówku TCP/UDP oraz jednakowe pola adresowe i rodzaj Type of Service zawarte w nagłówku protokołu IP. Klasyfikacja odbywa się na podstawie powyższych danych zatem klasyfikator nie jest konfigurowany statycznie.  
Główną ideą mechanizmu WFQ jest przyznawanie każdemu przepływowi a co za tym idzie każdej kolejce pewnej wagi. Jest ona wyliczana na podstawie wielkości i liczby pakietów w taki sposób, że im więcej pakietów i o większej długości należy do przepływu, tym większą wagę on otrzymuje. Przepływy o większej wadze są obsługiwane rzadziej, co w konsekwencji prowadzi do równego podziału dostępnego pasma pomiędzy przepływami. Do zalet mechanizmu WFQ należą prostota zarządzania i konfiguracji, eliminacja zawłaszczania łącza przez jeden przepływ i efektywna gospodarka pasmem. Do pozytywnych cech mechanizmu WFQ należy także zaliczyć możliwość współpracy z RSVP. Wadą mechanizmu WFQ jest brak pełnej kontroli nad opóźnieniem i pasmem. Eliminuje się to przez tworzenie kombinacji powyższej metody z innymi metodami kolejkowania. Do najważniejszych należą:

* PQWFQ (Priority Queuing WFQ). Prosta modyfikacja polegająca na dodaniu dodatkowej kolejki, która obsługiwana jest przed wszystkimi pozostałymi.
* CBWFQ (Class Based WFQ). Rozszerzenie mechanizmu WFQ przez przypisanie kolejce dodatkowego parametru prócz wagi. Tym parametrem jest klasa, która definiuje względny udział przepływu w paśmie łącza.
* PQCBWFQ (Priority Queuing Class Based WFQ). Jest to kombinacja dwu wyżej wymienionych metod.

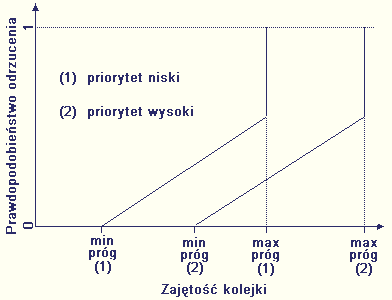
**6.4. Mechanizmy zapobiegania przeciążeniom**

Poprzednio opisane metody dotyczyły sytuacji, w której zaszło przeciążenie. Były to sposoby kolejkowania danych w pamięci buforowej. Gdy nadmiar pakietów jest długotrwały, pojemność pamięci buforowej nie wystarczy na zachowanie wszystkich pakietów docierających do węzła, zatem część z nich zostanie po prostu odrzucona. Aplikacje w reakcji na zaistniałą sytuację ponowią transmisję, co może pogłębić zjawisko przeciążenia, zwłaszcza, że odrzucane będą wszystkie pakiety, które nie zmieszczą się w kolejce.

**6.4.1. Mechanizmy RED (Random Early Detection) i WRED (Weighted RED)**

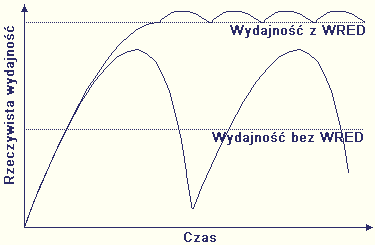
Jednym z rozwiązań jakie stosuje się podczas długotrwałego nadmiaru pakietów dochodzących do węzła, jest mechanizm zapobiegania zatorom Random Early Detection (RED). Jest on przeznaczony dla protokołów reagujących na gubienie pakietów [10].

Działa w ten sposób, że przed powstaniem zatoru, pakiety są losowo odrzucane tak, aby spowolnić niektóre źródła. Indywidualne spowalnianie sesji TCP zapobiega globalnej synchronizacji i powoduje lepsze wykorzystanie pasma.   
Działanie mechanizmu RED zależne jest od dwóch parametrów, minimalnej i maksymalnej zajętości kolejki oraz maksymalnego prawdopodobieństwa usunięcia pakietu. Kiedy wypełnienie kolejki osiągnie wskazany dolny próg rozpoczyna się losowe odrzucanie pakietów. Prawdopodobieństwo odrzucenia pakietu wzrasta wraz z poziomem wypełnienia kolejki. Kiedy wypełnienie kolejki przekroczy górny próg, następuje odrzucanie wszystkich pakietów. Statystycznie więcej pakietów będzie odrzucanych od użytkowników generujących dużo ruchu co powoduje, że ich ruch będzie bardziej tłumiony niż użytkowników generujących mało ruchu.



Rys 6.4. Zasada działania mechanizmu WRED

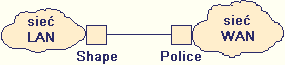
Odmianą mechanizmu RED rozpoznającą różne klasy ruchu (IP Precedence) jest WRED (Weighted Random Early Discarding). Dla każdej klasy definiowane są progi wypełnienia kolejki oraz maksymalne prawdopodobieństwo odrzucenia pakietu (rys. 6.4). Mechanizm WRED daje możliwość zapobiegania zatorom przez ograniczanie w pierwszej kolejności ruchu mniej istotnego.   
Mechanizm WRED, zakładający odrzucanie niektórych pakietów z kolejki, zanim się one całkowicie zapełnią ma bardzo istotny wpływ na efektywną transmisję. Schematycznie przedstawiono to na rys. 6.5.



Rys. 6.5. Wpływ stosowania mechanizmu WRED na wydajność kolejkowania

**6.4.2. Traffic Shaping i Traffic Policing**

W odróżnieniu od metody WRED, Traffic Shaping jest statyczną metodą polegająca na ograniczeniu prędkości wprowadzania danych do kolejek wyjściowych. Metoda ta ma za zadanie wygładzanie ruchu. Całość ruchu, kierowanego do interfejsu, jest dzielona na ten, który podlega wygładzaniu i pozostały. Pakiety niewygładzane są wprowadzane do kolejek w takim tempie, w jakim docierają do węzła. Pozostałe są wpisywane w ściśle określonym i stałym tempie, to znaczy, że jeśli przychodzą zbyt szybko, są opóźniane w buforze. Minimalizuje to prawdopodobieństwo odrzucania pakietów, kosztem zmienności opóźnienia. Protokoły adaptacyjne, takie jak TCP, reagują na wstrzymywanie pakietów spowalnianiem transmisji.   
Traffic Policing jest techniką polegająca na odrzucaniu pakietów. Węzeł odrzuca je z dokładnością do określonego parametru lub opcjonalnie przekwalifikowuje do niższej klasy. Zaletą tej technologii jest możliwość jej stosowania nie tylko na wyjściu ale i na interfejsach wejściowych. Zastosowanie jej na brzegu sieci na ruterach dostępowych umożliwia obronę przed nadmiernym, niezgodnym z umowami ruchem od obcych systemów. Przykład umiejscowienia omówionych technik przedstawiono na rys. 6.6.



Rys. 6.6. Umiejscowienie technik Traffic Shapingu i Trafic Policingu na tle systemu

**6.4.3. Link Fragmentation i Interleaving**

Techniki związane z zapewnieniem małego opóźnienia i stałości opóźnień, czyli istotnymi parametrami przy przesyłaniu głosu w czasie rzeczywistym w sieciach pakietowych. Potrzeba wprowadzenia powyższych technik, uzasadniona zostanie na przykładzie. Ruter z interfejsem wyjściowym 128 kb/s i kolejkowaniu Priority Queuing (patrz rys. 6.3), będzie gromadził w kolejce o najwyższym priorytecie pakiety VoIP, a w kolejce priorytecie średnim pakiety związane z innym ruchem w sieci. Pakiety głosowe są małe około 60 B, a pakiety pozostałe duże około 1500 B. Dodatkowo pakiety głosowe nadchodzą i powinny być wysyłane co 20 ms, o dopuszczalnej wariancji opóźnień 25 ms. Jeżeli w danej chwili nie będzie pakietów związanych z przesyłaniem głosu, zostanie rozpoczęte wysyłanie pakietów z kolejki o priorytecie średnim. Cały pakiet o wielkości 1500 B zostanie wysłany w czasie 94 ms. W tym momencie zostanie sprawdzona kolejka o priorytecie wysokim i jeżeli będą w niej dane, to mogą one czekać nawet do 94 ms, zatem dopuszczalne opóźnienie zostanie przekroczone. Zjawiska tego można uniknąć przez:

* Ograniczanie długości pakietu, przez ustawienie maksymalnej jego długości dla danego łącza na takim poziomie, aby wprowadzane przez nie opóźnienie nie przekraczało dopuszczalnej wartości przewidzianej dla pakietów VoIP. Spowoduje to oczywiście pogorszenie stosunku nagłówek/pole danych oraz odrzucanie pakietów większych od maksymalnej długości.
* Stosowanie techniki polegającej na podziale pola danych pakietu na stałej wielkości fragmenty i wysyłanie ich naprzemiennie z niewielkimi pakietami VoIP.

**6.5. Modele zapewniania QoS**

W chwili obecnej prowadzi się prace mające na celu rozwiązanie problemu jakości usług poprzez IP. Prace te obejmują dwa główne obszary. Pierwszy z nich już omówiony, dotyczy zmian związanych ze sprzętem sieciowym. Oznacza to tworzenie sprzętu dla użytkownika końcowego z lepszymi kodekami do cyfryzacji i kompresji głosu, oraz polepszenie transmisji poprzez sieć w wyniku zaimplementowania w węzłach mechanizmów kolejkowania uwzględniających priorytet transmisji głosu. Nie bez znaczenia pozostaje także rozbudowa i polepszanie jakości i przepustowości łączy. Drugim istotnym obszarem jest tworzenie nowych protokołów i mechanizmów sieciowych mających możliwość rezerwowania zasobów i priorytetowania ruchu. Aby strumień danych otrzymał wymaganą jakość usług, każdy węzeł sieci musi być powiadomiony o tych wymaganiach. Wyróżniamy dwie metody powiadamiania o wymaganiach na jakość usług [13]:

* Etykietowanie pakietów - powiadamianie poprzez oznaczanie pakietów.
* Sygnalizacja - powiadamianie poprzez specjalny protokół.

Istnieją dwa modele QoS. Są to model oparty na rezerwowaniu zasobów oraz model oparty na rozróżnianiu klas ruchu.

* cechy modelu opartego na rozróżnianiu klas ruchu.

W modelu tym nie ma jawnego zgłaszania przez aplikację wymagań co do jakości usługi, natomiast strumień danych generowany przez aplikację zaliczany jest do jednej z kilku klas ruchu. Każda klasa ruchu oznaczana jest odpowiednią etykietą zawartą w pakietach danych, na podstawie której węzły sieci dostarczają odpowiedniej jakości usługi. Węzły sieci nie dostarczają bezwzględnej jakości usług, lecz względną, **różnicując** ruch na podstawie przynależności do danej klasy. Model bardzo skalowalny z tego względu, że nie ma konieczności rozpoznawania pojedynczych strumieni danych.

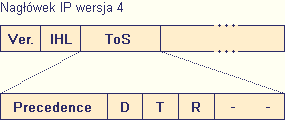
* cechy modelu opartego na rezerwacji zasobów.

Aplikacje przy pomocy protokołu sygnalizacyjnego zgłaszają sieci swoje wymagania w zakresie przepustowości i opóźnienia. Węzły sieci przeprowadzają kontrolę dostępności zasobów potrzebnych do zapewnienia żądanego poziomu usługi. W przypadku dostępności odpowiednich zasobów następuje ich rezerwacja tak, aby dany węzeł sieci mógł świadczyć żądaną jakość usługi. Rezerwacja gwarantuje aplikacji żądaną jakość usługi, o ile generowany przez nią ruch nie przekracza zgłoszonych parametrów. Węzeł sieciowy sprawdza i ewentualnie ogranicza ruch do zgłoszonych parametrów.

Przykładem mechanizmu opartego na pierwszym modelu jest IETF DiffServ, a mechanizmu opartego na drugim modelu jest IETF IntServ z użyciem protokołu RSVP (Resource Reservation Protocol).

**6.5.1. Mechanizm DiffServ**

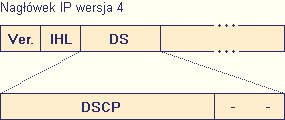
DiffServ definiuje sposób, w jaki bajt typu usług ToS (Type of Service) zawarty w nagłówku IP wersji 4 lub Traffic Class w nagłówku IP wersji 6 jest stosowany do specyfikowania informacji o wymaganych usługach [14]. Bajt typu usług określa jakość usług jakiej wymaga się od sieci. Znaczenie poszczególnych bitów tego słowa jest następujące (rys. 6.7).



Rys. 6.7. Pole Type of Service

Pierwsze trzy bity określają tzw. pierwszeństwo (IP Precedence). Dzięki temu możemy rozróżniać następujące typy datagramów:   
zwykłe (000),  
priorytetowe (001),  
natychmiastowe (010),  
błyskawiczne (011),  
superbłyskawiczne (100).

Bity DTR są to flagi oznaczające priorytet pod względem opóźnienia, przepustowości i niezawodności. Pole to zostało szczegółowiej omówione w rozdziale dotyczącym nagłówka protokołu IP.   
DiffServ odpowiada obecnemu użyciu wyżej opisanych bitów z obszaru ToS (rys. 6.8).



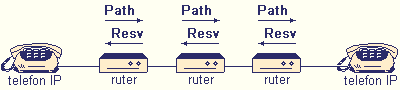
Rys. 6.8. Pole Differentiated Services

Ośmiobitowe pole DS (Differentiated Services) zawiera w sobie sześciobitowe pole DSCP (Differentiated Services Codepoint), oznaczające jakość usług. Istnieją w ramach tego pola 32 wartości zestandaryzowane, pozostałe możliwości pozostawiono do zastosowań lokalnych. Wartości zestandaryzowane zapewniają wsteczną kompatybilność z IP Precedence.  
Protokół DiffServ został przewidziany do przekazywania dla QoS ogólnych kategorii ruchu lub grup ruchu. Usługi zdefiniowane przez ten protokół działają wyłącznie na poziomie warstwy 3, bez przyjmowania jakichkolwiek założeń dotyczących niższego poziomu. W tym modelu zastosowanie QoS na poziomie urządzenia sieciowego implikuje cztery etapy.

* Klasyfikowanie według informacji przenoszonej przez nagłówek warstwy czwartej. Cechowanie w celu oznaczenia klasyfikacji.
* Sortowanie w sposób selektywny, głównie po to, aby uniknąć przeciążeń, wykonywane za pośrednictwem omawianego wcześniej algorytmu WRED (Weighted Random Early Detection).
* Dystrybuowanie, rozumiane przede wszystkim jako możliwość przejścia w stan oczekiwania i samo wysyłanie przy spełnieniu określonych warunków. Przeprowadzane jest ono dzięki licznym algorytmom, takim jak zrównoważony mechanizm zarządzania kolejkami (WFQ). Administratorzy sieciowi mogą konfigurować także algorytmy kształtowania ruchu Traffic Shaping i Traffic Policing.

**6.5.2. Protokół RSVP (Resource Reservation Protocol)**

RSVP jest protokołem umożliwiającym rezerwowanie "kanałów" dla strumieni danych w sieciach z protokołem IP, czyli zasobów sieci niezbędnych do przekazu informacji wymagającej odpowiedniej i gwarantowanej przepływności [13]. Rezerwacja zasobów dla telefonii internetowej inaczej niż w telefonii tradycyjnej jest odseparowana od fazy zestawiania połączenia.



Rys. 6.9. Sposób działania protokołu RSVP

Protokół RSVP definiuje dwie główne wiadomości sterujące, dzięki którym możliwe jest rezerwowanie zasobów na drodze transmisyjnej. Są to wiadomości Path i Resv (rys. 6.9). Wiadomość Path, określa rodzaj przesyłanych danych oraz wymagania dotyczące zasobów. Wiadomość Resv, umożliwia natomiast dokonanie rezerwacji. Wiadomość Path jest wysyłana okresowo od potencjalnego nadawcy do odbiorcy lub odbiorców. Każdy kolejny, ruter do którego przybywa ten pakiet, zapamiętuje adres rutera, z którego on przybył i na jego miejsce wpisuje swój adres i następnie przesyła pakiet do kolejnego węzła na ścieżce. W końcu pakiet Path dociera do odbiorcy, gdzie na podstawie otrzymanych informacji sporządza się pakiet Resv. Tak przygotowany pakiet wysyłany jest do rutera, z którego przyszła wiadomość Path. Ruter może przyjąć, bądź odrzucić wiadomość Resv. Gdy jednak przyjmie pakiet, to na podstawie informacji w nim przenoszonych ustawia określone parametry, a następnie kieruje pakiet do następnego rutera, którego adres zapamiętał podczas transmisji pakietu Path. Rezerwacja zostaje zakończona, gdy wiadomości Resv dotrą do nadawcy wiadomości Path. Aplikacja stacji końcowej może wówczas rozpocząć transmisję na przykład audiokonferencji.   
Zarezerwowane zasoby są zwalniane po upływie pewnego czasu, dlatego aktywne strumienie muszą co jakiś czas odświeżać rezerwację. Cechą charakterystyczną protokołu RSVP jest to, że rezerwacja dokonywana jest w kierunku od odbiorcy do nadawcy, co przy transmisji rozsiewczej (multicast), umożliwia każdemu odbiorcy strumienia danych dokonania rezerwacji z różnymi parametrami, pomimo tego, że nadawana wiadomość pochodzi z jednego źródła.   
Pakiety RSVP są transportowane w polu danych pakietów IP. Wartość 46 w odpowiednim polu nagłówka, sygnalizuje że w polu danych znajduje się pakiet RSVP. Wprowadzanie protokołów umożliwiających gwarantowanie parametrów QoS do sieci IP   
Administratorzy sieciowi przedsiębiorstw wprowadzą prawdopodobnie DiffServ dla większości warunków QoS, używając niekiedy RSVP dla bardzo wrażliwych aplikacji, jak na przykład VoIP, które wymagają rezerwowania zasobów i kontroli dopuszczeń wychodząc z założenia, że lepiej odrzucić wywołanie telefoniczne, niż dostarczyć usługę złej jakości.   
Obiektywnie patrząc, lepszym choć trudniejszym do wprowadzenia jest mechanizm bazujący na rezerwacji zasobów. RSVP jest protokołem sygnalizacji, który sygnalizuje węzłom na ścieżce do odbiorców, nadejście strumienia danych wymagającego określonej jakości usług. Wszystkie operacje przeprowadza się na strumieniu kierowanym do jednego lub do wielu odbiorców. Strumień jest identyfikowany przez adres IP, port przeznaczenia lub etykietę przepływu (flow label w IPv6). Te dobrze zdefiniowane mechanizmy ułatwiają implementację mechanizmów kolejkowania, podwyższających skuteczność protokołu. Jednak odpowiedzialność za spełnienie QoS spada na oprogramowanie rutera.   
Dla operatora RSVP jest protokołem ściśle związanym z rezerwacją, która musi być przeprowadzona we wszystkich węzłach sieci na ścieżce do odbiorcy, lub na ścieżkach określonych przez multicast. Aplikowanie algorytmów sterujących kolejkami i priorytetami staje się tak samo ważne jak sam protokół. Dlatego też w rozwiązaniach firmowych RSVP współpracuje najczęściej z WFQ (Weighted Fair Queuing) lub jego udoskonalonymi wersjami PQWFQ (Priority Queuing WFQ) lub CBWFQ (Class Based WFQ). Niestety brak jest jednolitych rozwiązań w tym kierunku, co doprowadzić może do różnych konfliktów, uniemożliwiając w konsekwencji wykorzystanie w pełni zalet protokołu RSVP zwłaszcza w Internecie, gdzie sprzęt pochodzi od różnych dostawców.   
Nie ulega wątpliwości, że realizacja QoS w sieciach IP jest obecnie kluczową kwestią, jeżeli sieci IP mają się stać uniwersalną platformą wielousługową. Wydaje się, że zaproponowane dotychczas rozwiązania nie są ostateczne i będą w dalszym ciągu rozwijane. Mechanizmy QoS będą wdrażane, a obserwacje wnioski z ich funkcjonowania będą wprowadzane do nowych i rozszerzonych wersji standardów tak aby zapewnić pełną funkcjonalność w realizacji QoS.   
Mechanizmy, które implementują producenci sprzętu sieciowego w swoich produktach, mogą na razie polepszyć QoS w sieciach prywatnych, gdzie istnieje możliwość nadzoru nad całą siecią, a zwłaszcza nad częścią dotyczącą usług związanych z transmisją głosu i obrazu w czasie rzeczywistym. Można tam wprowadzać urządzenia, które będą gwarantowały współpracę pomiędzy firmowymi rozwiązaniami. Przewiduje się jednak, że w późniejszym okresie również Internet będzie oferował lepsze QoS, zależnie od tego jak szybko techniki zapewniania QoS osiągną fazę dojrzałą i będą powszechnie dostępne. Stworzy to między innymi możliwość różnicowania opłat za korzystanie z różnych usług w sieci IP, ponieważ różne taryfy będą odpowiadać realizacji różnego poziomu QoS.