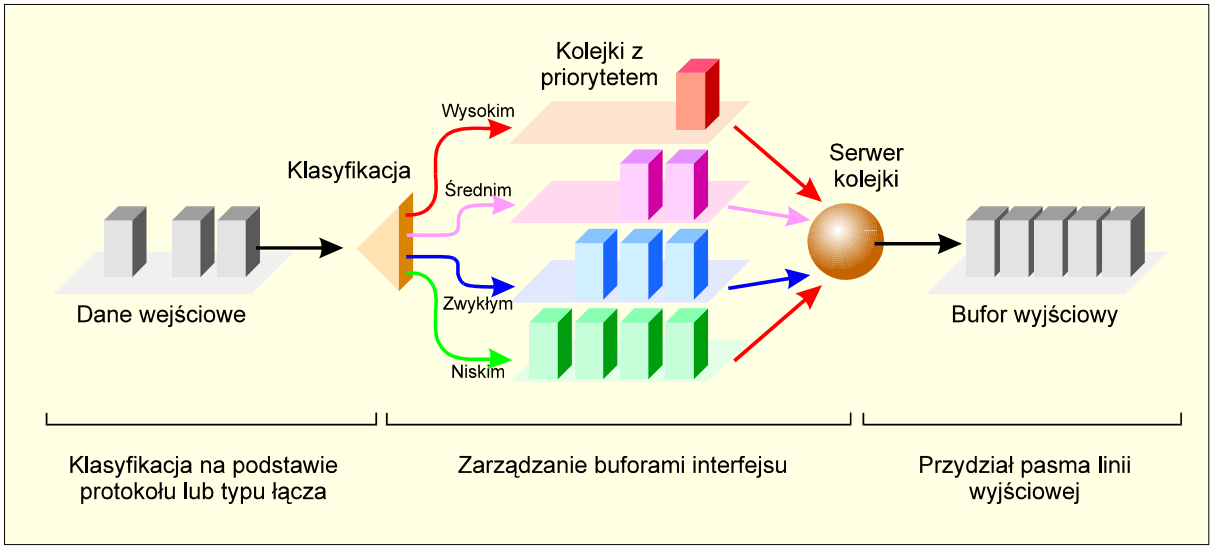
Mechanizmy realizacyjne

Kolejkowanie

Powszechnie stosowanym rozwiązaniem problemu przeciążenia ruchem elementów wyjściowych dużych węzłów sieci internetowych jest wykorzystanie schematu kolejkowania z ewentualną implementacją mniej lub bardziej zaawansowanych mechanizmów priorytetujących. Każde z występujących w praktyce eksploatacyjnej rozwiązań stanowi schemat przeznaczony do rozwiązywania konkretnego problemu ruchowego, a więc są to funkcje dedykowane określonym zastosowaniom. Zestaw najczęściej spotykanych implementacji systemów kolejkowych obejmuje następujące aplikacje:

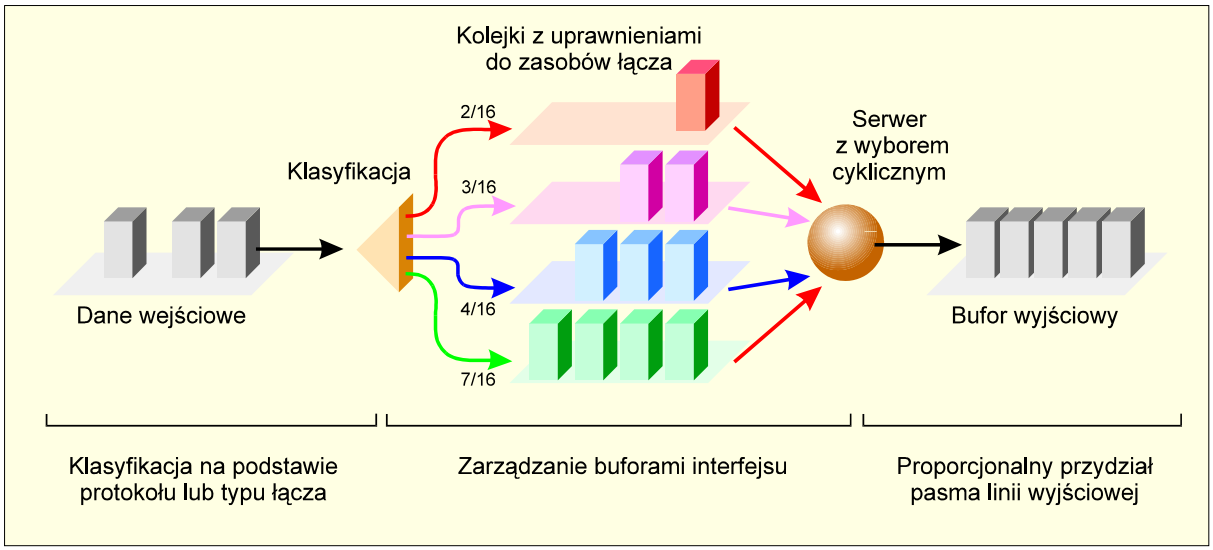
Rejestry FIFO – najprostsze rozwiązanie, w którym nadmiarowe pakiety są przechowywane w buforze do chwili zwolnienia się łącza, którym mogą opuścić węzeł. Jedyną zaletą rozwiązania jest brak konieczności konfiguracji, wada to negatywny wpływ źródeł z nierównomiernym ruchem na opóźnienia w innych strumieniach, a w tym aplikacji czasu rzeczywistego (mowa, wideo) oraz sygnalizacji i sterowania.

Kolejkowanie z priorytetowaniem – schemat, w którym pakiety uznawane za ważne są obsługiwane w pierwszej kolejności. Dzięki odpowiedniej konfiguracji istnieje możliwość wyróżniania przekazów generowanych przez wybrany protokół, dostarczonych do ustalonego portu wejściowego, posiadających określone rozmiary, kierowanych pod zadany adres docelowy itp. Schemat zakłada wykorzystanie kilku buforów o malejącym priorytecie – dane są wysyłane na wyjście o ile wszystkie kolejki o wyższej wadze nie zawierają pakietów, czyli zgodnie z poniższym schematem:



Wykorzystanie priorytetowania jest wystarczające, gdy istnieje potrzeba zapewnienia, by dane generowane przez krytyczne aplikacje były obsługiwane w pośredniczących sieciach WAN w pierwszej kolejności.

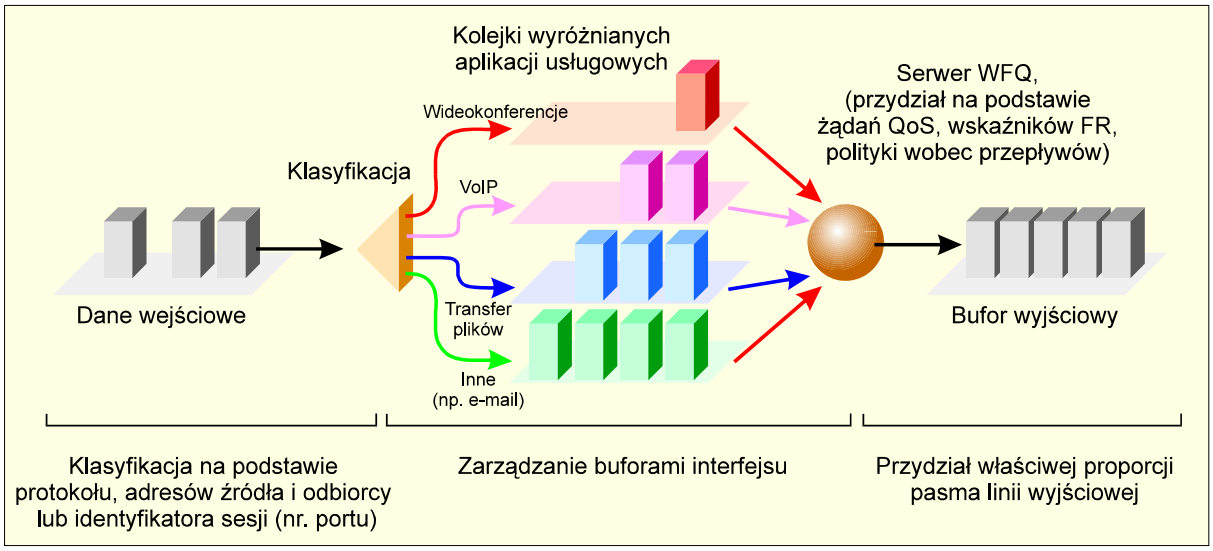
Gwarantowanego pasma – schemat użyteczny w przypadkach, gdy różne aplikacje lub jednostki organizacyjne przedsiębiorstwa muszą posiadać stały dostęp do sieci z gwarancjami pewnego minimalnego pasma lub maksymalnego opóźnienia przekazu. Oznacza to, że wystąpienie natłoku nie zablokuje transferu wskazanych strumieni, a jedynie zmniejszy jego efektywność, dzięki czemu pozostanie nieco pasma dla innych nie chronionych aplikacji. Realizacja schematu w praktyce polega na przypisaniu każdej z klas ruchowych ustalonej części bufora i obsługiwaniu nich kolejno, w sposób cykliczny.



Procedura odbiorcza umieszcza otrzymywane informacje w jednej z *n+1* kolejek (kolejka 0 jest przeznaczona do obsługi wiadomości systemowych. Serwer obsługuje kolejki od *1* do *n* cyklicznie pobierając z nich za każdym razem tyle pakietów ile ustalono w fazie konfiguracji. Gwarantuje się w ten sposób, że w przypadku przeciążenia każda z aplikacji otrzyma taki udział w dostępnym paśmie jaki dla niej przewidziano.

Schematy gwarantowania pasma i kolejkowania priorytetowanego funkcjonują w trybie statycznym tj. nie adaptują się do zmian sytuacji ruchowej w sieci.

Kolejkowanie ważone ze sprawiedliwym przydziałem (pasma) – najbardziej zaawansowany schemat obsługowy, użyteczny zwłaszcza w przypadkach, gdy sieć musi przenosić ruch ze źródeł o znacznym zróżnicowaniu natężeń. W typowej realizacji, w pierwszej kolejności obsługiwany jest ruch związany z interakcjami multimedialnymi, zaś pozostałe pasmo jest dzielone sprawiedliwie pomiędzy pozostałe aplikacje. W efekcie preferowane są sesje bezpośredniej komunikacji użytkowników, zaś wymiana danych komputerowych jako mniej krytyczna czasowo jest realizowana w dalszej kolejności. Opisany mechanizm działania, oznaczany w literaturze jako WFQ (*Weighted Fair Queuing*), ilustruje poniższy schemat:



Wysoka efektywność schematu przejawia się zwłaszcza w zdolności do zagospodarowania całości dysponowanego pasma na potrzeby ruchu o niższych priorytetach, o ile stojące wyżej w hierarchii kolejki są puste. Równie istotną zaletę algorytmu stanowi jego zdolność do minimalizowania zmienności opóźnienia w pętli (*round-trip delay*). Efekt ten jest szczególnie wyraźnie obserwowalny w systemach realizujących obsługę licznych sesji konwersacyjnych o dużym zapotrzebowaniu na pasmo, gdzie szybkość transmisji oraz interwały pomiędzy otrzymywaniem kolejnych pakietów stają się lepiej przewidywalne.

W szczególności WFQ znacznie poprawia wydajność typowych algorytmów sterowania łączem logicznym (*Logical Link Control – LLC*) klasycznych protokołów pakietowych, zaś w systemach internetowych usprawnia funkcjonowanie mechanizmów przeciwdziałania przeciążeniom i tzw. wolnego startu (*slow-start*) wbudowanych w protokół TCP.

Typowa realizacja sterowania WFQ jest w stanie rozpoznawać także priorytet pakietów IP dzięki analizie ich właściwego pola nagłówkowego, które może przenosić wartości z zakresu 0 – 7. Algorytm przydziela przy tym proporcjonalnie więcej pasma transmisjom oznaczanym wyższymi priorytetami, co sprawia, że są one obsługiwane szybciej niż inne, nawet w przypadku wystąpienia natłoku. Efekt ten osiąga się przypisując każdemu z przekazów odpowiedniej wagi (tym niższej im szybciej musi być obsługiwany), gdzie wskaźnik z nagłówka pakietu IP służy jako obiektywna miara znaczenia danego procesu. I tak np. pakiety oznaczone priorytetem 7 otrzymują niższą wagę niż opatrzone wartością 3 i w rezultacie uzyskują pierwszeństwo w module nadawczym.

Jeśli w systemie funkcjonuje protokół RSVP to jego mechanizmy są w stanie wykorzystywać funkcje WFQ w celu przydzielania przestrzeni buforów, ustalania kolejności wysyłki pakietów oraz gwarantowania pasma dla wyróżnionych przekazów. Natomiast w sieciach FR, gdzie natłok jest sygnalizowany flagami FECN (*Forward Explicit Congestion Notification*) i BECN (*Backward Explicit Congestion Notification*) proces przyznawania wag przez algorytm WFQ uwzględnia ich wartości, dzięki czemu częstotliwość występowania przeciążeń ulega zmniejszeniu.

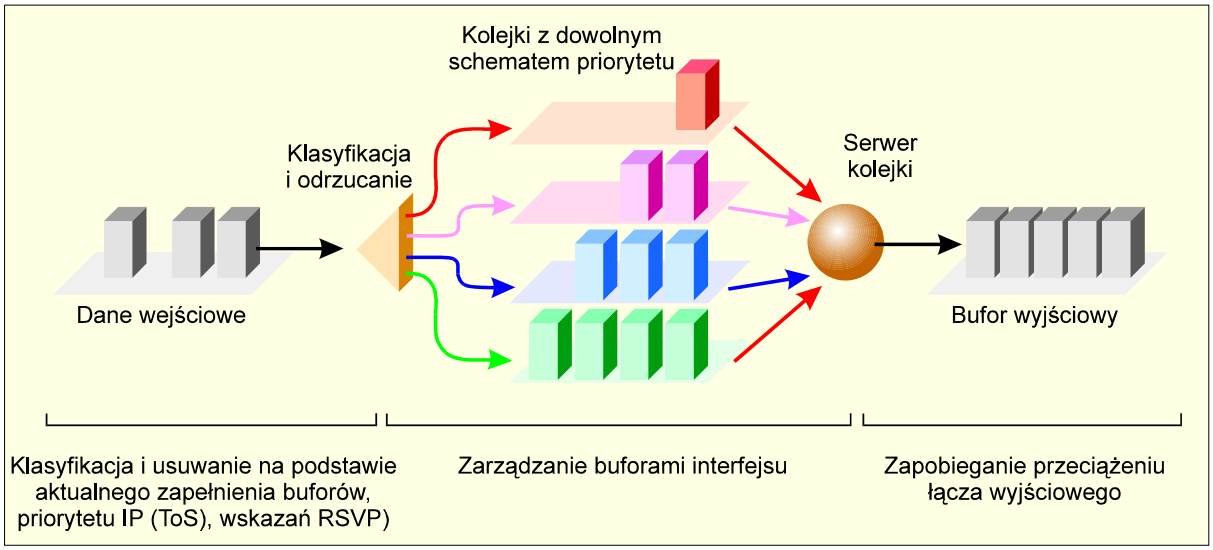
Z przedstawionych informacji wynika, że WFQ stanowi najbardziej zaawansowane rozwiązanie, zdolne do automatycznej adaptacji do aktualnych warunków ruchowych panujących w sieci. Ogranicza to nakłady niezbędne do realizacji optymalnej konfiguracji systemu, stąd WFQ domyślnie obsługuje interfejsy o przepustowościach rzędu 2048 kbit/s, których ilość w obecnie eksploatowanych sieciach jest największa.

Zapobieganie przeciążeniom

Mechanizmy zapobiegania przeciążeniom prowadzą ciągłe monitorowanie obciążenia sieci w celu możliwie wczesnego wykrycia symptomów narastającego natłoku i podjęcia odpowiednich działań o charakterze prewencyjnym. Podstawą sprawnego funkcjonowania systemu nadzorowania ruchu jest zawsze zestaw algorytmów realizujących swoje działania w sposób właściwy specyfice chronionego systemu.

Większość urządzeń instalowanych obecnie w systemach internetowych wykorzystuje schemat, w którym funkcje zapobiegawcze umiejscowione są w punktach współpracy międzysieciowej, tak aby problemy w jednym z segmentów nie degradowały właściwości użytkowych pozostałych zasobów. Typową implementację tej klasy rozwiązań stanowi algorytm RED (*Random Early Detection*), którego funkcjonowanie polega na losowym kasowaniu pakietów w przypadku narastania natłoku. Wymieniające informacje elementy systemu wykrywają rosnący poziom strat i w efekcie zmniejszają tempo wprowadzania danych do sieci, co minimalizuje szansę narastania sytuacji kryzysowej. RED powstał jako mechanizm wspomagający funkcjonowanie protokołu TCP w intersieciowym środowisku internetowym.

Mniej destrukcyjną funkcję sterującą stanowi implementacja schematu WRED (*Weighted Random Early Detection*), która stanowi uzupełnienie algorytmu RED możliwością selektywnego wyboru usuwanych pakietów w oparciu o priorytetowanie poziomu IP. W efekcie ruch o większym znaczeniu jest chroniony przed stratami zaś system może różnicować tryb obsługi transmisji stosownie do ich klasy usługowej. Ideę funkcjonowania algorytmu WRED ilustruje poniższy schemat:

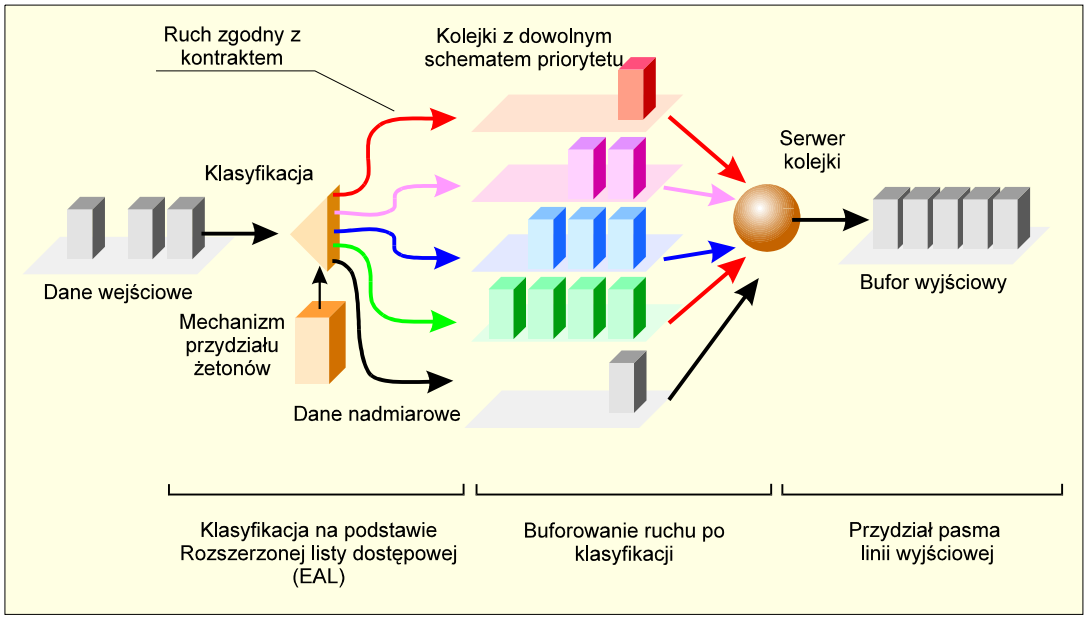


Choć WRED może współpracować z mechanizmami sterującymi protokołu RSVP i w efekcie jest w stanie realizować w ograniczonym zakresie politykę gwarantowania jakości zintegrowanych usług internetowych, jego ograniczenia spowodowały pojawienie się udoskonalonej wersji znanej jako D-WRED (*Distributed Weighted Random Early Detection*). Jest to mechanizm o większej szybkości przetwarzania zdolny do funkcjonowania w rozproszonym środowisku sterującym, oferujący ponadto możliwość konfigurowania wartości minimalnych i maksymalnych progów kolejek oraz elastycznego kształtowania polityki usuwania pakietów w odniesieniu do konkretnych klas usługowych.

Kształtowanie zależności czasowych i funkcje nadzorcze

Nierównomierność generacji ruchu przez źródła realizujące przekazy zintegrowanych multimediów sprawia, że we współczesnych sieciowych systemach internetowych występuje znaczne zagrożenie występowaniem przeciążeń. To niekorzystne zjawisko może być zwalczane przy wykorzystaniu specjalizowanych funkcji (tzw. shaperów) redukujących impulsowy charakter zmian obciążenia poszczególnych zasobów.

Klasyczne rozwiązanie problemu kształtowania zależności czasowych polega na wykorzystaniu tzw. schematu cieknącego zbiornika (*leaky bucket* lub *token bucket*), stanowiącego podstawę funkcjonowania powszechnie stosowanego w sieciach internetowych algorytmu GTS (*Generic Traffic Shaping*). GTS obsługuje pojedynczy interfejs wykorzystując przydzielony bufor do przejmowania chwilowego nadmiaru dostarczanych danych. Są one następnie nadawane do odbiorcy w chwilach zaniku aktywności źródła, co sprawia, że obciążenie łącza staje się równomierne i prawdopodobieństwo wystąpienia natłoku osiąga mniejsze wartości.



Wykorzystując odpowiednie wykazy sporządzane w chwili konfiguracji, GTS może ograniczać swoje działania do wskazanych strumieni danych, dzięki czemu bezkonfliktowo współpracuje z większością popularnych technologii warstwy 2 modelu OSI, a w tym: Frame Relay, ATM, SMDS oraz Ethernet. W przypadku funkcjonowania na interfejsie FR, GTS może być przystosowany do dynamicznej adaptacji szybkości nadawania, stosownie do stanu obciążenia wskazywanego sygnałami BECN albo też funkcjonować w podstawowym trybie, utrzymując transmisję ze stałą prędkością. Natomiast w systemie ATM właściwa konfiguracja GTS umożliwia współpracę z mechanizmami RSVP dzięki wymianie sygnalizacji za pośrednictwem stałego kanału wirtualnego PVC.

W przypadku, gdy podstawą funkcjonowania instalacji sieciowej jest technologia FR, kształtowanie zależności czasowych strumieni przenoszonych pakietów powierzane jest zazwyczaj dedykowanemu mechanizmowi FRTS (*Frame Relay Traffic Shaping*), który zoptymalizowano uwzględniając istotne wymagania środowiska. W odróżnieniu od GTS, algorytm FRTS wykorzystuje wszystkie sygnały sterujące dostępne w sieci FR, a więc nie tylko FECN i BECN, lecz również stan flagi DE, co sprzyja lepszym gwarancjom parametru CIR (*Committed Information Rate*). W efekcie system FR staje się lepiej skalowalny, osiąga lepsze własności użytkowe, a zatem może obsłużyć więcej kanałów wirtualnych przy

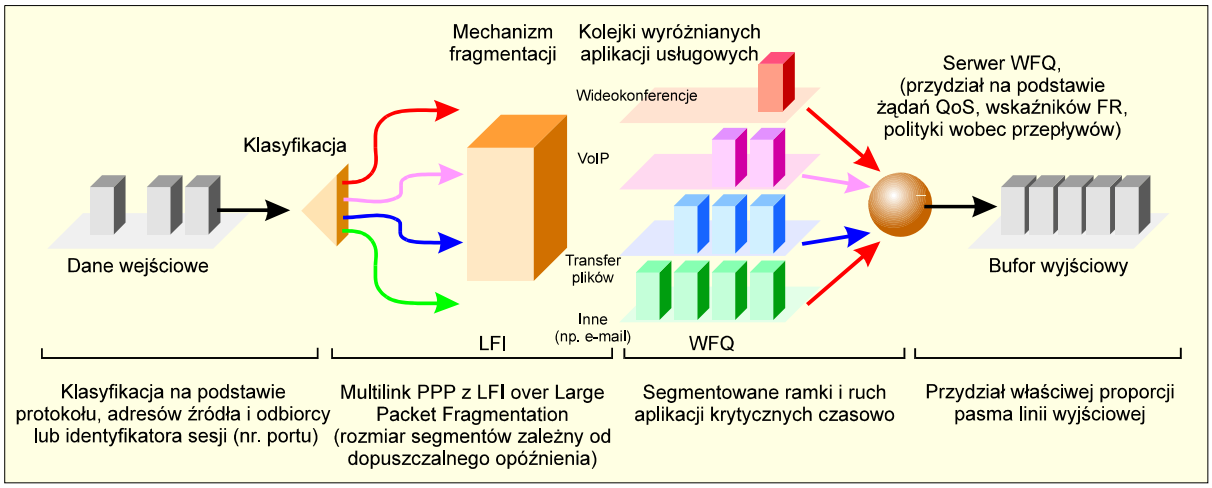
utrzymaniu czasu odpowiedzi na wymaganym poziomie. Dzięki wykorzystaniu opcji konfiguracyjnych staje się możliwe definiowanie priorytetów oraz organizacja kolejkowania z gwarantowaniem pasma i to bądź na poziomie wirtualnych kanałów, bądź w odniesieniu do całego podinterfejsu. Zestaw elementarnych opcji uzyskiwanych dzięki zastosowaniu FRTS obejmuje ponadto możliwość: programowego ustalania zezwoleń na wprowadzanie ruchu nadmiarowego opisanego parametrem EIR (*Excess Information Rate*), kombinowania różnych trybów kolejkowania, przesyłania w pojedynczym VC danych generowanych przez różne protokoły z niezależnym rezerwowaniem pasma, a także inteligentnego ograniczania ruchu w odpowiedzi na otrzymanie pakietów z ustawioną flagą BECN. W ostatniej opcji router przetrzymuje okresowo pakiety, aby zredukować obciążenie kierowane do sieci FR, zaś stopień ograniczania jest wyznaczany na podstawie liczby pakietów zawierających wskazanie natłoku.

Jakkolwiek już wymienione dotąd właściwości FRTS pozwalają na optymalne wykorzystanie każdego z dysponowanych kanałów transmisyjnych (VC) sieci FR, to do dyspozycji użytkownika stoją jeszcze inne funkcje, które choć bardziej rozbudowane oferują jeszcze bardziej istotne korzyści. I tak, w sieci korporacyjnej z szybkimi łączami do siedziby głównej i relatywnie wolniejszymi pomiędzy oddziałami terenowymi, FRTS jest w stanie łagodzić ograniczenia wynikające z niedostatku pasma dzięki programowemu ograniczaniu prędkości przekazu od siedziby głównej i priorytetowaniu wybranych łączy wskazywanych standardowo identyfikatorem DLCI (*Data-Link Connection Identifier*). Innym przykładem nowych możliwości jest wreszcie zdolność do kształtowania prędkości przekazu na podstawie kryteriów innych niż wskazania klasycznych parametrów CIR lub EIR, a to dzięki funkcji wstępnego przydziału pasma każdemu kanałowi VC. W ten sposób FRTS umożliwia m. in. konstruowanie wirtualnych sieci pakietowych realizujących filozofię TDM

Mechanizmy zwiększania efektywności wykorzystania łącza

Już na wczesnym etapie rozwoju sieci internetowych zaobserwowano, że ruch generowany przez źródła pozostające we wzajemnych interakcjach (Telnet, VoIP itp.) jest silnie zakłócany w relacjach czasowych (opóźnienie, jitter itp.) w wyniku przetwarzania przez zasoby systemu dużych pakietów obsługujących wymianę LAN-to-LAN, transfery FTP itd. Zjawiska te nasilają się zwłaszcza w przypadku, gdy sieć posiada wąskie gardła w postaci łączy o niskiej przepływności. Rozwiązaniem przedstawionych problemów okazała się implementacja specjalnych algorytmów, które w sposób inteligentny sterują przepływem danych tak, by odbywał się on bardziej równomiernie. Ich wykorzystanie poprawia efektywność oraz przewidywalność reakcji zasobów sieciowych, ocenianych z poziomu aplikacji usługowych.

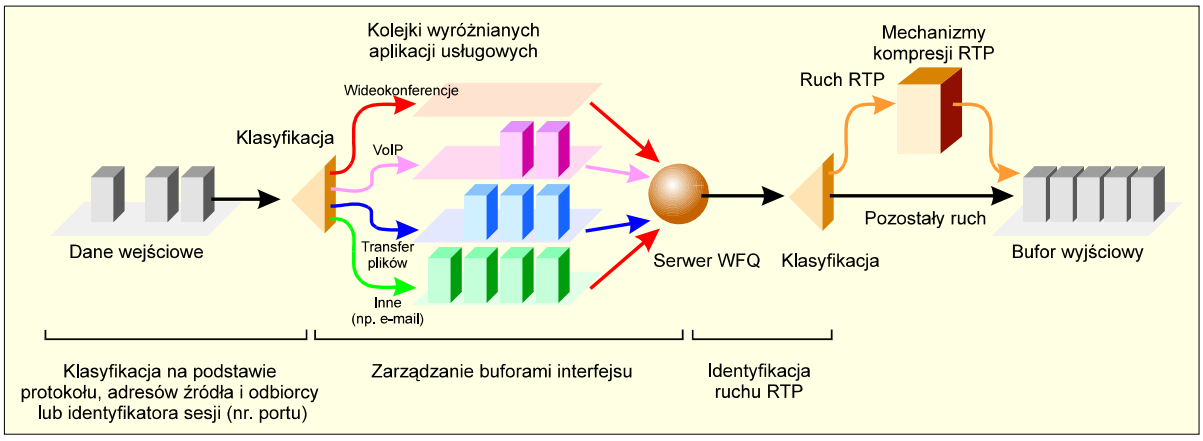
W przypadku systemów o relatywnie niskim obciążeniu i wolnych łączach, gdzie opóźnienie wnoszone przez proces szeregowego nadawania bitów jest znaczące, wystarczające jest wykorzystanie funkcji fragmentacji i przeplatania danych LFI (*Link Fragmentation and Interleaving*). Realizuje ona intuicyjnie oczywisty schemat, w którym duże pakiety dzielone są na części, nadawane na przemian z oczekującymi w kolejce ramkami o mniejszych rozmiarach.



LFI wymaga współpracy z protokołem PPP (*Point-to-Point Protocol*) realizującym opcję multilink, zaś jego implementacja jest zgodna z zapisami draftu IETF „Multiclass Extensions to Multilink PPP".

Opcją o wyższym stopniu zaawansowania, jakkolwiek łatwo realizowalną, jest rozwiązanie polegające na kompresji nagłówków protokołu RTP (*Real-Time Transport Protocol*), które znane jest pod nazwą *Real-Time Protocol Header Compression - RTP-HC*.

RTP stanowi klasyczny protokół internetowy funkcjonujący w układzie host-to-host i przeznaczony do obsługi transportu danych multimedialnych, a zwłaszcza pakietyzowanych transmisji głosowych oraz wideo. Pomysł na ulepszenie wynika ze spostrzeżenia, że typowy pakiet RTP przenosi 40 bajtowy nagłówek oraz 20 – 150 bajtowe pole danych użytkownika.



Zaproponowany mechanizm redukuje objętość nagłówka do 2 – 5 bajtów, co jest szczególnie cenne, gdy przesyłane jest niewiele danych (VoIP), zaś łącze posiada niewielką przepustowość (385 i mniej kbit/s). Mechanizm RTP-HC wykazuje zasadniczą zgodność z draftem IETF „Compressed RTP (CRTP)", może zaś być realizowany na łączach szeregowych zrealizowanych w technologii FR, HDLC (np. X.25), PPP, a także zgodnych z normalizacją ISDN.

Sygnalizacja QoS

Sygnalizacja QoS stanowi jedną z form wewnętrznej komunikacji elementów sieciowych, która umożliwia im wzajemne informowanie się o własnych oczekiwaniach i żądaniach. W efekcie możliwa jest koordynacja wykorzystania przedstawionych wcześniej technik i ustanowienie ścieżki funkcjonalnego gwarantowania jakości usługowej pomiędzy stacjami wymieniającymi informacje za pośrednictwem sieci (w relacji *end-to-end*). Oznacza to, że

każdy uczestniczących w przekazywaniu informacji element, a więc węzeł komutacyjny, firewall, host, klient itp., dostarcza w sposób powiązany z resztą zasobów systemu własnego wkładu w sumaryczną QoS postrzeganą przez finalnego odbiorcę.

Jakkolwiek proces wymiany danych i synchronizacji działań jakościowych wygląda prosto, gdy opisują go zgrabnie formułki, dla praktyka jest oczywiste, że problem pojawia się w chwili wdrażania konkretnych rozwiązań, tym bardziej, że środowisko współczesnych sieci internetowych jest silnie heterogeniczne. Wymusza to w pierwszym rzędzie potrzebę wykorzystania wielu niezależnych i obciążonych specyfiką systemów.

W istniejących uwarunkowaniach najbardziej celową strategią jest rezygnacja z wzajemnego dopasowywania lokalnych mechanizmów funkcjonujących zazwyczaj na poziomie 2 modelu OSI i zastąpienie ich jednolitym systemem komunikacji posadowionym w kolejnej, 3 warstwie funkcjonowania sieci. W ten sposób procedury komunikacji interdomenowej oraz inne, np. związane z ustanawianiem sesji pomiędzy użytkownikami mogą być w pełni kompatybilne, stanowiąc rodzaj spoiwa integrującego odrębne segmenty sieciowe w pojedynczą całość. Efektom tym sprzyja wykorzystanie standardowych protokołów, które z uwagi na posiadane właściwości najlepiej spełniają oczekiwania operatora oraz jego klientów. W praktyce eksploatacyjne spotykane są dwa alternatywne rozwiązania: bazujące na internetowym schemacie SIP (*Session Initiation Protocol*) albo zestawie normatywów ITU H.323. Wykorzystanie protokołu SIP oznacza, że jego wiadomości (np. INVITE) zawierają informację niezbędną do odnalezienia adresata (jego nazwę i domenę), wskazanie hosta (adresy IP oraz portu), identyfikację użytkownika i zakres jego uprawnień oraz dodatkowe informacje techniczne (np. sposób kodowania przekazów głosowych). Z kolei decyzja o użyciu zestawu H.323 powoduje, że rejestrację, autoryzację i obsługę wywołania prowadzić będą mechanizmy H.225, natomiast wymianę danych o wyposażeniu stacji i opcjach usługowych oraz ustanowienie sesji umożliwi schemat H.245.

Po ustanowieniu wzajemnej komunikacji następuje faza wymiany danych użytkowych. W jej trakcie zdecydowana większość współczesnych systemów internetowych wykorzystuje do różnicowania aplikacji pod względem jakościowym informację o priorytecie przenoszoną w nagłówku każdego z datagramów IP. Natomiast w razie potrzeby udzielania bardziej rygorystycznie pojmowanych gwarancji korzysta się z możliwości transferowych oferowanych przez protokół RSVP. Rozwiązania te zostaną w dalszym ciągu przedstawione bardziej szczegółowo.

Oczekiwania nadawcy odnośnie priorytetu generowanych przez niego danych wyznacza 3 bitowe pole nagłówka protokołu IPv4. Pole to stanowi składnik bajta ToS (*Type of Service*).

Ponieważ sieć rezerwuje dla własnych potrzeb dwie spośród ośmiu możliwych do ustawienia kombinacji bitowych, użytkownik dysponuje sześcioma poziomami priorytetu, które może wykorzystać odpowiednio do własnych potrzeb. Jednak realizując tą możliwość należy pamiętać, że sieć często ignoruje dane wpisane przez stację końcową, uznając za nadrzędny interes dostarczanie optymalnych gwarancji jakościowych całości globalnie pojmowanego obciążenia ruchowego. W ten sposób staje się możliwa realizacja szeregu zaawansowanych funkcji w rodzaju routingu warunkowanego polityką QoS (*Policy-Based Routing - PBR*), czy też zachowywania ustalonego pasma (*Committed Access Rate - CAR*). Funkcje te z kolei otwierają dostęp do bardziej elastycznego wykorzystania priorytetów, a w tym ich ustanawiania nie tylko przez aplikację bądź użytkownika, ale i sterowanie podsieci źródłowej i docelowej, rozmaite bramki pośredniczące itp. Opcja ta jest obecnie na tyle znacząca, że określa się ją specjalną nazwą – jest to ustalanie priorytetu na podstawie rozszerzonej, dostępowej listy klasyfikacyjnej. Typowo umiejscawia się ją tak blisko granicy komunikujących się podsieci lub domen administracyjnych, jak to tylko jest możliwe, co

pozwala każdemu realizującemu transmisję elementowi realizować spójną politykę gwarantowania QoS. Działania te realizowane są bezpośrednio przez systemy kolejkowania pakietów, które wykorzystują dostarczone wskazania do ustalania kolejności przekazywania ich do modułów wyjściowych. W ten sposób mechanizmy typu WFQ albo WRED mogą poprawnie obsługiwać klasy usługowe bez wprowadzania zmian w istniejących aplikacjach lub komplikowania sterujących mechanizmów sieciowych. Należy również podkreślić, że zastosowanie identycznego podejścia będzie możliwe po wprowadzeniu IPv6, którego nagłówki również posiadają pole priorytetów.

Podobnie jak apetyt rośnie w miarę jedzenia, tak dostępność priorytetowania zaostrza wymagania jakościowe, kierując je w stronę wyrażanych jawnie gwarancji. Pierwszą jak dotąd próbą sprostania nowym wyzwaniom była publikacja przez IETF dokumentu RFC 2205, który stanowi formalną definicję protokołu RSVP.

W dostępnych implementacjach RSVP może być również inicjowany we wnętrzu sieci, dzięki odpowiedniej konfiguracji elementu proxy RSVP. W ten sposób operator systemu może korzystać z unikalnych właściwości nowego protokołu niezależnie od postępów jego wdrażania na poziomie hostów oraz aplikacji. Jednakże realizacja wszystkich potencjalnych korzyści jest możliwa dopiero po kompleksowej implementacji we wszystkich elementach systemu. Mogą one wtedy wykorzystywać RSVP jako mechanizm transportowania własnych żądań do routerów na trasie przygotowywanej wymiany, a także utrzymywania ich w stanie zapewniającym dostarczanie usług o wymaganej jakości, wyrażanej zazwyczaj w kategoriach dostępnego pasma i gwarantowanego opóźnienia.

Mechanizmami wykonawczymi RSVP są zazwyczaj zaawansowane schematy kolejkowania oraz funkcje sterowania ruchem, które realizują samodzielnie klasyfikację transferowanych pakietów oraz wyznaczanie kolejności ich dalszej propagacji. I tak wykorzystanie WFQ pozwala na dostarczanie zintegrowanych usług o gwarantowanej jakości, zaś współpraca z WRED umożliwia precyzyjne sterowanie obciążeniem systemu. Niezależnie od działań realizowanych wspólnie z RSVP, sterowanie WFQ realizuje standardową obsługę ruchu o niegwarantowanych parametrach, przetwarzając strumienie danych interaktywnych i rozdzielając sprawiedliwie pozostałe pasmo pomiędzy pozostałe przepływy, zaś WRED kontynuuje własną działalność w odniesieniu do strumieni pakietów nie wymagających zaawansowanych działań nadzorczych.

Schematy pomocnicze

Routing warunkowy

Najczęściej stosowaną i zarazem najprostszą opcją oddziaływania na oferowaną jakość świadczenia usług internetowych jest routing warunkowany polityką QoS (*Policy-Based Routing - PBR*), który uzupełniając istniejące mechanizmy standardowych protokołów routingowych, umożliwia lepsze i bardziej efektywne wykorzystanie istniejących łączy. PBR pozwala przy tym na prowadzenie klasyfikacji obsługiwanego ruchu przy wykorzystaniu zapisów z tzw. rozszerzonej listy dostępowej, może zmieniać wartości bitów priorytetu z pola ToS, a także realizować transfer danych o dużym znaczeniu w wydzielonych ścieżkach transmisyjnych poddanych specjalnemu nadzorowi funkcji inżynierii ruchowej. W ten sposób, dzięki kombinowanym działaniom systemu priorytetów i zaawansowanych funkcji kolejkowania możliwe jest efektywne różnicowanie usług z uwagi na oczekiwane gwarancje jakościowe.

Typowym zastosowaniem PBR jest segregacja ruchu w sieciach korporacyjnych. Dzięki niej aplikacje o wysokich wymaganiach odnośnie parametrów czasowych (mowa, wideo) mogą efektywnie wykorzystywać relatywnie drogie, doraźnie zestawiane łącza o dużej

przepustowości, podczas gdy pozostałe usługi (transfer danych, e-mail) są realizowane w tańszych relacjach transmisyjnych zapewniających jedynie małe straty pakietów.

Zachowywanie ustalonego pasma

Często mechanizmem wspomagającym funkcjonowanie PBR jest schemat zachowywania ustalonego pasma (*Committed Access Rate - CAR*), który funkcjonując na interfejsach wejściowych systemu dokonuje wstępnej segregacji ruchu. CAR wykorzystując dane konfiguracyjne opisujące wybrane lub każdy z obsługiwanych strumieni pakietów nie dopuszcza, by objętość danych wprowadzanych do sieci przekroczyła ustalone granice. W przypadkach, gdy źródło nie stosuje się do ustaleń prowadzone jest albo usuwanie części dostarczonych danych, albo pakiety uznane za nadmiarowe są oznaczane w polu ToS najniższym z możliwych priorytetów.