# Mechanizmy zarządzania jakością ruchu w routerach firmy Juniper Networks

## Mechanizmy zarządzania jakością ruchu

Sieci teleinformatyczne spełniają obecnie zadania, które wymagają wysokiej jakości świadczonych usług. Co to oznacza? Powszechne stają się aplikacje czasu rzeczywistego, takie jak transmisja głosu oraz wideo, transakcje elektroniczne – walutowe czy też giełdowe. Gdy dane nie są przekazywane w sposób właściwy, to rozmowa czy wideokonferencja stają się niemożliwe. Również niemożność uzyskania informacji, na przykład finansowej we właściwym czasie powoduje, iż zawarcie transakcji na giełdzie lub rynku walutowym spowoduje poważne straty finansowe. Z tego powodu klienci, użytkownicy sieci teleinformatycznych oczekują, że dostawca zapewni odpowiedni poziom świadczonych usług. Dlatego definiujemy jakość usług (ang. *Quality of Services – QoS*) – jako zestaw wymagań stawianych parametrom sieci, które muszą być spełnione dla przesyłania konkretnych danych [RFC2386]. Parametry istotne dla jakości to:

- przepływność, pasmo (ang. *Troughtput, Bandwidth*) – prędkość, z jaką dane są przesyłane poprzez sieć (wyrażone w bitach na sekundę)
- opóźnienie (ang. *Delay, Latency*) – czas potrzebny, żeby pakiet przebył drogę od nadawcy do odbiorcy (wyrażone w sekundach)
- wariacja opóźnienia (ang. *Jitter*) – zmiany opóźnienia mierzone dla pakietów należących do danego strumienia danych (wyrażone w sekundach)
- prawdopodobieństwo zgubienia pakietu (ang. *Loss probability, Loss rate*) – wartość określająca, jakie jest prawdopodobieństwo utraty pakietu należących do danego strumienia danych

Przepływność określają właściwości interfejsu fizycznego (np. Fast Ethernet – 100Mbps), bądź logicznego (np. CIR). Na opóźnienie wpływ ma propagacja sygnału w medium transmisyjnym oraz czasy potrzebne do przetworzenia danych przez kolejne urządzenia sieciowe. Zmiany opóźnienia są powodowane na ogół przez różną obsługę poszczególnych pakietów należących do danego strumienia danych w kolejnych urządzeniach sieciowych. Prawdopodobieństwo zgubienia pakietu jest związane z powstawaniem spiętrzeń i

przepełnianiem kolejek. Gdy kolejka się przepełni, pakiety są odrzucane. Możliwe jest również zaimplementowanie świadomego odrzucania pakietów zanim kolejka się przepełni. Polepsza to właściwości transmisji, albowiem zapobiega spiętrzeniom.

Pojawia się pytanie – jak zapewnić odpowiednią jakość usług? Służy do tego szereg różnych mechanizmów wbudowanych w urządzenia sieciowe. W niniejszym opracowaniu skupimy się na modelu DiffServ (model usług zróżnicowanych).

Podstawową kwestią jest rozróżnienie poszczególnych strumieni danych tak, żeby móc zagwarantować im następnie odpowiednie parametry transmisji. Są dwie generalne metody klasyfikacji ruchu. Pierwsza z nich opiera się na sprawdzeniu pewnej wartości w nagłówku pakietu. Metoda ta jest określana jako klasyfikator typu BA (ang. *BA – Behavior Aggregate*). Sprawdzane są wartości tzw. punktu kodowego (ang. *code point*) ustawionego w nagłówku datagramu IP (wartość pola TOS), ramce IEEE802.1p lub polu EXP nagłówka MPLS i na tej podstawie pakiety są przypisywane do danej klasy ruchu (ang. *forwarding class, FC*). Ta metoda klasyfikacji znajduje zastosowanie w sieciach rdzeniowych. Wymagane jest, aby urządzenia przyjmujące pakiety z ustawionymi znacznikami dotyczącymi jakości usług ufały temu, kto te znaczniki ustawił. W przypadku, gdy nie obdarza się zaufaniem nadawcy, należy stosować inną metodę klasyfikacji opartą między innymi na analizie adresów źródłowych i docelowych, usług IP, portów TCP/UDP. Metoda ta jest określana jako klasyfikator typu MF (ang. MF – Multi field). Przypisanie konkretnego strumienia danych do klasy ruchu musi odbywać się na interfejsie wejściowym urządzenia sieciowego.

Również na wejściu można dokonywać przycinania ruchu (ang. *Policing*) do zadanych parametrów. Gdy ilość przychodzących danych przekracza dopuszczalną wielkość, urządzenie odrzuca pakiety w taki sposób, żeby zachować wymagane parametry transmisji. Najczęściej jest stosowany algorytm TBF (ang. *Token Bucket Filter*). Policery klasyfikują ruch na ogół w oparciu o klasyfikatory typu MF.

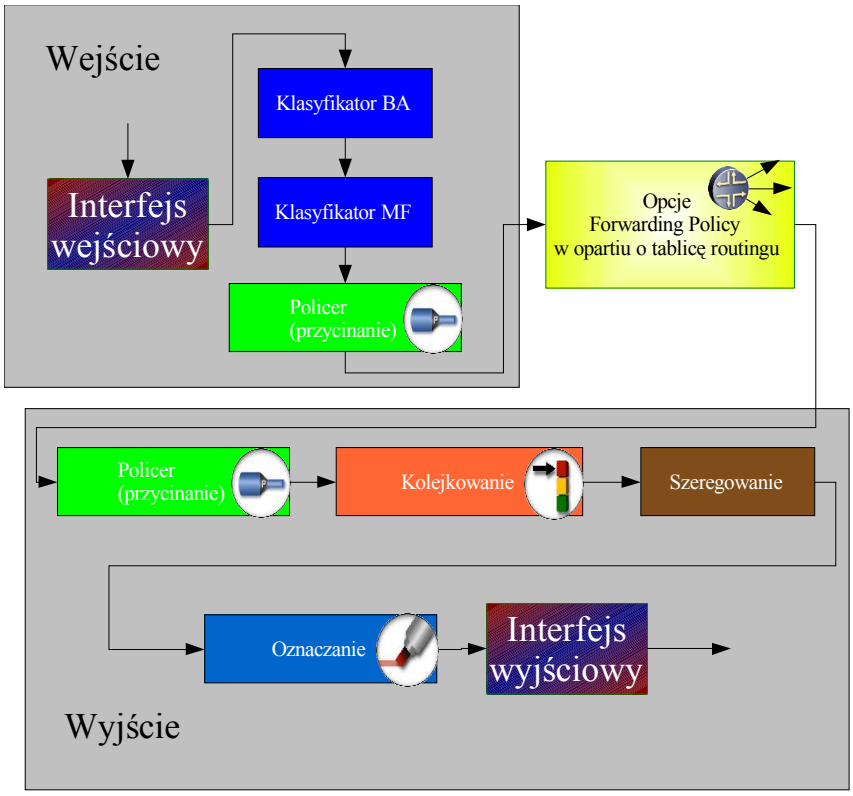
Gdy ruch został już oznakowany (przypisany do FC i przycięty), należy zapewnić obsługę na wyjściu. Służą temu mechanizmy kolejkowania (ang. *queuing*) i szeregowania(ang. *scheduling*). Kolejkowanie polega na przechowywaniu danych w buforach typu FIFO (ang. First In First Out). Kolejki maja określoną pojemność, pozwalającą przechować tylko pewną część danych, których nie można wysłać w danym momencie z powodu zajętości linii wyjściowej. Ponadto bufory mogą mieć wbudowany mechanizm wcześniejszego powiadamiania o przepełnieniu i losowego gubienia pakietów (ang. *RED – Random Early Drop*). Pojemność kolejek jest jednym z parametrów, które można definiować. Mechanizmy

szeregowania służą do obsługi kolejek poprzez wybór danej kolejki i pobranie z niej porcji danych. Gdy w kolejce znajdują się dane do wysłania, mechanizm szeregowania przydziela jej na określony czas dostęp do interfejsu wyjściowego. Kolejki wybiera się zgodnie ze zdefiniowanymi priorytetami, najczęściej z użyciem algorytmu cyklicznego wyboru z priorytetem (ang. *WRR- Weighted Round Robin*) – oznacza to, że kolejki z wyższym priorytetem mają przyznany częściej dostęp do interfejsu. W takim wypadku nie występują problemy głodzenia ani konwoju, natomiast mogą wystąpić problemy zmienności opóźnienia (*jitter*). Inne metody obsługi to kolejki o ścisłym priorytecie oraz pojedyncza kolejka. W przypadku kolejki o ścisłym priorytecie mechanizm szeregowania przydziela jej pasmo, aż zostanie ona opróżniona, a dopiero później obsługiwane są pozostałe kolejki z niższymi priorytetami. Przy takim algorytmie może wystąpić problem głodzenia (ang. *starvation*). Pojedyncza kolejka FIFO może powodować powstawanie problemu konwoju.

Ponadto z zapewnieniem jakości usług związany jest jeszcze mechanizm przepisywania znaczników. Pierwsze urządzenie, które dokona klasyfikacji ruchu na podstawie któregoś z wymienionych wcześniej kryteriów może zmienić przyporządkowanie poprzez zamianę wartości znaczników. Przykładowo, otrzymując ruch z określonym znacznikiem 802.1p router ustala na tej podstawie pewną wartość punktu kodowego DSCP. Możliwa jest również zmiana jednej wartości pewnego typu znacznika na inną w ramach tego samego typu.

## Mechanizmy zapewnienia jakości usług w routerach Juniper Networks serii J

Rysunek 1 przedstawia sposób w jaki dane są obrabiane pod kątem zapewnienia jakości usług. Możemy wyodrębnić trzy obszary, w których dane są obsługiwane – obszar interfejsu wejściowego, przekazywania pakietów (ang. *forwarding policy*) oraz inerfejsu wyjściowego. Po odebraniu przez interfejs wejściowy dane mogą podlegać klasyfikacji. Następnie pasmo może zostać ograniczone przez odpowiedni mechanizm *policingu*. W kolejnym kroku można dokonać manipulacji w ramach opcji przekazywania pakietów, przykładowo poprzez wybór adresu *next-hop* dla danej klasy ruchu. Obróbka danych w obszarze interfejsu wyjściowego może polegać na przycinaniu, kolejkowaniu ze wszystkimi mechanizmami z tym związanymi, szeregowaniu oraz oznaczaniu (zmianie oznaczeń) pakietów.




*Rysunek 1 Schemat mechanizmów CoS/QoS*

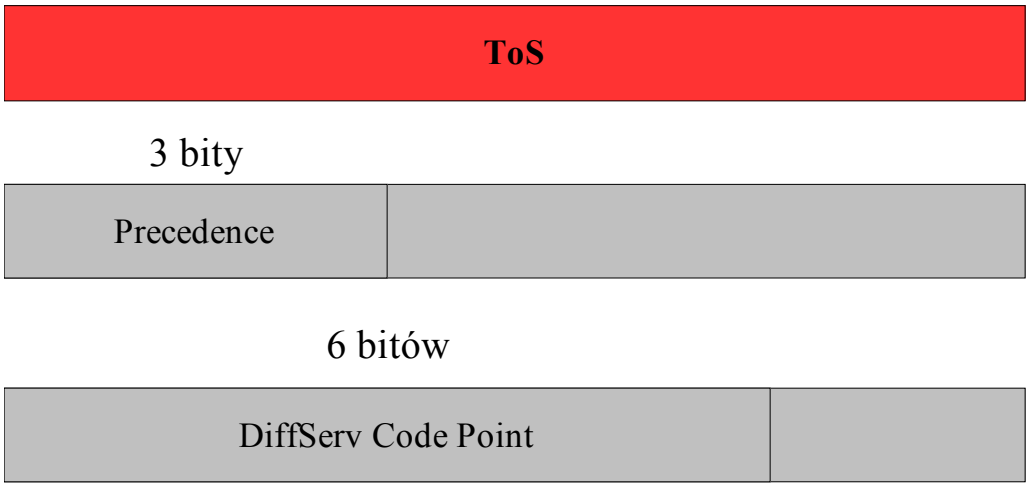
## Klasyfikacja BA

Mechanizmy klasyfikacji BA opierają się na sprawdzaniu wartości odpowiednich pól odpowiedzialnych za mechanizmy CoS w nagłówkach pakietów. W przypadku datagramów IP jest to ośmiobitowe pole ToS [RFC791]. Format nagłówka datagramu IP przedstawia rysunek 2.

| Wersja | Dł. nagłówka | **ToS** | Długość datagramu |
|---|---|---|---|
| ID datagramu | | Flagi | Offset fragmentu |
| TTL | Protokół | Suma kontrolna nagłówka | |
| Adres źródłowy | | | |
| Adres docelowy | | | |

*Rysunek 2 Nagłówek datagramu IP*

Klasyfikacja może się odbywać za pomocą mechanizmów IP Precedence lub DSCP. W zależności od tego, który z nich będzie zastosowany pole ToS zostanie odpowiednio wykorzystane. Mapowanie ToS na IP Precedence oraz DSCP przedstawia rysunek 3.




*Rysunek 3 Mapowanie DSCP/IP Precedence na pole ToS w nagłówku datagramu IP*

W przypadku IP Precedence wykorzystane są trzy bity, które dają możliwość przekazania informacji o ośmiu klasach ruchu. Natomiast DiffServ wykorzystuje sześć bitów, co teoretyczne daje możliwość zdefiniowania 64 różnych klas. Poniższa tabela przedstawia zestawienie wartości IP Precedence wraz z przypisaniem domyślnych klas ruchu oraz priorytetem gubienia pakietów.

| ***IP Precedence*** | ***Nazwa*** | ***Priorytet zgubienia pakietu*** | ***Klasa ruchu (domyślna)*** |
|---|---|---|---|
| 111B (7) | Network control | wysoki | network-control |
| 110B (6) | Interetwork control | niski | network-control |
| 101B (5) | Critical | wysoki | best-effort |
| 100B (4) | Flash Override | niski | best-effort |
| 011B (3) | Flash | wysoki | best-effort |
| 010B (2) | Immediate | niski | best-effort |
| 001B (1) | Priority | wysoki | best-effort |
| 000B (0) | Routine | niski | best-effort |

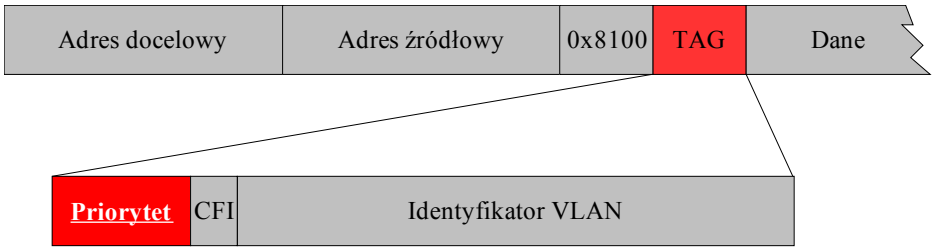
*Tabela 1 Wartości IP Precedence*

Tabela 2 przedstawia wartości punktów kodowych DSCP wraz z przypisaniem do konkretnego PHB (ang. *Per Hop Behavior)* czyli sposobu, w jaki każdy router będzie traktował daną klasę ruchu.

| ***Odpowiednik IP Precedence*** | ***Wartość DSCP*** | | | ***PHB*** |
|---|---|---|---|---|
| | ***Prawdopodobieństwo odrzucenia pakietu*** | | | |
| | Wysokie | Średnie | Niskie | |
| 0 | **BE** 000000B | | | BE (*Best Effort*) |
| 1 | **AF13** 001 110B | **AF12** 001 100B | **AF11** 001 010B | AF (*Assured Forwarding*) |
| 2 | **AF23** 010 110B | **AF22** 010 100B | **AF21** 010 010B | |
| 3 | **AF33** 011 110B | **AF32** 011 100B | **AF31** 011 010B | |
| 4 | **AF43** 100 110B | **AF42** 100 100B | **AF41** 100 010B | |
| 5 | EF 101 110B | | | EF (*Expedited Forwarding*) |

*Tabela 2 Wartości DSCP*

Klasyfikacja ruchu jest możliwa na podstawie wartości ustawianych w ramkach Ethernet przekazywanych przez łącza typu VLAN trunk. Ramka IEEE802.1q ma wyróżnione szesnastobitowe pole zwane tagiem vlan, które zawiera między innymi identyfikator sieci wirtualnej oraz priorytet ramki (802.1p). Priorytet jest trzybitowym polem, które pozwala na wyodrębnienie maksymalnie ośmiu różych klas ruchu. Ta metoda klasyfikacji znajduje zastosowanie w sieciach LAN oraz na styku pomiędzy siecią LAN i siecią WAN. Ramka standardu IEEE802.1q wraz z opisem pola VLAN TAG oraz polem priorytetów IEEE802.1p jest przedstawiona na rysunku 4.




*Rysunek 4 Ramka 802.1q/802.1p*

Możliwość przekazywania informacji o priorytetach dają również nagłówki MPLS. W trzydziestodwu bitowym nagłówku wyodrębnione jest trzybitowe pole EXP, które pozwala na

wyodrębnienie maksymalnie ośmiu różnych klas ruchu. Nagłówek MPLS jest przedstawiony na rysunku 5.


*Rysunek 5 Nagłówek MPLS z polem EXP*

Konfigurując klasyfikator przypisuje się do danej klasy ruchu wartości odpowiednich pól w stosownych nagłówkach ramek lub pakietów. Przykładowa konfiguracja może wyglądać następująco:

```
cjd@pepsi43# show class-of-service classifiers
dscp ba-classifier {
    forwarding-class voice {
        loss-priority low code-points af22;
    }
    forwarding-class data {
        loss-priority high code-points [ af11 af12 ];
    }
}
cjd@pepsi43# show class-of-service classifiers |display set
set class-of-service classifiers dscp ba-classifier forwarding-class voice loss-priority
low code-points af22
set class-of-service classifiers dscp ba-classifier forwarding-class data loss-priority
high code-points af11
set class-of-service classifiers dscp ba-classifier forwarding-class data loss-priority
high code-points af12
```

*Konfiguracja 1*

Do klasy ruchu *voice* zostaną przypisane te pakiety, które mają ustawioną wartość af22 w nagłówku dscp. Ponadto zostanie ustawiona niska wartość wewnętrznego statusu odrzucania pakietów. Do klasy ruchu *data* zostaną przypisane te pakiety, które mają ustawioną wartość af11 lub af12 w nagłówku dscp. Ponadto zostanie ustawiona wysoka wartość wewnętrznego statusu odrzucania pakietów.

## Klasyfikacja MF

W klasyfikatorze MF wykorzystuje się własności filtra pakietowego. Na podstawie parametrów takich jak adres źródłowy, docelowy, numery portów itd. można przypisać odpowiednią klasę ruchu.

```
cjd@pepsi43# show firewall
family inet {
    filter mf-classifier {
        term video-net {
            from {
                source-address {
                    10.1.1.0/24;
                }
            }
            then forwarding-class video;
        }
        term normal-traffic {
            then forwarding-class data;
        }
    }
}
cjd@pepsi43# show firewall |display set
set firewall family inet filter mf-classifier term video-net from source-address
 10.1.1.0/24
set firewall family inet filter mf-classifier term video-net then forwarding-cla
ss video
set firewall family inet filter mf-classifier term normal-traffic then forwardin
g-class data
```

*Konfiguracja 2*

Pakiety pochodzące z sieci 10.1.1.0/24 zostaną przypisane do klasy ruchu *video*, natomiast pozostałe do klasy ruchu *data*. Dowolne inne parametry, za pomocą których można budować filtry, są do wykorzystania przy klasyfikacji ruchu.

Klasyfikatory następnie należy przypisać do interfejsów w ramach konfiguracji *class-of-service*,

na przykład poniższa komenda przypisuje do wszystkich interfejsów **fe** klasyfikator dscp ba:

```
set class-of-service interfaces fe-* unit * classifiers dscp ba-classifier
```

## Policery

Przycinanie ruchu na wejściu jest możliwe i jest do tego wykorzystywany algorytm TBF. Algorytm działa w dużym przybliżeniu tak, że do kubełka (ang. *Bucket*) - bufora wpadają żetony (co określoną jednostkę czasu). Wysłanie konkretnej porcji danych powoduje pobranie żetonów z kubełka. Gdy przepływ danych opróżni kubełek z żetonów, ruch zostanie

wstrzymany, aż do momentu, gdy w kubełku znów znajdą się żetony. Policery można umieszczać zarówno na wejściu jak i na wyjściu routera.

## Konfiguracja policerów

W celu ograniczenia ruchu stosuje się filtry, podobnie jak w klasyfikatorze MF. Efektem zakwalifikowania ruchu przez policer (gdy zostaną przekroczone dopuszczalne wartości natężenia) może być odrzucenie kolejnych pakietów, zmiana klasy ruchu lub zmiana priorytetów odrzucania, które są następnie wykorzystywane przez mechanizmy szeregowania ruchu.

```
cjd@pepsi43# show firewall
policer bandwidth-policer {
    if-exceeding {
        bandwidth-limit 1m;
        burst-size-limit 10k;
    }
    then discard;
}
policer priority-policer {
    if-exceeding {
        bandwidth-limit 800k;
        burst-size-limit 10k;
    }
    then loss-priority low;
}

cjd@pepsi43# show firewall |display set
set firewall policer bandwidth-policer if-exceeding bandwidth-limit 1m
set firewall policer bandwidth-policer if-exceeding burst-size-limit 10k
set firewall policer bandwidth-policer then discard
set firewall policer priority-policer if-exceeding bandwidth-limit 800k
set firewall policer priority-policer if-exceeding burst-size-limit 10k
set firewall policer priority-policer then loss-priority low
```

*Konfiguracja 3*

Konfiguracja, w której policer zmienia klasę ruchu wykonuje się w sposób analogiczny do tej, gdzie zmieniany jest priorytet odrzucania ruchu. W klauzuli *then* zamiast *los-priority* **<wartość>** umieszcza się *forwarding-class* **<nazwa klasy ruchu>.**

Po stworzeniu policerów należy przypisać je do interfejsów oraz zaznaczyć kierunek działania. Różne policery mogą zostać przypisane zarówno do interfejsu w kierunku wejściowym (dane przychodzące) jak i wyjściowym (dane wychodzące).

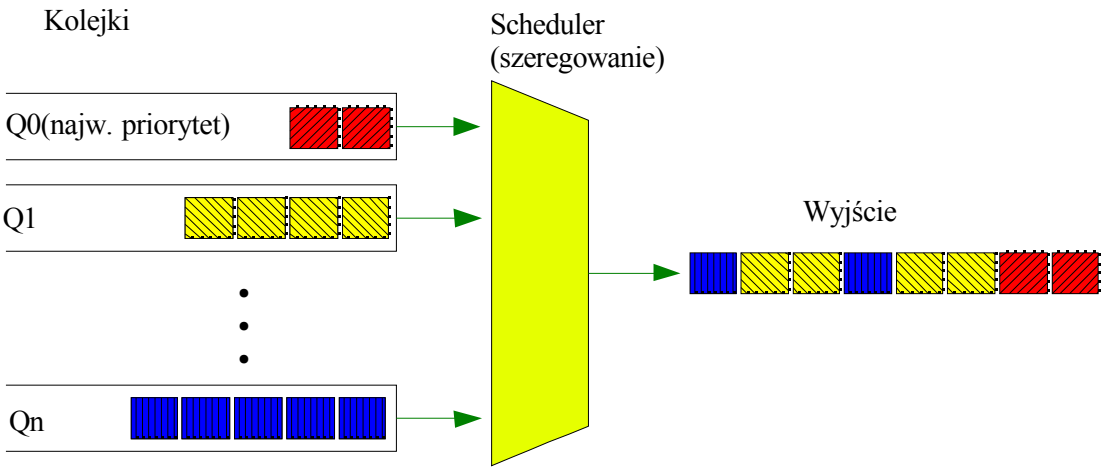
```
cjd@pepsi43# show interfaces fe-0/0/0
unit 0 {
    family inet {
        policer {
            input class-policer;
            output bandwidth-policer;
        }
        address 192.168.14.43/24;
    }
}
cjd@pepsi43# show interfaces fe-0/0/0 |display set
set interfaces fe-0/0/0 unit 0 family inet policer input class-policer
set interfaces fe-0/0/0 unit 0 family inet policer output bandwidth-policer
set interfaces fe-0/0/0 unit 0 family inet address 192.168.14.43/24
```

*Konfiguracja 4*

Mechanizmy kolejkowania i szeregowania pakietów

## Szeregowanie

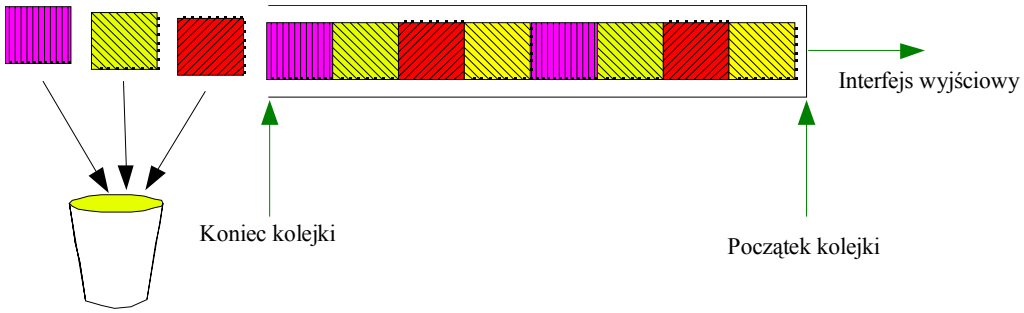
Gdy ruch zostanie zakwalifikowany do poszczególnych klas, a następnie przycięty przez odpowiednie policery należy zapewnić obsługę na wyjściu przez przypisanie do kolejek oraz ustawienie mechanizmów szeregowania. W routerach serii J obsługiwane jest do 8 kolejek dla każdego z interfejsów logicznych. Do kolejek (numerowanych od 0 do 7) przypisuje się klasy ruchu. Następnie mechanizm szeregowania opróżnia kolejki z danych (rysunek 6).




*Rysunek 6 Schemat mechanizmów szeregowania ruchu*

Kolejkom przypisywane jest pasmo (ułamek pasma interfejsu) oraz priorytet obsługi. Mechanizm szeregowana (*scheduler*) sprawdza kolejki jedna po drugiej. Jeżeli więcej niż w jednej kolejce znajdują się dane do wysłania oraz kolejki te mają niewykorzystany kredyt pasma (ang. *banwdwidth credit*), to wtedy kolejka o wyższym priorytecie jest obsługiwana w pierwszej kolejności. Jeżeli wszystkie mają ten sam priorytet, to są obsługiwane po kolei zgodnie z przyznanym pasmem. W przypadku, gdy dana kolejka wykorzystała swój kredyt pasma, nie jest obsługiwana, aż pasmo nie zostanie jej przyznane ponownie. Jednakże, gdy pozostałe kolejki są puste(nie mają danych do wysłania), a pasmo na interfejsie nie jest wykorzystane do końca, to kolejka taka, mimo iż nie posiada już przydziału pasma zostanie obsłużona. Możliwe jest też skonfigurowanie kolejki, która zawsze będzie obsłużona (ma nieograniczony kredyt). W takim wypadku może wystąpić problem głodzenia – pozostałe kolejki zostaną pozbawione dostępu do interfejsu. Kolejka, która zawsze jest obsługiwana ma przyznany priorytet *strict-high*.

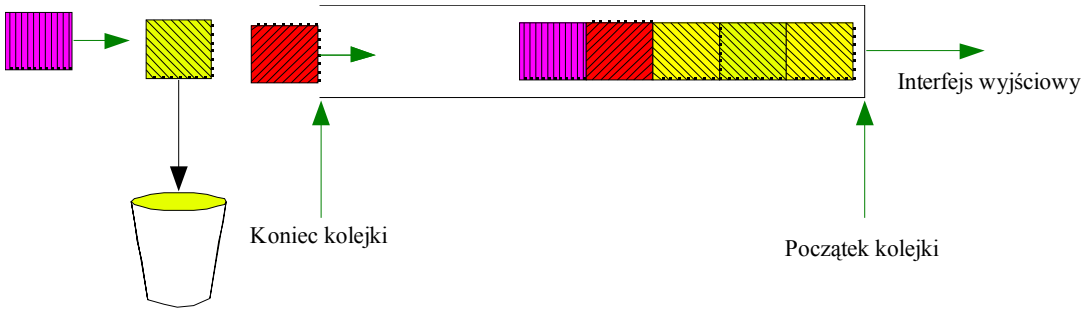
Pozostał jeszcze do rozwiązania przypadek, gdy danych przyjdzie tyle, że nie będzie można ich wysłać a kolejka w międzyczasie się zapełni. W przypadku, gdy nie ma aktywnego zarządzania pamięcią, jeżeli kolejka się zapełni w całości, dane są gubione. Mechanizm ten nazywa się *tail-drop* i jest przedstawiony na rysunku 7.




*Rysunek 7 Gubienie pakietów typu Tail-drop*

Metoda ta ma sporo wad. Pakiety są odrzucane dopiero, gdy kolejka jest w 100% pełna, a przyjmowane, gdy tylko zrobi się miejsce. Ma to bardzo negatywny wpływ na transmisje z użyciem protokołu TCP(wyposażonego w mechanizm zarządzania przepływem) albowiem powoduje drastyczne zmiany prędkości transmisji. Rozwiązaniem, które pozwala wyeliminować negatywne skutki stosowania gubienia pakietów typu *tail-drop* jest mechanizm RED (ang. *random early drop*) przedstawiony na rysunku 8. Router odrzuca losowo(z określonym prawdopodobieństwem) pakiet, gdy kolejka zostanie wypełniona w pewnym

stopniu. Powoduje to iż stos protokołów TCP/IP zmniejsza prędkość wysyłania danych, co powoduje zmniejszenie wypełnienia kolejek danymi.




*Rysunek 8 Mechanizm RED*

W celu zaimplementowania mechanizmu RED tworzy się profile odrzucania ruchu (ang. *drop-profile*), gdzie przypisuje się prawdopodobieństwo odrzucenia pakietu do stopnia wypełnienia kolejki oraz metodę interpolacji (liniowa, dyskretna). To, który profil zostanie zastosowany jest związane z ustawieniem wewnętrznego statusu odrzucania pakietów przez klasyfikator ruchu.

Konfigurując profil podaje się wartości wypełnienia bufora oraz prawdopodobieństwo odrzucenia kolejki, uprzednio zaznaczywszy czy profil jest liniowy, czy dyskretny (domyślnie).

```
cjd@pepsi43# show drop-profiles
discrete-drop-profile {
        fill-level 60 drop-probability 70;
[...]
        fill-level 100 drop-probability 100;
    }
    cont-drop-profile {
        interpolate {
            fill-level [ 50 60 70 80 90 95 100 ];
            drop-probability [ 30 50 90 100 ];
        }
    }
set class-of-service drop-profiles discrete-drop-profile fill-level 60 drop-probability
70
[...]
set class-of-service drop-profiles discrete-drop-profile fill-level 100 drop-probability
100
set class-of-service drop-profiles cont-drop-profile interpolate fill-level [ 50 60 70 80
90 95 100 ] drop-probability [ 30 50 90 100 ]
```

*Konfiguracja 5*

Kształt profili można zawsze obejrzeć wydając stosowną komendą z poziomu monitorowania pracy routera.

```
cjd@pepsi43> show class-of-service drop-profile
Drop profile: cont-drop-profile, Type: interpolated, Index: 23196
  Fill level     Drop probability
           0                    0
          72                   92
[...]
         100                  100
Drop profile: discrete-drop-profile, Type: discrete, Index: 19002
  Fill level     Drop probability
[...]
           95                   99
          100                  100
```

*Konfiguracja 6*

Mając rozwiązany problem odrzucania pakietów w przepełnionych kolejkach, można już zdefiniować w pełni mechanizm szeregowania, na który składa się przydział pasma, priorytetu oraz właśnie sposób postępowania przy przepełnieniach.

```
cjd@pepsi43# show schedulers
Q1 {
    transmit-rate 1m;
    buffer-size percent 20;
    priority high;
}
Q2 {
    transmit-rate 5m;
    buffer-size percent 50;
    priority low;
    drop-profile-map loss-priority high protocol any drop-profile cont-drop-profile;
    drop-profile-map loss-priority medium-high protocol any drop-profile discrete-drop-
profile;
}
cjd@pepsi43# show schedulers Q2 |display set
set class-of-service schedulers Q2 transmit-rate 5m
set class-of-service schedulers Q2 buffer-size percent 50
set class-of-service schedulers Q2 priority low
set class-of-service schedulers Q2 drop-profile-map loss-priority high protocol any drop-
profile cont-drop-profile
```

*Konfiguracja 7*

Przy różnych priorytetach wewnętrznego statusu odrzucania pakietów można zastosować różne profile odrzucania ruchu. Ostatnim krokiem jest przypisanie zdefiniowanych uprzednio mechanizmów do odpowiednich interfejsów.

```
cjd@pepsi43# show scheduler-maps
map-Q12 {
    forwarding-class voice scheduler Q1;
    forwarding-class data scheduler Q2;
}
cjd@pepsi43# show scheduler-maps |display set
set scheduler-maps map-Q12 forwarding-class voice scheduler Q1
set scheduler-maps map-Q12 forwarding-class data scheduler Q2
cjd@pepsi43# show interfaces
fe-* {
    scheduler-map map-Q12;
}
cjd@pepsi43# show interfaces |display set
set class-of-service interfaces fe-* scheduler-map map-Q12
```

*Konfiguracja 8*

## Przepisywanie znaczników

W procesie obróbki danych przez mechanizmy CoS/QoS ostatnim krokiem jest ustawienie znaczników(np. DSCP, EXP). Gdy ruch raz zostanie zakwalifikowany przez pierwszy router w sieci, to dalej można zamiast klasyfikatorów MF używać BA, co może znacząco wpływać na uproszczenie przetwarzania pakietów, a co za tym idzie na wydajność pracy urządzeń w sieci rdzeniowej. W związku z tym router po zakwalifikowaniu pakietu do klasy ruchu może ustawić stosowne znaczniki.

```
cjd@pepsi43# show rewrite-rules
dscp voice-rr {
    forwarding-class voice {
        loss-priority low code-point af22;
    }
}
cjd@pepsi43# show rewrite-rules |display set
set class-of-service rewrite-rules dscp voice-rr forwarding-class voice loss-priority low
code-point af22
```

*Konfiguracja 9*

Po skonfigurowaniu przepisywania znaczników należy dokonać przyporządkowania reguł do odpowiednich interfejsów wyjściowych. Można posłużyć się wildcardami w postaci gwiazdek.

```
cjd@pepsi43# show interfaces
fe-* {
    scheduler-map map-Q12;
    unit * {
        rewrite-rules {
            dscp voice-rr;
        }
    }
}
cjd@pepsi43# show interfaces |display set
set class-of-service interfaces fe-* unit * rewrite-rules dscp voice-rr
```

*Konfiguracja 10*

## Podsumowanie

Nie zostały wyczerpane wszystkie zagadnienia związane z zarządzaniem jakością usług. Warto jednakże podkreślić, że routery JUNIPER Networks zapewniają wyjątkową stabilność pracy oraz gwarantowaną wydajność bez względu na ilość i rodzaj zaimplementowanych mechanizmów QoS/CoS.

Marek Krauze, *JNCIA-J*