



Systemy IBM - iSeries  
Jakość usług sieciowych

*Wersja 5 Wydanie 4*







Systemy IBM - iSeries  
Jakość usług sieciowych

*Wersja 5 Wydanie 4*

**Uwaga**

Przed korzystaniem z tych informacji oraz z produktu, którego dotyczą należy przeczytać informacje znajdujące się w dodatku "Uwagi", na stronie 69.

**Wydanie piąte (luty 2006)**

To wydanie dotyczy wersji 5, wydania 4, modyfikacji 0 systemu operacyjnego IBM i5/OS (numer produktu 5722-SS1) oraz wszystkich kolejnych wydań i modyfikacji, o ile w nowych wydaniach nie określono inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

© Copyright International Business Machines Corporation 1998, 2006. Wszelkie prawa zastrzeżone.

---

## Spis treści

|  |          |  |           |
|--|----------|--|-----------|
| <b>Jakość usług (QoS)</b> . . . . .                          | <b>1</b> | Konfigurowanie jakości usług . . . . .                     | 51        |
| Co nowego w wersji V5R4 . . . . .                            | 1        | Konfigurowanie jakości usług za pomocą kreatorów. . . . .  | 51        |
| Drukowanie dokumentów PDF . . . . .                          | 1        | Konfigurowanie serwera katalogów . . . . .                 | 53        |
| Pojęcia . . . . .  | 2        | Kolejność strategii jakości usług . . . . .                | 54        |
| Usługa DiffServ . . . . .                                    | 2        | Zarządzanie usługą QoS . . . . .                           | 54        |
| Usługa zintegrowana . . . . .                                | 6        | Uzyskiwanie pomocy dotyczącej QoS w programie              |           |
| Strategia akceptowania ruchu przychodzącego . . . . .        | 11       | iSeries Navigator . . . . .                                | 55        |
| Klasa usług . . . . .  | 13       | Składowanie strategii . . . . .                            | 55        |
| Funkcje API QoS . . . . .                                    | 17       | Kopiowanie istniejącej strategii . . . . .                 | 56        |
| Serwer katalogów . . . . .                                   | 25       | Edytowanie strategii . . . . .                             | 56        |
| Scenariusze . . . . .  | 28       | Monitorowanie QoS . . . . .                                | 56        |
| Scenariusz: ograniczanie ruchu danych do przeglądarki        | 28       | Rozwiązywanie problemów z jakością usług . . . . .         | 60        |
| Scenariusz: bezpieczny i przewidywalny ruch danych           |          | Kronikowanie strategii jakości usług . . . . .             | 61        |
| (sieć VPN i jakość usług). . . . .                           | 32       | Protokołowanie zadań serwera jakości usług . . . . .       | 62        |
| Scenariusz: ograniczanie połączeń przychodzących . . . . .   | 36       | Monitorowanie transakcji serwera . . . . .                 | 63        |
| Scenariusz: przewidywalny ruch danych firma-firma            |          | Śledzenie aplikacji TCP/IP . . . . .                       | 64        |
| (B2B) . . . . .  | 38       | Informacje związane z jakością usług . . . . .             | 66        |
| Scenariusz: dedykowane dostarczanie (telefonía IP) . . . . . | 42       | <b>Dodatek. Uwagi</b> . . . . .                            | <b>69</b> |
| Scenariusz: Monitorowanie bieżących statystyk sieci          | 46       | Informacje na temat interfejsu programistycznego . . . . . | 71        |
| Planowanie jakości usług. . . . .                            | 48       | Znaki towarowe . . . . .                                   | 71        |
| Wymagania dotyczące uprawnień . . . . .                      | 48       | Warunki. . . . .   | 71        |
| Wymagania dotyczące systemu . . . . .                        | 49       |  |           |
| Umowa dotycząca poziomu usług . . . . .                      | 49       |  |           |
| Sprzęt i oprogramowanie sieciowe . . . . .                   | 50       |  |           |



---

## Jakość usług (QoS)

Rozwiązanie QoS iSeries pozwala na zastosowanie strategii określających priorytet pakietów i przepustowość sieci dla aplikacji TCP/IP.

Wszystkie dane przesyłane w sieci mają identyczny priorytet. Przepływ danych do przeglądarki WWW jest więc równie ważny, jak przepływ danych do krytycznych aplikacji biznesowych. Priorytet pakietów IP nabiera znaczenia, gdy na przykład główny menedżer ma prezentację z wykorzystaniem aplikacji audio i wideo. Jest ważne, aby w trakcie prezentacji aplikacja mogła uzyskać większą wydajność niż pozostałe.

Priorytet pakietów jest istotny, gdy aplikacje wymagają przewidywalnych i niezawodnych połączeń, tak jak na przykład aplikacje multimedialne. Strategie QoS na serwerze iSeries umożliwiają także ograniczenie danych opuszczających serwer, zarządzanie żadaniami połączeń oraz sterowanie obciążeniem serwera. Serwer usług QoS musi być uruchomiony w celu aktywowania strategii wykrywania włamań.

Zanim rozpocznie się konfigurowanie strategii, trzeba dobrze rozumieć zagadnienia QoS.

---

## Co nowego w wersji V5R4

### Nowa funkcja wykrywania włamań

- | W wersji V5R4, serwer QoS zapewnia możliwość wykrywania włamań poprzez strategię wykrywania włamań. Aby
- | aktywować tę strategię, uruchomiony musi być serwer QoS. Za pomocą strategii wykrywania włamań QoS, możliwe
- | jest wykrywanie włamań, tworzenie rekordów kontroli, a także wysyłanie wiadomości informujących o możliwych
- | próbach włamań. Szczegółowe informacje na ten temat znajdują się w sekcji Funkcja wykrywania włamań.

### Gdzie szukać informacji o wprowadzonych zmianach i nowościach

Aby wyróżnić zmiany wprowadzone w tekście dokumentu, używa się:

- symbolu ➤ do oznaczenia miejsca, w którym zaczynają się informacje nowe i zmienione,
- symbolu ➤ do oznaczenia miejsca, w którym kończą się informacje nowe lub zmienione.

Więcej informacji dotyczących nowych lub zmienionych funkcji systemu można znaleźć w temacie Informacje dla użytkowników.

---

## Drukowanie dokumentów PDF

Przeglądanie i drukowanie poniższych informacji w formacie PDF.


Aby wyświetlić albo pobrać dokument w formacie PDF, wybierz Jakość usługi (wielkość zbioru 255 kB).

### Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu późniejszego wydrukowania lub przeglądania:

1. Prawym przyciskiem myszy kliknij plik PDF w używanej przeglądarce (prawym przyciskiem myszy kliknij odsyłacz powyżej).
2. Wybierz opcję lokalnego zapisu pliku PDF.
3. Przejdź do katalogu, w którym chcesz zapisać plik PDF.
4. Kliknij przycisk **Zapisz**.

## Pobieranie programu Adobe Reader

Do przeglądania lub drukowania plików PDF potrzebny jest program Adobe Reader. Darmową wersję programu można pobrać ze strony internetowej Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

---

## Pojęcia

Podstawowe pojęcia związane z funkcją QoS. Podane tu informacje umożliwiają zrozumienie działania QoS i współpracy różnych funkcji wykorzystywanych do jej zapewnienia.

Przed przystąpieniem do realizacji usługi QoS należy dokładnie zapoznać się z jej problematyką i upewnić się, że usługa spełnia stawiane przed nią wymagania. Zagadnienia związane z jakością usług (QoS) można znaleźć w wielu źródłach, dlatego w sekcji tej podano jedynie podstawowe informacje.

Aby wykonać funkcję QoS, trzeba najpierw skonfigurować strategię za pomocą kreatorów w programie iSeries Navigator. *Strategia* to zestaw reguł opisujących pewne działanie. Określa ona, jaką usługę powinien otrzymać dany klient, aplikacja lub harmonogram. Można skonfigurować strategię trzech typów:

- Usługa DiffServ
- Usługa zintegrowana
- Akceptowanie ruchu przychodzącego

Usługi DiffServ i usługi zintegrowane stosowane są dla strategii dotyczących pasma dla ruchu wychodzącego. Strategie ruchu wychodzącego ograniczają ruch danych opuszczających sieć i pomagają sterować obciążeniem serwera. Szybkości ustalone w ramach strategii ruchu wychodzącego określają, które dane z serwera podlegają ograniczeniom, oraz jakie to są ograniczenia. Aby transmisje danych w ramach strategii rzeczywiście mogły uzyskiwać żądane priorytety, konieczne jest zawarcie z dostawcą ISP odpowiedniej umowy dotyczącej poziomu usług (SLA).

*Strategie akceptowania ruchu przychodzącego* sterują połączeniami przychodzącymi z zewnątrz do danej sieci. Strategie ruchu przychodzącego nie są zależne od poziomu usług zapewnionego przez dostawcę ISP. Aby wybrać właściwy rodzaj strategii, należy sobie uświadomić, z jakiego powodu chce się zastosować QoS, oraz wziąć pod uwagę funkcję pełnioną przez dany serwer iSeries.

Jednym z najważniejszych elementów w realizacji QoS jest sam serwer. Trzeba nie tylko rozumieć pojęcia opisane w dalszej części, ale także zdawać sobie sprawę z roli, jaką odgrywa serwer w ich realizacji. Serwer iSeries może pełnić funkcję klienta lub serwera, nie może natomiast funkcjonować jako router. Na przykład, serwer iSeries funkcjonujący jako klient może stosować strategię usług DiffServ, aby zapewnić, że żądania informacji skierowane do innych serwerów uzyskają w sieci wyższy priorytet. Serwer iSeries funkcjonujący jako serwer może stosować strategię akceptowania ruchu przychodzącego w celu ograniczania żądań URI akceptowanych przez serwer.

### Pojęcia pokrewne

“Umowa dotycząca poziomu usług” na stronie 49

Początek zmian Sekcja ta ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

### Odsyłacze pokrewne

“Informacje związane z jakością usług” na stronie 66

Znajdują się tu podręczniki IBM Redbooks (w formacie PDF), serwisy WWW, oraz tematy Centrum informacyjnego związane z zagadnieniem Jakości usług. Wszystkie dokumenty w formacie PDF można wyświetlać lub drukować.

## Usługa DiffServ

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

### Pojęcia pokrewne



“Rozszerzenia funkcji API QoS sendmsg()” na stronie 24

Funkcja sendmsg() używana jest do wysyłania danych, danych pomocniczych lub ich kombinacji przez połączone lub niepołączone gniazdo.

“Limity dotyczące zasobnika tokenów i limity przepustowości” na stronie 10

Limity dotyczące zasobnika tokenów i limity przepustowości noszą wspólną nazwę limitów wydajności. Limity te umożliwiają gwarantowane dostarczanie pakietów w strategiach ruchu wychodzącego, to znaczy w strategii usług zintegrowanych i strategii usług DiffServ.

“Klasa usług” na stronie 13

Gdy tworzy się strategię usług DiffServ lub strategię akceptowania połączeń przychodzących, konieczne jest także utworzenie i wykorzystanie klasy usług.

“Scenariusz: ograniczanie ruchu danych do przeglądarki” na stronie 28

Monitorowanie można wykorzystać do sterowania wydajnością ruchu danych w sieci. Aby ograniczyć lub zwiększyć wydajność aplikacji w danej sieci, należy skorzystać ze strategii usług DiffServ.

“Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług)” na stronie 32

W sieci VPN także można tworzyć strategię QoS. Ilustruje to przedstawiony w sekcji przykład.

### Odsyłacze pokrewne

“Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci” na stronie 14

W jakości usług (QoS) charakterystykę w ramach segmentu sieci określa się, korzystając z punktów kodowych.

“Konfigurowanie jakości usług za pomocą kreatorów” na stronie 51

Aby skonfigurować strategię QoS, należy użyć kreatorów znajdujących się w programie iSeries Navigator.

### Informacje pokrewne

Zarządzanie adresami i portami serwera HTTP (opartego na Apache)

## Klasy z priorytetami: sposób klasyfikacji ruchu w sieci

W ramach usług DiffServ ruch danych identyfikowany jest jako *klasy*. Klasy te najczęściej określa się przy użyciu adresów IP klientów, portów aplikacji, typu serwera, protokołu, lokalnego adresu IP oraz harmonogramu. Wszystkie transmisje należące do tej samej klasy są traktowane jednakowo.

W przypadku bardziej zaawansowanej klasyfikacji niektóre aplikacje iSeries mogą korzystać z różnych poziomów usług dzięki podaniu danych serwera. Użycie danych serwera jest opcjonalne, ale może być przydatne, gdy potrzebna jest klasyfikacja na niższym poziomie. Dane serwera są oparte na dwóch różnych typach danych aplikacji: *token aplikacji* lub *URI*. Jeśli parametry transmisji danych są takie same, jak token lub URI podane dla strategii, to dla żądania wychodzącego zostanie zastosowana ta strategia. W ten sposób wychodzący ruch danych uzyskuje priorytet określony w danej strategii usług DiffServ. W ten sposób wychodzący ruch danych uzyskuje priorytet określony w danej strategii usług DiffServ.

## Użycie tokenu aplikacji w strategiach usług DiffServ

Użycie danych aplikacji powoduje, że zastosowana będzie strategia zgodna z określonymi parametrami (token i priorytet) przekazanymi przez aplikację do serwera za pośrednictwem funkcji API sendmsg(). Ustawienie to jest opcjonalne. Jeśli w strategiach ruchu wychodzącego nie jest potrzebny taki poziom szczegółowości, w kreatorze należy wybrać opcję **Wszystkie tokeny**. Jeśli jednak taka potrzeba istnieje, możliwe jest porównywanie tokenu i priorytetu aplikacji z ustawieniami tokenu i priorytetu w strategii ruchu wychodzącego. Dane aplikacji (token i priorytet) ustawia się w dwóch częściach strategii.

- Co to jest token aplikacji?

Token aplikacji jest to dowolny łańcuch znaków reprezentujący określony zasób, na przykład mojeFTP. Token podany w strategii QoS jest porównywany z tokenem aplikacji zewnętrznej. Aplikacja udostępnia wartość tokenu za pomocą funkcji API sendmsg(). Jeśli tokeny są zgodne, ruch danych generowany przez daną aplikację jest uwzględniany w strategii usług DiffServ.

Aby w strategii usług DiffServ korzystać z tokenu aplikacji, należy wykonać następujące czynności:

1. W oknie konfiguracji QoS kliknij prawym przyciskiem myszy **DiffServ** i wybierz opcję **Nowa strategia**. Uruchom kreatora.
2. Na stronie Żądanie serwera danych wybierz **Wybrany token aplikacji**.

3. Kliknij przycisk **Nowy**, aby utworzyć nowy token. Pojawi się okno URI.
  4. W polu **Nazwa** wpisz znaczącą nazwę tokenu aplikacji.
  5. W polu **URI** skasuj znak (/) i wpisz token aplikacji (łańcuch liczący nie więcej niż 128 znaków). Zamiast typowego adresu URI może to być na przykład mojaaplikacjaFTP.
- Co to jest priorytet aplikacji?

Priorytet aplikacji podany przez użytkownika jest porównywany z priorytetem aplikacji dostarczonym przez aplikację zewnętrzną. Aplikacja dostarcza wartość priorytetu za pomocą funkcji API sendmsg(). Jeśli priorytety są zgodne, ruch danych generowany przez daną aplikację jest uwzględniany w strategii usług DiffServ. Ruch danych zgodny z ustawieniami strategii DiffServ uzyska priorytet nadany całej strategii.

Jeśli zostanie podany token aplikacji, w kodzie aplikacji dostarczającym te informacje do serwera należy wykorzystać funkcję API Sendmsg(). Jest to zadanie programisty aplikacji. W dokumentacji aplikacji należy zamieścić poprawne wartości (tokenu i priorytetu), które administrator QoS będzie mógł wykorzystać w strategii usług DiffServ. W stosunku do ruchu danych zgodnego z tokenem podanym w strategii zostanie zastosowany priorytet i klasyfikacja danej strategii usług DiffServ. Jeśli w aplikacji nie istnieją wartości zgodne z wartościami ustawionymi w strategii, należy zaktualizować aplikację lub do zdefiniowania strategii usług DiffServ wykorzystać inne parametry danych aplikacji.

## Użycie nazw URI w strategii usług DiffServ

Podczas tworzenia strategii usług DiffServ za pomocą kreatora można ustawić dane serwera omówione w sekcji “Użycie tokenu aplikacji w strategii usług DiffServ”. Chociaż pola kreatora są przeznaczone dla tokenu aplikacji, można je wykorzystać do podania względnej nazwy URI. To ustawienie także jest opcjonalne. Jeśli w strategiach ruchu wychodzącego nie jest potrzebny taki poziom szczegółowości, w kreatorze należy wybrać opcję **Wszystkie tokeny**. Możliwe jest uzgodnienie konkretnego zbioru nazw URI ze strategią ruchu wychodzącego.

Nazwy względne URI stanowią podzbiór nazw pełnych URI (nazwy te przypominają nazwy pełne URL). Rozważmy następujący przykład: `http://www.ibm.com/software`. Segment `http://www.ibm.com/software` stanowi nazwę pełną URI. Natomiast segment `/software` to nazwa względna URI. Wszystkie nazwy względne URI muszą rozpoczynać się ukośnikiem (/). Oto przykłady poprawnych nazw względnych:

- `/market/jedzenie#D5`
- `/oprogramowanie`
- `/market/jedzenie?q=warzywa`

Przed skonfigurowaniem strategii usług DiffServ korzystającej z nazw URL trzeba się upewnić, że port aplikacji przypisany do URI jest taki sam, jak port podany za pomocą dyrektywy Listen FRCA w konfiguracji serwera WWW Apache. Informacje na temat sposobu zmiany lub wyświetlenia portu serwera HTTP zawiera artykuł Zarządzanie adresami i portami serwera HTTP opartego na serwerze Apache.

W przypadku każdego wychodzącego żądania HTTP, nazwa URI będzie identyfikowana przez opcję FRCA (Fast Response Cache Accelerator). Nazwa URI związana z żądaniem wychodzącym jest porównywana z nazwami URI zdefiniowanymi w poszczególnych strategiach usług DiffServ. Pierwsza strategia z łańcuchem tokenu (URI) najlepiej dopasowanym do nazwy URI zidentyfikowanej przez opcję FRCA będzie stosowana do wszystkich żądań dotyczących danej nazwy URI.

### Pojęcia pokrewne

“Rozszerzenia funkcji API QoS sendmsg()” na stronie 24

Funkcja sendmsg() używana jest do wysyłania danych, danych pomocniczych lub ich kombinacji przez połączone lub niepołączone gniazdo.

## Ustawianie priorytetów: sposób obsługi klas

W usługach DiffServ oprócz sklasyfikowania ruchu danych potrzebne jest także podanie charakterystyki w ramach segmentu sieci określającej sposób obsługi ruchu.

Serwer na podstawie nagłówka IP identyfikuje poziom usług odpowiadający pakietowi. Routery i przełączniki przydzielają swoje zasoby, korzystając z informacji o PHB zawartej w polu oktetu typu usług nagłówka IP. Pole oktetu typu usług zostało zdefiniowane w dokumencie RFC usług QoS 1349 systemu operacyjnego OS/400 w wersji V5R1. Dane o PHB określają sposób przekazywania pakietu w węzle sieci. Dane te mają postać liczby zwanej *punktem kodowym*. Pakiety mogą być oznaczone na serwerze lub w innych węzłach sieci, na przykład w routerach. Aby pakiet zachował wymagany poziom usług, każdy węzeł sieci musi obsługiwać usługi DiffServ. Oznacza to, że urządzenia potrafią wymusić odpowiednie przekazywanie pakietu. Aby tego dokonać, węzeł sieci musi obsługiwać planowanie kolejek i zarządzanie priorytetami połączeń wychodzących. Więcej informacji na ten temat obsługi usług DiffServ zawiera sekcja “Funkcje warunkujące ruch danych”.

Gdy pakiet dociera do routera lub przełącznika, który nie obsługuje usług DiffServ, traci określony wcześniej poziom usług. Pakiet jest co prawda przekazywany, lecz jego dostarczenie do węzła końcowego może się opóźnić. W przypadku serwera iSeries można użyć predefiniowanych punktów kodowych lub zdefiniować własny punkt kodowy. Nie zaleca się tworzenia własnych punktów kodowych, gdy pakiety będą przesyłane poza daną siecią prywatną. Jeśli nie wiadomo, jakie punkty kodowe przypisać danym, należy zapoznać się z sekcją “Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci” na stronie 14.

W przeciwieństwie do usług zintegrowanych usługi DiffServ nie wymagają ani rezerwacji zasobów, ani specyficznej obsługi przepływów danych. Wszystkie transmisje umieszczone w tej samej klasie są traktowane jednakowo.

Usługi DiffServ można stosować także w celu ograniczania szybkości ruchu danych opuszczających serwer. Oznacza to, że serwer iSeries może używać usług DiffServ do ograniczenia wydajności aplikacji. Ograniczenie wydajności mniej ważnych aplikacji umożliwia danym pochodzącym z aplikacji o niewrażliwym znaczeniu wcześniejsze opuszczenie sieci prywatnej. Podczas tworzenia klasy usług dla danej strategii określa się limity dotyczące serwera. Limity te obejmują wielkość zasobnika tokenów, limit szybkości szczytowej i limit szybkości średniej. Szczegółowe informacje na ten temat zawierają sekcje pomocy programu iSeries Navigator.

## Funkcje warunkujące ruch danych

Aby korzystać ze strategii QoS, urządzenia sieciowe (routery i przełączniki) muszą obsługiwać funkcje warunkujące. Funkcjami warunkującymi nazywamy funkcje klasyfikujące, mierzące, znakujące, kształtujące i odrzucające.

Jeśli urządzenie sieciowe zawiera wszystkie funkcje warunkujące ruch danych, to takie urządzenie nazywamy *obsługującym usługi DiffServ*.

**Uwaga:** Niniejsze wymagania sprzętowe nie są specyficzne dla systemu iSeries. Terminy te nie występują w interfejsie QoS, ponieważ serwer nie może sterować sprzętem zewnętrznym. Konieczne jest spełnienie ogólnych wymagań QoS przez sprzęt poza siecią prywatną. W dokumentacji poszczególnych urządzeń należy sprawdzić, czy spełniają one wymagania usług DiffServ. Ponadto, przed zaimplementowaniem strategii trzeba zapoznać się z ogólnymi pojęciami i wymaganiami wstępnymi dla funkcji QoS.

Na poniższym rysunku przedstawiono schemat współpracy poszczególnych funkcji.



Rysunek 1. Funkcje warunkujące ruch danych

Oto szczegółowy opis funkcji warunkujących ruch danych.

### Funkcje klasyfikujące

Funkcje te klasyfikują pakiety w strumieniu danych na podstawie nagłówka IP. W systemie iSeries zdefiniowano dwa rodzaje funkcji klasyfikujących. Funkcje BA klasyfikują pakiety tylko na podstawie punktu kodowego usług DiffServ. Funkcje MF klasyfikują pakiety na podstawie jednego lub kilku pól nagłówka. Wykorzystywany może być na przykład adres źródłowy, adres docelowy, pole usług DiffServ, identyfikator protokołu, numer portu źródłowego, URI, typ serwera czy numer portu docelowego.

### Funkcje mierzące

Ich zadanie polega na sprawdzaniu, czy pakiety IP przekazywane przez funkcje klasyfikujące są zgodne z profilem. Dane w nagłówku IP wynikają z wartości ustalonych w strategii QoS. Funkcje mierzące przesyłają dane do innych funkcji, aby uruchomić obsługę pakietu. Obsługę uruchamia się dla każdego pakietu, niezależnie od tego, czy jest on zgodny z profilem, czy nie.

### Funkcje znakujące

Działanie tych funkcji polega na określeniu wartości pola DS (pole usług zróżnicowanych). W zależności od konfiguracji funkcji znakujących pakietom przypisywany jest ten sam punkt kodowy lub różne punkty kodowe określające charakterystykę w ramach segmentu sieci.

### Funkcje kształtujące

Funkcje kształtujące opóźniają wysyłanie pakietów tak, aby dostosować strumień danych do profilu. Funkcje te dysponują buforem o skończonej wielkości. Po jego zapełnieniu kolejne pakiety są usuwane przez router.

### Funkcje odrzucające

Funkcje odrzucające usuwają pakiety ze strumienia danych. Uruchamia się je w celu zapewnienia zgodności z profilem ruchu danych.

#### Pojęcia pokrewne

“Sprzęt i oprogramowanie sieciowe” na stronie 50

Możliwości urządzeń znajdujących się wewnątrz i na zewnątrz sieci mają ogromny wpływ na QoS.

## Usługa zintegrowana

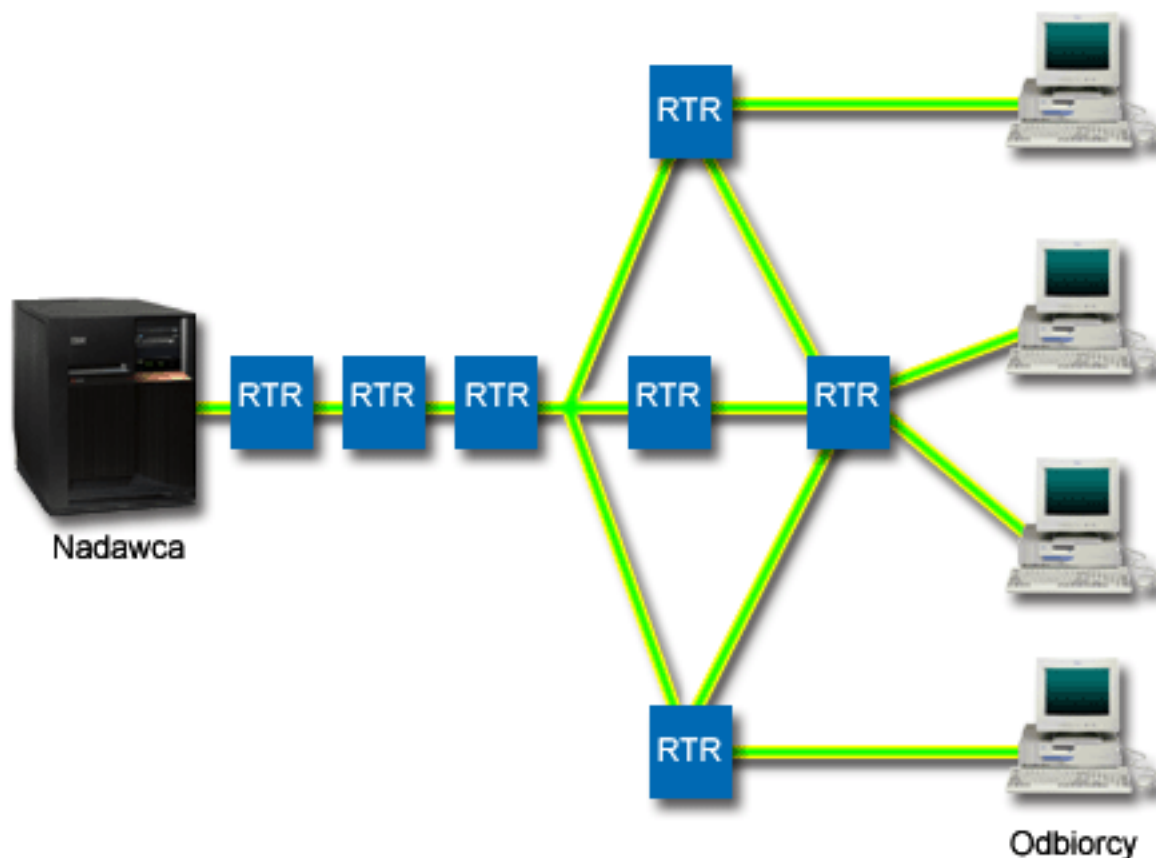
Jest to drugi typ strategii połączeń wychodzących. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API dotyczących QoS.

Strategie usług zintegrowanych korzystają z protokołu RSVP oraz funkcji API RAPI (lub funkcji API gniazd qtoq), aby zagwarantować określoną jakość połączenia między węzłami końcowymi. Jest to najwyższy poziom usług, jaki można określić, ale też najbardziej złożony.

Usługi zintegrowane dotyczą czasu dostarczenia danych i związane są z określaniem specjalnej obsługi ruchu danych. Ważne jest, aby nie nadużywać strategii usług zintegrowanych, ponieważ są one nadal stosunkowo kosztowne. Jeszcze bardziej kosztowne może być jednak niewłaściwe wykorzystanie zasobów sieci.

Usługi zintegrowane wymuszają rezerwację zasobów dla określonej strategii jeszcze przed rozpoczęciem przesyłania danych. Routerom sygnalizuje się żądanie przesłania. Sieć po zaakceptowaniu żądania zarządza przesłaniem między węzłami końcowymi, korzystając z wybranej strategii. *Strategia* to zestaw reguł opisujących pewne działania. W zasadzie jest to lista sterująca dostępem do sieci. Klient wysyła najpierw żądanie rezerwacji przepustowości. Jeśli wszystkie routery na trasie do węzła końcowego zaakceptują wymagania klienta, żądanie klienta trafia do serwera QoS i strategii IntServ. Jeśli żądanie mieści się w limitach ustalonych w strategii, serwer QoS udziela zgody na połączenie RSVP i ustala przepustowość tego połączenia. Rezerwacji dokonuje się za pomocą protokołu RSVP (Resource Reservation Protocol) i funkcji API RAPI oraz funkcji API gniazd QoS qtoq.

Każdy węzeł leżący na trasie połączenia musi obsługiwać protokół RSVP. Routery udostępniają QoS za pomocą następujących funkcji sterowania ruchem danych: funkcja planująca, funkcja klasyfikująca, funkcja sterowania dostępem. Możliwości sterowania ruchem często określa się jako obsługę protokołu RSVP. W związku z tym najważniejszym elementem realizacji strategii usług zintegrowanych jest możliwość sterowania zasobami sieci i przewidywania ich dostępności. Aby uzyskać pożądaną efekt, każdy węzeł w sieci musi obsługiwać protokół RSVP. W normalnym trybie trasa danych wybierana jest na podstawie dostępnych zasobów, nie na podstawie danych o tym, czy routery obsługują protokół RSVP. Przepływ danych przez routery nieobsługujące tego protokołu może spowodować obniżenie wydajności transmisji. W takim przypadku połączenie także jest nawiązywane, lecz router nie gwarantuje pożądaną przepustowości. Poniższy rysunek obrazuje sposób funkcjonowania usług zintegrowanych.



Rysunek 2. Ścieżka RSVP między klientem i serwerem

Aplikacja obsługująca protokół RSVP uruchomiona na serwerze nasłuchuje żądań połączenia od klientów. Po odebraniu żądania aplikacja serwera wysyła do klienta komendę PATH. Komenda ta uruchamiana jest za pomocą funkcji API RAPI lub funkcji API gniazd QoS qtoq i zawiera dane o adresach IP routerów. Zawiera także dane o dostępnych zasobach serwera i poszczególnych routerów oraz dane o trasie połączenia. Aplikacja obsługująca protokół RSVP uruchomiona na komputerze klienta wysyła do serwera komendę RESV sygnalizującą, że zasoby sieci zostały przydzielone. Komenda ta dokonuje rezerwacji zasobów na podstawie danych o routerach pochodzących z komendy PATH. Serwer i wszystkie routery na trasie połączenia rezerwują zasoby dla połączenia RSVP. Po odebraniu przez serwer komendy RESV aplikacja rozpoczyna transmisję danych do klienta. Dane są przesyłane wzdłuż tej samej trasy, na której nastąpiła rezerwacja zasobów. Potwierdza to ponownie, jak duże znaczenie dla pomyślnej realizacji strategii ma możliwość rezerwacji zasobów przez routery.

Usługi zintegrowane nie zostały zaprojektowane z myślą o krótkotrwałych połączeniach RSVP, takich jak na przykład połączenia HTTP. Oczywiście wszystko zależy od administratora. Tylko on może zdecydować, jakie rozwiązanie jest najlepsze w danej sieci. Należy zastanowić się, w jakich obszarach i w przypadku jakich aplikacji występują problemy z wydajnością sieci, w związku z czym wymagają one QoS. Aplikacje korzystające ze strategii usług zintegrowanych muszą obsługiwać protokół RSVP. Serwer iSeries w obecnej wersji nie ma żadnych aplikacji tego typu. Trzeba więc utworzyć je samodzielnie.

Gdy pakiet napływa do buforu i ma zostać wysłany, serwer sprawdza, czy istnieją wystarczające zasoby, aby można go było obsłużyć. Decyzja zależy od wielkości wolnego miejsca w zasobniku tokenów. Administrator samodzielnie ustawia następujące dane: liczba bitów w zasobniku tokenów, limity przepustowości, limity szybkości tokenów i maksymalną liczbę połączeń, które zaakceptuje serwer. Wartości te nazywa się limitami wydajności. Jeśli pakiety nie powodują naruszenia limitów, uznaje się je za zgodne i wysyła. W przypadku usług zintegrowanych każde połączenie uzyskuje własny zasobnik tokenów.

## Usługi zintegrowane wykorzystujące oznakowanie stosowane w usługach zróżnicowanych

Strategię usług zintegrowanych można utworzyć nawet jeśli nie ma pewności, czy połączenia RSVP są zagwarantowane w całej sieci. Jeśli zasoby sieciowe nie są w stanie obsługiwać protokołu RSVP, nie ma pewności, czy połączenie się powiedzie. W takiej sytuacji można do strategii zastosować punkt kodowy. Z punktów kodowych zwykle korzysta się w strategiach usług DiffServ w celu przydzielenia ruchu danych do odpowiedniej klasy usług. Punkt kodowy powoduje uzyskanie przez połączenie pewnego priorytetu, nawet jeśli połączenie nie jest gwarantowane.

### Pojęcia pokrewne

“Funkcje API QoS” na stronie 17

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSeRVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

“Usługi zintegrowane wykorzystujące oznakowanie stosowane w usługach DiffServ” na stronie 11

Korzystanie z oznakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu dla liczby pakietów wysłanych w środowisku zróżnicowanym.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 38

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

“Scenariusz: dedykowane dostarczanie (telefonía IP)” na stronie 42

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa rodzaje takich strategii: usługi gwarantowane i usługi sterowanego obciążenia. W tym przykładzie wykorzystano usługi gwarantowane.

## Funkcje sterujące ruchem danych

Funkcje sterujące ruchem danych stosowane są tylko w usługach zintegrowanych i nie są specyficzne dla serwera iSeries.

Terminy te nie występują w interfejsie QoS, ponieważ serwer nie może sterować sprzętem zewnętrznym. Konieczne jest spełnienie ogólnych wymagań QoS przez sprzęt poza siecią prywatną. W niniejszej sekcji omówiono ogólne wymagania strategii usług zintegrowanych dotyczące routerów. Przed zaimplementowaniem strategii zalecane jest zapoznanie się z ogólnymi pojęciami i wymaganiami wstępnymi QoS.

Aby uzyskać pożądaną wydajność ruchu danych, na jego trasie muszą działać urządzenia obsługujące protokół RSVP. Routery muszą spełniać pewne funkcje sterujące ruchem aby korzystać z protokołu RSVP. Mówi się wówczas o nich, że *obsługują protokół RSVP* lub że *obsługują QoS*. Należy pamiętać, że serwer iSeries może pełnić jedynie funkcje klienta lub serwera. Nie można go natomiast wykorzystać jako routera. W dokumentacji urządzeń sieciowych należy sprawdzić, czy spełniają one wymagania QoS.

Wyróżnia się następujące funkcje sterujące ruchem danych:

#### **Funkcja planująca**

Funkcja planująca zarządza przekazywaniem pakietów na podstawie danych umieszczonych w nagłówku IP. Zapewnia ona dostosowanie sposobu dostarczania pakietów do parametrów określonych w strategii. Funkcja planująca umieszczona jest w tym miejscu, w którym istnieje kolejka pakietów.

#### **Funkcja klasyfikująca**

W funkcji tej identyfikuje się pakiety uzyskujące określony poziom usług na podstawie nagłówka IP. Każdy napływający pakiet jest zaliczany do pewnej klasy. Pakiety umieszczone w tej samej klasie są traktowane jednakowo. Poziom usług jest określany na podstawie strategii.

#### **Funkcja sterowania dostępem**

Funkcja sterowania dostępem zawiera algorytm decyzyjny umożliwiający routerowi określenie, czy wystarczy zasobów na realizację żądania QoS. Jeśli zasobów jest zbyt mało, żądanie zostanie odrzucone. Jeśli żądanie jest akceptowane, router korzysta z funkcji klasyfikującej i funkcji planującej, aby zarezerwować zasoby. Sterowanie dostępem odbywa się w każdym routerze na trasie rezerwacji (między węzłami końcowymi).

#### **Pojęcia pokrewne**

“Funkcje API QoS” na stronie 17

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSerVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

#### **Odsyłacze pokrewne**

“Informacje związane z jakością usług” na stronie 66

Znajdują się tu podręczniki IBM Redbooks (w formacie PDF), serwisy WWW, oraz tematy Centrum informacyjnego związane z zagadnieniem Jakości usług. Wszystkie dokumenty w formacie PDF można wyświetlać lub drukować.

## **Rodzaje usług zintegrowanych**

Istnieją dwa rodzaje usług zintegrowanych: usługi sterowanego obciążenia i usługi gwarantowane.

### **Usługi sterowanego obciążenia**

Usługę sterowanego obciążenia wykorzystuje się w przypadku aplikacji szczególnie czułych na przeciążenie sieci, takich jak aplikacje czasu rzeczywistego. Aplikacje muszą tolerować jednak niewielki poziom strat i opóźnień. Gdy aplikacja korzysta z usługi sterowanego obciążenia, jej wydajność nie spadnie po zwiększeniu się obciążenia sieci. Zostanie jej zapewniony poziom transmisji taki, jak w normalnych warunkach przy niewielkim obciążeniu sieci.

Routery muszą zapewniać odpowiednią przepustowość i zasoby konieczne do przetwarzania pakietów. Dlatego muszą obsługiwać QoS oraz usługi zintegrowane. Administrator musi sprawdzić w specyfikacji routerów, czy udostępniają one QoS za pomocą funkcji sterowania ruchem danych. Sterowanie ruchem danych obejmuje następujące funkcje obsługi pakietów: funkcję planującą, funkcję klasyfikującą i funkcję sterowania dostępem.

## Usługi gwarantowane

Usługi gwarantowane zapewniają dostarczenie pakietów w określonym czasie. Usług gwarantowanych wymagają między innymi systemy rozgłaszające audio i wideo korzystające z technik strumieniowych. Usługa gwarantowana określa maksymalne opóźnienie, z jakim mogą być przesyłane pakiety umieszczone w kolejce. Aby zapewnić dostarczenie pakietów na czas, każdy router na trasie połączenia musi obsługiwać protokół RSVP. Usługę gwarantowaną definiuje się, określając limity dotyczące zasobnika tokenów i limity przepustowości. Usługi gwarantowane można stosować tylko w przypadku aplikacji korzystających z protokołu TCP.

### Pojęcia pokrewne

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 38

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

“Scenariusz: dedykowane dostarczanie (telefonía IP)” na stronie 42

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa rodzaje takich strategii: usługi gwarantowane i usługi sterowanego obciążenia. W tym przykładzie wykorzystano usługi gwarantowane.

## Limity dotyczące zasobnika tokenów i limity przepustowości

Limity dotyczące zasobnika tokenów i limity przepustowości noszą wspólną nazwę limitów wydajności. Limity te umożliwiają gwarantowane dostarczanie pakietów w strategiach ruchu wychodzącego, to znaczy w strategii usług zintegrowanych i strategii usług DiffServ.

## Wielkość zasobnika tokenów

Wielkość zasobnika tokenów określa ilość informacji, jaką może przetworzyć serwer w danej chwili. Jeśli aplikacja przesyła dane do serwera szybciej, niż ten może przesłać dane do sieci, następuje przepełnienie buforu. Wszelkie pakiety danych przekraczające ten limit są traktowane jako spoza profilu. Wyjątek stanowią strategie usług zintegrowanych. Można wybrać brak ograniczenia, co zezwoli na żądanie połączenia RSVP. Dla pozostałych strategii można określić sposób obsługi ruchu spoza profilu. Maksymalna wielkość zasobnika tokenów wynosi 1 GB.

## Limit szybkości tokenów

Limit szybkości określa długoterminową szybkość transmisji lub liczbę bitów na sekundę przyjmowanych przez sieć. Żądaną przepustowość porównywana jest z limitami szybkości i przepływu określonymi w strategii QoS. Serwer odrzuca żądanie, jeśli spowodowałoby ono przekroczenie limitów. Limit szybkości tokenów używany jest jedynie w sterowaniu dostępem w ramach strategii usług zintegrowanych. Wartość limitu może wynosić od 10 Kbps do 1 Gbps. Można również ustawić brak ograniczenia. Przy ustawieniu brak ograniczenia jedynym ograniczeniem szybkości będą możliwości sprzętu.

**Wskazówka:** Aby określić właściwe limity, można skorzystać z monitora. W tym celu należy utworzyć strategię, w której limit szybkości tokenów jest na tyle duży, aby można było obsłużyć większość ruchu danych. Następnie należy uruchomić zbieranie danych w tej strategii. Scenariusz dotyczący monitorowania bieżących statystyk sieci opisuje jeden ze sposobów określania całkowitych szybkości aktualnie używanych aplikacji i zasobów sieciowych. Na podstawie otrzymanych wyników można odpowiednio zmniejszyć limity.

W celu przeglądania danych monitora czasu rzeczywistego zamiast zebranych danych wystarczy uruchomić monitor. Monitor podaje statystyki w czasie rzeczywistym dla wszystkich aktywnych strategii.

### Pojęcia pokrewne

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.



“Scenariusz: Monitorowanie bieżących statystyk sieci” na stronie 46

W trakcie pracy z kreatorami ustawić należy limity wydajności. Nie można w tym przypadku zalecić żadnych wartości, ponieważ zależą one od konkretnych wymagań dotyczących danej sieci.

## Usługi zintegrowane wykorzystujące oznakowanie stosowane w usługach DiffServ

Korzystanie z oznakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu dla liczby pakietów wysłanych w środowisku zróżnicowanym.

Środowisko jest mieszane, gdy rezerwacja usług zintegrowanych jest przesyłana między routerami, które nie obsługują usług zintegrowanych, obsługują natomiast usługi DiffServ. Ponieważ dane przesyłane są w różnych domenach i przy różnych uzgodnieniach dotyczących poziomu usługi, a ponadto obsługują je urządzenia o różnych możliwościach, nie zawsze można uzyskać pożądaną usługę.

Aby nieco złagodzić ten problem, w strategii usług zintegrowanych można skorzystać z oznakowania stosowanego w usługach DiffServ. W takim przypadku, gdy dane docierają do routera nieobsługującego protokołu RSVP, nadal zachowują pewien priorytet. Wykorzystywane oznakowanie nazywa się charakterystyką w ramach segmentu sieci.

## Brak sygnalizacji

Oprócz oznakowania można używać także funkcji *no signal* (brak sygnalizacji). Po wybraniu funkcji API w wersji "no signal" można utworzyć aplikacje pozwalające serwerowi na pobranie reguły RSVP w sytuacji, gdy protokół RSVP jest obsługiwany tylko przez aplikację serwera. Sygnalizacja w protokole RSVP wykonuje się automatycznie w imieniu klienta. W ten sposób połączenie RSVP może zostać nawiązane nawet wtedy, gdy klient nie obsługuje protokołu RSVP.

Funkcja "no signal" dotyczy strategii usług zintegrowanych. Aby aktywować brak sygnalizacji, wykonaj następujące czynności:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz **Konfiguracja**.
3. Rozwiń **Strategie połączeń wychodzących** → **Właściwości usług zintegrowanych**.
4. Prawym przyciskiem myszy kliknij odpowiednią nazwę strategii usług zintegrowanych i wybierz opcję **Właściwości**. Zostanie wyświetlone okno dialogowe właściwości usług zintegrowanych.
5. Aby wyłączyć lub włączyć sygnalizację, wybierz zakładkę **Zarządzanie ruchem danych**. W oknie tym można również określić harmonogram, klienta, aplikację i sposób zarządzania ruchem danych.

### Pojęcia pokrewne

“Klasa usług” na stronie 13

Gdy tworzy się strategię usług DiffServ lub strategię akceptowania połączeń przychodzących, konieczne jest także utworzenie i wykorzystanie klasy usług.

“Usługa zintegrowana” na stronie 6

Jest to drugi typ strategii połączeń wychodzących. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API dotyczących QoS.

## Strategia akceptowania ruchu przychodzącego

Strategia akceptowania ruchu przychodzącego służy do sterowania żadaniami połączeń przychodzącymi do sieci.

Strategia ruchu przychodzącego służy do ograniczenia ruchu danych uzyskujących dostęp do serwera iSeries. Istnieje możliwość ograniczenia dostępu na podstawie klienta, URI, aplikacji lub lokalnego interfejsu serwera iSeries. Można ponadto poprawić wydajność serwera stosując dla ruchu przychodzącego klasę usług. Strategię tę definiuje się za pomocą kreatora akceptowania ruchu przychodzącego w programie iSeries Navigator.

Poniżej podano informacje na temat trzech komponentów strategii ruchu przychodzącego. Obejmują one zastosowanie zasobów URI do ograniczenia ruchu, szybkości połączeń definiowane w klasach usług oraz kolejki priorytetowe, w których umieszczane są zaakceptowane połączenia. Więcej informacji na ten temat zawiera sekcja “Zasób URI” na stronie 12, “Szybkość połączeń” na stronie 12, a także sekcja “Wagi kolejek priorytetowych” na stronie 13.

## Zasób URI

Strategie ruchu przychodzącego można zastosować w celu ograniczenia ruchu HTTP przychodzącego do serwera WWW. W takim przypadku można utworzyć strategię akceptowania ruchu przychodzącego ograniczającą ruch danych według określonych zasobów URI. Strategie szybkości dostępu do zasobów URI stanowią część rozwiązania umożliwiającego zabezpieczenie serwerów przed przeciążeniem. Określenie konkretnych zasobów URI umożliwia sterowanie dostępem do zasobów URI serwera na podstawie danych o aplikacji. Dzięki temu ogranicza się liczbę zaakceptowanych żądań. Rozwiązanie to znane jest również jako *sterowanie połączeniami na podstawie nagłówków*. Wykorzystuje ono identyfikatory URI do określenia priorytetów żądań.

W strategiach wykorzystujących identyfikatory URI sprawdzane są nie tylko nagłówki pakietów, ale także ich zawartość. Sprawdzona zawartość stanowi nazwę URI. W przypadku serwera iSeries można stosować względne nazwy URI (na przykład, **/produkty/ubrania** ). W poniższych przykładach wyjaśniono nazwy względne zasobów URI.

## Nazwa względna URI

Nazwy względne URI stanowią podzbiór nazw pełnych URI (nazwy te przypominają nazwy pełne URL). Rozważmy następujący przykład: `http://www.ibm.com/software`. Segment `http://www.ibm.com/software` stanowi nazwę pełną URI. Natomiast segment `/software` to nazwa względna URI. Wszystkie nazwy względne URI muszą rozpoczynać się ukośnikiem (/). Oto przykłady poprawnych nazw względnych:

- `/market/jedzenie#D5`
- `/oprogramowanie`
- `/market/jedzenie?q=warzywa`

### Uwagi:

1. W przypadku korzystania z identyfikatorów URI konieczne jest stosowanie protokołu TCP. Ponadto port i adres IP muszą być takie same jak port i adres IP skonfigurowane dla serwera HTTP. Zwykle używany jest port 80.
2. Do nazwy URI automatycznie dodawany jest znak zastępczy. Na przykład nazwa `/oprogramowanie` obejmuje wszystkie zasoby znajdujące się w katalogu `oprogramowanie`.
3. Podczas definiowania URI nie należy używać znaku `*`. Ten znak nie jest poprawny.
4. Informacje o URI można wykorzystywać w strategiach ruchu przychodzącego lub w strategii usług DiffServ (ruchu wychodzącego).

Przed skonfigurowaniem strategii ruchu przychodzącego korzystającej z nazw URI, należy się upewnić, że port aplikacji przypisany do URI jest taki sam, jak port podany za pomocą dyrektywy `Listen` FRCA w konfiguracji serwera WWW Apache. Informacje na temat sposobu zmiany lub wyświetlenia portu serwera HTTP zawiera artykuł *Zarządzanie adresami i portami serwera HTTP opartego na serwerze Apache*.

## Szybkość połączeń

Podczas tworzenia strategii akceptowania ruchu przychodzącego trzeba wybrać klasę usług. Określa ona szybkości połączeń, co umożliwia sterowanie dostępem w celu ograniczenia liczby połączeń akceptowanych przez serwer.

Stosowanie limitów szybkości połączeń powoduje akceptowanie lub odrzucanie nowych pakietów na podstawie średniej liczby połączeń na sekundę i maksymalnej liczby chwilowych połączeń podanych w utworzonej strategii. Limity dotyczące połączeń to limit szybkości średniego połączenia i limit porcji dla połączenia, których określenie wymagane jest przez kreatory w programie iSeries Navigator. Kiedy zgłoszenie połączenia przychodzącego dotrze do serwera, analizuje on informacje zawarte w nagłówku pakietu, aby określić, czy ten ruch danych jest zgodny z definicją strategii. Porównuje on dane z nagłówków z danymi profilu określającymi limity połączenia. Jeśli pakiet nie powoduje przekroczenia limitów podanych w strategii, jest umieszczany w kolejce.

Podczas wypełniania pól kreatora akceptowania ruchu przychodzącego należy korzystać z podanych powyżej informacji. Podczas tworzenia strategii w programie iSeries Navigator można skorzystać również z informacji zawartych w pomocy.

## Wagi kolejek priorytetowych

W ramach sterowania ruchem przychodzącym można określić priorytet, z jakim obsługiwane są żądania połączeń po zaakceptowaniu ich przez strategię. Przypisując kolejkom priorytetowym wagi, można sterować czasem odpowiedzi po nadejściu połączenia dla poszczególnych kolejek. Połączenia umieszczone w kolejce będą obsługiwane w porządku zgodnym z priorytetem kolejki (wysoki, średni, niski lub najlepsza próba). Jeśli nie ma pewności, jakie wagi należy wybrać, można skorzystać z wartości domyślnych. Suma wszystkich wag musi wynosić 100. Na przykład, jeśli dla wszystkich kolejek zostanie podana waga 25, to będą one traktowane jednakowo. Załóżmy, że dla priorytetów podano następujące wagi: Wysoki (50), Średni (30), Niski (15) i Najlepsza próba (5). Wśród zaakceptowanych połączeń będzie:

- 50% połączeń o wysokim priorytecie
- 30% połączeń o średnim priorytecie
- 15% połączeń o niskim priorytecie
- 5% połączeń o priorytecie najlepsza próba

### Pojęcia pokrewne

“Klasa usług”

Gdy tworzy się strategię usług DiffServ lub strategię akceptowania połączeń przychodzących, konieczne jest także utworzenie i wykorzystanie klasy usług.

“Limity średniej szybkości połączeń i porcji połączeń” na stronie 16

Limity dotyczące szybkości połączeń i porcji połączeń są nazywane *limitami szybkości*. Umożliwiają one ograniczanie połączeń przychodzących do serwera. Limity szybkości ustawia się w klasie usług używanej wraz ze strategiami akceptowania ruchu przychodzącego.

## Klasa usług

Gdy tworzy się strategię usług DiffServ lub strategię akceptowania połączeń przychodzących, konieczne jest także utworzenie i wykorzystanie klasy usług.

Klasa usług jest używana w strategiach usług DiffServ oraz strategiach akceptowania ruchu przychodzącego w celu pogrupowania ruchu danych. Podział na grupy i ich priorytet określa administrator, za resztę obsługi odpowiada sprzęt.

Pierwszym etapem realizacji QoS jest zdefiniowanie strategii. Strategie odpowiadają na pytania: kto, co, gdzie i kiedy (może zrobić). Każdej strategii trzeba przypisać klasę usług. Klasy te są definiowane oddzielnie i mogą być wielokrotnie wykorzystywane w strategiach. Podczas definiowania klasy usług określa się, czy może ona być stosowana w strategiach ruchu wychodzącego, przychodzącego, czy też w obu typach strategii. Jeśli zostaną wybrane oba typy (ruch wychodzący i przychodzący), to daną klasę usług będzie można wykorzystać w strategii usług DiffServ oraz w strategii akceptowania ruchu przychodzącego.

Ustawienia w ramach klasy usług zależą od typu strategii, w którym ma być wykorzystywana. Podczas tworzenia klasy usług można napotkać następujące wymagania:

### Oznaczenie punktem kodowym

W jakości usług (QoS) charakterystykę w ramach segmentu sieci określa się, korzystając z punktów kodowych. Routery i przełączniki na podstawie punktów kodowych wyznaczają priorytet ruchu danych. Serwer iSeries nie używa punktów kodowych, ponieważ nie może funkcjonować jako router. Rodzaj punktów kodowych należy określić uwzględniając konkretne potrzeby w danej sieci. Należy zastanowić się, które aplikacje są najistotniejsze i jakie strategie muszą uzyskać wysoki priorytet. Najważniejsze jest zachowanie zgodności z wybranym oznakowaniem, co zagwarantuje uzyskanie pożądaných wyników. Punkty kodowe są kluczowym elementem różniącym klasy ruchu danych.

### Pomiar ruchu

QoS korzysta z limitów sterowania szybkością, aby ograniczyć ruch danych przechodzący przez sieć. Limity

te obejmują wielkość zasobnika tokenów, limit szybkości szczytowej i limit szybkości średniej. Więcej informacji na temat wartości specyficznych znajduje się w sekcji “Limity dotyczące zasobnika tokenów i limity przepustowości” na stronie 10.

### **Ruch spoza profilu**

Ostatni element definicji klasy usług to obsługa danych spoza profilu. Limity sterowania szybkością narzucają ilościowe ograniczenia na ruch danych. Gdy ruch danych powoduje przekroczenie tych ograniczeń, pakiety otrzymują status danych spoza profilu. Obsługa danych spoza profilu stanowi informację dla serwera, czy należy odrzucać pakiety UDP i zmniejszać okno zapełnienia TCP, czy też opóźnić (kształtować) lub ponownie znakować pakiety spoza profilu.

*Odrzucanie pakietów UDP lub zmniejszanie okna zapełnienia TCP:* Jeśli wybrane zostanie odrzucanie i dopasowywanie pakietów spoza profilu, pakiety UDP będą odrzucane. Natomiast okno zapełnienia TCP będzie zmniejszane, tak że szybkość transmisji będzie zgodna z szybkością zasobnika tokenów. W wyniku zmniejszenia zapełnienia następuje zmniejszenie liczby pakietów, które mogą być przesyłane w sieci w dowolnym czasie.

*Opóźnianie (Kształtowanie):* Jeśli zostanie wybrane opóźnianie pakietów spoza profilu, ruch danych będzie kształtowany zgodnie z zadaną charakterystyką obsługi.

*Ponowne znakowanie za pomocą punktu kodowego DiffServ:* Jeśli pakiety spoza profilu zostaną wybrane do ponownego oznakowania za pomocą punktu kodowego, otrzymają nową wartość punktu kodowego. Nie nastąpi ograniczenie szybkości transmisji pakietów w celu dostosowania do charakterystyk obsługi; pakiety zostaną po prostu ponownie oznakowane. Podczas pracy z kreatorem szczegółowe informacje dostępne są po kliknięciu opcji Pomoc.

### **Priorytet**

Połączeniom z serwerem realizowanym za pomocą różnych strategii akceptowania ruchu przychodzącego można nadawać różne priorytety. Pozwala to na określenie kolejności obsługiwanego przez serwer zaakceptowanych połączeń. Możliwe wartości priorytetu to: wysoki, średni, niski i najlepsza próba.

#### **Pojęcia pokrewne**

“Usługi zintegrowane wykorzystujące oznakowanie stosowane w usługach DiffServ” na stronie 11  
Korzystanie z oznakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu dla liczby pakietów wysłanych w środowisku zróżnicowanym.

“Strategia akceptowania ruchu przychodzącego” na stronie 11

Strategia akceptowania ruchu przychodzącego służy do sterowania żądaniami połączeń przychodzącymi do sieci.

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

#### **Odsyłacze pokrewne**

“Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci”

W jakości usług (QoS) charakterystykę w ramach segmentu sieci określa się, korzystając z punktów kodowych.

## **Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci**

W jakości usług (QoS) charakterystykę w ramach segmentu sieci określa się, korzystając z punktów kodowych.

W kreatorku klasy usług trzeba podać charakterystykę w ramach segmentu sieci dla strategii. Rodzaj punktów kodowych należy określić uwzględniając konkretne potrzeby w danej sieci. Sam administrator musi zdecydować, jakie schematy punktów kodowych są sensowne w danym środowisku. Należy zastanowić się, które aplikacje są najistotniejsze i jakie strategie powinny uzyskać wysoki priorytet. Najważniejsze jest zachowanie zgodności z wybranym oznakowaniem, co zagwarantuje uzyskanie pożądanych wyników. Na przykład dla strategii o podobnej ważności powinny być używane podobne punkty kodowe, dzięki czemu uzyskiwane dla nich wyniki będą spójne. Jeśli nie ma pewności jaki punkt kodowy przypisać, można skorzystać z metody prób i błędów. Można utworzyć strategię testową, uruchomić monitor i na podstawie obserwowanych wyników odpowiednio dostosować ustawienia.

W poniższej tabeli przedstawione są punkty kodowe zalecane na podstawie standardów przemysłowych. Większość dostawców ISP uwzględnia punkty kodowe, można więc sprawdzić czy te punkty kodowe są obsługiwane przez danego dostawcę ISP. Dostawcy muszą zapewniać obsługę QoS we wszystkich domenach. Umowy muszą zapewniać odpowiedni poziom usług, tak aby wymagania zawarte w strategiach mogły zostać spełnione. Należy też sprawdzić, czy uzyskiwany poziom usług jest odpowiedni do wymagań. W przeciwnym wypadku można ponieść straty. Stosowanie strategii QoS jest podstawą do negocjowania poziomów usług z dostawcą ISP, co może umożliwić obniżenie kosztów usług sieciowych. Można utworzyć także własne punkty kodowe; nie jest to jednak zalecane w przypadku zastosowań zewnętrznych. Najlepiej wykorzystywać je w środowisku testowym.

## Przyspieszone przekazywanie

Przyspieszone przekazywanie to jedna z charakterystyk w ramach segmentu sieci. Wykorzystuje się je przede wszystkim po to, aby zagwarantować usługę między sieciami. Przyspieszone przekazywanie zapewnia transmisję między węzłami charakteryzującą się niskim poziomem strat i zaburzeń dzięki gwarantowanej przepustowości połączeń. Rezerwacji przepustowości dokonuje się przed wysłaniem pakietu. Głównym celem rezerwacji jest uniknięcie opóźnień i dostarczenie pakietu we właściwym czasie.

*Tabela 1. Zalecane punkty kodowe: przyspieszone przekazywanie*

| Przyspieszone przekazywanie |
|-----------------------------|
| 101110                      |

**Uwaga:** Zwykle przyspieszone przekazywanie wiąże się z wysokimi kosztami, nie zaleca się więc jego częstego stosowania.

## Selektor klasy

Punkty kodowe selektora klasy to inny rodzaj charakterystyki. Istnieje siedem klas. Klasa 0 odpowiada najniższemu priorytetowi pakietów, a Klasa 7 najwyższemu priorytetowi. Selektor klasy to najczęściej stosowana grupa charakterystyk w ramach segmentu sieci, ponieważ podobnych punktów kodowych używa już większość routerów.

*Tabela 2. Zalecane punkty kodowe: selektor klas*

| Selektor klasy   |
|------------------|
| Klasa 0 - 000000 |
| Klasa 1 - 001000 |
| Klasa 2 - 010000 |
| Klasa 3 - 011000 |
| Klasa 4 - 100000 |
| Klasa 5 - 101000 |
| Klasa 6 - 110000 |
| Klasa 7 - 111000 |

## Zapewnione przekazywanie

Zapewnione przekazywanie obejmuje cztery klasy charakterystyk, z których każda ma trzy poziomy odrzucania: niski, średni i wysoki. Poziom odrzucania określa prawdopodobieństwo odrzucenia pakietów. Poszczególnym klasom odpowiadają różne poziomy przepustowości. Klasa 1, Wysoki, określa strategię o najniższym priorytecie, a Klasa 4, Niski, strategię o najwyższym priorytecie. Niski poziom odrzucania oznacza, że prawdopodobieństwo odrzucenia pakietów jest najniższe w obrębie danej klasy.

Tabela 3. Zalecane punkty kodowe: zapewnione przekazywanie

|  |
|--|
| <b>Zapewnione przekazywanie</b>                    |
| Zapewnione przekazywanie, Klasa 1, Niski - 001010  |
| Zapewnione przekazywanie, Klasa 1, Średni - 001100 |
| Zapewnione przekazywanie, Klasa 1, Wysoki - 001110 |
| Zapewnione przekazywanie, Klasa 2, Niski - 010010  |
| Zapewnione przekazywanie, Klasa 2, Średni - 010100 |
| Zapewnione przekazywanie, Klasa 2, Wysoki - 010110 |
| Zapewnione przekazywanie, Klasa 3, Niski - 011010  |
| Zapewnione przekazywanie, Klasa 3, Średni - 011100 |
| Zapewnione przekazywanie, Klasa 3, Wysoki - 011110 |
| Zapewnione przekazywanie, Klasa 4, Niski - 100010  |
| Zapewnione przekazywanie, Klasa 4, Średni - 100100 |
| Zapewnione przekazywanie, Klasa 4, Wysoki - 100110 |

### Pojęcia pokrewne

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

“Klasa usług” na stronie 13

Gdy tworzy się strategię usług DiffServ lub strategię akceptowania połączeń przychodzących, konieczne jest także utworzenie i wykorzystanie klasy usług.

## Limity średniej szybkości połączeń i porcji połączeń

Limity dotyczące szybkości połączeń i porcji połączeń są nazywane *limitami szybkości*. Umożliwiają one ograniczanie połączeń przychodzących do serwera. Limity szybkości ustawia się w klasie usług używanej wraz ze strategiami akceptowania ruchu przychodzącego.

### Limit porcji dla połączenia

Wielkość porcji połączeń określa pojemność buforu przechowującego porcje połączeń (jednoczesne żądania połączenia). Porcje połączeń mogą napływać do serwera w tempie nieodpowiadającym możliwościom serwera lub założeniom administratora. Jeśli liczba połączeń w porcji przekracza określony limit, kolejne połączenia są odrzucane.

### Średnia szybkość połączeń

Średnia szybkość połączeń określa limit nawiązywanych połączeń lub dopuszczalną szybkość żądań dostępu do zasobów URI. Serwer odrzuca żądania, których obsługa spowodowałaby przekroczenie określonych wcześniej limitów. Limit szybkości średniej połączeń określa liczbę połączeń na sekundę.

**Wskazówka:** Aby określić właściwe limity, można skorzystać z monitora. W sekcji Monitorowanie bieżących statystyk sieci przedstawiono przykładową strategię umożliwiającą obsługę większości danych przesyłanych do serwera. Na podstawie otrzymanych wyników można odpowiednio dostosować limity.

W celu przeglądania danych monitora czasu rzeczywistego zamiast zebranych danych należy uruchomić monitor. Monitor podaje statystyki w czasie rzeczywistym dla wszystkich aktywnych strategii.

### Pojęcia pokrewne

“Strategia akceptowania ruchu przychodzącego” na stronie 11

Strategia akceptowania ruchu przychodzącego służy do sterowania żądaniami połączeń przychodzącymi do sieci.

“Scenariusz: Monitorowanie bieżących statystyk sieci” na stronie 46

W trakcie pracy z kreatorami ustawić należy limity wydajności. Nie można w tym przypadku zalecić żadnych wartości, ponieważ zależą one od konkretnych wymagań dotyczących danej sieci.

## Funkcje API QoS

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSerVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

Większość strategii QoS wymaga zastosowania funkcji API. Poniżej opisano funkcje API, które można wykorzystywać w strategiach usług DiffServ lub strategiach usług zintegrowanych. Omówiono także funkcje API wykorzystywane przez monitor QoS.

- “Funkcje API dotyczące usług zintegrowanych”
- “Funkcje API dotyczące usług DiffServ” na stronie 18
- “Funkcje API dotyczące monitorowania” na stronie 18

## Funkcje API dotyczące usług zintegrowanych

Protokół RSVP wraz z funkcjami API RAPI lub funkcjami API gniazd QoS qtoq umożliwiają rezerwację przepustowości w ramach usług zintegrowanych. Każdy węzeł leżący na trasie połączenia musi obsługiwać protokół RSVP. Możliwość realizacji strategii usług zintegrowanych nazywa się często *obsługą protokołu RSVP*. Funkcje kontroli połączenia są używane do określania, które funkcje routera są wymagane dla protokołu RSVP.

Protokół RSVP umożliwia rezerwację zasobów we wszystkich węzłach sieci znajdujących się na trasie połączenia. Rezerwacja obowiązuje do chwili zrealizowania usługi określonej w strategii. Rezerwacja określa sposób obsługi danych i wymaganą przepustowość połączenia. Każdy węzeł sieci zgadza się udostępnić obsługę podaną w rezerwacji.

Protokół RSVP jest prosty ze względu na to, że rezerwacje wykonuje się tylko w jednym kierunku (od odbiorcy). W przypadku bardziej skomplikowanych połączeń, na przykład wideokonferencji, każdy nadawca jest także odbiorcą. Wówczas należy uruchomić dwie sesje RSVP po obu stronach połączenia.

Aby można było skorzystać z usług zintegrowanych, oprócz routerów obsługujących protokół RSVP potrzebne są także obsługujące ten protokół aplikacje. W obecnej wersji systemu iSeries nie są dostępne aplikacje RSVP. Należy je utworzyć za pomocą funkcji RAPI API lub API gniazd QoS qtoq. Wykorzystanie tych funkcji umożliwi obsługę protokołu RSVP. Szczegółowe wyjaśnienia dotyczące stosowanych modeli, ich działania i obsługi komunikatów można znaleźć w wielu dostępnych źródłach. Konieczna jest jedynie gruntowna znajomość protokołu RSVP i dokumentu RFC 2205.

### Funkcje API gniazd qtoq

Aby ułatwić wykorzystanie protokołu RSVP w systemie iSeries, w obecnej wersji można skorzystać z funkcji API gniazd qtoq. Funkcje te wywołują funkcje RAPI i odpowiadają za wykonanie bardziej skomplikowanych zadań. Funkcje gniazd qtoq nie są tak elastyczne jak funkcje RAPI, ale udostępniają te same możliwości przy mniejszym wysiłku ze strony programisty. Wersje "no signal" funkcji API umożliwiają utworzenie:

- aplikacji ładującej na serwer regułę RSVP,
- aplikacji wymagającej obsługi protokołu RSVP tylko po stronie serwera (w połączeniu TCP/IP).

Sygnalizacja w protokole RSVP wykonuje się automatycznie w imieniu klienta.

Typowy przykład komunikacji w przypadku aplikacji korzystających z funkcji gniazd qtoq zawierają sekcje Komunikacja za pomocą funkcji API QoS w trybie z nawiązaniem połączenia i Komunikacja za pomocą funkcji API QoS w trybie bez nawiązywania połączenia.

## Funkcje API dotyczące usług DiffServ

**Uwaga:** Funkcja API `Sendmsg()` jest wykorzystywana w tych strategiach usług DiffServ, w których określony jest token aplikacji. Podczas tworzenia strategii usług DiffServ można (opcjonalnie) podać parametry aplikacji (token i priorytet). Parametry te są używane podczas definiowania zaawansowanych strategii, w innych przypadkach funkcja API nie będzie używana. Należy jednak pamiętać, że routery i inne serwery w sieci zawsze muszą mieć możliwość obsługi usług DiffServ.

Jeśli w strategii usług DiffServ ma być używany token aplikacji, w kodzie aplikacji dostarczającym tę informację należy wykorzystać funkcję API `Sendmsg()`. Jest to zadanie programisty aplikacji. W dokumentacji aplikacji należy zamieścić poprawne wartości (tokenu i priorytetu), które administrator QoS będzie mógł wykorzystać w strategii usług DiffServ. W stosunku do ruchu danych zgodnego z tokenem podanym w strategii zostanie zastosowany priorytet i klasyfikacja danej strategii usług DiffServ. Jeśli w aplikacji nie istnieją wartości zgodne z wartościami ustawionymi w strategii, należy zmodyfikować aplikację lub do zdefiniowania strategii usług DiffServ wykorzystać inne parametry danych aplikacji.

Poniżej krótko opisano parametry danych serwera: token aplikacji i priorytet aplikacji.

### Co to jest token aplikacji?

*Token aplikacji* to nazwa URI reprezentująca określony zasób. Token podany w strategii QoS jest porównywany z tokenem aplikacji zewnętrznej. Aplikacja udostępnia wartość tokenu za pomocą funkcji API `sendmsg()`. Jeśli tokeny są zgodne, ruch danych generowany przez daną aplikację jest uwzględniany w strategii usług DiffServ.

### Co to jest priorytet aplikacji?

Priorytet aplikacji podany przez użytkownika jest porównywany z priorytetem aplikacji dostarczonym przez aplikację zewnętrzną. Aplikacja udostępnia wartość priorytetu za pomocą funkcji API `sendmsg()`. Jeśli priorytety są zgodne, ruch danych generowany przez daną aplikację jest uwzględniany w strategii usług DiffServ. Ruch danych zgodny z ustawieniami strategii DiffServ uzyska priorytet nadany całej strategii.

Więcej informacji na temat typu strategii usług DiffServ znajduje się w sekcji “Usługa DiffServ” na stronie 2.

## Funkcje API dotyczące monitorowania

Funkcje API protokołu RSVP zawierają funkcje API monitorowania. Funkcje API dotyczące monitorowania mają w tytule słowo *monitor*. Na przykład, *QgyOpenListQoSMonitorData*. Poniżej podano krótkie opisy poszczególnych funkcji API dotyczących monitorowania:

- Funkcja *QgyOpenListQoSMonitorData* (Otwieranie listy danych monitora QoS) zbiera informacje odnoszące się do usług QoS.
- Funkcja *QtoqDeleteQoSMonitorData* (Usuwanie danych monitora QoS) usuwa jeden lub więcej zestawów zebranych danych monitora QoS.
- Funkcja *QtoqEndQoSMonitor* (Zakończenie monitora QoS) zatrzymuje zbieranie informacji odnoszących się do usług QoS.
- Funkcja *QtoqListSavedQoSMonitorData* (Lista zapisanych danych monitora QoS) zwraca listę wszystkich zebranych danych monitora, które zostały wcześniej zapisane.
- Funkcja *QtoqSaveQoSMonitorData* (Zapisywanie danych monitora QoS) zapisuje kopię zebranych danych monitora do późniejszego wykorzystania.
- Funkcja *QtoqStartQoSMonitor* (Uruchomienie monitora QoS) zbiera informacje odnoszące się do usług QoS.

### Pojęcia pokrewne

“Usługa zintegrowana” na stronie 6

Jest to drugi typ strategii połączeń wychodzących. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API dotyczących QoS.



“Funkcje sterujące ruchem danych” na stronie 8

Funkcje sterujące ruchem danych stosowane są tylko w usługach zintegrowanych i nie są specyficzne dla serwera iSeries.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 38

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

“Sprzęt i oprogramowanie sieciowe” na stronie 50

Możliwości urządzeń znajdujących się wewnątrz i na zewnątrz sieci mają ogromny wpływ na QoS.

#### **Odsyłacze pokrewne**

Funkcje RAPI API

“Konfigurowanie jakości usług za pomocą kreatorów” na stronie 51

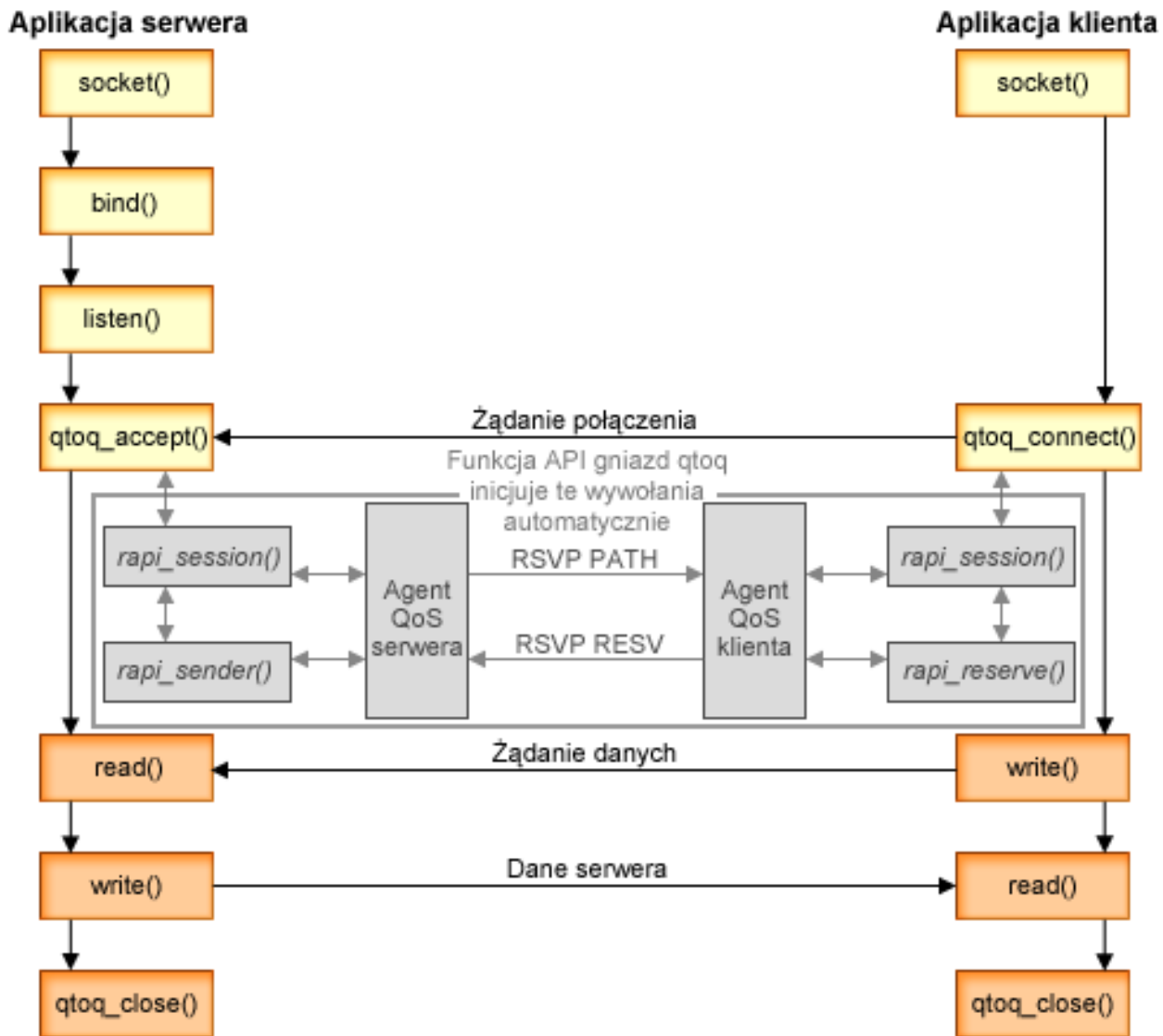
Aby skonfigurować strategię QoS, należy użyć kreatorów znajdujących się w programie iSeries Navigator.

### **Komunikacja za pomocą funkcji API QoS w trybie z nawiązaniem połączenia**

Przykłady serwera i klienta przedstawione w tym temacie pokazują działanie funkcji API QoS dla trybu z nawiązaniem połączenia.

Na poniższym rysunku przedstawiono przebieg komunikacji między klientem i serwerem (za pomocą funkcji gniazd qtoq) w przypadku, gdy protokół wymaga nawiązania połączenia. Przykładem jest protokół TCP.

Wywołanie funkcji API QoS w celu uruchomienia komunikacji RSVP z nawiązaniem połączenia powoduje również zainicjowanie pewnych innych funkcji. Umożliwiają one konfigurację protokołu RSVP po stronie klienta i serwera pod kątem transmisji, która ma nastąpić.



**Przebieg komunikacji z wykorzystaniem funkcji qtoq.** Poniżej opisano przedstawioną na rysunku sekwencję wywołań funkcji gniazd. Omówiono też komunikację z nawiązaniem połączenia między klientem i serwerem. Wykorzystywane tu funkcje stanowią modyfikację podstawowych funkcji API gniazd.

## Po stronie serwera

### Funkcja `qtoq_accept()` w przypadku reguły oznaczonej jako "brak sygnalizacji"

1. Aplikacja wywołuje funkcję `socket()` i uzyskuje deskryptor gniazda.
2. Aplikacja wywołuje funkcję `listen()` umożliwiającą określenie połączeń, których będzie oczekiwać.
3. Aplikacja wywołuje funkcję `qtoq_accept()` umożliwiającą rozpoczęcie oczekiwania na zgłoszenia klientów.
4. Wywoływana jest funkcja API o nazwie `rapi_session()`. Jeśli wywołanie jest pomyślne, zostaje zwrócony identyfikator sesji QoS.
5. Wywoływana jest standardowa funkcja `accept()` oczekująca na zgłoszenia klientów.
6. Po odebraniu zgłoszenia uruchamia się sterowanie dostępem dla żądanej reguły. Regułę umieszcza się w stosie TCP/IP i jeśli jest poprawna, odsyła się ją do aplikacji wywołującej wraz z wynikami i identyfikatorem sesji.
7. Aplikacje serwera i klienta przeprowadzają odpowiednie transmisje danych.

8. Aplikacja wywołuje funkcję `qtoq_close()`, aby zamknąć gniazdo i usunąć z pamięci regułę.
9. Serwer QoS usuwa regułę za pomocą menedżera QoS, usuwa sesję QoS i wykonuje wszelkie inne potrzebne procedury.

### **Funkcja `qtoq_accept()` w przypadku zwykłej sygnalizacji RSVP**

1. Aplikacja wywołuje funkcję `socket()` i uzyskuje deskryptor gniazda.
2. Aplikacja wywołuje funkcję `listen()` umożliwiającą określenie połączeń, których będzie oczekiwać.
3. Aplikacja wywołuje funkcję `qtoq_accept()` umożliwiającą rozpoczęcie oczekiwania na zgłoszenia klientów.
4. Po nadejściu zgłoszenia połączenia wywoływana jest funkcja `rapi_session()`, która tworzy nową sesję z serwerem QoS i pobiera identyfikator sesji zwracany następnie klientowi.
5. Wywoływana jest funkcja `rapi_sender()` powodująca wysłanie komunikatu PATH z serwera QoS i informująca go, że od klienta nadejdzie komunikat RESV.
6. Wywoływana jest funkcja `rapi_getfd()`. Zwraca ona deskryptor, który wykorzystują aplikacje oczekujące na komunikaty o zdarzeniach QoS.
7. Do aplikacji przekazywane są deskryptor akceptacji zgłoszenia i deskryptor QoS.
8. Serwer QoS oczekuje nadejścia komunikatu RESV. Po odebraniu go ładuje odpowiednią regułę za pomocą menedżera QoS i wysyła komunikat do aplikacji, jeśli zażądała ona powiadomienia o wywołaniu funkcji `qtoq_accept()`.
9. Serwer QoS okresowo odświeża nawiązane sesje.
10. Po zakończeniu połączenia aplikacja wywołuje funkcję `qtoq_close()`.
11. Serwer QoS usuwa regułę za pomocą menedżera QoS, usuwa sesję QoS i wykonuje wszelkie inne potrzebne procedury.

### **Po stronie klienta**

#### **Funkcja `qtoq_connect()` w przypadku zwykłej sygnalizacji RSVP**

1. Aplikacja wywołuje funkcję `socket()` i uzyskuje deskryptor gniazda.
2. Aplikacja wywołuje funkcję `qtoq_connect()` informującą aplikację serwera o żądaniu nawiązania połączenia.
3. Funkcja ta wywołuje z kolei funkcję API `rapi_session()` umożliwiającą utworzenie sesji z serwerem QoS.
4. Serwer QoS będzie oczekiwał komendy PATH w danym połączeniu.
5. Wywoływana jest funkcja `rapi_getfd()`. Zwraca ona deskryptor, który wykorzystują aplikacje oczekujące na komunikaty QoS.
6. Wywoływana jest funkcja `connect()`. Jej wynik i deskryptor QoS przekazywane są aplikacji.
7. Serwer QoS oczekuje nadejścia komunikatu PATH. Po odebraniu go wysyła do serwera QoS komunikat RESV.
8. Jeśli zażądano powiadomienia, serwer QoS przesyła do aplikacji deskryptor QoS.
9. Serwer QoS okresowo odświeża nawiązane sesje.
10. Po zakończeniu połączenia aplikacja wywołuje funkcję `qtoq_close()`.
11. Serwer QoS zamyka sesję QoS i wykonuje wszelkie niezbędne procedury.

#### **Funkcja `qtoq_connect()` w przypadku reguły oznaczonej jako "brak sygnalizacji"**

Takie zgłoszenie nie dotyczy klienta, nie wymaga bowiem żadnej jego interwencji.

##### **Odsyłacze pokrewne**

Funkcja API `qtoq_accept()`

Funkcja API `qtoq_close()`

Funkcja API `rapi_session()`

Funkcja API `rapi_sender()`

Funkcja API `rapi_getfd()`

Funkcja API qtoq\_connect()

## Komunikacja za pomocą funkcji API QoS w trybie bez nawiązywania połączenia

Przykłady serwera i klienta zaprezentowane w tym temacie pokazują działanie funkcji API QoS dla trybu bez nawiązywania połączenia.

Wywołanie funkcji API w celu uruchomienia komunikacji RSVP bez nawiązywania połączenia powoduje również zainicjowanie pewnych innych funkcji. Umożliwiają one konfigurację protokołu RSVP po stronie klienta i serwera pod kątem transmisji, która ma nastąpić.



**Przebieg komunikacji z wykorzystaniem funkcji qtoq.** Poniżej opisano sekwencję wywołań funkcji gniazd przedstawioną na rysunku. Omówiono także komunikację między klientem i serwerem w trybie bez nawiązywania połączenia. Wykorzystywane tu funkcje stanowią modyfikację podstawowych funkcji API gniazd.

### Po stronie serwera

## **Funkcja `qtoq_ioctl()` w przypadku reguły oznaczonej jako "brak sygnalizacji"**

1. Funkcja API `qtoq_ioctl()` wysyła do serwera QoS komunikat z informacją, że należy uruchomić sterowanie dostępem dla żądanej reguły.
2. Jeśli regułę można zaakceptować, wywoływana jest funkcja, która do serwera QoS wysyła komunikat powodujący pobranie reguły.
3. Do klienta zwracany jest status określający akceptację reguły lub jej odrzucenie.
4. Gdy aplikacja kończy obsługę połączenia, wywoływana jest funkcja `qtoq_close()` powodująca zamknięcie połączenia.
5. Serwer QoS usuwa regułę z menedżera QoS, usuwa sesję QoS i wykonuje wszelkie inne potrzebne procedury.

## **Funkcja `qtoq_ioctl()` w przypadku zwykłej sygnalizacji RSVP**

1. Funkcja API `qtoq_ioctl()` wysyła do serwera QoS komunikat z informacją, z żądaniem uruchomienia sterowania dostępem dla żądanej reguły.
2. Wywoływana jest funkcja `rapi_session()`. Umożliwia ona nawiązanie sesji dla wybranej reguły i zwraca klientowi identyfikator tej sesji.
3. Wywoływana jest funkcja `rapi_sender()` powodująca wysłanie do klienta komunikatu PATH.
4. Wywoływana jest funkcja `rapi_getfd()` zwracająca deskryptor pliku używany podczas oczekiwania na zdarzenia QoS.
5. Do klienta zwracany jest deskryptor `select()`, identyfikator sesji QoS i status.
6. Serwer QoS pobiera regułę po odebraniu komunikatu RESV.
7. Po zakończeniu połączenia aplikacja wywołuje funkcję `qtoq_close()`.
8. Serwer QoS usuwa regułę z menedżera QoS, usuwa sesję QoS i wykonuje wszelkie inne potrzebne procedury.

## **Po stronie klienta**

### **Funkcja `qtoq_ioctl()` w przypadku zwykłej sygnalizacji RSVP**

1. Wywoływana jest funkcja `rapi_session()` umożliwiająca nawiązanie sesji. Funkcja ta wymaga od serwera użycia sterowania dostępem. Połączenie zostanie odrzucone po stronie klienta tylko wtedy, gdy reguła skonfigurowana na komputerze klienta nie jest w danej chwili aktywna. Funkcja zwraca ID sesji. Wartość ta jest przekazywana do aplikacji.
2. Wywoływana jest funkcja `rapi_getfd()` zwracająca deskryptor pliku używany podczas oczekiwania na zdarzenia QoS.
3. Funkcja `qtoq_ioctl()` zwraca do klienta deskryptor oczekiwania i ID sesji.
4. Serwer QoS oczekuje nadejścia komunikatu PATH. Po odebraniu go wysyła komunikat RESV, a następnie za pomocą deskryptora sesji sygnalizuje aplikacji wystąpienie zdarzenia.
5. Serwer QoS okresowo odświeża nawiązane sesje.
6. Po zakończeniu połączenia kod klienta wywołuje funkcję `qtoq_close()`.

### **Funkcja `qtoq_ioctl()` w przypadku reguły oznaczonej jako "brak sygnalizacji"**

Takie zgłoszenie nie dotyczy klienta, nie wymaga bowiem żadnej jego interwencji.

#### **Odsyłacze pokrewne**

Funkcja API `qtoq_close()`

Funkcja API `rapi_session()`

Funkcja API `rapi_sender()`

Funkcja API `rapi_getfd()`

Funkcja API `qtoq_ioctl()`

## Rozszerzenia funkcji API QoS sendmsg()

Funkcja sendmsg() używana jest do wysyłania danych, danych pomocniczych lub ich kombinacji przez połączone lub niepołączone gniazdo.

Funkcja API sendmsg() uwzględnia dane klasyfikacyjne QoS. Funkcja sendmsg() jest wykorzystywana w strategiach QoS w celu określenia bardziej szczegółowej klasyfikacji wychodzącego lub przychodzącego ruchu TCP/IP. W strategiach zwykle wykorzystywane są pomocnicze typy danych odnoszące się do warstwy IP. Używany jest typ komunikatu IP\_QOS\_CLASSIFICATION\_DATA. Dane pomocnicze mogą być używane przez aplikację do określania atrybutów ruchu w danym połączeniu TCP. Jeśli atrybuty przekazane przez aplikację są zgodne z atrybutami zdefiniowanymi w strategii QoS, to ruch TCP będzie podlegał ograniczeniom wynikającym z tej strategii.

Poniżej podano informacje dotyczące inicjowania struktury komunikatu IP\_QOS\_CLASSIFICATION\_DATA:

- ip\_qos\_version: Oznacza wersję struktury. Należy użyć stałej *IP\_QOS\_CURRENT\_VERSION*
- ip\_qos\_classification\_scope: Określa zasięg klasyfikacji na poziomie połączenia (należy użyć stałej *IP\_QOS\_CONNECTION\_LEVEL*) lub na poziomie komunikatu (stała *IP\_QOS\_MESSAGE\_LEVEL*).  
Zasięg na poziomie połączenia wskazuje, że poziom usług QoS uzyskany za pośrednictwem danych klasyfikacyjnych z tego komunikatu będzie ważny dla wszystkich następnym komunikatów wysyłanych do momentu następnego wywołania funkcji sendmsg() z danymi klasyfikacyjnymi QoS. Zasięg na poziomie komunikatu wskazuje, że przypisany poziom usług QoS będzie używany tylko dla danych komunikatu uwzględnionych w tym wywołaniu funkcji sendmsg(). Dane, które będą później wysyłane bez danych klasyfikacyjnych QoS, będą dziedziczyć poziom usług QoS przypisany poprzednio na poziomie połączenia (z ostatniej klasyfikacji QoS na poziomie połączenia ustalonej za pośrednictwem funkcji sendmsg() lub z oryginalnej klasyfikacji połączenia TCP ustalonej podczas nawiązywania połączenia).
- ip\_qos\_classification\_type: Ten parametr wskazuje typ przekazywanych danych klasyfikacyjnych. Możliwe jest przekazywanie tokenu zdefiniowanego w aplikacji, priorytetu określonego w aplikacji lub obu tych parametrów jednocześnie. W przypadku wybrania tej ostatniej opcji, dwa wybrane typy klasyfikacji muszą być połączone warunkiem "OR". Można użyć następujących typów:

– Klasyfikacja na podstawie tokenu zdefiniowanego w aplikacji. Należy podać jeden typ; w przypadku podania większej liczby typów wyniki będą nieprzewidywalne.

- IP\_SET\_QOSLEVEL\_W\_APPL\_TOKEN\_ASCII : Wskazuje, że klasyfikacja dokonywana jest na podstawie łańcucha znaków w formacie ASCII. W przypadku podania tej opcji token aplikacji powinien być przekazywany w polu ip\_qos\_appl\_token.

**Uwaga:** Jeśli jako dane klasyfikacyjne aplikacja powinna przekazywać wartości liczbowe, to powinny one zostać najpierw przekształcone w format ASCII możliwy do wydrukowania. Trzeba też pamiętać, że podany łańcuch może składać się z wielkich i małych liter i będzie używany do celów porównawczych w dokładnym formacie.

- IP\_SET\_QOSLEVEL\_W\_APPL\_TOKEN\_EBCDIC : Podobnie jak powyżej, z tą różnicą, że łańcuch jest w formacie EBCDIC.

**Uwaga:** Użycie opcji IP\_SET\_QOSLEVEL\_W\_APPL\_TOKEN\_ASCII daje nieco lepszą wydajność, ponieważ dane aplikacji określone w strategii są zapisywane wewnątrz stosu TCTCP/IP w formacie ASCII i dzięki temu nie ma potrzeby konwersji tokenu zdefiniowanego w aplikacji przy każdym zgłoszeniu funkcji sendmsg().

- Klasyfikacja na podstawie priorytetu zdefiniowanego w aplikacji. Należy podać jeden typ; w przypadku podania większej liczby priorytetów typów wyniki będą nieprzewidywalne.
  - IP\_SET\_QOSLEVEL\_EXPEDITED: Wskazuje, że żądany jest priorytet Przyspieszony.
  - IP\_SET\_QOSLEVEL\_HIGH: Wskazuje, że żądany jest priorytet Wysoki.
  - IP\_SET\_QOSLEVEL\_MEDIUM: Wskazuje, że żądany jest priorytet Średni.
  - IP\_SET\_QOSLEVEL\_LOW: Wskazuje, że żądany jest priorytet Niski.
  - IP\_SET\_QOSLEVEL\_EFFORT: Wskazuje, że żądany jest priorytet Najlepsza próba.
- ip\_qos\_appl\_token\_len: Długość tokenu podanego w polu ip\_qos\_appl\_token.

- `ip_qos_appl_token`: To "pole wirtualne" następuje zaraz po polu `ip_qos_classification_type`. Użycie łańcucha tokenu aplikacji w formacie ASCII lub EBCDIC zależy od tego, którą z opcji `IP_SET_QOSLEVEL_W_APPL_TOKEN_xxxx` podano jako typ klasyfikacji. To pole jest wykorzystywane tylko wtedy, gdy jako typ klasyfikacji podany jest typ tokenu zdefiniowanego w aplikacji. Długość łańcucha nie może przekraczać 128 bitów. Jeśli zostanie podany łańcuch o większej długości, to użytych zostanie tylko 128 początkowych bitów. Trzeba przy tym pamiętać, że długość łańcucha jest wyznaczana na podstawie wartości podanej dla parametru `msg_len` (`msg_len - sizeof(msg_hdr) - sizeof(ip_qos_classification_data)`). Tak wyliczona długość nie uwzględnia znaków końcowych o kodzie null.

### Pojęcia pokrewne

"Usługa DiffServ" na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

"Klasy z priorytetami: sposób klasyfikacji ruchu w sieci" na stronie 3

W ramach usług DiffServ ruch danych identyfikowany jest jako *klasy*. Klasy te najczęściej określa się przy użyciu adresów IP klientów, portów aplikacji, typu serwera, protokołu, lokalnego adresu IP oraz harmonogramu. Wszystkie transmisje należące do tej samej klasy są traktowane jednakowo.

### Odsyłacze pokrewne

Funkcja API `Sendmsg()` - Wysyłanie komunikatu przez gniazdo

## Serwer katalogów

Strategie można eksportować do serwera katalogów. W tej sekcji opisano korzyści wynikające z obu metod: eksportowania strategii do serwera katalogów oraz z zaniechania eksportu, a także konfigurowanie protokołu LDAP i związane z nim pojęcia, oraz schemat QoS.

Konfigurację strategii QoS można eksportować do serwera katalogów za pomocą protokołu LDAP w wersji 3.

## Korzyści wynikające ze stosowania serwera katalogów

Eksportowanie strategii QoS do serwera katalogów ułatwia zarządzanie strategiami. Istnieją trzy sposoby wykorzystania serwera:

- Dane konfiguracyjne mogą być przechowywane na jednym lokalnym serwerze katalogów i współużytkowane przez wiele systemów.
- Dane konfiguracyjne mogą być konfigurowane, przechowywane i wykorzystywane tylko w jednym systemie (nie są współużytkowane).
- Dane konfiguracyjne rezydują na serwerze katalogów, na którym istnieją także dane innych systemów, ale nie są współużytkowane przez inne systemy. Dzięki temu w jednym miejscu składa się i zapisuje dane różnych systemów.

## Korzyści wynikające z zapisywania konfiguracji wyłącznie na serwerze lokalnym

Zapisywanie strategii QoS na serwerze lokalnym jest prostsze. Lokalne użytkowanie strategii przynosi wiele korzyści:

- Użytkownicy, którzy nie muszą wykorzystywać protokołu LDAP, nie muszą wykonywać złożonego procesu konfigurowania.
- Następuje poprawa wydajności, ponieważ zapisywanie za pomocą protokołu LDAP nie jest najszybszą metodą.
- Łatwiejsze jest duplikowanie konfiguracji między różnymi serwerami iSeries iSeries. Wystarczy skopiować zbiór z jednego systemu do drugiego. Ponieważ nie ma podziału na maszyny podstawowe i dodatkowe, każdą strategię można dostosować do potrzeb konkretnego serwera.

## Zasoby serwera LDAP

Przed wyeksportowaniem strategii do serwera LDAP trzeba zapoznać się z koncepcją serwera LDAP oraz strukturami katalogów. Za pomocą funkcji QoS w programie iSeries Navigator, można skonfigurować serwer katalogów używany zgodnie ze strategią QoS.

### Pojęcia pokrewne

Serwer katalogów IBM dla iSeries (LDAP)

“Konfigurowanie serwera katalogów” na stronie 53

Konfiguracje strategii QoS można eksportować do serwera katalogów LDAP.

## Słowa kluczowe

Konfigurując serwer katalogów trzeba określić, czy z każdą konfiguracją QoS będą skojarzone słowa kluczowe.

Słowa kluczowe są opcjonalne i można je pominąć. Poniżej wyjaśniono pojęcie słów kluczowych oraz sens ich używania.

W kreatorze konfiguracji początkowej QoS można skonfigurować serwer katalogów. Można między innymi określić, czy jest on systemem podstawowym, czy dodatkowym. Serwer, na którym przechowywane są wszystkie strategie QoS, to podstawowy serwer katalogów.

Słowa kluczowe wykorzystuje się do identyfikacji danych konfiguracyjnych utworzonych w podstawowych serwerach katalogów (systemach podstawowych). Chociaż słowa kluczowe tworzone są w systemie podstawowym, faktycznie korzysta się z nich w systemach dodatkowych. Umożliwiają one systemom dodatkowym pobieranie i wykorzystywanie konfiguracji utworzonych w systemie podstawowym. Poniższe informacje pomogą zrozumieć, jak używać słów kluczowych w poszczególnych systemach.

### Słowa kluczowe a systemy podstawowe

Słowa kluczowe dotyczą konfiguracji QoS tworzonych i obsługiwanych w systemie podstawowym. Używa się ich po to, aby systemy dodatkowe mogły zidentyfikować konfiguracje w systemie podstawowym.

### Słowa kluczowe a systemy dodatkowe

Systemy dodatkowe korzystają ze słów kluczowych przy wyszukiwaniu konfiguracji. System dodatkowy pobiera i wykorzystuje konfiguracje utworzone w systemie podstawowym. Podczas konfigurowania systemu dodatkowego można wybrać określone słowa kluczowe. System dodatkowy pobiera konfiguracje skojarzone z wybranymi słowami kluczowymi. Umożliwia to pobranie kilku konfiguracji utworzonych w kilku systemach podstawowych.

Aby uzyskać szczegółowe instrukcje podczas konfigurowania serwera katalogów w programie iSeries Navigator, należy skorzystać z pomocy dotyczącej QoS.

### Pojęcia pokrewne

“Nazwa wyróżniająca”

Aby zarządzać częścią katalogu, należy użyć *nazwy wyróżniającej (DN)* lub słowa kluczowego (jeśli jest to potrzebne).

“Konfigurowanie serwera katalogów” na stronie 53

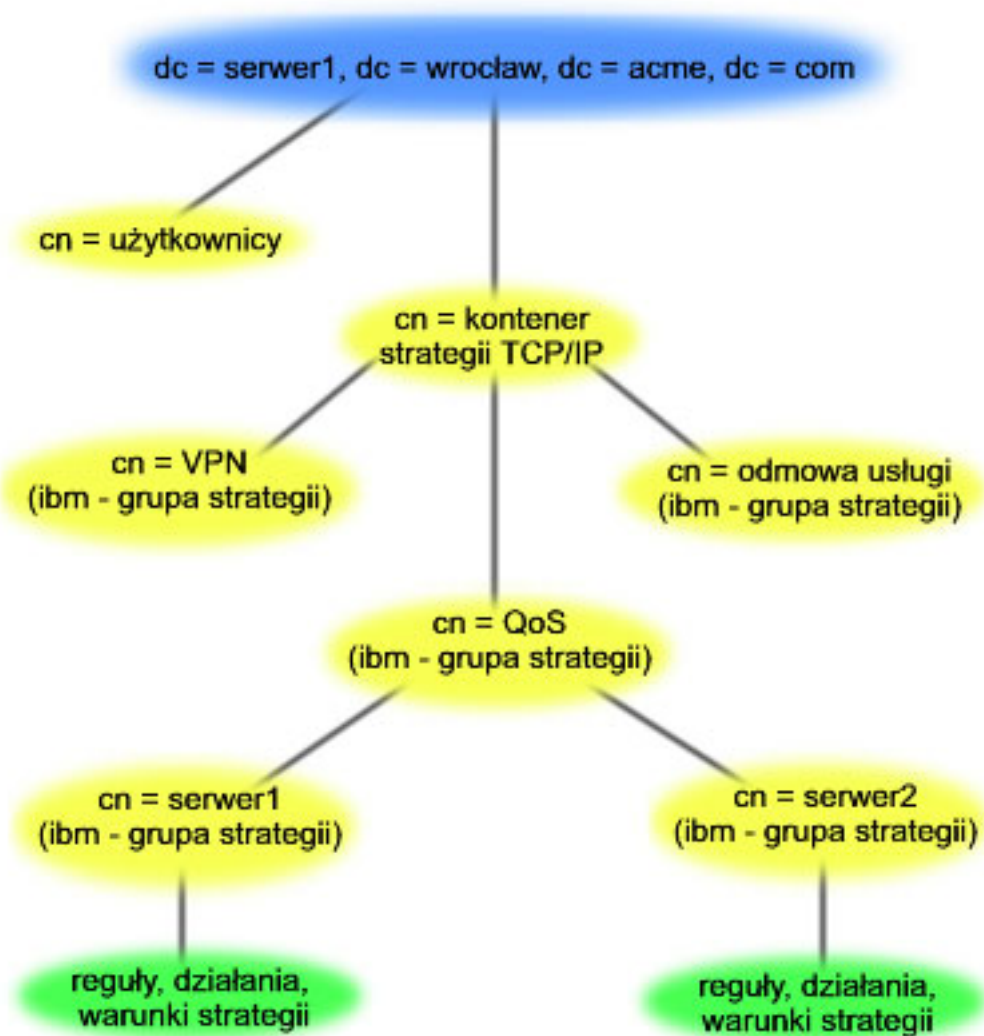
Konfiguracje strategii QoS można eksportować do serwera katalogów LDAP.

## Nazwa wyróżniająca

Aby zarządzać częścią katalogu, należy użyć *nazwy wyróżniającej (DN)* lub słowa kluczowego (jeśli jest to potrzebne).

Nazwę wyróżniającą podaje się podczas konfigurowania serwera katalogów w kreatorze konfiguracji początkowej QoS. Nazwa taka składa się zwykle z nazwy pozycji i nazwy obiektów znajdujących się wyżej w hierarchii (w kolejności od góry do dołu). Serwer ma dostęp do wszystkich obiektów znajdujących się poniżej nazwy wyróżniającej. Na przykład, serwer LDAP może zawierać strukturę katalogów taką, jaką przedstawia poniższy rysunek:





Rysunek 3. Przykładowa struktura katalogów QoS

Serwer1 umieszczony u góry (dc = serwer1, dc = wroclaw, dc = acme, dc = com) to nazwa komputera, na którym uruchomiono serwer katalogów. QoS uruchomiono na innych serwerach, między innymi na cn = QoS i cn = strategii TCP/IP. Domyślną nazwą wyróżniającą serwera cn = serwer1 jest cn = serwer1, cn = QoS, cn = strategii TCP/IP, dc = serwer1, dc = wroclaw, dc = acme, dc = com. Domyślną nazwą wyróżniającą serwera cn = serwer2 jest cn = serwer2, cn = QoS, cn = strategii TCP/IP, dc = serwer1, dc = wroclaw, dc = acme, dc = com.

Aby zarządzać katalogiem, w nazwie wyróżniającej należy podać właściwy serwer, to znaczy cn lub dc. Trzeba ostrożnie zmieniać nazwę wyróżniającą, łańcuch znaków jest bowiem zwykle zbyt długi i nie mieści się w polu.

#### Pojęcia pokrewne

“Słowa kluczowe” na stronie 26

Konfigurując serwer katalogów trzeba określić, czy z każdą konfiguracją QoS będą skojarzone słowa kluczowe.

“Konfigurowanie serwera katalogów” na stronie 53

Konfiguracje strategii QoS można eksportować do serwera katalogów LDAP.

#### Odsyłacze pokrewne

“Informacje związane z jakością usług” na stronie 66

Znajdują się tu podręczniki IBM Redbooks (w formacie PDF), serwisy WWW, oraz tematy Centrum informacyjnego związane z zagadnieniem Jakości usług. Wszystkie dokumenty w formacie PDF można wyświetlać lub drukować.

---

## Scenariusze

Niniejsze strategie usługi mogą się okazać przydatne w zrozumieniu celu i sposobu używania usługi QoS.

Jednym z najlepszych sposobów zrozumienia zasad wykorzystania usługi QoS jest zapoznanie się z typowymi przykładami jej zastosowania. Poniższe przykłady ilustrują sens stosowania strategii QoS i zawierają instrukcje dotyczące tworzenia strategii oraz klas usług.

**Uwaga:** Adresy IP i diagramy są fikcyjne i zostały użyte jedynie na potrzeby przykładu.

### Pojęcia pokrewne

“Monitorowanie transakcji serwera” na stronie 63

W sekcji tej omówiono monitor QoS umożliwiający sprawdzenie, czy strategie QoS działają zgodnie z oczekiwaniami.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

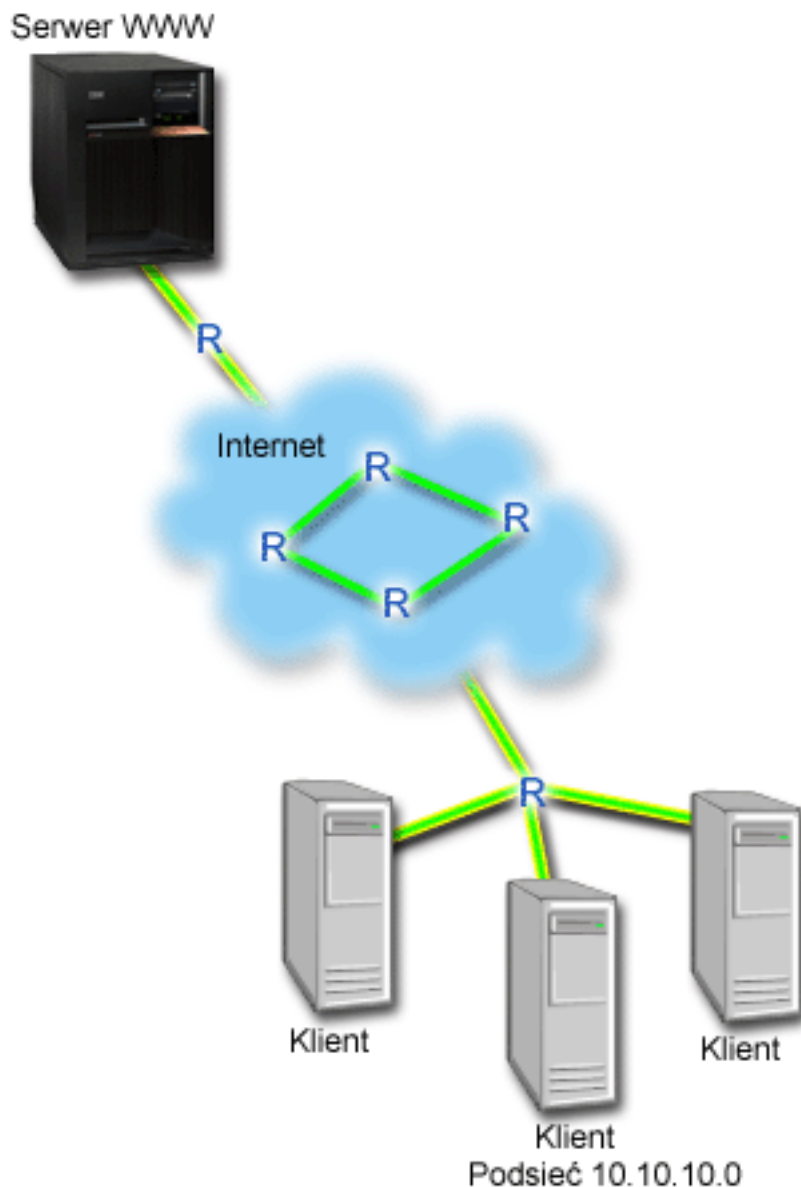
Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Scenariusz: ograniczanie ruchu danych do przeglądarki

Monitorowanie można wykorzystać do sterowania wydajnością ruchu danych w sieci. Aby ograniczyć lub zwiększyć wydajność aplikacji w danej sieci, należy skorzystać ze strategii usług DiffServ.

## Sytuacja

Pewna firma rejestruje wysoki poziom transmisji danych do przeglądarek grupy projektowej UCD występujący w piątce. Transmisje te kolidują z potrzebami działu księgowości, którego aplikacje właśnie w piątce wymagają wysokiej wydajności sieci. Należy więc ograniczyć ruch danych do grupy projektowej. Poniższy rysunek ilustruje konfigurację sieci w tym scenariuszu.



Rysunek 4. Serwer WWW ogranicza ruch danych do klienta

## Cele

Aby ograniczyć ruch danych opuszczających sieć, można utworzyć strategię usług DiffServ. Strategia tego typu powoduje podział transmisji danych na klasy. Każdej transmisji przypisywany jest punkt kodowy. Stanowi on informację dla routerów określającą sposób obsługi danej transmisji. W tym scenariuszu strategii można przypisać niski punkt kodowy, który odpowiada niskiemu priorytetowi transmisji danych do przeglądarki.

## Wymagania wstępne i założenia:

- Aby transmisje danych w ramach strategii rzeczywiście mogły uzyskiwać żądane priorytety, konieczne jest zawarcie z dostawcą ISP odpowiedniej umowy dotyczącej poziomu usług (SLA). Dzięki strategii QoS utworzonej na serwerze iSeries ruch danych zgodny z ustawieniami danej strategii może uzyskiwać w sieci priorytet. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może być podstawą do negocjowania z dostawcą pewnych poziomów usług i szybkości.

- Aby możliwe było korzystanie ze strategii usług DiffServ, wszystkie routery na ścieżce sieciowej muszą mieć możliwość obsługi usług DiffServ. Większość routerów ma możliwość obsługi usług DiffServ.

## Konfiguracja

Po spełnieniu wymagań wstępnych można przystąpić do tworzenia strategii usług DiffServ.

### Pojęcia pokrewne

“Umowa dotycząca poziomu usług” na stronie 49

Początek zmian Sekcja ta ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Utwórz strategię usług DiffServ.

1. W programie iSeries Navigator, rozwiń iSeries A → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem **Jakość usługi** i wybierz opcję **Konfiguracja** aby otworzyć okno interfejsu usług QoS.
3. W interfejsie QoS kliknij prawym przyciskiem myszy typ strategii DiffServ i wybierz opcję **Nowa strategia**, aby uruchomić kreatora.
4. Przeczytaj stronę powitania i kliknij przycisk **Dalej**, aby przejść do strony Nazwa.
5. W polu **Nazwa** wpisz UCD. Opcjonalnie można także wpisać opis ułatwiający zapamiętanie, w jakim celu utworzono daną strategię. Kliknij przycisk **Dalej**.
6. Na stronie Klienci wybierz opcję **Konkretny adres lub adresy** i kliknij przycisk **Nowy**, aby zdefiniować klienta.
7. W oknie Nowy klient wpisz następujące informacje i kliknij przycisk **OK**:
  - **Nazwa:** Klient UCD
  - **Adres i maska IP:** 10.10.10.0 / 24

Po kliknięciu przycisku OK nastąpi powrót do kreatora strategii. Jeśli wcześniej utworzono jakichś klientów, należy anulować ich wybór i wybrać tylko klientów odpowiednich dla danej strategii.
8. Na stronie Żądanie serwera danych, sprawdź czy wybrane są opcje **Dowolny token** i **Wszystkie priorytety** i kliknij przycisk **Dalej**.
9. Na stronie Aplikacje wybierz opcję **Określony port, zakres portów lub typ serwera** i kliknij przycisk **Nowy**.
10. W oknie Nowa aplikacja wpisz następujące informacje i kliknij przycisk **OK**, aby powrócić do kreatora:
  - **Nazwa:** HTTP
  - **Port:** 80
11. Na stronie Aplikacje wybierz opcję **Protokół** i sprawdź, czy wybrana jest wartość **TCP**. Kliknij przycisk **Dalej**.
12. Na stronie Lokalny adres IP sprawdź, czy wybrana jest opcja **Wszystkie adresy IP** i kliknij przycisk **Dalej**.
13. Na stronie Klasa usług DiffServ kliknij przycisk **Nowy**, aby zdefiniować parametry wydajności. Zostanie uruchomiony kreator nowej klasy usług.
14. Przeczytaj stronę powitania i kliknij przycisk **Dalej**.
15. Na stronie Nazwa wpisz Usługa\_UCD. Opcjonalnie można wpisać opis ułatwiający zapamiętanie przeznaczenia danej strategii. Kliknij przycisk **Dalej**.
16. Na stronie Typ usług wybierz opcję **Tylko wychodzące** i kliknij przycisk **Dalej**. Ta klasa usług będzie używana tylko dla strategii ruchu wychodzącego.

17. Na stronie Oznaczanie ruchu wychodzącego punktem kodowym DiffServ, wybierz opcję **Klasa 4** i kliknij przycisk **Dalej**. Charakterystyka w ramach segmentu sieci określa, jaką wydajność ruchu danych zapewnią routery i inne serwery w sieci. Przy wybieraniu wartości parametrów skorzystaj z pomocy.
18. Na stronie Wykonuj pomiar ruchu wychodzącego sprawdź, czy wybrano opcję **Tak** i kliknij przycisk **Dalej**.
19. Na stronie Sterowanie limitem szybkości ruchu wychodzącego wpisz następujące informacje i kliknij przycisk **Dalej**.
  - **Wielkość zasobnika tokenów:** 100 kilobitów
  - **Ograniczenie średniej szybkości:** 512 kilobitów na sekundę
  - **Ograniczenie szybkości szczytowej:** 1 megabit na sekundę
20. Na stronie Wychodzący ruch poza profilem wybierz opcję **Porzuć pakiety UDP lub zmniejsz okno zapełnienia TCP** i kliknij przycisk **Dalej**.
21. Przejrzyj informacje podsumowujące dotyczące klasy usług. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć klasę usług. Po kliknięciu przycisku Zakończ nastąpi powrót do kreatora strategii, w którym wybrana będzie utworzona klasa usług. Kliknij przycisk **Dalej**.
22. Na stronie Harmonogram wybierz opcję Aktywność w trakcie wybranego harmonogramu i kliknij przycisk **Nowy**.
23. W oknie Dodaj Nowy harmonogram wpisz następujące informacje i kliknij przycisk **OK**:
  - **Nazwa:** Harmonogram\_UCD
  - **Godzina:** Aktywność 24 godziny
  - **Dzień tygodnia:** Piątek
24. Kliknij przycisk **Dalej**, aby wyświetlić podsumowanie strategii. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**. Nowa strategia będzie wyświetlana na liście w prawym panelu okna Konfiguracja serwera usług QoS.

Zakończono proces konfigurowania strategii usług DiffServ na serwerze iSeries A. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: Uruchomienie lub aktualizacja serwera QoS

W oknie konfiguracji serwera usług QoS należy wybrać **Serwer** → **Uruchom** lub **Serwer** → **Aktualizuj**.

## Szczegóły scenariusza: Użycie monitora w celu sprawdzenia, czy strategia działa właściwie

Aby sprawdzić, czy strategia działa tak, jak powinna i jak została skonfigurowana, skorzystaj z monitora.

1. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Monitorowanie**. Zostanie wyświetlone okno Monitor QoS.
2. Wybierz folder typu strategii DiffServ. Zostaną wyświetlone wszystkie strategie DiffServ. Wybierz z listy **UCD**.  
Najbardziej interesujące są pola, których wartości wynikają z ruchu danych. Sprawdź pola: Bity łącznie, Bity w profilu i Pakiety w profilu. Na podstawie liczby bitów spoza profilu można stwierdzić, kiedy ruch danych powoduje przekroczenie wartości określonych w strategii. W strategii usług DiffServ liczba bitów spoza profilu (dla pakietów UDP) określa liczbę bitów odrzuconych. Dla protokołu TCP, liczba bitów spoza profilu określa liczbę bitów przekraczających szybkość zasobnika tokenów, które zostały wysłane do sieci. W przypadku pakietów TCP nigdy nie następuje odrzucanie bitów. Liczba pakietów w profilu określa liczbę pakietów sterowanych za pomocą danej strategii (od momentu wysłania pakietu do chwili obecnej).

Ważna jest także wartość wpisywana w polu Limit szybkości średniej. Jeśli szybkość napływających pakietów spowoduje przekroczenie tego limitu, kolejne pakiety będą odrzucane przez serwer. W konsekwencji nastąpi zwiększenie wartości w polu Bity spoza profilu. Oznacza to, że strategia działa tak, jak powinna. Sekcja "Monitorowanie QoS" na stronie 56 zawiera opis wszystkich pól w oknie monitora.

**Uwaga:** Należy pamiętać, że wyniki będą poprawne, tylko jeśli dana strategia jest aktywna. Trzeba to sprawdzić w harmonogramie określonym dla danej strategii.

## Szczegóły scenariusza: Zmiana właściwości (w razie potrzeby)

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby lepiej dostosować działanie strategii do potrzeb.

Można zmienić każdy z parametrów strategii, wykonując następujące czynności:

1. W oknie Konfiguracja serwera usług QoS wybierz folder **DiffServ**. Na liście w prawym panelu kliknij prawym przyciskiem myszy pozycję **UCD** i wybierz opcję **Właściwości**, aby edytować strategię. Zostanie wyświetlone okno Właściwości, które zawiera wartości sterujące ogólną strategią.
2. Zmień odpowiednie wartości.
3. W celu edytowania klasy usług wybierz folder **Klasy usług**. Na liście w prawym panelu prawym przyciskiem myszy kliknij pozycję **Usługa\_UCD** i wybierz opcję **Właściwości**, aby edytować klasę usług. Zostanie wyświetlone okno dialogowe QoS zawierające wartości sterujące sposobem zarządzania ruchem danych.
4. Zmień odpowiednie wartości.
5. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Aktualizuj** aby zaakceptować zmiany.

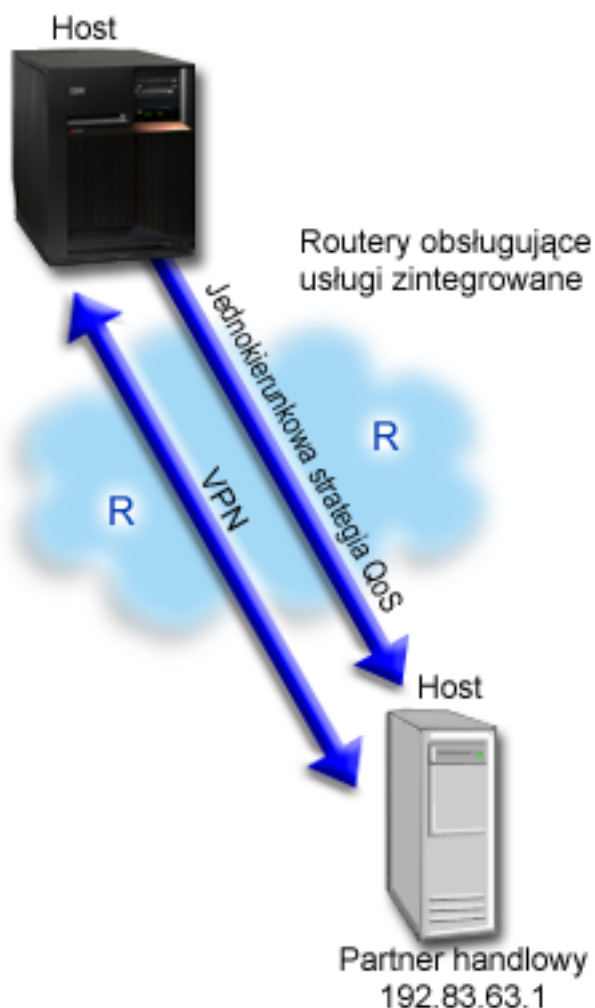
## Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług)

W sieci VPN także można tworzyć strategie QoS. Ilustruje to przedstawiony w sekcji przykład.

### Sytuacja

Pewna firma i jej partner handlowy znajdują się w tej samej sieci VPN. Zamierzamy połączyć funkcje sieci VPN i QoS, aby uzyskać ochronę i ustalony poziom transmisji danych o niewrażliwym znaczeniu dla działalności firmy. Dane konfiguracyjne QoS wysyłane są tylko w jednym kierunku. Dlatego w przypadku aplikacji audio/wideo należy zapewnić QoS po obu stronach połączenia.

Na rysunku pokazano serwery firmy i jej klienta realizujące połączenie w sieci VPN. Litera R oznacza routery znajdujące się na trasie połączenia i udostępniające usługi DiffServ. Jak widać, strategie QoS przesyłane są tylko w jednym kierunku.



Rysunek 5. Połączenie host-host w sieci VPN korzystające ze strategii usług DiffServ

## Cele

Aby zapewnić ochronę i priorytet ruchu danych, należy skorzystać z funkcji sieci VPN i funkcji QoS. W pierwszej kolejności trzeba skonfigurować połączenie host-host w sieci VPN. Po zapewnieniu ochrony połączenia można przystąpić do konfigurowania strategii QoS. Zastosujemy strategię usług DiffServ. Określa się w niej wysoką wartość punktu kodowego odpowiadającą przyspieszonemu przekazywaniu. W ten sposób zostanie ustalony wysoki priorytet danych o newralgicznym znaczeniu.

## Wymagania wstępne i założenia:

- Aby transmisje danych w ramach strategii rzeczywiście mogły uzyskiwać żądane priorytety, konieczne jest zawarcie z dostawcą ISP odpowiedniej umowy dotyczącej poziomu usług (SLA). Dzięki strategii QoS utworzonej na serwerze iSeries ruch danych zgodny z ustawieniami danej strategii może uzyskiwać w sieci priorytet. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może być podstawą do negocjowania z dostawcą pewnych poziomów usług i szybkości. Więcej informacji podano w opisie umów dotyczących poziomu usług, do których prowadzi stosowny odsyłacz.
- Aby możliwe było korzystanie ze strategii usług DiffServ, wszystkie routery na ścieżce sieciowej muszą mieć możliwość obsługi usług DiffServ. Większość routerów ma możliwość obsługi usług DiffServ.

## Konfiguracja

Po spełnieniu wymagań wstępnych można przystąpić do tworzenia strategii usług DiffServ.

### Pojęcia pokrewne

“Umowa dotycząca poziomu usług” na stronie 49

Początek zmian Sekcja ta ma na celu zwrócić uwagę na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Konfigurowanie połączenia host-host w sieci VPN

Podczas konfigurowania przydatny może być przykład opisany w sekcji Konfiguracja połączenia host-host w sieci VPN.

### Szczegóły scenariusza: Utwórz strategię usług DiffServ.

1. W programie iSeries Navigator, rozwiń iSeries A → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usługi** i wybierz opcję **Konfiguracja**, aby otworzyć okno Konfiguracja serwera usług QoS.
3. W oknie Konfiguracja serwera usług QoS kliknij prawym przyciskiem myszy typ strategii DiffServ i wybierz opcję **Nowa strategia**, aby uruchomić kreatora.
4. Przeczytaj stronę powitania i kliknij przycisk **Dalej**, aby przejść do strony **Nazwa**.
5. W polu **Nazwa** wpisz **VPN** i kliknij przycisk **Dalej**. Opcjonalnie można wpisać opis ułatwiający zapamiętanie przeznaczenia danej strategii.
6. Na stronie Klienci wybierz opcję **Konkretny adres lub adresy** i kliknij przycisk **Nowy**, aby zdefiniować klienta.
7. W oknie dialogowym Nowy klient wpisz następujące informacje:
  - **Nazwa:** Klient\_VPN
  - **Adres IP:** 192.83.63.1
  - Kliknij przycisk **OK**, aby utworzyć klienta i powrócić do kreatora usług DiffServ.
8. Po kliknięciu przycisku OK nastąpi powrót do kreatora strategii. Jeśli wcześniej utworzono jakichś klientów, należy anulować ich wybór i wybrać tylko klientów odpowiednich dla danej strategii.
9. Na stronie Żądanie serwera danych, sprawdź czy wybrane są opcje **Dowolny token** i **Wszystkie priorytety**.
10. Na stronie Aplikacje sprawdź, czy wybrane są opcje **Wszystkie porty** i **Wszystkie**.
11. Kliknij przycisk **Dalej**.
12. Na stronie Lokalny adres IP zaakceptuj wartość domyślną i kliknij przycisk **Dalej**.
13. Na stronie Klasa usług DiffServ kliknij przycisk **Nowy**, aby zdefiniować parametry wydajności. Zostanie uruchomiony kreator nowej klasy usług.
14. Przeczytaj stronę powitania i kliknij przycisk **Dalej**.
15. Na stronie Nazwa wpisz **EF\_VPN**.
16. Na stronie Typ usług wybierz opcję **Tylko wychodzące** i kliknij przycisk **Dalej**. Ta klasa usług będzie używana tylko dla strategii ruchu wychodzącego.
17. Na stronie Oznaczanie ruchu wychodzącego punktem kodowym DiffServ wybierz opcję **Klasa 3**. Charakterystyka w ramach segmentu sieci określa jaką wydajność ruchu danych zapewnią routery i inne serwery w sieci. Przy wybieraniu wartości parametrów skorzystaj z pomocy.
18. Na stronie Wykonuj pomiar ruchu wychodzącego sprawdź, czy wybrano opcję **Tak** i kliknij przycisk **Dalej**.



18. Na stronie Sterowanie limitem szybkości ruchu wychodzącego wpisz następujące informacje i kliknij przycisk **Dalej**.
  - **Wielkość zasobnika tokenów:** 100 kilobitów
  - **Ograniczenie średniej szybkości:** 64 kilobity na sekundę
  - **Ograniczenie szybkości szczytowej:** Brak ograniczeń
19. Na stronie Wychodzący ruch poza profilem wybierz opcję **Porzuć pakiety UDP lub zmniejsz okno zapełnienia TCP** i kliknij przycisk **Dalej**.
20. Przejrzyj informacje podsumowujące klasy usług i kliknij przycisk **Zakończ**, aby powrócić do kreatora strategii.
21. Należy się upewnić, czy na stronie Klasa usług DiffServ wybrana jest pozycja **EF\_VPN** i kliknąć przycisk **Dalej**.
22. Na stronie Harmonogram wybierz opcję **Aktywność w trakcie wybranego harmonogramu** i kliknij przycisk **Nowy**.
23. W oknie Dodaj Nowy harmonogram wpisz następujące informacje i kliknij przycisk **OK**:
  - **Nazwa:** PierwszaZmiana
  - **Godzina:** wybierz opcję Aktywność o określonych godzinach i dodaj godziny od 9:00 do 17:00.
  - **Dzień tygodnia:** wybierz opcję Aktywność w określonych dniach i dni od poniedziałku do piątku.
24. Na stronie Harmonogram kliknij przycisk **Dalej**.
25. Przejrzyj informacje podsumowujące. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. Lista wszystkich strategii utworzonych na serwerze wyświetlona jest w oknie Konfiguracja serwera usług QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii usług DiffServ na serwerze iSeries A. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: Uruchomienie lub aktualizacja serwera QoS

W oknie konfiguracji serwera usług QoS należy wybrać **Serwer** → **Uruchom** lub **Serwer** → **Aktualizuj**.

## Szczegóły scenariusza: Użycie monitora w celu sprawdzenia, czy strategia działa właściwie

Aby sprawdzić, czy strategia działa tak, jak powinna i jak została skonfigurowana, skorzystaj z monitora.

1. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Monitorowanie**. Zostanie wyświetlone okno Monitor QoS.
2. Wybierz typ strategii DiffServ. Zostaną wyświetlone wszystkie strategie DiffServ.

Podobnie jak w przykładzie 1, najbardziej interesujące są pola, których wartości wynikają z ruchu danych. Są to pola zawierające łączną liczbę bitów, liczbę bitów w profilu i liczbę pakietów spoza profilu. Na podstawie liczby bitów spoza profilu można stwierdzić, kiedy ruch danych powoduje przekroczenie wartości określonych w strategii. Liczba pakietów w profilu określa liczbę pakietów sterowanych za pomocą danej strategii. Bardzo ważne są wartości podane przez administratora w polu Limit szybkości średniej. Kiedy pakiety TCP przekroczą ten limit, będą wysyłane do sieci do momentu gdy nastąpi zmniejszenie okna zapełnienia TCP umożliwiające kolejnowanie pakietów spoza profilu. W konsekwencji nastąpi zwiększenie wartości w polu Bity spoza profilu. Różnica między strategią tu opisywaną a strategią ze scenariusza dotyczącego ograniczania ruchu danych do przeglądarki polega na tym, że pakiety są chronione za pomocą protokołu VPN. Pokazano więc, że funkcji QoS można używać w sieci VPN. Opis wszystkich pól w oknie monitora zawiera sekcja "Monitorowanie QoS" na stronie 56.

**Uwaga:** Należy pamiętać, że wyniki będą poprawne, tylko jeśli dana strategia jest aktywna. Trzeba to sprawdzić w harmonogramie określonym dla danej strategii.

## Szczegóły scenariusza: Zmiana właściwości (w razie potrzeby)

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby lepiej dostosować działanie strategii do potrzeb.

W celu edytowania klasy usług po jej utworzeniu należy wykonać następujące czynności:

1. W oknie Konfiguracja serwera usług QoS wybierz folder **DiffServ**. Na liście w prawym panelu kliknij prawym przyciskiem myszy pozycję **VPN** i wybierz opcję **Właściwości**, aby edytować strategię. Zostanie wyświetlone okno dialogowe Właściwości, które zawiera wartości sterujące ogólną strategią.
2. Zmień odpowiednie wartości.
3. W celu edytowania klasy usług wybierz folder **Klasy usług**. Na liście w prawym panelu prawym przyciskiem myszy kliknij pozycję **EF\_VPN** i wybierz opcję **Właściwości**, aby edytować klasę usług. Zostanie wyświetlone okno dialogowe zawierające wartości sterujące sposobem zarządzania ruchem danych.
4. Zmień odpowiednie wartości.
5. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Aktualizuj** aby zaakceptować zmiany.

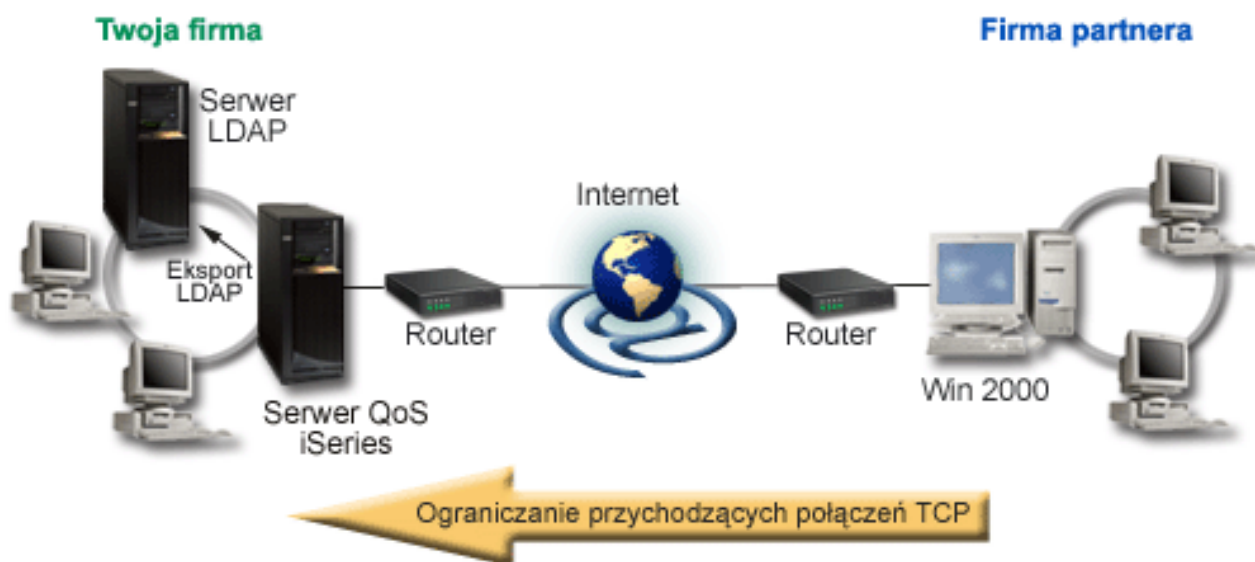
## Scenariusz: ograniczanie połączeń przychodzących

Jeśli chce się sterować połączeniami przychodzącymi do serwera, należy skorzystać ze strategii połączeń przychodzących.

### Sytuacja

Zasoby serwera WWW są przeciążone zgłoszeniami klientów napływającymi do sieci. Należy zmniejszyć szybkość ruchu danych HTTP napływających do serwera WWW na interfejsie lokalnym 192.168.1.1. QoS umożliwia ograniczenie liczby akceptowanych połączeń przychodzących na podstawie atrybutów połączenia (na przykład adresu IP). W tym celu można zastosować strategię akceptowania ruchu przychodzącego.

Rysunek przedstawia Twoją firmę i firmę klienta. Strategia tu prezentowana może sterować przepływem danych tylko w jednym kierunku.



Rysunek 6. Ograniczanie przychodzących połączeń TCP

przez serwer

### Cele

Aby skonfigurować strategię ruchu przychodzącego, należy określić, czy ograniczenia transmisji mają dotyczyć interfejsu lokalnego czy określonej aplikacji. Można także zastosować ograniczenia dla konkretnego klienta. W rozważanym tu przypadku chcemy utworzyć strategię ograniczającą połączenia napływające od klienta Firma\_partnera do portu 80 (protokół HTTP) na interfejsie lokalnym 192.168.1.1.

## Konfiguracja

Następujące tematy opisują tworzenie strategii akceptowania ruchu przychodzącego.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Tworzenie strategii akceptowania ruchu przychodzącego

1. W programie iSeries Navigator, rozwiń iSeries A → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usługi** i wybierz opcję **Konfiguracja**, aby otworzyć okno Konfiguracja serwera usług QoS.
3. W oknie Konfiguracja serwera usług QoS kliknij prawym przyciskiem myszy pozycję **Strategie połączeń przychodzących** i wybierz opcję **Nowa strategia**, aby uruchomić kreatora.
4. Przeczytaj stronę powitania i kliknij przycisk **Dalej**.
5. W polu **Nazwa** wpisz **Ogranicz\_firmę\_part** i kliknij przycisk **Dalej**. Opcjonalnie można wpisać opis ułatwiający zapamiętanie przeznaczenia danej strategii.
6. Na stronie Klienci wybierz opcję **Konkretny adres lub adresy** i kliknij przycisk **Nowy**, aby zdefiniować klienta.
7. W oknie dialogowym Nowy klient wpisz następujące informacje:
  - **Nazwa:** Firma\_part
  - **Zakres adresów IP:** 10.1.1.1 do 10.1.1.10
  - Kliknij przycisk **OK**, aby utworzyć klienta i powrócić do kreatora strategii.

Po kliknięciu przycisku OK nastąpi powrót do kreatora strategii. Jeśli wcześniej utworzono jakichś klientów, należy anulować ich wybór i wybrać tylko klientów odpowiednich dla danej strategii.
8. Na stronie URI sprawdź, czy wybrana jest opcja **Dowolny URI** i kliknij przycisk **Dalej**.
9. Na stronie Aplikacje wybierz opcję **Określony port, zakres portów lub typ serwera** i kliknij przycisk **Nowy**.
10. W oknie Nowa aplikacja wpisz następujące informacje i kliknij przycisk **OK**, aby powrócić do kreatora:
  - **Nazwa:** HTTP
  - **Port:** 80
11. Kliknij przycisk **Dalej**, aby przejść do strony Punkt kodowy.
12. Na stronie Punkt kodowy sprawdź, czy wybrana jest opcja **Wszystkie punkty kodowe** i kliknij przycisk **Dalej**.
13. Na stronie Lokalny adres IP wybierz opcję **Adres IP** oraz interfejs, na który napływają zgłoszenia do systemu lokalnego. W tym przykładzie należy użyć interfejsu 192.168.1.1.
14. Na stronie Klasa usług kliknij przycisk **Nowy**, aby zdefiniować parametry wydajności. Zostanie uruchomiony kreator nowej klasy usług.
15. Przeczytaj stronę powitania i kliknij przycisk **Dalej**.
16. Na stronie Nazwa wpisz **przychodzące** i kliknij przycisk **Dalej**. Opcjonalnie można dodać opis ułatwiający zapamiętanie przeznaczenia danej klasy usług.
17. Na stronie Typ usług wybierz opcję **Tylko przychodzące**. Ta klasa usług będzie używana tylko dla strategii ruchu przychodzącego.
18. Na stronie Limity ruchu przychodzącego wpisz następujące informacje i kliknij przycisk **Dalej**:
  - Średnia szybkość połączenia: 50 na sekundę
  - Limit porcji dla połączenia: 50 połączeń
  - Priorytet: Średni
19. Kliknij przycisk **Zakończ**, aby powrócić do kreatora strategii.
20. Na stronie Klasa usług sprawdź, czy nowo utworzona klasa usług jest wybrana i kliknij przycisk **Dalej**.
21. Na stronie Harmonogram wybierz opcję **Aktywność w trakcie wybranego harmonogramu** i kliknij przycisk **Nowy**.
22. W oknie Nowy harmonogram wpisz następujące informacje i kliknij przycisk **OK**:

- Nazwa: PierwszaZmiana
- Godzina: wybierz opcję Aktywność o określonych godzinach i dodaj godziny od 9:00 do 17:00.
- Dzień tygodnia: wybierz opcję Aktywność w określonych dniach i dni od poniedziałku do piątku.

23. Na stronie Harmonogramy kliknij przycisk **Dalej**.

24. Przejrzyj informacje podsumowujące. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. Lista wszystkich strategii utworzonych na serwerze wyświetlona jest w oknie Konfiguracja serwera usług QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii akceptowania ruchu przychodzącego na serwerze iSeries A. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: Uruchomienie lub aktualizacja serwera QoS

W oknie konfiguracji serwera usług QoS należy wybrać **Serwer** → **Uruchom** lub **Serwer** → **Aktualizuj**.

## Szczegóły scenariusza: Użycie monitora w celu sprawdzenia, czy strategia działa właściwie

Aby sprawdzić, czy strategia działa tak, jak powinna i jak została skonfigurowana, skorzystaj z monitora.

1. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Monitorowanie**. Zostanie wyświetlone okno Monitor QoS.

2. Wybierz typ strategii Akceptacja ruchu przychodzącego. Zostaną wyświetlone wszystkie strategie akceptowania ruchu przychodzącego. Wybierz z listy pozycję **Ogranicz\_firmę\_part**.

Sprawdź wszystkie pola, których wartości wynikają z ruchu danych, na przykład Żądania zaakceptowane, Żądania odrzucone, Szybkość połączeń. Na podstawie liczby żądań odrzuconych można stwierdzić, kiedy ruch danych powoduje przekroczenie wartości określonych w strategii. Pole Żądania zaakceptowane określa liczbę bitów sterowanych za pomocą danej strategii (od momentu wysłania pakietu do chwili obecnej).

Ważna jest także wartość wpisywana w polu Szybkość średnia połączeń. Jeśli szybkość napływających pakietów spowoduje przekroczenie tego limitu, kolejne pakiety będą odrzucane przez serwer. W konsekwencji nastąpi zwiększenie wartości w polu Żądania odrzucone. Oznacza to, że strategia działa tak, jak powinna. Sekcja "Monitorowanie QoS" na stronie 56 zawiera opis wszystkich pól w oknie monitora.

**Uwaga:** Należy pamiętać, że wyniki będą poprawne, tylko jeśli dana strategia jest aktywna. Trzeba to sprawdzić w harmonogramie określonym dla danej strategii.

## Szczegóły scenariusza: Zmiana właściwości (w razie potrzeby)

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby lepiej dostosować działanie strategii do potrzeb.

1. W oknie Konfiguracja serwera usług QoS wybierz folder **Akceptowanie ruchu przychodzącego**. Na liście w prawym panelu kliknij prawym przyciskiem myszy pozycję **Ogranicz\_firmę\_part** i wybierz opcję **Właściwości**, aby edytować strategię. Zostanie wyświetlone okno Właściwości, które zawiera wartości sterujące ogólną strategią.

2. Zmień odpowiednie wartości.

3. W celu edytowania klasy usług wybierz folder **Klasy usług**. Na liście w prawym panelu prawym przyciskiem myszy kliknij pozycję **przychodzące** i wybierz opcję **Właściwości**, aby edytować klasę usług. Zostanie wyświetlone okno dialogowe QoS zawierające wartości sterujące sposobem zarządzania ruchem danych.

4. Zmień odpowiednie wartości.

5. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Aktualizuj** aby zaakceptować zmiany.

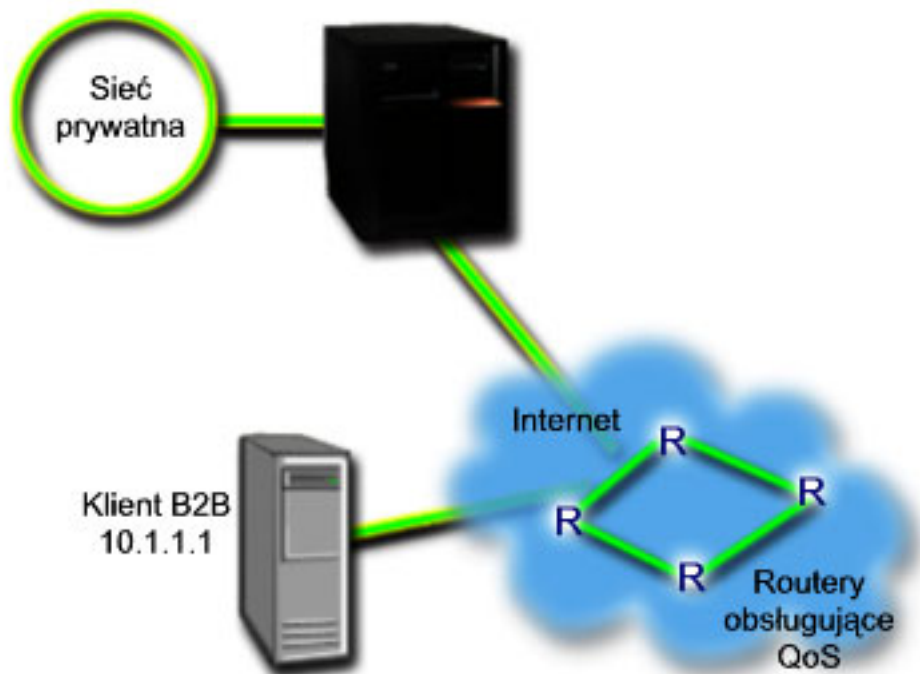
## Scenariusz: przewidywalny ruch danych firma-firma (B2B)

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

## Sytuacja

Dział sprzedaży zgłasza problemy związane z niewystarczającą szybkością transmisji danych. Serwer iSeries należący do firmy działa w środowisku typu firma-firma (B2B), wymagającym przewidywalnej obsługi usług biznesowych. Należy zapewnić partnerom handlowym określoną szybkość obsługi transakcji. W tym celu aplikacja obsługująca zamówienia uruchomiona w dziale sprzedaży powinna otrzymać wyższą jakość usług (QoS) w godzinach największego ruchu (między 10:00 i 16:00).

Na poniższym rysunku dział sprzedaży znajduje się w obrębie sieci prywatnej. Wzdłuż ścieżki sieciowej pomiędzy klientami B2B znajdują się routery, aktywowane przez protokół RSVP. Oznaczono je literą R.



Rysunek 7. Strategia usług zintegrowanych dla partnera handlowego korzystająca z routerów obsługujących protokół RSVP

## Cele

Usługa sterowanego obciążenia dotyczy aplikacji szczególnie wrażliwych na przeciążenie sieci, dopuszczających jednak niewielkie utraty pakietów i niewielkie opóźnienia. Gdy aplikacja korzysta z usługi sterowanego obciążenia, jej wydajność nie spadnie po zwiększeniu się obciążenia sieci. Zostanie jej zapewniony poziom transmisji taki, jak w normalnych warunkach przy niewielkim obciążeniu sieci. Ponieważ rozważana tu aplikacja toleruje niewielkie opóźnienia, można skorzystać ze strategii usług zintegrowanych (IntServ) i usługi sterowanego obciążenia.

Stosowanie strategii usług zintegrowanych wymaga, aby routery znajdujące się na trasie transmisji obsługiwały protokół RSVP.

## Wymagania wstępne i założenia:

Strategia usług zintegrowanych jest zaawansowaną strategią wymagającą znacznych zasobów. Stosowanie strategii usług zintegrowanych możliwe jest po spełnieniu następujących wymagań wstępnych:

- Aplikacje obsługujące protokół RSVP

Na serwerze nie ma takich aplikacji, trzeba je więc utworzyć samodzielnie. W tym celu można skorzystać z funkcji API RAPI (Resource Reservation Setup Protocol), funkcji API gniazd QoS qtoq, lub funkcji API usług zintegrowanych.

- **Routery i serwery na ścieżce sieciowej obsługujące protokół RSVP**

QoS jest rozwiązaniem dotyczącym całej sieci. Nawet jeśli nie ma pewności, że wszystkie urządzenia sieciowe obsługują protokół RSVP, można utworzyć strategię usług zintegrowanych i zastosować oznakowanie w celu nadania jej pewnego priorytetu; priorytet ten jednak nie może być zagwarantowany.

- **Umowa dotycząca poziomu usług**

Aby transmisje danych w ramach strategii rzeczywiście mogły uzyskiwać żądane priorytety, konieczne jest zawarcie z dostawcą ISP odpowiedniej umowy dotyczącej poziomu usług (SLA). Dzięki strategii QoS utworzonej na serwerze iSeries ruch danych zgodny z ustawieniami danej strategii może uzyskiwać w sieci priorytet. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może być podstawą do negocjowania z dostawcą pewnych poziomów usług i szybkości. Więcej informacji podano w opisie umów dotyczących poziomu usług, do których prowadzi stosowny odsyłacz.

**Uwaga:** Jeśli ruch danych odbywa się tylko w obrębie sieci prywatnej, umowa ta nie jest potrzebna.

## Konfiguracja

Po spełnieniu wymagań wstępnych można przystąpić do tworzenia strategii usług zintegrowanych.

### Pojęcia pokrewne

“Rodzaje usług zintegrowanych” na stronie 9

Istnieją dwa rodzaje usług zintegrowanych: usługi sterowanego obciążenia i usługi gwarantowane.

“Usługa zintegrowana” na stronie 6

Jest to drugi typ strategii połączeń wychodzących. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API dotyczących QoS.

“Funkcje API QoS” na stronie 17

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSerVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

“Umowa dotycząca poziomu usług” na stronie 49

Początek zmian Sekcja ta ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Tworzenie strategii usług zintegrowanych

1. W programie iSeries Navigator, rozwiń iSeries A → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usługi** i wybierz opcję **Konfiguracja**, aby otworzyć okno Konfiguracja serwera usług QoS.
3. W oknie Konfiguracja serwera usług QoS kliknij prawym przyciskiem myszy typ strategii IntServ i wybierz opcję **Nowa strategia**, aby uruchomić kreatora.
4. Przeczytaj stronę powitania i kliknij przycisk **Dalej**, aby przejść do strony **Nazwa**.
5. W polu **Nazwa** wpisz **B2B\_CL** i kliknij przycisk **Dalej**. Opcjonalnie można wpisać opis ułatwiający zapamiętanie przeznaczenia danej strategii.
6. Na stronie Klienci wybierz opcję **Konkretny adres lub adresy** i kliknij przycisk **Nowy**, aby zdefiniować klienta.
7. W oknie dialogowym Nowy klient wpisz następujące informacje:
  - **Nazwa:** Klient\_CL
  - **Adres IP:** 10.1.1.1

- Kliknij przycisk **OK**, aby utworzyć klienta i powrócić do kreatora strategii.

Po kliknięciu przycisku OK nastąpi powrót do kreatora strategii. Jeśli wcześniej utworzono jakichś klientów, należy anulować ich wybór i wybrać tylko klientów odpowiednich dla danej strategii.

8. W oknie Nowa aplikacja wpisz następujące informacje i kliknij przycisk **OK**, aby powrócić do kreatora:
  - **Nazwa:** apl\_biznes
  - **Zakres portów:** 7000-8000
9. Na stronie Aplikacje wybierz opcję **Protokół** i sprawdź, czy wybrana jest wartość **TCP**. Kliknij przycisk **Dalej**.

**Uwaga:** Aplikacja wybrana do strategii usług zintegrowanych musi być napisana tak, aby mogła korzystać z funkcji API RAPI lub funkcji API gniazd qtoq. Funkcje te wraz z protokołem RSVP (Resource Reservation Protocol) umożliwiają rezerwację przepustowości sieci w ramach usług zintegrowanych. Jeśli wspomniane funkcje API nie będą wykorzystywane, aplikacja nie uzyska priorytetu ani usługi gwarantowanej. Trzeba także pamiętać, że ta strategia umożliwia aplikacjom uzyskanie priorytetu w sieci, ale go nie gwarantuje. Aby rezerwacja była zagwarantowana, konieczna jest obsługa protokołu RSVP przez wszystkie routery i serwery na ścieżce ruchu danych. Rezerwacja na całej trasie jest zależna od udziału w sieci.

10. Na stronie Lokalny adres IP zaakceptuj wartość domyślną i kliknij przycisk **Dalej**.
11. Na stronie Typ zintegrowanych usług wybierz opcję **Sterowane przeciążenie** i kliknij przycisk **Dalej**.
12. Na stronie Znakowanie zintegrowanych usług wybierz opcję **Nie, nie przypisuj zachowania przy przeskoku** i kliknij przycisk **Dalej**.
13. Na stronie Ograniczenia wydajności zintegrowanych usług wpisz następujące informacje i kliknij przycisk **Dalej**:
  - **Maksymalna liczba przepływów:** 5
  - **Ograniczenia szybkości tokenu (R):** Brak ograniczeń
  - **Wielkość zasobnika tokenów:** 100 kilobitów
  - **Ograniczenia szybkości tokenu (R):** 25 megabitów na sekundę
14. Na stronie Harmonogram wybierz opcję **Aktywność w trakcie wybranego harmonogramu** i kliknij przycisk **Nowy**.
15. Na stronie Nowy harmonogram wpisz następujące informacje i kliknij przycisk **OK**:
  - **Nazwa:** godziny\_szczytu
  - **Godzina:** wybierz opcję Aktywność w określonych godzinach i dodaj godziny od 10:00 do 16:00.
  - **Dzień tygodnia:** wybierz opcję Aktywność w określonych dniach i dni od poniedziałku do piątku.
16. Na stronie Harmonogramy kliknij przycisk **Dalej**.
17. Przejrzyj informacje podsumowujące. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. Lista wszystkich strategii utworzonych na serwerze wyświetlona jest w głównym oknie Konfiguracja serwera usług QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii usług zintegrowanych na serwerze iSeries iSeries A. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: Uruchomienie lub aktualizacja serwera QoS

W oknie konfiguracji serwera usług QoS należy wybrać **Serwer** → **Uruchom** lub **Serwer** → **Aktualizuj**.

## Szczegóły scenariusza: Użycie monitora w celu sprawdzenia, czy strategia działa właściwie

Aby sprawdzić, czy strategia działa tak, jak powinna i jak została skonfigurowana, skorzystaj z monitora.

1. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Monitorowanie**. Zostanie wyświetlone okno Monitor QoS.
2. Wybierz typ strategii IntServ. Zostaną wyświetlone wszystkie strategie IntServ.

Najbardziej interesujące są pola, których wartości wynikają z ruchu danych. Sprawdź pola zawierające łączną liczbę bitów, liczbę bitów w profilu i liczbę pakietów w profilu. Liczba bitów spoza profilu wskazuje, że pewne dane są wstrzymywane lub odrzucane w celu spełnienia wymagań określonych w strategii usług zintegrowanych. Pełny opis pól wyświetlanych w oknie monitora zawiera sekcja “Monitorowanie QoS” na stronie 56.

**Uwaga:** Należy pamiętać, że wyniki będą poprawne, tylko jeśli dana strategia jest aktywna. Trzeba to sprawdzić w harmonogramie określonym dla danej strategii. Ponadto, monitor może pokazać informacje dotyczące strategii IntServ dopiero po uruchomieniu aplikacji. Przed monitorowaniem muszą zostać ustanowione rezerwacje protokołu RSVP.

## Szczegóły scenariusza: Zmiana właściwości (w razie potrzeby)

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii, aby lepiej dostosować działanie strategii do potrzeb.

Po utworzeniu strategii można zmienić wartości określone wcześniej w trakcie pracy z kreatorem.

1. W oknie Konfiguracja serwera usług QoS wybierz folder **IntServ**. Na liście w prawym panelu kliknij prawym przyciskiem myszy pozycję **B2B\_CL** i wybierz opcję **Właściwości**, aby edytować strategię. Zostanie wyświetlone okno Właściwości, które zawiera wartości sterujące ogólną strategią.
2. Zmień odpowiednie wartości.
3. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Aktualizuj** aby zaakceptować zmiany.

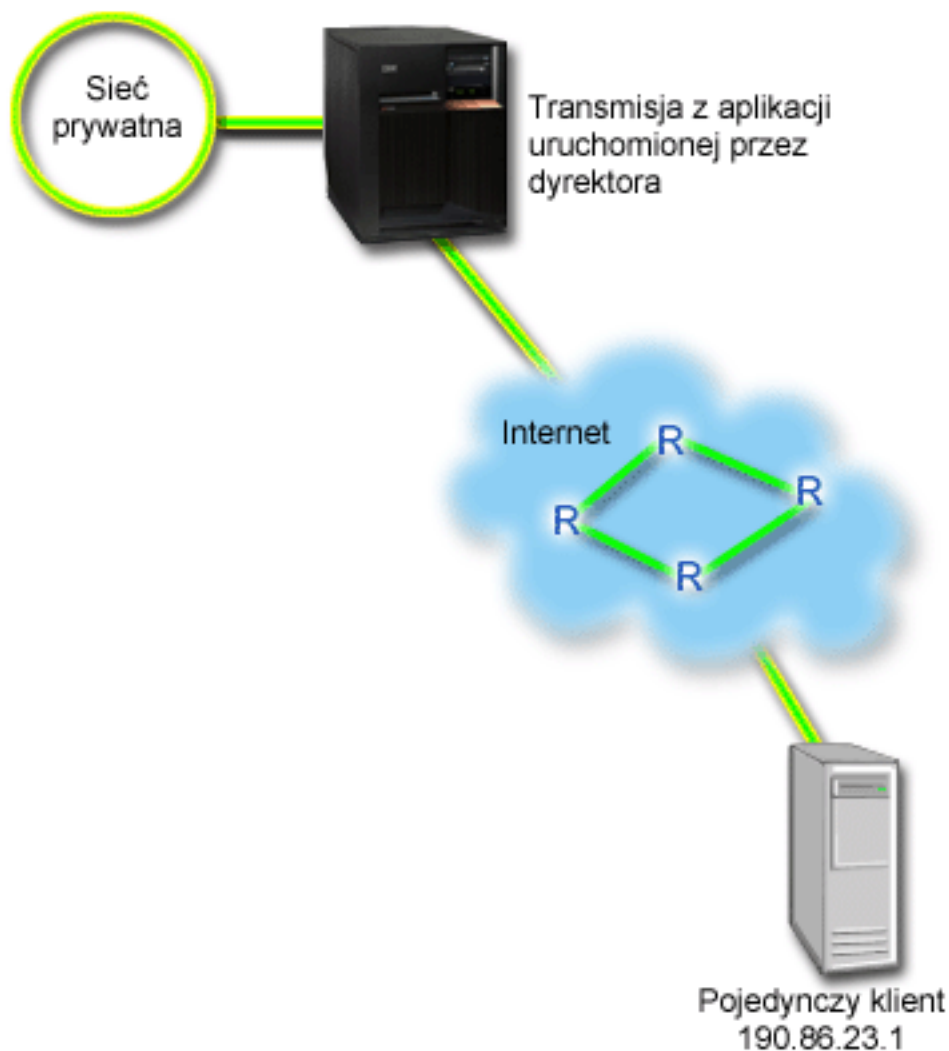
## Scenariusz: dedykowane dostarczanie (telefonía IP)

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa rodzaje takich strategii: usługi gwarantowane i usługi sterowanego obciążenia. W tym przykładzie wykorzystano usługi gwarantowane.

### Sytuacja

Dyrektor generalny firmy zamierza przeprowadzić transmisję na żywo w godzinach między 13:00 a 14:00 do klienta znajdującego się w odległej części kraju. Trzeba zagwarantować uzyskanie odpowiedniej przepustowości przez telefonię IP, dzięki czemu nie wystąpią przerwy w transmisji. W prezentowanym tu scenariuszu aplikacja obsługująca transmisję działa na serwerze.





Rysunek 8. Prezentacja dyrektora generalnego przesyłana do klienta, zagwarantowana przez strategię usług zintegrowanych.

## Cele

Ponieważ aplikacja, której używa dyrektor generalny, wymaga ciągłej transmisji, należy skorzystać ze strategii usług zintegrowanych. Usługa gwarantowana określa maksymalne opóźnienie, z jakim mogą być przesyłane pakiety umieszczone w kolejce.

## Wymagania wstępne i założenia:

Strategia usług zintegrowanych jest zaawansowaną strategią wymagającą znacznych zasobów. Stosowanie strategii usług zintegrowanych możliwe jest po spełnieniu następujących wymagań wstępnych:

- **Istnieją aplikacje obsługujące protokół RSVP**

Na serwerze nie ma takich aplikacji, trzeba je więc utworzyć samodzielnie. W tym celu można skorzystać z funkcji API RAPI lub funkcji API gniazd QoS qtoq. Więcej informacji na ten temat zawiera sekcja "Funkcje API QoS" na stronie 17 w części o funkcjach API dotyczących usług zintegrowanych.

- **Routery i serwery na ścieżce sieciowej obsługujące protokół RSVP**

QoS jest rozwiązaniem dotyczącym całej sieci. Nawet jeśli nie ma pewności, że wszystkie urządzenia sieciowe obsługują protokół RSVP, można utworzyć strategię usług zintegrowanych i zastosować oznakowanie w celu nadania jej pewnego priorytetu; priorytet ten jednak nie może być zagwarantowany.

- **Umowa dotycząca poziomu usług**

Aby transmisje danych w ramach strategii rzeczywiście mogły uzyskiwać żądane priorytety, konieczne jest zawarcie z dostawcą ISP odpowiedniej umowy dotyczącej poziomu usług (SLA). Dzięki strategii QoS utworzonej na serwerze iSeries ruch danych zgodny z ustawieniami danej strategii może uzyskiwać w sieci priorytet. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może być podstawą do negocjowania z dostawcą pewnych poziomów usług i szybkości. Więcej informacji podano w opisie umów dotyczących poziomu usług, do których prowadzi stosowny odsyłacz.

## Konfiguracja

Po spełnieniu wymagań wstępnych można przystąpić do tworzenia strategii usług zintegrowanych.

### Pojęcia pokrewne

“Rodzaje usług zintegrowanych” na stronie 9

Istnieją dwa rodzaje usług zintegrowanych: usługi sterowanego obciążenia i usługi gwarantowane.

“Usługa zintegrowana” na stronie 6

Jest to drugi typ strategii połączeń wychodzących. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API dotyczących QoS.

“Umowa dotycząca poziomu usług” na stronie 49

Początek zmian Sekcja ta ma na celu zwrócić uwagę na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Tworzenie strategii usług zintegrowanych

1. W programie iSeries Navigator, rozwiń iSeries A → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usługi** i wybierz opcję **Konfiguracja**, aby otworzyć okno Konfiguracja serwera usług QoS.
3. W oknie Konfiguracja serwera usług QoS kliknij prawym przyciskiem myszy typ strategii IntServ i wybierz opcję **Nowa strategia**, aby uruchomić kreatora.
4. Przeczytaj stronę powitania i kliknij przycisk **Dalej**, aby przejść do strony **Nazwa**.
5. W polu **Nazwa** wpisz **gwarantowana\_dyrektor** i kliknij przycisk **Dalej**. Opcjonalnie można wpisać opis ułatwiający zapamiętanie przeznaczenia danej strategii.
6. Na stronie Klienci wybierz opcję **Konkretny adres lub adresy** i kliknij przycisk **Nowy**, aby zdefiniować klienta.
7. W oknie dialogowym Nowy klient wpisz następujące informacje:
  - **Nazwa:** Oddział1
  - **Adres IP:** 190.86.23.1
  - Kliknij przycisk **OK**, aby utworzyć klienta i powrócić do kreatora usług zintegrowanych.

Po kliknięciu przycisku OK nastąpi powrót do kreatora strategii. Jeśli wcześniej utworzono jakichś klientów, należy anulować ich wybór i wybrać tylko klientów odpowiednich dla danej strategii. Na stronie Aplikacje wybierz opcję **Określony port, zakres portów lub typ serwera** i kliknij przycisk **Nowy**.

8. W oknie Nowa aplikacja wpisz następujące informacje i kliknij przycisk **OK**, aby powrócić do kreatora:
  - **Nazwa:** telefonia IP
  - **Port:** 2427
9. Na stronie Aplikacje wybierz opcję **Protokół** i sprawdź, czy wybrana jest wartość **TCP**. Kliknij przycisk **Dalej**.

**Uwaga:** Aplikacja wybrana do strategii usług zintegrowanych musi być napisana tak, aby mogła korzystać z funkcji API RAPI lub funkcji API gniazd qtoq. Funkcje te wraz z protokołem RSVP (Resource Reservation Protocol) umożliwiają rezerwację przepustowości sieci w ramach usług zintegrowanych. Jeśli wspomniane funkcje API nie będą wykorzystywane, aplikacja nie uzyska priorytetu ani usługi gwarantowanej. Trzeba także pamiętać, że ta strategia umożliwia aplikacjom uzyskanie priorytetu w sieci, ale go nie gwarantuje. Aby rezerwacja była zagwarantowana, konieczna jest obsługa protokołu RSVP przez wszystkie routery i serwery na ścieżce ruchu danych. Rezerwacja na całej trasie jest zależna od udziału w sieci.

10. Na stronie Lokalny adres IP zaakceptuj wartość domyślną **Wszystkie adresy IP**.
11. Na stronie Typ zintegrowanych usług wybierz opcję **Gwarantowane** i kliknij przycisk **Dalej**.
12. Na stronie Znakowanie zintegrowanych usług wybierz opcję **Nie, nie przypisuj zachowania przy przeskoku** i kliknij przycisk **Dalej**.
13. Na stronie Ograniczenia wydajności zintegrowanych usług wpisz następujące informacje i kliknij przycisk **Dalej**:
  - **Maksymalna liczba przepływów:** 1
  - **Agreguj granice szerokości pasma (R):** Brak ograniczeń
  - **Wielkość zasobnika tokenów:** 100 kilobitów
  - **Ograniczenie przepustowości (R):** 16 megabitów na sekundę
14. Na stronie Harmonogram wybierz opcję **Aktywność w trakcie wybranego harmonogramu** i kliknij przycisk **Nowy**.
15. Na stronie Nowy harmonogram wpisz następujące informacje i kliknij przycisk **OK**:
  - **Nazwa:** jedna\_godzina
  - **Godzina:** wybierz opcję Aktywność o określonych godzinach i dodaj godziny od 13:00 do 14:00.
  - **Dzień tygodnia:** wybierz opcję Aktywność w określonych dniach i wybierz poniedziałek
16. Na stronie Harmonogram kliknij przycisk **Dalej**.
17. Przejrzyj informacje podsumowujące. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. Lista wszystkich strategii utworzonych na serwerze wyświetlona jest w głównym oknie Konfiguracja serwera usług QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii usług zintegrowanych na serwerze iSeries iSeries A. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: Uruchomienie lub aktualizacja serwera QoS

W oknie konfiguracji serwera usług QoS należy wybrać **Serwer** → **Uruchom** lub **Serwer** → **Aktualizuj**.

## Szczegóły scenariusza: Użycie monitora w celu sprawdzenia, czy strategia działa właściwie

Aby sprawdzić, czy strategia działa tak, jak powinna i jak została skonfigurowana, skorzystaj z monitora.

1. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Monitorowanie**. Zostanie wyświetlone okno Monitor QoS.
2. Wybierz folder typu strategii IntServ. Zostaną wyświetlone wszystkie strategie IntServ.

Najbardziej interesujące są pola, których wartości wynikają z ruchu danych. Są to pola zawierające łączną liczbę bitów, liczbę bitów w profilu i liczbę pakietów w profilu. Liczba bitów spoza profilu wskazuje, że pewne dane są wstrzymywane lub odrzucane w celu spełnienia wymagań określonych w strategii usług zintegrowanych. Opis wszystkich pól w oknie monitora zawiera sekcja "Monitorowanie QoS" na stronie 56.

**Uwaga:** Należy pamiętać, że wyniki będą poprawne, tylko jeśli dana strategia jest aktywna. Trzeba to sprawdzić w harmonogramie określonym dla danej strategii. Ponadto, monitor może pokazać informacje dotyczące strategii IntServ dopiero po uruchomieniu aplikacji. Przed monitorowaniem muszą zostać ustanowione rezerwacje protokołu RSVP.

## Szczegóły scenariusza: Zmiana właściwości (w razie potrzeby)

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii, aby lepiej dostosować działanie strategii do potrzeb.

Po przejrzaniu wyników w oknie monitora można zmienić wartości określone wcześniej w trakcie pracy z kreatorem.

1. W oknie Konfiguracja serwera usług QoS wybierz folder **IntServ**. Na liście w prawym panelu kliknij prawym przyciskiem myszy pozycję **gwarantowana\_dyrektor** i wybierz opcję **Właściwości**, aby edytować strategię. Zostanie wyświetlone okno Właściwości, które zawiera wartości sterujące ogólną strategią.
2. Zmień odpowiednie wartości.
3. W oknie Konfiguracja serwera usług QoS wybierz **Serwer** → **Aktualizuj** aby zaakceptować zmiany.

## Scenariusz: Monitorowanie bieżących statystyk sieci

W trakcie pracy z kreatorem należy ustawić limity wydajności. Nie można w tym przypadku zalecić żadnych wartości, ponieważ zależą one od konkretnych wymagań dotyczących danej sieci.

### Cele

Aby można je było określić, niezbędne jest dokładne zrozumienie bieżącej wydajności sieci. Przystępując do konfigurowania strategii QoS, administrator powinien mieć dobre pojęcie o potrzebach występujących w sieci. Aby określić dokładne limity, na przykład ustawienia szybkości tokenów, można uruchomić monitorowanie całego ruchu danych obsługiwanych przez serwer.

### Rozwiązanie

Utwórz bardzo szeroką strategię usług DiffServ, która nie zawiera ograniczeń (wartości maksymalnych) i dotyczy wszystkich interfejsów i adresów IP. Za pomocą monitora QoS uruchom zbieranie danych dla tej strategii.

#### Pojęcia pokrewne

“Limity dotyczące zasobnika tokenów i limity przepustowości” na stronie 10

Limity dotyczące zasobnika tokenów i limity przepustowości noszą wspólną nazwę limitów wydajności. Limity te umożliwiają gwarantowane dostarczanie pakietów w strategiach ruchu wychodzącego, to znaczy w strategii usług zintegrowanych i strategii usług DiffServ.

“Limity średniej szybkości połączeń i porcji połączeń” na stronie 16

Limity dotyczące szybkości połączeń i porcji połączeń są nazywane *limitami szybkości*. Umożliwiają one ograniczanie połączeń przychodzących do serwera. Limity szybkości ustawia się w klasie usług używanej wraz ze strategiami akceptowania ruchu przychodzącego.

#### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

## Szczegóły scenariusza: Otwieranie usługi QoS w programie iSeries Navigator

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz **Konfiguracja**.
3. Rozwiń pozycję **Strategie połączeń wychodzących**.
4. Kliknij prawym przyciskiem myszy pozycję **DiffServ** i wybierz opcję **Nowa strategia**. Zostanie wyświetlone nowe okno kreatora strategii QoS.

## Szczegóły scenariusza: Utwórz strategię usług DiffServ.

Ponieważ strategia ma dotyczyć większości danych napływających do sieci, można ją nazwać **Sieć**. Strategię należy zastosować do wszystkich adresów IP, numerów portów, lokalnych adresów IP i określić, że ma być aktywna cały czas (jeśli odpowiada to potrzebom). W trakcie pracy z kreatorem należy zatem użyć następujących wartości:

**Nazwa** = Sieć (dowolna nazwa określona przez administratora)  
**Klient** = Wszystkie adresy IP  
**Aplikacja** = Wszystkie porty  
**Protokół** = Wszystkie protokoły  
**Harmonogram** = Wszystkie godziny

W programie iSeries Navigator dostępna jest lista wszystkich strategii usług utworzonych na danym serwerze.

### Szczegóły scenariusza: Utwórz nową klasę usług.

Kończąc pracę z kreatorem należy określić charakterystykę w ramach segmentu sieci, limity wydajności i obsługę danych spoza profilu. Podane wartości definiują klasę usług. Należy podać bardzo duże wartości, aby umożliwić obsługę jak największej części ruchu.

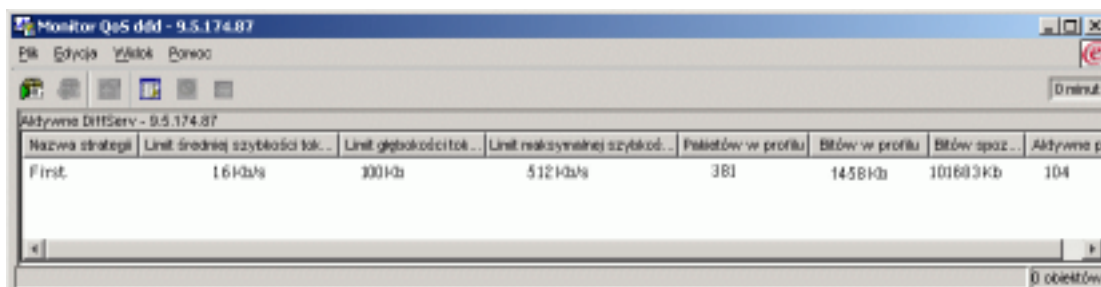
Klasa usług określa poziom wydajności ruchu danych gwarantowany przez router. Określoną tu klasę usług można nazwać **Bez\_ograniczeń**, ponieważ ruch danych uzyskuje wysoki poziom wydajności. W programie iSeries Navigator dostępna jest lista wszystkich klas usług zdefiniowanych na danym serwerze.

### Szczegóły scenariusza: Uruchom monitorowanie strategii.

Aby sprawdzić, czy ruch danych jest obsługiwany tak, jak to określono w strategii, skorzystaj z monitora.

1. Wybierz określony folder strategii (DiffServ, IntServ lub Akceptacja ruchu przychodzącego).
2. Kliknij prawym przyciskiem myszy strategię, którą chcesz monitorować, i wybierz **Monitoruj**.

Na rysunku przedstawiono przykładowe dane wyjściowe monitora odpowiadające powyższej strategii.



| Nazwa strategii | Limit średniej szybkości tok... | Limit głębokości tok... | Limit maksymalnej szybkoś... | Pakietów w profilu | Bitów w profilu | Bitów spoz... | Aktywne p... |
|-----------------|---------------------------------|-------------------------|------------------------------|--------------------|-----------------|---------------|--------------|
| First           | 1610kb/s                        | 1001kb                  | 51210kb/s                    | 381                | 14581kb         | 1016031kb     | 104          |

Rysunek 9. Monitorowanie QoS

Sprawdź pola, których wartości wyznaczone są na podstawie ruchu danych. W szczególności sprawdź pola: Bity łącznie, Bity w profilu, Pakiety w profilu i Bity spoza profilu. Na podstawie liczby bitów spoza profilu można stwierdzić, kiedy ruch danych powoduje przekroczenie wartości określonych w strategii. W strategii usług DiffServ liczba ta jest równa liczbie odrzuconych bitów. Pole Pakiety w profilu określa liczbę bajtów sterowanych za pomocą tej strategii (od chwili wysłania pakietu do chwili obecnej).

Ważny jest także limit szybkości średniej tokenów. Jeśli szybkość napływających pakietów spowoduje przekroczenie tego limitu, kolejne pakiety będą odrzucane przez serwer. W konsekwencji nastąpi zwiększenie wartości w polu Bity spoza profilu. Oznacza to, że strategia działa tak, jak powinna. Aby zmienić liczbę bitów spoza profilu, trzeba odpowiednio dopasować limity wydajności. Monitorowanie QoS udostępnia pełny opis wszystkich pól w oknie monitora.

### Szczegóły scenariusza: Zmień wartości, jeśli to konieczne.

Po zakończeniu monitorowania można zmienić dowolne wartości. Kliknij prawym przyciskiem myszy nazwę klasy usług utworzonej w danej strategii. Po wybraniu opcji **Właściwości** zostanie wyświetlone okno dialogowe Właściwości usługi QoS zawierające wartości sterujące ruchem danych.

## Szczegóły scenariusza: Ponownie uruchom monitorowanie strategii.

Aby wyznaczyć limity optymalne w danej sieci, można stopniowo zmieniać poszczególne wartości i sprawdzać wyniki monitorowania.

---

## Planowanie jakości usług

Najważniejszy etap wprowadzania QoS to planowanie. Aby uzyskać pożądane efekty, należy zrobić przegląd urządzeń dostępnych w danej sieci i uruchomić monitorowanie ruchu.

Temat ten dotyczy doradcy planowania. Doradca planowania QoS prezentuje najważniejsze pytania, które warto zadać sobie w fazie planowania QoS. Oprócz tego przed skonfigurowaniem QoS trzeba rozważyć następujące zagadnienia.

## Wydajność sieci

QoS to nic innego jak wydajność sieci. Jeśli zaczyna się rozważać zastosowanie QoS w danej sieci, prawdopodobnie występują w niej przeciążenia lub zdarza się utrata pakietów. Zanim rozpocznie się realizację strategii, można skorzystać z monitora QoS i sprawdzić bieżący poziom wydajności ruchu IP. Na podstawie tych danych można określić, gdzie występują przeciążenia.

### Pojęcia pokrewne

“Monitorowanie transakcji serwera” na stronie 63

W sekcji tej omówiono monitor QoS umożliwiający sprawdzenie, czy strategię QoS działają zgodnie z oczekiwaniami.

“Konfigurowanie jakości usług” na stronie 51

W sekcji tej przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych (IntServ) oraz akceptowania ruchu przychodzącego.

## Wymagania dotyczące uprawnień

Strategie QoS mogą zawierać dane istotne dla poprawnej pracy sieci. W związku z tym uprawnienia do administrowania funkcją QoS należy nadawać tylko wtedy, gdy jest to konieczne.

Do skonfigurowania strategii QoS i (opcjonalnie) serwerów katalogów LDAP niezbędne są opisane poniżej uprawnienia.

## Nadawanie uprawnień do zarządzania serwerem katalogów

Administrator funkcji QoS potrzebuje uprawnień \*ALLOBJ i \*IOSYSCFG. Inne możliwości opisano w sekcji Konfigurowanie serwera katalogów.

## Nadawanie uprawnień do uruchamiania serwera TCP/IP

Aby nadać uprawnienia do komend STRTCPSVR i ENDTCPSSVR, wykonaj następujące czynności:

1. **STRTCPSVR:** W wierszu komend wpisz komendę GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (\*CMD) USER (PROFIL\_ADMINISTRATORA) AUT (\*USE), w której PROFIL\_ADMINISTRATORA należy zastąpić nazwą profilu administratora, i naciśnij klawisz Enter.
2. **ENDTCPSVR:** W wierszu komend wpisz komendę GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (\*CMD) USER (PROFIL\_ADMINISTRATORA) AUT (\*USE), w której PROFIL\_ADMINISTRATORA należy zastąpić nazwą profilu administratora, i naciśnij klawisz Enter.

## Nadawanie uprawnień do wszystkich obiektów i uprawnień do konfigurowania systemu.

Zaleca się, aby użytkownicy mający możliwość konfigurowania funkcji QoS mieli uprawnienia szefa ochrony. Aby nadać uprawnienia do wszystkich obiektów i uprawnienia do konfigurowania systemu, wykonaj następujące czynności:

1. W programie iSeries Navigator, rozwiń opcję → **Użytkownicy i grupy** serwera.
2. Dwukrotnie kliknij pozycję **Wszyscy użytkownicy**.
3. Kliknij prawym przyciskiem myszy profil administratora i wybierz opcję **Właściwości**.
4. W oknie Właściwości kliknij **Możliwości**.
5. Na stronie Możliwości wybierz opcję **Dostęp do wszystkich obiektów i konfigurowanie systemu**.
6. Aby zamknąć stronę Możliwości, kliknij **OK**.
7. Kliknij **OK**, aby zamknąć okno Właściwości.

## Wymagania dotyczące systemu

Jakość usług (QoS) to integralna część systemu operacyjnego.

Muszą być spełnione następujące wymagania:

1. Zainstalowane narzędzia TCP/IP Connectivity Utilities (57xx-TC1).
2. Zainstalowane oprogramowanie iSeries Navigator. Podczas instalacji oprogramowania iSeries Access należy zainstalować opcję Sieć. Usługa QoS jest umieszczona w pozycji Sieć - Strategie IP.

### Pojęcia pokrewne

iSeries Navigator

### Odsyłacze pokrewne

“Informacje związane z jakością usług” na stronie 66

Znajdują się tu podręczniki IBM Redbooks (w formacie PDF), serwisy WWW, oraz tematy Centrum informacyjnego związane z zagadnieniem Jakości usług. Wszystkie dokumenty w formacie PDF można wyświetlać lub drukować.

## Umowa dotycząca poziomu usług

Początek zmian Sekcja ta ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (SLA), istotne w realizacji QoS.

QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią lokalną, może być konieczne zawarcie umowy z dostawcą ISP.

### Kiedy wymagane jest zawarcie umowy?

Umowa dotycząca poziomu usług jest potrzebna tylko wtedy, gdy stosowane strategie wymagają uzyskiwania priorytetu poza siecią prywatną. W przypadku strategii ruchu wychodzącego, stosowanej w celu ograniczenia szybkości ruchu danych opuszczających serwer, nie jest potrzebny gwarantowany poziom usług. Inaczej jest w sytuacji, gdy na serwerze utworzono na przykład strategię, dzięki której jedna z aplikacji uzyskuje wyższy priorytet niż pozostałe. Priorytet ten jest rozpoznawany przez ten serwer, ale nie będzie rozpoznawany w żadnym innym miejscu. Jeśli routery w sieci prywatnej zostaną skonfigurowane tak, aby rozpoznawać oznakowanie punktem kodowym (używane w strategiach ruchu wychodzącego w celu przypisania poziomu usług), ruch danych będzie uzyskiwał priorytet w ramach sieci prywatnej. Jednak po opuszczeniu sieci prywatnej priorytet ten nie będzie zagwarantowany. Jeśli nie zawarto umowy dotyczącej poziomu usług, nie można mieć wpływu na sposób obsługi ruchu danych przez sprzęt sieciowy. Aby poza siecią prywatną zagwarantować priorytet dla klasy usług lub rezerwacji zasobów, trzeba zawrzeć odpowiednią umowę.

### Dlaczego wymagane jest zawarcie umowy?

Strategie i rezerwacje zasobów są tak dobre jak najslabszy element użyty w realizacji QoS. Strategie QoS umożliwiają aplikacjom uzyskiwanie priorytetu w sieci. Jeśli jednak przynajmniej jeden węzeł na trasie między klientem i serwerem nie może właściwie obsłużyć ruchu danych (obsługę tę opisano w sekcjach dotyczących usług Diffserv i usług zintegrowanych), strategie nie zostaną obsłużone tak, jak powinny. Jeśli umowa dotycząca poziomu usług nie gwarantuje wystarczających zasobów, nawet najlepsze strategie nie rozwiążą problemu przeciążenia sieci.

Dotyczy to również umów między różnymi dostawcami usług internetowych. Dostawcy muszą zapewniać obsługę QoS we wszystkich domenach. Współdziałanie rozwiązań różnych dostawców może okazać się dość kłopotliwe.

Należy znać poziom usług zapewniany przez dostawców. Umowy związane z warunkowaniem ruchu danych dotyczą sposobu obsługi ruchu: kiedy pakiety są odrzucane, oznaczane, kształtowane i retransmitowane. QoS stosuje się przede wszystkim ze względu na możliwość sterowania opóźnieniem, zaburzeniem, szerokością pasma, utratą pakietów, dostępnością i przepustowością. Umowy muszą zapewniać odpowiedni poziom usług, tak aby wymagania zawarte w strategiach mogły zostać spełnione. Należy też sprawdzić, czy uzyskiwany poziom usług jest odpowiedni do wymagań. W przeciwnym wypadku można ponieść straty. Gdy na przykład dla telefonii IP zarezerwowano przepustowość 500 kb/s, a aplikacja używa jedynie przepustowości 20 kb/s, może się zdarzyć, że poniesiemy niepotrzebne koszty i nie uzyskamy na ten temat żadnych informacji od dostawcy.

**Uwaga:** Stosowanie strategii QoS jest podstawą do negocjowania poziomów usług z dostawcą ISP, co może umożliwić obniżenie kosztów usług sieciowych. Na przykład można z dostawcą ISP uzgodnić pewną stawkę, która będzie obowiązywać, o ile nie zostanie przekroczony ustalony poziom przepustowości. Korzystając ze strategii QoS można też ustalić, że w dzień używana będzie przepustowość "x", a w nocy przepustowość "y", i uzgodnić stawki obowiązujące w poszczególnych okresach. W przypadku przekroczenia ustalonej przepustowości dostawca ISP mógłby zastosować wyższą stawkę. Dostawca ISP powinien zgodzić się na zapewnienie określonego poziomu usług i mieć możliwość śledzenia wykorzystywanej przepustowości.

### Pojęcia pokrewne

"Pojęcia" na stronie 2

Podstawowe pojęcia związane z funkcją QoS. Podane tu informacje umożliwiają zrozumienie działania QoS i współpracy różnych funkcji wykorzystywanych do jej zapewnienia.

"Scenariusz: ograniczanie ruchu danych do przeglądarki" na stronie 28

Monitorowanie można wykorzystać do sterowania wydajnością ruchu danych w sieci. Aby ograniczyć lub zwiększyć wydajność aplikacji w danej sieci, należy skorzystać ze strategii usług DiffServ.

"Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług)" na stronie 32

W sieci VPN także można tworzyć strategię QoS. Ilustruje to przedstawiony w sekcji przykład.

"Scenariusz: przewidywalny ruch danych firma-firma (B2B)" na stronie 38

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

"Scenariusz: dedykowane dostarczanie (telefonii IP)" na stronie 42

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa rodzaje takich strategii: usługi gwarantowane i usługi sterowanego obciążenia. W tym przykładzie wykorzystano usługi gwarantowane.

## Sprzęt i oprogramowanie sieciowe

Możliwości urządzeń znajdujących się wewnątrz i na zewnątrz sieci mają ogromny wpływ na QoS.

### Aplikacje

Strategie usług zintegrowanych wymagają aplikacji obsługiwanych przez protokół RSVP. Aplikacje iSeries nie obsługują protokołu RSVP. Obsługę tę należy dopiero włączyć. W tym celu trzeba utworzyć specjalne programy korzystające z funkcji API RAPI lub funkcji API gniazd QoS qtoq. Umożliwią one aplikacjom korzystanie z protokołu RSVP.

### Węzły sieci

Routerzy, przełączniki i serwery muszą mieć funkcje umożliwiające zastosowanie QoS. Aby można było użyć strategii usług DiffServ, urządzenia muszą udostępniać te usługi. Oznacza to, że węzeł sieci musi umieć klasyfikować, mierzyć, znakować, kształtować i odrzucać pakiety IP (funkcje warunkujące).

Aby można było użyć strategii usług zintegrowanych, urządzenia muszą udostępniać te usługi. Oznacza to, że węzły sieci muszą obsługiwać protokół RSVP.



### Pojęcia pokrewne

“Funkcje API QoS” na stronie 17

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSerVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

“Funkcje warunkujące ruch danych” na stronie 5

Aby korzystać ze strategii QoS, urządzenia sieciowe (routery i przełączniki) muszą obsługiwać funkcje warunkujące. Funkcjami warunkującymi nazywamy funkcje klasyfikujące, mierzące, znakujące, kształtujące i odrzucające.

---

## Konfigurowanie jakości usług

W sekcji tej przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych (IntServ) oraz akceptowania ruchu przychodzącego.

Po zakończeniu planowania QoS należy utworzyć strategię QoS, korzystając z kreatorów dostępnych w programie iSeries Navigator. Znakomicie ułatwiają one proces konfigurowania strategii.

We wcześniej skonfigurowanej strategii można wprowadzić zmiany korzystając z obiektów konfiguracyjnych w programie iSeries Navigator. Obiekty te stanowią części składowe strategii. Pozycja QoS obejmuje następujące foldery w programie iSeries Navigator: klienci, aplikacje, harmonogramy, strategie, klasy usług, charakterystyki przeskoku i zasoby URI. Obiekty te umożliwiają utworzenie strategii. Szczegółowe informacje na temat poszczególnych obiektów zawiera temat Przegląd QoS dostępny w pomocy programu iSeries Navigator.

## Włączanie strategii QoS

Aby uaktywnić strategię, trzeba je najpierw włączyć. Jeśli korzystano z kreatorów, serwer włącza strategię automatycznie. Jeśli jednak wprowadzono zmiany w strategii używając obiektów konfiguracyjnych, aby uaktywnić zmiany, należy dynamicznie zaktualizować serwer. Przed włączeniem danych strategii należy sprawdzić, czy istnieją strategię nakładające się na nią. Może to być bowiem przyczyną problemów.

### Pojęcia pokrewne

“Planowanie jakości usług” na stronie 48

Najważniejszy etap wprowadzania QoS to planowanie. Aby uzyskać pożądane efekty, należy zrobić przegląd urządzeń dostępnych w danej sieci i uruchomić monitorowanie ruchu.

iSeries Navigator

### Zadania pokrewne

“Kolejność strategii jakości usług” na stronie 54

Jeśli pewne strategię nakładają się, istotna jest kolejność, w jakiej są one wyświetlane w programie iSeries Navigator.

### Odsyłacze pokrewne

“Zarządzanie usługą QoS” na stronie 54

Procedur tych można użyć przy zarządzaniu bieżącymi strategiami i właściwościami usługi QoS.

## Konfigurowanie jakości usług za pomocą kreatorów

Aby skonfigurować strategię QoS, należy użyć kreatorów znajdujących się w programie iSeries Navigator.

Opiszemy funkcje każdego z nich.

### Kreator konfiguracji początkowej

Kreator ten umożliwia skonfigurowanie danych charakterystycznych dla systemu i danych dotyczących serwera katalogów.

### Kreator nowej strategii IntServ

Kreator ten umożliwia utworzenie strategii usług zintegrowanych. Strategie tego typu sterują dopuszczaniem

zgłoszeń RSVP, co wpływa na przepustowość serwera. Limity wydajności określone w strategii decydują, czy serwer może udostępnić żadaną przepustowość aplikacji RSVP klienta. Aby zrealizować strategię usług zintegrowanych, routery i aplikacje muszą obsługiwać protokół RSVP.

**Uwaga:** Zanim skonfiguruje się strategię usług zintegrowanych, należy utworzyć aplikacje umożliwiające korzystanie z protokołu RSVP.

### **Kreator nowej strategii DiffServ**

Kreator ten umożliwia zróżnicowanie obsługi ruchu danych TCP/IP i przypisanie danym priorytetów. Zróżnicowanie obsługi uzyskuje się tworząc strategię. W ramach strategii do wychodzącego ruchu danych przypisuje się poziomy usług na podstawie źródłowych/docelowych adresów IP, portów, aplikacji, a nawet klientów. W wersji V5R3 poziomy usług mogą być przypisywane do aplikacji iSeries na podstawie bardziej szczegółowych informacji o aplikacji. Przed utworzeniem strategii tego typu należy zapoznać się z koncepcją usług DiffServ.

### **Kreator nowej klasy usług**

Kreator ten umożliwia zdefiniowanie znakowania pakietów, które jest wykorzystywane później przez routery i przełączniki w sieciach. Za jego pomocą można także określić limity wydajności dotyczące pakietów opuszczających daną sieć. Klasy usług wykorzystuje się w strategiach usług DiffServ i w strategiach akceptowania ruchu przychodzącego.

### **Kreator akceptacji nowych połączeń przychodzących**

Kreator ten umożliwia ograniczenie połączeń nawiązywanych z serwerem. Dostęp do serwera można ograniczyć na podstawie adresu TCP/IP, aplikacji, interfejsu lokalnego lub nazwy URI. Dzięki temu administrator systemu steruje dostępem określonych klientów do serwera, a także wykorzystaniem określonych aplikacji i dostępem do określonych zasobów URI. Ponadto, korzystając z tego kreatora, można zwiększyć wydajność serwera.

**Uwaga:** Przed skonfigurowaniem strategii ruchu przychodzącego korzystającej z nazw URI, należy się upewnić, że port aplikacji przypisany do URI jest taki sam, jak port podany za pomocą dyrektywy Listen FRCA w konfiguracji serwera WWW Apache.

Po wybraniu typu strategii można ją skonfigurować za pomocą jednego z opisanych tu kreatorów.

## **Dostęp do kreatorów QoS w programie iSeries Navigator**

Aby uruchomić kreator QoS i utworzyć strategię w programie iSeries Navigator, należy wykonać odpowiednie czynności.

Aby uruchomić kreator QoS i utworzyć strategię, wykonaj następujące czynności:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług**, a następnie kliknij opcję **Konfiguracja**.

**Uwaga:** W następujących przypadkach uruchamiany jest kreator konfiguracji początkowej:

- Interfejsu graficznego QoS używa się po raz pierwszy.
  - Ręczne usuwanie poprzednich danych konfiguracji i określanie nowych. W takiej sytuacji interfejs QoS musi być otwarty.
3. Wykonaj czynności zalecane w kreatorze konfiguracji początkowej. Jeśli kreator ten nie zostanie uruchomiony, przejdź do punktu 4.
  4. Wybierz **Strategie**. Prawym przyciskiem myszy kliknij pozycję **IntServ**, **DiffServ** lub **Akceptowanie ruchu przychodzącego**.
  5. Wybierz opcję **Nowa strategia**.

### **Pojęcia pokrewne**

“Funkcje API QoS” na stronie 17

Ten temat zawiera informacje o protokołach, funkcjach API oraz wymaganiach routera włączonego dla protokołu ReSerVation (RSVP). Bieżące funkcje API QoS to: funkcja RAPI API, funkcja API gniazd qtoq, funkcja API sendmsg() i monitorujące funkcje API.

“Usługa DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących. W ramach usług DiffServ ruch danych dzielony jest na klasy. Aby możliwe było stosowanie strategii usług DiffServ, należy określić sposób klasyfikacji ruchu danych oraz sposób obsługi poszczególnych klas.

#### **Informacje pokrewne**

Zarządzanie adresami i portami serwera HTTP (opartego na Apache)

## **Konfigurowanie serwera katalogów**

Konfiguracje strategii QoS można eksportować do serwera katalogów LDAP.

W ten sposób można łatwiej zarządzać usługą QoS. Zamiast konfigurować strategię QoS na wszystkich serwerach, można zapisać dane konfiguracyjne na lokalnym serwerze katalogów i udostępnić je innym systemom. Podczas pierwszej konfiguracji QoS uruchamia się kreator konfiguracji początkowej. W trakcie pracy z nim konfiguruje się serwer katalogów.

Aby skonfigurować serwer katalogów, należy:

- podać nazwę serwera katalogów,
- wybrać nazwę wyróżniającą (DN), która będzie odnosić się do strategii QoS,
- określić, czy ma być używana ochrona SSL na serwerze katalogów LDAP,
- określić, czy mają być używane słowa kluczowe ułatwiające wyszukiwanie strategii na serwerze katalogów.

**Uwaga:** W obecnej wersji systemu nie można wybrać protokołu Kerberos jako metody uwierzytelniania używanej przez serwer QoS podczas dostępu do katalogów.

Aby można było administrować serwerem katalogów LDAP, trzeba mieć jeden z poniższych zestawów uprawnień:

- uprawnienia \*ALLOBJ i \*IOSYSCFG,
- uprawnienie \*JOBCTL i uprawnienia do obiektu dla komend Zakończenie pracy TCP/IP (End TCP/IP - STRTCP), Uruchomienie TCP/IP (Start TCP/IP - ENDTCP), Uruchomienie serwera TCP/IP (Start TCP/IP Server - STRTCPSVR) i Zakończenie pracy serwera TCP/IP (End TCP/IP Server - ENDTCPSVR),
- uprawnienie \*AUDIT authority do konfiguracji kontroli ochrony w systemie i5/OS

Jeśli użytkownik korzysta się z programu iSeries Navigator, dostępny jest schemat domyślny QoS. Schemat ten znajduje się na serwerze iSeries w katalogu /QIBM/UserData/OS400/DirSrv. Jeśli jednak używa się innego edytora niż iSeries Navigator, konieczne będzie zaimportowanie pliku LDIF opisanego poniżej. Można to uczynić także wtedy, gdy po wprowadzeniu zmian chce się powrócić do oryginalnej, domyślnej wersji pliku.

## **Schemat QoS**

*Schemat* to pewien zestaw reguł określających typy obiektów LDAP, z których może korzystać serwer QoS. Zawiera reguły niezbędne do poprawnego funkcjonowania QoS. W przypadku gdy serwer LDAP nie jest serwerem iSeries trzeba zaimportować reguły do serwera LDAP. W tym celu korzysta się z pliku w formacie LDIF (LDAP Data Interchange Format). Plik LDIF można pobrać z serwisu WWW iSeries. Jest on dostępny w lewym panelu pod hasłem **Categories** → **TCP/IP Policies**. Przykładowy schemat QoS opisano w sekcji *Konceptje serwera katalogów*.

#### **Pojęcia pokrewne**

“Serwer katalogów” na stronie 25

Strategie można eksportować do serwera katalogów. W tej sekcji opisano korzyści wynikające z obu metod: eksportowania strategii do serwera katalogów oraz z zaniechania eksportu, a także konfigurowanie protokołu LDAP i związane z nim pojęcia, oraz schemat QoS.

“Nazwa wyróżniająca” na stronie 26

Aby zarządzać częścią katalogu, należy użyć *nazwy wyróżniającej (DN)* lub słowa kluczowego (jeśli jest to potrzebne).

Serwer katalogów IBM dla iSeries (LDAP)

Ochrona SSL dla serwera katalogów LDAP

“Słowa kluczowe” na stronie 26

Konfigurując serwer katalogów trzeba określić, czy z każdą konfiguracją QoS będą skojarzone słowa kluczowe.

### Informacje pokrewne

Strona WWW iSeries LDAP

## Kolejność strategii jakości usług

Jeśli pewne strategie nakładają się, istotna jest kolejność, w jakiej są one wyświetlane w programie iSeries Navigator.

Strategie nakładają się, jeśli mają wspólny jeden z następujących parametrów: klienta, aplikacja, harmonogram, lokalny adres IP, nazwa URI, dane serwera, punkt kodowy lub protokół. Strategie w programie iSeries Navigator uporządkowane są w postaci listy. Kolejność przetwarzania strategii jest identyczna jak kolejność strategii na tej liście. Jeśli pewna strategia ma mieć wyższy priorytet niż inna, musi pojawić się wcześniej.

Aby sprawdzić, czy strategia nakłada się na inną strategię, wykonaj następujące czynności:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług**.
3. Wybierz opcję **Konfiguracja**.
4. Wybierz określony folder strategii.
5. Kliknij prawym przyciskiem myszy nazwę strategii, która nakłada się na inne strategie. Przed nazwami takich strategii umieszczona jest odpowiednia ikona.
6. Wybierz opcję **Pokaż nakładanie się**. Zostanie wyświetlone okno nakładania się strategii.

Aby zmienić kolejność strategii na ekranie, wykonaj następujące czynności:

- Zaznacz strategię i korzystając ze strzałki w dół lub strzałki w górę zmień jej pozycję na liście.
- Kliknij prawym przyciskiem myszy nazwę strategii i wybierz opcję **W górę** lub **W dół**.
- Aktualizacja serwera QoS. W celu aktualizacji serwera QoS należy użyć przycisku **Zaktualizuj serwer** znajdującego się w pasku narzędzi. Więcej informacji na ten temat zawierają tematy pomocy QoS.

### Pojęcia pokrewne

“Konfigurowanie jakości usług” na stronie 51

W sekcji tej przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych (IntServ) oraz akceptowania ruchu przychodzącego.

“Kopiowanie istniejącej strategii” na stronie 56

Zamiast tworzyć każdą strategię od nowa, można skopiować oryginalną strategię i wprowadzić zmiany w sekcjach, w których występują różnice.

“Rozwiązywanie problemów z jakością usług” na stronie 60

Jakość usług (QoS) udostępnia wiele metod rozwiązywania problemów związanych z QoS.

### Zadania pokrewne

“Uzyskiwanie pomocy dotyczącej QoS w programie iSeries Navigator” na stronie 55

Aby uzyskać dostęp do pomocy dla usługi QoS, można użyć programu iSeries Navigator.

---

## Zarządzanie usługą QoS

Procedur tych można użyć przy zarządzaniu bieżącymi strategiami i właściwościami usługi QoS.

W tematach tych opisano, gdzie znajdują się zadania związane z edycją, włączaniem, przeglądaniem i innymi technikami zarządzania strategiami. Opisano także sposób wykorzystania monitora QoS oraz kolekcjonowania danych do analizy ruchu IP na serwerze.

#### Pojęcia pokrewne

“Konfigurowanie jakości usług” na stronie 51

W sekcji tej przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych (IntServ) oraz akceptowania ruchu przychodzącego.

## Uzyskiwanie pomocy dotyczącej QoS w programie iSeries Navigator

Aby uzyskać dostęp do pomocy dla usługi QoS, można użyć programu iSeries Navigator.

Aby uzyskać dostęp do pomocy dla usługi QoS, należy użyć programu iSeries Navigator:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług**, a następnie kliknij opcję **Konfiguracja**.
3. Kliknij menu **Pomoc** → **Tematy pomocy** z paska menu. Zostanie wyświetlone okno pomocy.

#### Zadania pokrewne

“Kolejność strategii jakości usług” na stronie 54

Jeśli pewne strategie nakładają się, istotna jest kolejność, w jakiej są one wyświetlane w programie iSeries Navigator.

## Składowanie strategii

Należy składać strategie QoS aby zapobiec potrzebie ich odtwarzania w razie wyłączenia serwera lub przerwy w dostawie prądu.

Strategie można przechowywać lokalnie lub eksportować do serwera katalogów. Należy w szczególności wykonać składowanie następujących katalogów zintegrowanego systemu plików: QIBM/UserData/OS400/QOS/ETC, QIBM/UserData/OS400/QOS/TEMP i QIBM/UserData/OS400/QOS/USR. Należy również przeprowadzić składowanie agenta udostępniającego serwer katalogów serwerowi QoS). Agent ten zawiera nazwę serwera katalogów, nazwę wyróżniającą serwera QoS, numer portu, na którym korzysta się z serwera katalogów i dane dotyczące uwierzytelniania. W razie utraty danych wykorzystanie kopii pozwoli zaoszczędzić czas i pracę, które trzeba by poświęcić na utworzenie strategii od początku. Oto ogólne wskazówki umożliwiające łatwe zastąpienie utraconych plików:

1. **Użyj programów do składowania i odtwarzania dostępnych w zintegrowanym systemie plików.**

Podręcznik *Składowanie i odzyskiwanie* zawiera instrukcje na temat odzyskiwania danych z zintegrowanego systemu plików.

2. **Wydrukuj strategie.**

Wydruki należy przechowywać w bezpiecznym miejscu, a w razie potrzeby ponownie wprowadzić zawarte w nich dane.

3. **Skopiuj dane na dysk.**

Kopiowanie ma przewagę nad drukowaniem, nie wymaga bowiem ręcznego wprowadzania danych, które istnieją już w postaci cyfrowej. Jest to prosta metoda przenoszenia danych z jednego źródła elektronicznego do innego.

**Uwaga:** System iSeries kopiuje informacje na dysk systemowy, nie na dyskietkę. Pliki reguł znajdują się w katalogu QIBM/UserData/OS400/QOS/ETC, a także w ramach nazwy wyróżniającej określonej na serwerze katalogów. Pliki te nie są natomiast przechowywane na komputerze PC. Aby ochronić dane znajdujące się na dysku systemowym, można skorzystać z metody zabezpieczania dysków.

Gdy korzysta się z serwera iSeries, należy zaplanować strategię składowania i odzyskiwania.

#### Informacje pokrewne

Składowanie i odtwarzanie

## Kopiowanie istniejącej strategii

Zamiast tworzyć każdą strategię od nowa, można skopiować oryginalną strategię i wprowadzić zmiany w sekcjach, w których występują różnice.

W programie iSeries Navigator, ta funkcja usługi QoS nosi nazwę *Nowa w oparciu o*. Aby skopiować strategię, należy skorzystać z programu iSeries Navigator i wyświetlić okno dialogowe Jakość usług.

Aby utworzyć kopię istniejącej strategii, należy wykonać czynności opisane w temacie pomocy **Tworzenie nowej strategii opartej na istniejącej strategii** w programie iSeries Navigator.

Aby uaktywnić strategię, trzeba je włączyć, uruchamiając serwer QoS lub wykonując dynamiczną aktualizację serwera. Przed włączeniem danej strategii należy sprawdzić, czy istnieją strategie nakładające się na nią. Może to być bowiem przyczyną problemów.

### Zadania pokrewne

“Kolejność strategii jakości usług” na stronie 54

Jeśli pewne strategie nakładają się, istotna jest kolejność, w jakiej są one wyświetlane w programie iSeries Navigator.

## Edytowanie strategii

Gdy zmienia się wymagania dotyczące wydajności sieci, konieczne będzie także wprowadzenie zmian w strategii aby utrzymać wydajność na wysokim poziomie.

Przed aktywowaniem strategii należy poprawić ewentualne błędy i wprowadzić niezbędne zmiany. W ten sposób najłatwiej zapobiec komplikacjom związanym z działaniem strategii.

We wcześniej skonfigurowanej strategii można wprowadzić zmiany korzystając z obiektów konfiguracyjnych w programie iSeries Navigator. Obiekty te stanowią części składowe strategii. Pozycja QoS obejmuje następujące foldery w programie iSeries Navigator: klienci, aplikacje, harmonogramy, strategie, klasy usług, charakterystyki przeskoku i zasoby URI. Obiekty te umożliwiają edytowanie strategii.

Aby wprowadzić zmiany w strategii korzystając z programu iSeries Navigator, wykonaj czynności opisane w pomocy programu iSeries Navigator na stronie Edytowanie strategii QoS.

## Monitorowanie QoS

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

Umożliwia on określenie przyczyn powstawania przeciążeń w sieci. Narzędzie to jest przydatne nie tylko podczas planowania QoS, ale także przy rozwiązywaniu problemów. Monitor QoS ułatwia monitorowanie sieci i odpowiednie dopasowanie strategii. Aby monitorować wszystkie aktywne strategie, należy w oknie Konfiguracja serwera usług QoS wybrać opcję **Server** → **Monitorowanie**. Aby monitorować jedną strategię, należy kliknąć strategię prawym przyciskiem myszy i wybrać opcję **Monitorowanie**.

Funkcję monitorowania strategii można wykorzystać w następujących celach:

- **Wyświetlenie danych czasu rzeczywistego dotyczących aktywnych strategii**

W momencie otwierania monitora zawsze wyświetlane są dane czasu rzeczywistego dla aktywnych strategii. Nie ma potrzeby uruchamiania kolekcjonowania danych.

- **Zbieranie i zapisywanie danych w pewnym okresie**

Jeśli wyniki monitorowania mają być zapisywane, trzeba uruchomić kolekcjonowanie danych QoS. Monitor będzie zbierał dane do momentu zatrzymania funkcji kolekcjonowania. Zamknięcie okna monitora nie powoduje zatrzymania kolekcjonowania danych. Istnieje także możliwość zmiany właściwości wykorzystywanych przez monitor podczas kolekcjonowania danych. W tym celu należy w oknie Monitor QoS podświetlić pozycję *Monitor QoS* i wybrać opcję *Plik-->Właściwości*. Więcej informacji na ten temat zawiera pomoc elektroniczna.

Jeśli kolekcjonowanie danych QoS jest włączone i ulegną zmianie właściwości monitora, to aby zmiany zostały uwzględnione w sposobie zbierania danych, trzeba wykonać następujące czynności:

1. Zatrzymaj kolekcjonowanie danych QoS.
2. Zmień właściwości monitora.
  - a. W oknie Monitor kliknij **Monitor QoS**.
  - b. Wybierz **Zbiór** → **Właściwości**.
  - c. Zmień właściwości monitora i kliknij przycisk **OK**.
3. Zaktualizuj serwer QoS.
4. Uruchom kolekcjonowanie danych QoS.

## Dane wyjściowe monitora

Dane wyjściowe monitora zależą od typu strategii, która jest monitorowana. Jak wiadomo, dostępne są następujące typy strategii: DiffServ, IntServ (sterowane obciążenie), IntServ (gwarantowana przepustowość) oraz Akceptacja ruchu przychodzącego. Pola wyświetlane w oknie monitora zależą od strategii. Najbardziej interesujące są wartości uzyskane w wyniku pomiarów. Są to następujące wartości: liczba zaakceptowanych zgłoszeń, liczba aktywnych połączeń, liczba połączeń obsłużonych, szybkości połączeń, liczba usuniętych zgłoszeń, liczba pakietów w profilu, liczba bitów w profilu, liczba bitów spoza profilu, łączna liczba bitów, łączna liczba pakietów i łączna liczba zgłoszeń.

Zmierzone wartości dają dobry obraz tego, jak ruch w sieci dostosowany jest do wykorzystywanych strategii. Poniżej zamieszczono szczegółowy opis pól monitora w przypadku różnych strategii. Sekcja Scenariusze wykorzystania QoS zawiera przykłady zastosowań monitora.

## Strategie usług DiffServ

Tabela 4. Strategie usług DiffServ

| Pole                               | Opis   |
|------------------------------------|--|
| Nazwa strategii                    | Nazwa strategii określona przez administratora.  |
| Protokół                           | UDP, TCP, ALL  |
| Limit szybkości średniej tokenów   | Średnia szybkość tokenów określona w strategii dla każdego routera i serwera znajdującego się na trasie połączenia.  |
| Limit liczby tokenów               | Maksymalna wielkość buforu tokenów określona w strategii dla każdego routera i serwera znajdującego się na trasie połączenia.  |
| Limit szybkości szczytowej tokenów | Maksymalna szybkość tokenów dopuszczalna w danym połączeniu.   |
| Pakiety w profilu                  | Liczba nadanych pakietów IP, które spełniały ograniczenia określone w strategii.   |
| Bity w profilu                     | Liczba nadanych bitów, które spełniały ograniczenia określone w strategii.   |
| Bity spoza profilu                 | Liczba nadanych bitów, które naruszały ograniczenia określone w strategii.   |
| Szybkość w bitach                  | Zmierzona liczba bitów przesyłanych w danym połączeniu.  |
| Aktywne połączenia                 | Łączna liczba aktywnych połączeń.  |
| Profil ruchu danych                | Sposób obsługi pakietów spoza profilu. Format może obejmować: <ul style="list-style-type: none"> <li>• ponowne znakowanie,</li> <li>• kształtowanie,</li> <li>• odrzucanie.</li> </ul> |
| Bity łącznie                       | Liczba bitów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.   |

Tabela 4. Strategie usług DiffServ (kontynuacja)

| Pole                       | Opis  |
|----------------------------|---|
| Punkt kodowy w profilu     | Jeśli pakiety są ponownie znakowane (otrzymują nowy punkt kodowy), jest to punkt kodowy nadawany pakietom IP spełniającym ograniczenia określone w profilu. |
| Punkt kodowy spoza profilu | Jeśli pakiety są ponownie znakowane (otrzymują nowy punkt kodowy), jest to punkt kodowy nadawany pakietom IP naruszającym ograniczenia określone w profilu. |
| Zakres adresów docelowych  | Zakres adresów określających punkt docelowy pakietów (sterowanych za pomocą danej strategii).   |
| Pakiety łącznie            | Liczba pakietów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.   |
| Zakres portów źródłowych   | Określa aplikacje sterowane za pomocą danej strategii.  |

## Strategie usług zintegrowanych (sterowane obciążenie)

Informacje o strategiach usług zintegrowanych będą wyświetlane w monitorze dopiero po uruchomieniu aplikacji i ustanowieniu rezerwacji. Jeśli strategie IntServ mają więcej niż jedną rezerwację, w monitorze będzie widocznych kilka pozycji.

Tabela 5. Strategie usług zintegrowanych (sterowane obciążenie)

| Pole                               | Opis  |
|------------------------------------|---|
| Nazwa strategii                    | Nazwa strategii określona przez administratora.   |
| Protokół                           | UDP lub TCP   |
| Adres docelowy                     | Zakres adresów określających punkt docelowy pakietów (sterowanych za pomocą danej strategii).   |
| Limit szybkości średniej tokenów   | Średnia szybkość tokenów określona w strategii dla każdego routera i serwera znajdującego się na trasie połączenia.   |
| Limit liczby tokenów               | Maksymalna wielkość buforu tokenów określona w strategii dla każdego routera i serwera znajdującego się na trasie połączenia.   |
| Limit szybkości szczytowej tokenów | Maksymalna szybkość tokenów dopuszczalna w danym połączeniu.  |
| Pakiety łącznie                    | Liczba pakietów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.   |
| Bity spoza profilu                 | Liczba nadanych bitów, które naruszały ograniczenia określone w strategii.  |
| Bity łącznie                       | Liczba bitów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.  |
| Szybkość w bitach                  | Zmierzona liczba bitów przesyłanych w danym połączeniu.   |
| Bity w profilu                     | Liczba nadanych bitów, które spełniały ograniczenia określone w strategii.  |
| Maksymalna wielkość pakietu        | Maksymalna wielkość pakietu określona w danej strategii.  |
| Minimalna jednostka strategii      | Najmniejsza liczba bitów usuwanych z zasobnika tokenów. Jeśli na przykład liczba ta wynosi 100 bitów, pakiety o wielkości mniejszej od 100 bitów będą usuwane w taki sam sposób, jak pakiety o wielkości 100 bitów. |
| Pakiety w profilu                  | Liczba nadanych pakietów IP, które spełniały ograniczenia określone w strategii.  |
| Zakres portów źródłowych           | Określa aplikacje sterowane za pomocą danej strategii.  |



## Strategie usług zintegrowanych (gwarantowana przepustowość)

Informacje o strategiach usług zintegrowanych będą wyświetlane w monitorze dopiero po uruchomieniu aplikacji i ustanowieniu rezerwacji. Jeśli strategie IntServ mają więcej niż jedną rezerwację, w monitorze będzie widocznych kilka pozycji.

Tabela 6. Strategie usług zintegrowanych (gwarantowana przepustowość)

| Pole                               | Opis  |
|------------------------------------|---|
| Nazwa strategii                    | Nazwa strategii określona przez administratora.   |
| Protokół                           | UDP lub TCP   |
| Adres docelowy                     | Zakres adresów określających punkt docelowy pakietów (sterowanych za pomocą danej strategii).   |
| Limit szybkości średniej tokenów   | Dozwolona średnia szybkość tokenów dla każdego routera i serwera znajdującego się na trasie połączenia.   |
| Limit liczby tokenów               | Maksymalna wielkość buforu tokenów określona w strategii dla każdego routera i serwera znajdującego się na trasie połączenia.   |
| Limit szybkości szczytowej tokenów | Maksymalna szybkość tokenów dopuszczalna w danym połączeniu.  |
| Pakiety łącznie                    | Liczba pakietów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.   |
| Bity łącznie                       | Liczba bitów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.  |
| Bity spoza profilu                 | Liczba nadanych bitów, które naruszały ograniczenia określone w strategii.  |
| Szybkość gwarantowana              | Szybkość gwarantowana podana w bitach na sekundę.   |
| Bity w profilu                     | Liczba nadanych bitów, które spełniały ograniczenia określone w strategii.  |
| Maksymalna wielkość pakietu        | Maksymalna wielkość pakietu określona w danej strategii.  |
| Minimalna jednostka strategii      | Najmniejsza liczba bitów usuwanych z zasobnika tokenów. Jeśli na przykład liczba ta wynosi 100 bitów, pakiety o wielkości mniejszej od 100 bitów będą usuwane w taki sam sposób, jak pakiety o wielkości 100 bitów. |
| Pakiety w profilu                  | Liczba nadanych pakietów IP, które spełniały ograniczenia określone w strategii.  |
| Okres zastoju                      | Różnica (w sekundach) między wymaganym a uzyskanym opóźnieniem.   |
| Zakres portów źródłowych           | Określa aplikacje sterowane za pomocą danej strategii.  |

## Strategie akceptowania ruchu przychodzącego

Tabela 7. Strategie akceptowania ruchu przychodzącego

| Pole                              | Opis   |
|-----------------------------------|--|
| Nazwa strategii                   | Nazwa strategii określona przez administratora.                          |
| Szybkość połączeń                 | Liczba akceptowanych połączeń na sekundę.                                |
| Żądania łącznie                   | Łączna liczba żądań połączenia z danym serwerem.                         |
| Żądania zaakceptowane             | Łączna liczba żądań połączenia zaakceptowanych przez serwer.             |
| Żądania odrzucone                 | Łączna liczba żądań połączenia odrzuconych przez serwer.                 |
| Limit szybkości średniej połączeń | Dozwolona średnia liczba akceptowanych przez serwer połączeń na sekundę. |

Tabela 7. Strategie akceptowania ruchu przychodzącego (kontynuacja)

| Pole                                       | Opis  |
|--|---|
| Limit porcji połączeń                      | Maksymalna liczba połączeń akceptowanych równocześnie.                              |
| Limit szybkości szczytowej połączeń        | Maksymalna szybkość, z którą serwer może akceptować połączenia napływające z sieci. |
| Priorytet                                  | Priorytet nadawany regułom pobieranym przez menedżera QoS.                          |
| Priorytet w kolejce                        | Priorytet nadawany połączeniom umieszczanym w kolejce listen.                       |
| Zakres portów docelowych                   | Zakres numerów portów, z którymi nawiązywane są połączenia na danym serwerze.       |
| Adres interfejsu                           | Adres IP monitorowanego interfejsu systemu.   |
| Zakres adresów źródłowych                  | Zakres adresów IP klientów wysyłających żądania do serwera.                         |
| Uniform Resource Locator (URL) (adres URL) | Określa zasób URI sterowany za pomocą danej strategii.                              |

### Pojęcia pokrewne

“Scenariusz: ograniczanie ruchu danych do przeglądarki” na stronie 28

Monitorowanie można wykorzystać do sterowania wydajnością ruchu danych w sieci. Aby ograniczyć lub zwiększyć wydajność aplikacji w danej sieci, należy skorzystać ze strategii usług DiffServ.

“Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług)” na stronie 32

W sieci VPN także można tworzyć strategię QoS. Ilustruje to przedstawiony w sekcji przykład.

“Scenariusz: ograniczanie połączeń przychodzących” na stronie 36

Jeśli chce się sterować połączeniami przychodzącymi do serwera, należy skorzystać ze strategii połączeń przychodzących.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 38

Jeśli potrzebne jest przewidywalne dostarczanie i chce się zarezerwować zasoby, również należy skorzystać ze strategii usług zintegrowanych. W przykładzie wykorzystano usługi typu obciążenie sterowane.

“Scenariusz: dedykowane dostarczanie (telefonía IP)” na stronie 42

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa rodzaje takich strategii: usługi gwarantowane i usługi sterowanego obciążenia. W tym przykładzie wykorzystano usługi gwarantowane.

“Scenariusze” na stronie 28

Niniejsze strategię usługi mogą się okazać przydatne w zrozumieniu celu i sposobu używania usługi QoS.

“Monitorowanie transakcji serwera” na stronie 63

W sekcji tej omówiono monitor QoS umożliwiający sprawdzenie, czy strategię QoS działają zgodnie z oczekiwaniami.

“Scenariusz: Monitorowanie bieżących statystyk sieci” na stronie 46

W trakcie pracy z kreatorami ustawić należy limity wydajności. Nie można w tym przypadku zalecić żadnych wartości, ponieważ zależą one od konkretnych wymagań dotyczących danej sieci.

## Rozwiązywanie problemów z jakością usług

Jakość usług (QoS) udostępnia wiele metod rozwiązywania problemów związanych z QoS.

### Śledzenie komunikacji

Serwer iSeries umożliwia śledzenie komunikacji na określonym łączu, na przykład na łączu obsługiwany przez interfejs sieci lokalnej lub rozległej. Przeciętny użytkownik może nie rozumieć wszystkich danych dotyczących śledzenia. Na ich podstawie może jednak sprawdzić, czy między dwoma węzłami nastąpiła faktycznie wymiana danych.

## Włączanie QoS na serwerze

Jeśli serwer QoS nie uruchamia się, należy przede wszystkim sprawdzić, czy funkcja QoS serwera jest włączona. Jeśli strategię konfiguruje się po raz pierwszy, kreator konfiguracji początkowo automatycznie włączy funkcję QoS serwera. Jeśli jednak z jakiejś przyczyny konfigurację zmieniono, serwer nie uruchomi się.

Aby sprawdzić, czy funkcja QoS na serwerze jest włączona:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz opcję **Konfiguracja**.
3. Po wyświetleniu interfejsu QoS kliknij prawym przyciskiem myszy pozycję **QoS** i wybierz opcję **Właściwości**.
4. Na stronie Właściwości QoS sprawdź, czy wybrana jest opcja **Włącz QoS**.

### Pojęcia pokrewne

Śledzenie komunikacji

### Zadania pokrewne

“Kolejność strategii jakości usług” na stronie 54

Jeśli pewne strategie nakładają się, istotna jest kolejność, w jakiej są one wyświetlane w programie iSeries Navigator.

## Kronikowanie strategii jakości usług

QoS obejmuje funkcję kronikowania. Funkcja ta umożliwi śledzenie czynności związanych ze strategiami QoS, takimi jak dodawanie, usuwanie, modyfikacja.

Jeśli kronikowanie jest włączone, wszystkie czynności są zapisywane w protokole. Ułatwia to wykrywanie błędów i określanie ustawień powodujących, że strategię nie działają tak, jak powinny. Na przykład, jeśli zgodnie z konfiguracją strategia powinna być uruchomiona w godzinach od 9:00 do 16:00, w protokole można sprawdzić, czy strategia została faktycznie dodana o godzinie 9:00 i usunięta o 16:00.

Jeśli kronikowanie jest włączone, pozycje kroniki generowane są podczas dodawania, usuwania i modyfikowania strategii. Przy pomocy kronik tworzy się ogólny plik na serwerze iSeries. Na podstawie danych zapisanych w kronikach można zorientować się, jak system jest wykorzystywany. Ułatwiają one określenie zmian, które należy wprowadzić do strategii.

Trzeba uważnie wybierać czynności podlegające kronikowaniu. Funkcja ta może być bowiem dużym obciążeniem dla zasobów systemu. Uruchamianie i zatrzymywanie kronikowania wykonuje się w programie iSeries Navigator. Przeglądanie kronik uruchamia się z wiersza komend.

Aby uruchomić lub zatrzymać kronikowanie, wykonaj następujące czynności:

1. W programie iSeries Navigator, rozwiń → **Sieć** → **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz **Konfiguracja**.
3. Kliknij prawym przyciskiem myszy **QoS** i wybierz **Właściwości**.
4. Zaznacz pole **Uruchom kronikowanie**, aby włączyć funkcję kronikowania.
5. Anuluj zaznaczenie pola **Uruchom kronikowanie**, aby wyłączyć funkcję kronikowania.

**Uwaga:** Jeśli serwer został uruchomiony przed wykonaniem powyższych czynności, należy go zatrzymać i uruchomić ponownie. Po włączeniu funkcji kronikowania można ją aktywować na dwa sposoby. Można zatrzymać i ponownie uruchomić serwer lub wykonać jego aktualizację. W obu przypadkach zostanie ponownie odczytany plik policy.conf i sprawdzony atrybut kronikowania.

## Przeglądanie pozycji kronik na ekranie

Aby przeglądać pozycje kronik, należy wykonać następujące czynności:

1. W wierszu komend, wpisz komendę `DSPJRN JRN(QUSRSYS/QQOS)`.

2. Obok pozycji kroniki, która ma być wyświetlona, wpisz opcję 5.

## Przeglądanie pozycji kroniki za pomocą zbioru wyjściowego

Jeśli chcesz przeglądać sformatowane pozycje kroniki umieszczone jednym folderze, wyświetl zbiór MODEL.OUT znajdujący się w katalogu QUSRSYS. Skopiowanie pozycji kroniki do zbioru wyjściowego umożliwia łatwe przeglądanie danych za pomocą narzędzi zapytań, na przykład Query/400 lub SQL. Można także utworzyć własne programy w języku HLL przetwarzające pozycje w zbiorze wyjściowym.

Aby skopiować pozycje kroniki QoS do systemowego zbioru wyjściowego:

1. Utwórz kopię systemowego zbioru wyjściowego QSYS/QATOQQOS w bibliotece użytkownika. W tym celu można użyć komendy Tworzenie duplikatu obiektu (Create Duplicate Object - CRTDUPOBJ). Oto przykład zastosowania komendy CRTDUPOBJ:
  - CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(\*FILE) TOLIB(*biblioteka użytkownika*) NEWOBJ(*zbiór użytkownika*)
2. Aby skopiować pozycje z kroniki QUSRSYS/QQOS do zbioru wyjściowego utworzonego w poprzednim punkcie, uruchom komendę Wyświetlenie kroniki (Display Journal - DSPJRN). Jeśli poda się nieistniejący zbiór wyjściowy, zostanie on automatycznie utworzony, nie będzie jednak zawierał właściwych opisów pól.
  - DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYPE(MP) CMTCYCID(\*ALL) OUTPUT(\*OUTFILE) OUTFILFMT(\*TYPE4) OUTFILE(*biblioteka użytkownika/zbiór użytkownika*)
  - DSPF FILE(*biblioteka użytkownika/zbiór użytkownika*)

## Protokołowanie zadań serwera jakości usług

Gdy wystąpią problemy ze strategiami QoS, należy przeanalizować protokoły zadań serwera iSeries. Protokoły te zawierają komunikaty o błędach i inne dane związane z jakością usług.

Tylko jedno zadanie QoS QTOQSRVR uruchamia się w podsystemie QSYSWRK. Poprzednie i bieżące protokoły zadań serwera QoS można przeglądać, korzystając z programu iSeries Navigator.

Aby przeglądać protokoły zadań, wykonaj poniższe czynności:

1. Rozwiń pozycję **Sieć** i kliknij **Strategie IP**.
2. Kliknij prawym przyciskiem myszy **Jakość usług**.
3. Kliknij **Narzędzia diagnostyczne** → **Protokół serwera QoS**.

Pojawia się okno umożliwiające pracę z zadaniem.

Dwa najważniejsze zadania to:

**QTCP** Jest to podstawowe zadanie uruchamiające wszystkie interfejsy TCP/IP. Jeśli wystąpiły zasadnicze problemy z protokołem TCP/IP, należy przeanalizować protokół zadania QTCPIP.

### QTOQSRVR

Jest to podstawowe zadanie związane z jakością usług. Dane w protokole dotyczą bezpośrednio funkcji QoS. Rozpocznij pracę ze zbiorami buforowymi (WRKSPLF) i znajdź protokół QTOQSRVR.

## Sprawdzenie roboczego zbioru buforowego pod kątem występowania błędów:

Aby sprawdzić, czy w roboczym zbiorze buforowym nie występują błędy, wykonaj następujące czynności:

1. W wierszu komend, wpisz WRKSPLF QTCP i naciśnij klawisz Enter. Zostanie wyświetlone okno Praca ze wszystkimi zbiorami buforowymi (Work with All Spooled Files).
2. Aby sprawdzić, czy wystąpiły błędy z serwerem QoS, w kolumnie Dane użytkownika znajdź pozycję QTOQSRVR.
3. Wybierz **opcję 5** dla pozycji, którą chcesz wyświetlić. Przeczytaj podane informacje i zapisz ID komunikatu wyjaśniającego problem. Na przykład, TCP920C.

4. Naciśnij dwukrotnie Wyjście, aby powrócić do głównego menu.
5. W wierszu komend, wpisz **WRKMSGF** i naciśnij klawisz Enter.
6. W panelu Praca ze zbiorem komunikatów (Work with Message File) wpisz poniższe dane i naciśnij klawisz Enter.  
Zbiór komunikatów: QTCPSMSG Biblioteka: \*LIBL
7. Aby wyświetlić wybrany zbiór komunikatu, w panelu Praca ze zbiorem komunikatów (Work with Message File) wybierz **opcję 5** i naciśnij **Enter**.
8. W panelu Wyświetlenie opisu komunikatu podaj następujące informacje: **Pozycja:** wpisz *ID komunikatu uzyskane w punkcie 3* i naciśnij klawisz Enter. Na przykład, TCP920C.
9. Dla wybranego ID komunikatu wybierz **opcję 5** i naciśnij klawisz Enter.
10. Dla pola Wybierz szczegóły komunikatu wybierz **opcja 30 (Wszystkie powyższe)** i naciśnij klawisz Enter.  
Pojawi się szczegółowy opis komunikatu.

## Monitorowanie transakcji serwera

W sekcji tej omówiono monitor QoS umożliwiający sprawdzenie, czy strategie QoS działają zgodnie z oczekiwaniami.

Monitor QoS może być przydatny w fazie planowania QoS i rozwiązywania problemów dotyczących tej funkcji.

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer. Umożliwia on określenie przyczyn powstawania przeciążeń w sieci. Monitor QoS ułatwia monitorowanie sieci i odpowiednie dopasowanie strategii.

## Planowanie i utrzymywanie wydajności

Jednym z najtrudniejszych etapów w realizacji QoS jest określenie limitów wydajności, które są elementem strategii. Nie zaleca się żadnych konkretnych wartości, ponieważ każda sieć jest inna. Aby wyznaczyć wartości orientacyjne, można skorzystać z monitora jeszcze przed uruchomieniem strategii związanych z działalnością przedsiębiorstwa.

Aby uzyskać charakterystykę ruchu w sieci, można utworzyć strategię usług DiffServ, w której nie wybrano mierzenia. Strategię tę należy włączyć, a następnie uruchomić monitor. Dane pojawiające się w oknie monitora ułatwią dostosowanie strategii do konkretnych potrzeb. Określenie charakterystyki bieżącego ruchu w sieci przedstawia przykładowa strategia monitora.

## Rozwiązywanie problemów z wydajnością

Monitor stosuje się także podczas rozwiązywania problemów. Na podstawie danych wyjściowych monitora można sprawdzić, czy parametry ustawione w strategii są faktycznie realizowane. Jeśli strategie są widoczne w monitorze, ale nie widać ich wpływu na ruch danych, należy

- Sprawdzić, czy opcja FRCA jest włączona i odpowiednio skonfigurowana (jeśli w strategii stosowane jest filtrowanie na podstawie nazw URI). Przed skonfigurowaniem strategii ruchu przychodzącego korzystającej z nazw URI trzeba upewnić się, że port aplikacji przypisany do URI jest taki sam, jak port podany za pomocą dyrektywy Listen FRCA w konfiguracji serwera WWW Apache.
- Sprawdzić harmonogram strategii. Być może monitorowanie wykonano w godzinach, gdy strategia nie jest aktywna.
- Sprawdzić, czy poprawny jest numer portu.
- Sprawdzić, czy poprawny jest adres IP.

Przykładowe dane wyjściowe zawiera sekcja Scenariusze wykorzystania QoS. Pola w oknie monitora opisano natomiast w sekcji Monitorowanie QoS.

### Pojęcia pokrewne

“Planowanie jakości usług” na stronie 48

Najważniejszy etap wprowadzania QoS to planowanie. Aby uzyskać pożądane efekty, należy zrobić przegląd urządzeń dostępnych w danej sieci i uruchomić monitorowanie ruchu.

“Scenariusze” na stronie 28

Niniejsze strategie usługi mogą się okazać przydatne w zrozumieniu celu i sposobu używania usługi QoS.

### Odsyłacze pokrewne

“Monitorowanie QoS” na stronie 56

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez serwer.

### Informacje pokrewne

Zarządzanie adresami i portami serwera HTTP (opartego na Apache)

## Śledzenie aplikacji TCP/IP

Komenda śledzenia QoS umożliwia pracę z funkcjami śledzenia i przeglądanie bieżącego buforu śledzenia.

Aby uruchomić śledzenie na serwerze, w wierszu komend wpisz TRCTCPAPP (Komenda aplikacji śledzenia TCP/IP).

Poniżej pokazano przykładowe wartości jej opcji:

```
Aplikacja TCP/IP .....> *QOS
Ustawienia opcji śledzenia.....> *ON
Maksymalna wielkość pamięci śledzenia.....> *APP
Działanie po zapełnieniu.....> *WRAP
Lista argumentów.....> 'lvl=4'
Typ śledzenia QoS.....> *ALL
```

W poniższej tabeli zebrano możliwe parametry komendy śledzenia. Jeśli ustawienie nie pojawia się na ekranie, należy je podać w komendzie. Na przykład TRCTCPAPP APP(\*QOS) MAXSTG(1000) TRCFULL(\*STOPTRC) ARGLIST('l=4 c=i').

| Ustawienia                               | Opcje   |
|--|---|
| Aplikacja TCP/IP                         | QOS   |
| Ustawienia opcji śledzenia               | *ON, *OFF, *END, *CHK   |
| Maksymalna pamięć dla śledzenia (MAXSTG) | 1-16000, *APP   |
| Działanie po zapełnieniu (TRCFULL)       | *WRAP, *STOPTRC   |
| Lista argumentów (ARGLIST)               | Poziomy: 'lvl=1', 'lvl=2', 'lvl=3', 'lvl=4' Zawartość: 'c=a', 'c=i', 'c=d', 'c=m' |
| Typ śledzenia QoS                        | *ALL  |

## Maksymalna wielkość pamięci dla śledzenia

### 1-16000

Jest to maksymalna wielkość pamięci przeznaczona na dane śledzenia. Po zapełnieniu pamięci śledzenie zostaje zatrzymane lub rozpoczyna się zapisywanie od początku buforu. Wartością domyślną są 4 MB. Aby przyjąć tę wartość, wybierz opcję \*APP.

**\*APP** Jest to opcja domyślna. Oznacza, że aplikacja ma przyjąć wielkość domyślną pamięci śledzenia. W przypadku serwera QoS są to 4 MB.

## Działanie po zapełnieniu

### \*WRAP

Opcja ta powoduje, że po zapełnieniu buforu pamięci dane śledzenia zapisywane są od początku buforu. W ten sposób najstarsze dane są zastępowane nowymi i można kontynuować śledzenie. Jeśli opcja ta nie zostanie wybrana, po zapełnieniu buforu śledzenie zatrzymuje się.

### \*STOPTRC

Opcja ta powoduje zatrzymanie zbierania danych po zapełnieniu buforu.

## Lista argumentów

Opcja ta określa poziomy błędów i rodzaj informacji, które będą zapisywane. W komendzie TRCTCPAPP dopuszczalne są dwa argumenty: poziom śledzenia i zawartość. Podając oba argumenty, należy umieścić je w tym samym cudzysłowie. Na przykład, TRCTCPAPP 'l=4 c=a'

**Uwaga:** Poziomy protokołowania tworzą hierarchię zawierania. Oznacza to, że wybierając określony poziom, wybiera się także wszystkie niższe poziomy. Na przykład wybranie poziomu 3 powoduje automatyczne wybranie poziomów 1 i 2. W przypadku typowego śledzenia zalecane jest wybranie poziomu 'l=4'.

## Poziomy śledzenia

### Poziom 1: Błędy systemowe (SYSERR)

Protokołowane są błędy pojawiające się w operacjach systemowych. W razie wystąpienia błędu tego typu serwer QoS nie może dalej działać. Błąd systemowy może na przykład wystąpić, gdy zabraknie pamięci systemowej lub pojawią się problemy z komunikacją TCP/IP. Jest to poziom domyślny.

### Poziom 2: Błędy obiektów (OBJERR)

Protokołowane są błędy pojawiające się podczas wykonywania programu serwera QoS. Błąd tego typu może na przykład wystąpić, gdy działanie serwera wywoła niespodziewane wyniki. Zazwyczaj jest to poważny błąd, który należy zgłosić pracownikom serwisu.

### Poziom 3: Konkretne zdarzenia (EVENT)

Protokołowane są wszelkie operacje dotyczące QoS. W protokole zdarzeń są na przykład zapisywane komendy i żądania. Wyniki są podobne jak w przypadku funkcji kronikowania QoS.

### Poziom 4: Komunikaty śledzenia (TRACE)

Zapisywane są informacje dotyczące wszystkich transmisji danych do i z serwera QoS. Można to wykorzystać do protokołowania informacji pomocnych w wykrywaniu błędów. Dane w protokole umożliwiają określenie, gdzie wystąpił błąd i jak go odtworzyć.

## Zawartość śledzenia

Należy wybrać jeden typ zawartości. Jeśli nic nie zostanie wybrane, wówczas śledzeniu podlegać będzie cała zawartość.

### Zawartość = Wszystko ('c=a')

Opcja ta określa śledzenie wszystkich funkcji serwera QoS. Jest to wartość domyślna.

### Zawartość = Intserv ('c=i')

Opcja ta określa śledzenie czynności związanych z usługami IntServ. Należy z niej skorzystać, jeśli problem dotyczy właśnie tych usług.

### Zawartość = Diffserv ('c=d')

Opcja ta określa śledzenie czynności związanych z usługami DiffServ. Należy z niej skorzystać, jeśli problem dotyczy właśnie tych usług.

### Zawartość = Monitor ('c=m')

Opcja ta określa śledzenie czynności monitora.

Informacje pomocne w interpretacji danych wyjściowych śledzenia zawiera przykład dotyczący danych wyjściowych śledzenia w serwisie WWW poświęconym wyjściowym danym śledzenia. Zawarte w nim są przykładowe dane wyjściowe opatrzone komentarzem, co pomoże w jego zrozumieniu. Funkcja TRCTCPAPP jest zwykle używana przez pracowników serwisu, więc w przypadku wystąpienia problemów z odczytaniem danych wyjściowych można skontaktować się z przedstawicielem serwisu.

### Odsyłacze pokrewne

Opis komendy TRCTCPAPP (Śledzenie aplikacji TCP/IP - Trace TCP/IP Application)

## Przykłady: Odczytywanie danych wyjściowych śledzenia

W sekcji tej nie omówiono danych wyjściowych śledzenia w sposób wyczerpujący. Wyróżniono jedynie najistotniejsze zdarzenia, na które należy zwracać uwagę podczas przeglądania tych danych.

W przypadku *strategii usług zintegrowanych* najważniejsze jest, czy połączenie RSVP nie zostało odrzucone z powodu braku odpowiedniej strategii. Jeśli połączenie powiodło się, w protokole śledzenia zostanie zapisany komunikat o treści podobnej do przedstawionej poniżej:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Znaleziono nazwę działania
vreStnl_kraMoNICvreStnl dla przepływu[sesja=x.x.x.x:y:z:s, źródło=x.x.x.x:y]
```

Jeśli połączenie nie powiodło się, w protokole zostanie zapisany komunikat o treści podobnej do przedstawionej poniżej:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Nie można znaleźć nazwy działania dla przepływu
[sesja=x.x.x.x:y]
```

W przypadku *strategii usług DiffServ* najważniejsze jest, czy serwer pobrał reguły strategii, czy może wystąpił błąd w pliku konfiguracyjnym strategii.

Przykład:

```
01/11 14:07:52 [376,57] TRCE :..... KernelAddPolicyRule: Installing rule = timed_42ring.
01/11 14:07:52 [376,57] EVNT :..... create_tcp_resv: No value in config file for
DiffServInProfilePeakRate, defaulted to 100000 00.
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: Create resv - bRate: 537395
5722SS1 V5R1M0 010525 TRCTCPAPP Output RS004
Date-01/11/01 Time-14:08:03 Page-6
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: bDepth: 32768
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: peakR: 10000000
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: m: 128
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: M: 41452
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: mark(TOS): a0
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flags: 15
01/11 14:07:52 [376,57] TRCE :.....create_tcp_resv: flowspe.form = 1,
QOS_FORMAT_DS = 1
```

W protokole mogą także wystąpić komunikaty informujące, że znaczniki w pliku konfiguracyjnym strategii były niepoprawne. Poniżej podano przykładowe komunikaty:

```
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Nieznany atrybut %s w StrategiiUsług-Pomijanie.
12/15 11:36:14 [336,80] TRCE :.....rpapi_getPolicyData: Nieznany atrybut %s w Odwzorowaniu
priorytetu-Pomijanie.
```

**Uwaga:** Znak % reprezentuje nieznaną znacznik.

---

## Informacje związane z jakością usług

Znajdują się tu podręczniki IBM Redbooks (w formacie PDF), serwisy WWW, oraz tematy Centrum informacyjnego związane z zagadnieniem Jakości usług. Wszystkie dokumenty w formacie PDF można wyświetlać lub drukować.

## Dokumenty RFC (Request for Comments) usługi QoS

Dokumenty RFC (Requests for Comments) zawierają definicje standardów dotyczących protokołu oraz proponowanych standardów używanych w Internecie. W celu zrozumienia działania QoS i funkcji pokrewnych można zapoznać się z następującymi dokumentami RFC:

- **RFC 1349.**

W dokumencie tym omówiono nową definicję pola typ usługi będącego elementem nagłówka pakietu IP

- **RFC 2205.**

W dokumencie tym wyjaśniono definicję protokołu RSVP (Resource ReSerVation Protocol).



- **RFC 2210.**



W dokumencie tym omówiono sposób wykorzystania protokołu RSVP w przypadku usług zintegrowanych IETF.

- **RFC 2474.**




W dokumencie tym zdefiniowano Pole DS (Differentiated Services Field).

- **RFC 2475.**

W dokumencie tym przedstawiono architekturę usług DiffServ.

Wymienione powyżej dokumenty dostępne są w serwisie Wyszukiwanie dokumentów RFC  znajdujący się w serwisie WWW Edytor RFC .

## Dokumentacja techniczna IBM (Redbooks)

- Podręcznik iSeries IP Networks: Dynamic!  (około 16 589 KB). Jest to najnowsza dokumentacja techniczna (redbook) dotycząca sieci IP. Opisuje sposób zaprojektowania odpornej na błędy, wydajnej sieci IP z możliwością autokonfigurowania. Publikacja ta zawiera opisy wielu funkcji, między innymi omawia teoretyczne podstawy funkcji QoS oraz jej implementację na serwerze iSeries. Można tam znaleźć więcej przykładowych scenariuszy ze szczegółowymi instrukcjami.
- Podręcznik TCP/IP More Cool Things than Ever  (około 10 035 KB). W podręczniku tym przedstawiono scenariusze demonstrujące typowe rozwiązania i konfiguracje protokołu TCP/IP. Podane informacje ułatwiają planowanie, instalowanie, dostosowywanie i konfigurowanie TCP/IP na serwerze iSeries, a także rozwiązywanie problemów. Nie opisano w nim funkcji QoS, zamieszczono jednak informacje na temat serwera katalogów LDAP.
- Podręcznik TCP/IP Tutorial and Technical Overview  (około 7885 KB). Podręcznik ten stanowi wprowadzenie do protokołu TCP/IP. Zawiera także opis zestawu protokołów i aplikacji TCP/IP. Funkcję QoS omówiono w rozdziale 22 w części *Part 3. Advanced concepts and new technologies*.

## Inne informacje

- Usługi katalogowe (LDAP). W tym temacie omówiono konfigurowanie, administrowanie i rozwiązywanie problemów. Zamieszczono również odsyłacze do innych zasobów związanych z konfigurowaniem serwera katalogów.
- Wykrywanie włamań. Niniejszy temat zawiera informacje o próbach włamań i ataków przez sieć TCP/IP. Administratorzy ochrony mogą analizować rekordy kontroli udostępniane przez program wykrywania włamań, czyniąc sieć iSeries odporną na tego typu ataki.



---

## Dodatek. Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji, omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie tej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przysyłać na adres:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokio 106-0032, Japonia

**Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:** INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE (“AS IS”), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŻNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW STRON TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjodawcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N  
Rochester, MN 55901  
USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

- | Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla
- | tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej
- | Umowie Licencyjnej IBM na Program, Licencyjnej Umowie IBM na Kod Maszynowy lub w innych podobnych
- | umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy są fikcyjne i jakiegokolwiek ich podobieństwo do nazwisk, nazw i adresów używanych w rzeczywistych przedsiębiorstwach jest całkowicie przypadkowe.

#### LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Kody te nie zostały kompleksowo przetestowane we wszelkich możliwych warunkach. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia programu przykładowego lub jakiegokolwiek jego fragment, jak też jakiegokolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. (wpisać rok lub lata). Wszelkie prawa zastrzeżone.

Przy przeglądaniu tych informacji w formie elektronicznej, fotografie i ilustracje kolorowe mogą się nie pojawić.

---

## Informacje na temat interfejsu programistycznego

Niniejsza publikacja opisuje planowane interfejsy programistyczne, pozwalające na pisanie programów umożliwiających korzystanie z usług systemu operacyjnego IBM i5/OS.

---

## Znaki towarowe

Następujące nazwy są znakami towarowymi International Business Machines Corporation w Stanach Zjednoczonych i/lub w innych krajach:

- | IBM
- | IBM (logo)
- | iSeries
- | i5/OS
- | Redbooks

Nazwy innych przedsiębiorstw, produktów i usług mogą być znakami towarowymi lub znakami usług innych podmiotów.

---

## Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

**Użytek osobisty:** Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

**Użytek służbowy:** Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ ("AS IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.





**IBM**