



System i  
Praca w sieci  
Jakość usługi (QoS)

*Wersja 6 wydanie 1*







System i  
Praca w sieci  
Jakość usługi (QoS)

*Wersja 6 wydanie 1*

**Uwaga**

Przed skorzystaniem z tych informacji oraz z produktu, którego dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi”, na stronie 69.

To wydanie dotyczy systemu operacyjnego IBM i5/OS (numer produktu 5761-SS1) wersja 6, wydanie 1, modyfikacja 0, a także wszystkich kolejnych wydań i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej. Wersja ta nie działa na wszystkich modelach komputerów z procesorem RISC ani na modelach z procesorem CISC.

© Copyright International Business Machines Corporation 1998, 2008. Wszelkie prawa zastrzeżone.

# Spis treści

## Jakość usługi (QoS) . . . . . 1

Plik PDF z informacjami dotyczącymi usługi QoS . . . . . 1

Pojęcia . . . . . 1

Usługi DiffServ . . . . . 2

Klasy z priorytetami: sposób klasyfikacji ruchu w sieci . . . . . 3

Ustawianie priorytetów: sposób obsługi klas . . . . . 4

Funkcje warunkujące ruch danych . . . . . 5

Usługi zintegrowane . . . . . 6

Funkcje sterujące ruchem danych. . . . . 8

Rodzaje usług zintegrowanych . . . . . 9

Limity dotyczące zasobnika tokenów i limity przepustowości. . . . . 10

Usługi zintegrowane wykorzystujące znakowanie usług DiffServ . . . . . 10

Strategia akceptowania ruchu przychodzącego . . . . . 11

Klasa usług . . . . . 13

Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci . . . . . 14

Limity średniej szybkości połączeń i porcji połączeń 16

Interfejsy API jakości usługi (QoS). . . . . 16

Komunikacja za pomocą funkcji API QoS w trybie z nawiązaniem połączenia . . . . . 19

Komunikacja za pomocą funkcji API QoS w trybie bez nawiązywania połączenia . . . . . 21

Rozszerzenia funkcji API QoS sendmsg(). . . . . 23

Serwer katalogów . . . . . 25

Słowa kluczowe . . . . . 25

Nazwa wyróżniająca . . . . . 26

Scenariusze: strategię QoS . . . . . 28

Scenariusz: ograniczanie ruchu danych do przeglądarki 28

Szczegóły scenariusza: tworzenie strategii usług DiffServ. . . . . 30

Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS. . . . . 31

Szczegóły scenariusza: sprawdzanie poprawnego działania strategii . . . . . 31

Szczegóły scenariusza: zmiana właściwości . . . . . 32

Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług). . . . . 32

Szczegóły scenariusza: konfigurowanie połączenia host-host w sieci VPN . . . . . 34

Szczegóły scenariusza: tworzenie strategii usług DiffServ. . . . . 34

Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS. . . . . 35

Szczegóły scenariusza: sprawdzanie poprawnego działania strategii . . . . . 35

Szczegóły scenariusza: zmiana właściwości . . . . . 36

Scenariusz: ograniczanie połączeń przychodzących . . . . . 36

Szczegóły scenariusza: tworzenie strategii akceptowania ruchu przychodzącego . . . . . 37

Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS. . . . . 38

Szczegóły scenariusza: sprawdzanie poprawnego działania strategii . . . . . 38

Szczegóły scenariusza: zmiana właściwości . . . . . 38

Scenariusz: przewidywalny ruch danych firma-firma (B2B) . . . . . 39

Szczegóły scenariusza: tworzenie strategii usług zintegrowanych . . . . . 41

Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS. . . . . 42

Szczegóły scenariusza: sprawdzanie poprawnego działania strategii . . . . . 42

Szczegóły scenariusza: zmiana właściwości . . . . . 42

Scenariusz: dedykowane dostarczanie (telefonia IP). . . . . 42

Szczegóły scenariusza: tworzenie strategii usług zintegrowanych . . . . . 44

Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS. . . . . 45

Szczegóły scenariusza: sprawdzanie poprawnego działania strategii . . . . . 45

Szczegóły scenariusza: zmiana właściwości . . . . . 46

Scenariusz: monitorowanie bieżących statystyk sieci 46

Szczegóły scenariusza: otwieranie funkcji QoS w programie System i Navigator . . . . . 46

Szczegóły scenariusza: tworzenie strategii usług DiffServ. . . . . 47

Szczegóły scenariusza: kończenie tworzenia klasy usług. . . . . 47

Szczegóły scenariusza: monitorowanie strategii . . . . . 47

Szczegóły scenariusza: zmiana wartości . . . . . 48

Szczegóły scenariusza: ponowne monitorowanie strategii . . . . . 48

Planowanie wprowadzenia usługi QoS. . . . . 48

Wymagania dotyczące uprawnień . . . . . 48

Wymagania systemowe . . . . . 49

Umowa dotycząca poziomu usług . . . . . 49

Sprzęt i oprogramowanie sieciowe . . . . . 50

Konfigurowanie usługi QoS . . . . . 51

Konfigurowanie usługi QoS za pomocą kreatorów . . . . . 52

Konfigurowanie serwera katalogów . . . . . 53

Definiowanie kolejności strategii QoS . . . . . 54

Zarządzanie usługą QoS . . . . . 55

Korzystanie z pomocy dotyczącej usługi QoS w programie System i Navigator . . . . . 55

Składowanie strategii QoS . . . . . 55

Kopiowanie istniejącej strategii . . . . . 56

Edytowanie strategii QoS . . . . . 56

Monitorowanie usługi QoS . . . . . 57

Rozwiązywanie problemów z usługą QoS. . . . . 61

Kronikowanie strategii QoS . . . . . 62

Wyświetlanie pozycji kroniki na ekranie . . . . . 62

Przeglądanie pozycji kroniki za pośrednictwem zbioru wyjściowego . . . . . 62

Protokołowanie zadań serwera QoS . . . . . 63

Monitorowanie transakcji w systemie . . . . . 64

Śledzenie aplikacji TCP/IP . . . . . 64

Przykłady: odczytywanie danych wyjściowych śledzenia . . . . . 66

Informacje pokrewne dotyczące usługi QoS . . . . . 67

**Dodatek. Uwagi . . . . . 69**  
Informacje dotyczące interfejsu programistycznego . . . . 71

Znaki towarowe . . . . . 71  
Warunki. . . . . 71

---

## Jakość usługi (QoS)

Rozwiązanie QoS w systemie i5/OS pozwala na stosowanie 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. Ważne jest, aby w trakcie prezentacji aplikacja miała większą wydajność niż pozostałe.

Priorytet pakietów jest istotny, gdy aplikacje wymagają przewidywalnych i niezawodnych połączeń, tak jak na przykład aplikacje multimedialne. Strategie QoS umożliwiają zarządzanie priorytetami pakietów, a dodatkowo również limitowanie danych opuszczających system, zarządzanie żądaniami połączeń oraz sterowanie obciążeniem systemu. Serwer usług QoS musi być uruchomiony w celu aktywowania strategii wykrywania włamań.

---

## Plik PDF z informacjami dotyczącymi usługi QoS

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

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

### Zapisywanie plików PDF

Aby zapisać plik PDF na stacji roboczej w celu jego wyświetlenia lub wydrukowania, wykonaj następujące czynności:

1. Kliknij prawym przyciskiem myszy odsyłacz do pliku PDF w przeglądarce.
2. Kliknij opcję zapisania pliku PDF lokalnie.
3. Przejdź do katalogu, w którym ma zostać zapisany plik PDF.
4. Kliknij opcję **Zapisz**.

### Pobieranie programu Adobe Reader

Do przeglądania i drukowania plików PDF potrzebny jest program Adobe Reader. Bezpłatną kopię tego programu można pobrać z serwisu WWW firmy Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html)) .

#### Odsyłacze pokrewne

“Informacje pokrewne dotyczące usługi QoS” na stronie 67

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego.

Wszystkie pliki PDF można wyświetlić lub wydrukować.

---

## Pojęcia

Przed rozpoczęciem pracy z usługą QoS należy poznać podstawową terminologię i pojęcia związane z jakością usługi. Zrozumienie tych pojęć pomoże określić, czy dana usługa odpowiada potrzebom.

Wprowadzanie usługi QoS polega na konfigurowaniu strategii za pomocą kreatorów dostępnych w programie System i Navigator. *Strategia* to zestaw reguł opisujących pewne działania. Ogólnie rzecz ujmując, strategia określa, jaki poziom usług powinien otrzymać wskazany klient, aplikacja lub harmonogram. Można definiować strategie następujących typów:

- Usługi DiffServ
- Usługi zintegrowane

- Akceptacja ruchu przychodzącego

*Usługi DiffServ i usługi zintegrowane* to strategie kontroli przepustowości ruchu wychodzącego. Strategie ruchu wychodzącego ograniczają ruch danych opuszczających sieć i pomagają kontrolować obciążenie systemu. Szybkości ustalone w ramach strategii ruchu wychodzącego określają, które dane podlegają ograniczeniom systemu i jakie to są ograniczenia. W przypadku obu typów strategii dotyczących ruchu wychodzącego może być konieczne zawarcie z dostawcą usług internetowych (ISP) odpowiedniej umowy dotyczącej poziomu usług.

*Strategie akceptowania ruchu przychodzącego* kontrolują żądania połączenia przychodzące do sieci ze źródeł zewnętrznych. Strategie ruchu przychodzącego nie są zależne od poziomu usług zapewnianego przez dostawcę ISP. Decyzję o wyborze strategii należy podjąć na podstawie oceny powodów wprowadzenia QoS oraz roli używanego systemu.

Jednym z najważniejszych elementów w realizacji usługi QoS jest sam system operacyjny. Należy nie tylko zrozumieć pojęcia związane z usługą QoS, lecz również zdawać sobie sprawę z roli, jaką w ich realizacji odgrywa system operacyjny. System operacyjny i5/OS może pełnić wyłącznie funkcje klienta lub serwera, ale nie routera. Na przykład system operacyjny funkcjonujący jako klient może stosować strategię usług DiffServ, aby zapewnić wyższy priorytet przekazywanym do innych systemów w sieci żądaniom przesłania danych. Gdy system pracuje jako serwer, może on stosować strategię akceptowania ruchu przychodzącego w celu ograniczania zakresu akceptowanych żądań URI.

#### **Pojęcia pokrewne**

“Umowa dotycząca poziomu usług” na stronie 49

Temat ten ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

#### **Odsyłacze pokrewne**

“Informacje pokrewne dotyczące usługi QoS” na stronie 67

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

## **Usługi DiffServ**

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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 23

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 wydajności umożliwiają zagwarantowanie dostarczenia pakietów w strategiach ruchu wychodzącego, zarówno w przypadku strategii usług zintegrowanych, jak 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.

#### **Odsyłacze pokrewne**



“Zastosowanie punktów kodowych do określania charakterystyk w ramach segmentu sieci” na stronie 14  
W usłudze QoS charakterystykę w ramach segmentu sieci określa się za pomocą sugerowanych punktów kodowych.

“Konfigurowanie usługi QoS za pomocą kreatorów” na stronie 52

Do konfigurowania strategii jakości usługi (QoS) należy używać kreatorów QoS dostępnych w programie System i Navigator.

### Informacje pokrewne

Zarządzanie adresami i portami serwera HTTP (opartego na Apache)

## Klasy z priorytetami: sposób klasyfikacji ruchu w sieci

Ruch w sieci jest w przypadku usług DiffServ identyfikowany według klas. 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.

Bardziej zaawansowaną klasyfikację można wprowadzić poprzez ustawianie różnych poziomów usług dla danych wybranych aplikacji uruchamianych w systemie i5/OS. Używanie danych aplikacji jest opcjonalne, ale może być przydatne, gdy potrzebna jest klasyfikacja na niższym poziomie. Istnieją dwa typy danych aplikacji: token aplikacji i identyfikator URI (Uniform Resource Identifier). Jeśli dane przesyłane w sieci pasują do tokenu lub identyfikatora URI określonego w strategii, strategia ta zostanie zastosowana do wychodzącej odpowiedzi. W ten sposób wychodzące dane uzyskują priorytet określony w danej strategii usług DiffServ.

## Używanie tokenu aplikacji w strategiach usług DiffServ

Wykorzystanie danych aplikacji pozwala uwzględnić w stosowaniu strategii konkretne parametry (token i priorytet) przekazane przez aplikację do systemu operacyjnego na 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**. Token i priorytet aplikacji mogą być porównywane z ustawieniami tokenu i priorytetu w strategii ruchu wychodzącego. Ustawienie danych aplikacji w strategii składa się z dwóch części: tokenu i priorytetu.

- Co to jest token aplikacji?

*Token aplikacji* to dowolny łańcuch znaków reprezentujący określony zasób, na przykład mojeFTP. Token podany w strategii QoS jest porównywany z tokenem aplikacji zewnętrznej. Aplikacja przekazuje 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. Zostanie otwarte okno Nowy URI (New 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 wychodzącą. Aplikacja przekazuje 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 token aplikacji jest podawany jako typ danych aplikacji, w kodzie aplikacji dostarczającym te informacje do systemu należy wykorzystać funkcję API sendmsg(). Jest to zadanie programisty aplikacji. W dokumentacji aplikacji należy zamieścić poprawne wartości (token i priorytet), które administrator usługi 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.

## Używanie nazwy URI w strategii usług DiffServ

Podczas tworzenia strategii usług DiffServ za pomocą kreatora można podawać informacje dotyczące danych systemu, zgodnie z opisem w sekcji "Używanie 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 sprawdzanie zgodności z konkretną nazwą URI zdefiniowaną w strategii 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 URI należy się upewnić, że port aplikacji przypisany do nazwy URI jest taki sam, jak port określony w dyrektywie Listen akceleratora pamięci podręcznej (fast response cache accelerator - FRCA) w konfiguracji serwera WWW Apache. Informacje na temat sprawdzenia i zmiany portu używanego przez serwer HTTP można znaleźć w temacie *Manage addresses and ports for HTTP Server*

(powered by 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 określonej przez akcelerator FRCA będzie stosowana do wszystkich żądań dotyczących danej nazwy URI.

### Pojęcia pokrewne

"Rozszerzenia funkcji API QoS `sendmsg()`" na stronie 23

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.

System identyfikuje poziom usług odpowiadający pakietowi na podstawie nagłówka IP. 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 1349 i w systemie operacyjnym OS/400 w wersji V5R1.

*Zachowanie w ramach segmentu sieci* określa sposób przekazywania pakietu w określonym węźle sieci. Dane te mają postać liczby zwanej *punktem kodowym*. Pakiety mogą być znakowane w systemie operacyjnym 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 temat "Funkcje warunkujące ruch danych" na stronie 5.

Jeśli pakiet przechodzi przez router lub przełącznik, który nie obsługuje usług DiffServ, traci on w tym momencie swój poziom usług. Pakiet jest wprawdzie przekazywany dalej, lecz jego dostarczenie do węzła końcowego może się opóźnić. Można na swoim systemie skorzystać z predefiniowanych punktów kodowych zachowania w ramach segmentu sieci lub zdefiniować własne punkty kodowe. Nie zaleca się tworzenia własnych punktów kodowych, jeśli

będą one używane poza siecią prywatną. Jeśli nie masz pewności, które punkty kodowe należy przypisać, zapoznaj się z tematem “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 służą też do ograniczania ruchu danych opuszczających system. W praktyce oznacza to, że system korzysta z usług DiffServ w celu ograniczania wydajności. Ograniczenie wydajności mniej ważnych aplikacji umożliwia danym pochodzącym z aplikacji o niewalczym znaczeniu wcześniejsze opuszczenie sieci prywatnej. Podczas tworzenia klasy usług dla takiej strategii należy określić szereg limitów systemowych. Limity wydajności obejmują wielkość zasobników tokenów, limity szybkości szczytowej i limity szybkości średniej. Szczegółowe informacje o tych limitach można znaleźć w tematach pomocy programu System i Navigator dotyczących usług QoS.

## 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, jest ono uznawane za urządzenie obsługujące usługi DiffServ.

**Uwaga:** Opisane wymagania sprzętowe dotyczą nie tylko produktów System i. Terminy te nie występują w interfejsie QoS, ponieważ system 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. Przed zaimplementowaniem strategii należy się zapoznać z ogólnymi pojęciami i wymaganiami wstępnymi usługi QoS.

Na poniższym rysunku przedstawiono schemat współpracy poszczególnych funkcji.



Rysunek 1. Funkcje warunkujące ruch danych

Oto bardziej szczegółowy opis funkcji warunkujących ruch danych:

### Funkcje klasyfikujące

Funkcje klasyfikujące wybierają pakiety ze strumienia danych na podstawie treści nagłówka IP pakietu. W systemie operacyjnym i5/OS zdefiniowane są dwa typy funkcji klasyfikujących. Funkcje agregacji charakterystyki (behavior aggregate) klasyfikują pakiety wyłącznie na podstawie punktu kodowego usług DiffServ. Funkcje klasyfikacji wielopolowej (multi-field classifier) klasyfikują pakiety na podstawie jednego lub kilku pól nagłówka, takich jak na przykład adres źródłowy, adres docelowy, pole usług DiffServ, identyfikator protokołu, numer portu źródłowego, URI, typ serwera czy numer portu docelowego.

### Funkcje mierzące

Zadaniem funkcji mierzących ruch jest sprawdzanie, czy pakiety IP przekazywane przez funkcje klasyfikujące są zgodne z profilem nagłówków IP ruchu w sieci. Dane w nagłówku IP są określane na podstawie wartości

zdefiniowanych w strategii QoS dla danego typu ruchu. 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 funkcji znakujących pakietu polega na ustawieniu wartości pola usług DiffServ. W zależności od konfiguracji funkcji znakujących, pakietom może być przypisywany 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 wypełnieniu 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.

## **Usługi zintegrowane**

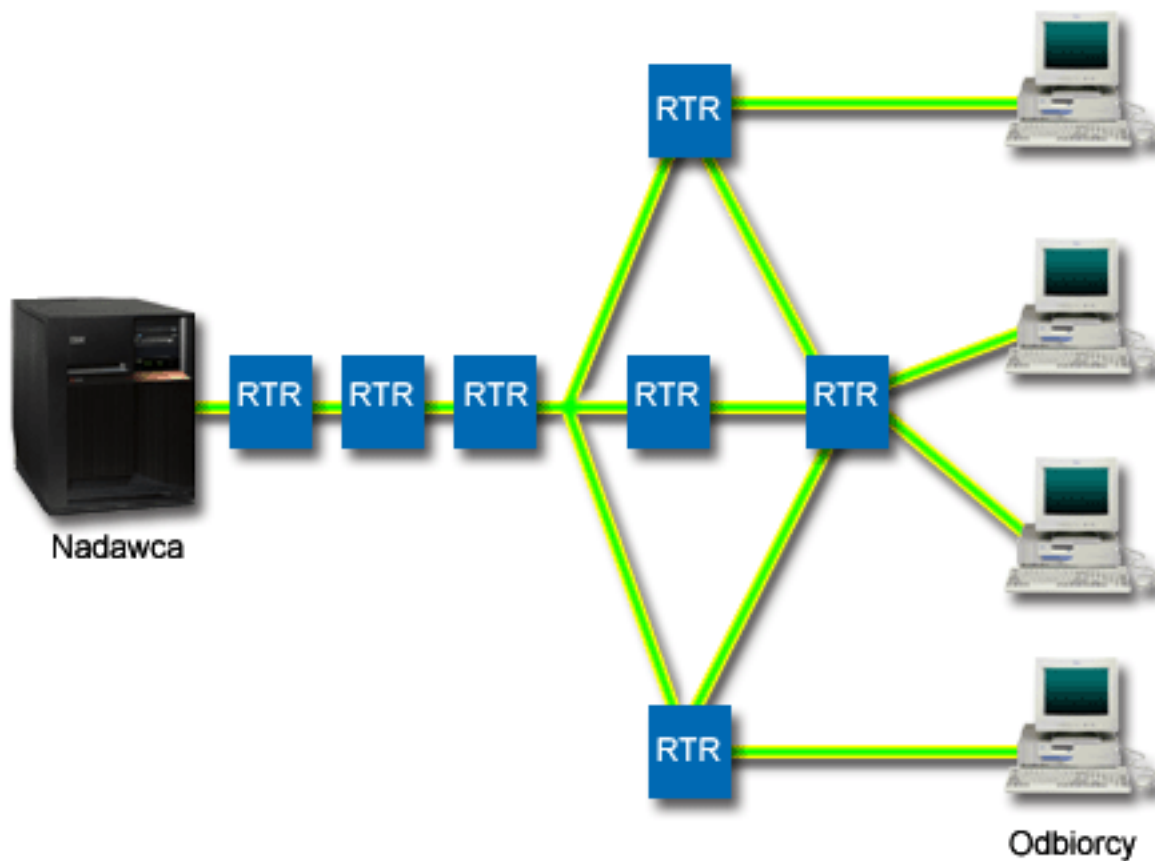
Drugim z dostępnych typów strategii pasma połączeń wychodzących jest strategia usług zintegrowanych. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API usługi QoS.

Strategie usług zintegrowanych korzystają z protokołu RSVP oraz funkcji API tego protokołu (RAPI) lub funkcji API gniazd qtoq, aby zagwarantować określoną jakość połączenia na całej trasie. Jest to najwyższy poziom usług, jaki można określić, ale zarazem 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 działanie. 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 usług zintegrowanych. 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 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 pożądany 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 pożądanej przepustowości. Poniższy rysunek obrazuje sposób funkcjonowania usług zintegrowanych.



Rysunek 2. Ścieżka RSVP między klientem a serwerem

Aplikacja obsługująca protokół RSVP uruchomiona na serwerze, oznaczona na powyższym rysunku jako nadawca, nasłuchuje żądań połączenia od klientów (odbiorców). Po odebraniu żądania aplikacja wysyła do klienta komendę PATH. Komenda ta wydawana jest za pomocą funkcji API RAPI lub funkcji API gniazd QoS qtoq i zawiera dane o adresach IP routerów (RTR). Komenda PATH zawiera także dane o dostępnych zasobach serwera i poszczególnych routerów na trasie, jak również dane o trasach między serwerem a klientem. Aplikacja obsługująca protokół RSVP uruchomiona na komputerze klienta odsyła ścieżką sieciową 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 używane w ramach strategii usług zintegrowanych muszą obsługiwać protokół RSVP. Sam system operacyjny i5/OS nie ma żadnych aplikacji obsługujących protokół RSVP, więc aby korzystać z protokołu RSVP należy dostarczyć aplikację go obsługującą.

Dla każdego przychodzącego pakietu system operacyjny ustala, czy dysponuje odpowiednimi zasobami, aby ten pakiet przesłać dalej. Decyzja zależy od wielkości wolnego miejsca w zasobniku tokenów. Administrator ręcznie ustawia maksymalną liczbę bitów w zasobniku tokenów, ewentualne limity przepustowości, limity szybkości tokenów oraz

maksymalną liczbę połączeń akceptowaną przez system. Wartości te nazywa się limitami wydajności. Jeśli pakiety nie powodują naruszenia limitów, są one uznawane za zgodne i wysyłane. W przypadku usług zintegrowanych każde połączenie uzyskuje własny zasobnik tokenów.

## Usługi zintegrowane wykorzystujące znakowanie usług DiffServ

Strategię usług zintegrowanych można utworzyć nawet jeśli nie ma pewności, czy połączenia RSVP są zagwarantowane w całej sieci. Jeśli jednak 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 pozwoli podjąć próbę nadania połączeniu pewnego priorytetu, nawet jeśli połączenie nie jest gwarantowane.

### Pojęcia pokrewne

“Interfejsy API jakości usługi (QoS)” na stronie 16

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazd qtoq, API sendmsg() i API monitorowania.

“Usługi zintegrowane wykorzystujące znakowanie usług DiffServ” na stronie 10

W tym temacie opisano korzystanie ze znakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu pakietów wysyłanych w środowisku mieszanym.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 39

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

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

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa typy strategii usług zintegrowanych: usługi gwarantowane i usługi sterowanego przeciążenia. 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 produktów System i.

Terminy te nie występują w interfejsie QoS, ponieważ serwer nie może sterować sprzętem zewnętrznym. Sprzęt poza siecią prywatną musi mieć możliwość obsłużenia ogólnych wymagań usługi QoS. W następnej sekcji omówiono ogólne wymagania względem routerów w zakresie strategii usług zintegrowanych. Przed zaimplementowaniem strategii zalecane jest zapoznanie się z ogólnymi pojęciami i wymaganiami wstępnymi QoS.

Aby uzyskać planowane wyniki, na całej trasie ruchu danych muszą być używane urządzenia obsługujące protokół RSVP. Obsługa protokołu RSVP wymaga, aby routery udostępniały określone funkcje sterujące ruchem w sieci. Jest to często określane mianem obsługi protokołu RSVP lub obsługi QoS. Należy pamiętać, że system operacyjny może pełnić jedynie funkcje klienta lub serwera. Nie można go natomiast wykorzystać jako routera. W dokumentacji urządzeń sieciowych należy sprawdzić, czy spełniają one wymagania usługi QoS.

Wyróżnia się między innymi następujące funkcje sterujące ruchem danych:

### Funkcja planująca pakiety

Funkcja planująca pakiety zarządza przekazywaniem pakietów na podstawie danych umieszczonych w nagłówku IP. Zadaniem funkcji planującej pakiety jest zapewnienie zgodności dostarczania pakietów z parametrami określonymi w strategii. Funkcja planująca umieszczona jest w tym miejscu, w którym istnieje kolejka pakietów.

### Funkcja klasyfikująca pakiety

Funkcja klasyfikująca pakiety określa na podstawie informacji zawartych w nagłówku IP, które pakiety strumienia danych IP mają otrzymać określony poziom usług. Każdy napływający pakiet jest zaliczany do pewnej klasy. Pakiety umieszczone w tej samej klasie są traktowane jednakowo. Poziom usług jest określany na podstawie informacji podanych w strategii.

## **Funkcje sterowania dostępem**

Sterowanie dostępem udostępnia algorytm decyzyjny umożliwiający routerowi określenie, czy wystarczy zasobów routingu na zapewnienie poziomu usług żadanego dla nowego strumienia danych. 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**

“Interfejsy API jakości usługi (QoS)” na stronie 16

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazd qtoq, API sendmsg() i API monitorowania.

### **Odsyłacze pokrewne**

“Informacje pokrewne dotyczące usługi QoS” na stronie 67

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

## **Rodzaje usług zintegrowanych**

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

### **Usługi sterowanego przeciążenia**

Usługi sterowanego przeciążenia 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 przeciążenia, jej wydajność nie spadnie po zwiększeniu się obciążenia sieci. Zostanie zapewniony poziom transmisji danych niemal taki, jak w normalnych warunkach przy niewielkim obciążeniu sieci.

Routerzy muszą zapewniać usłudze sterowanego przeciążenia odpowiednią przepustowość i zasoby konieczne do przetwarzania pakietów. W tym celu muszą one obsługiwać usługę QoS oraz usługi zintegrowane. Należy sprawdzić w specyfikacji routera, czy udostępnia on usługę QoS z wykorzystaniem 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 kolejkowania pakietów, dzięki czemu opóźnienie pakietów nie przekracza określonego czasu. 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 39

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

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

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa typy strategii usług zintegrowanych: usługi gwarantowane i usługi sterowanego przeciążenia. 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 wydajności umożliwiają zagwarantowanie dostarczenia pakietów w strategiach ruchu wychodzącego, zarówno w przypadku strategii usług zintegrowanych, jak i strategii usług DiffServ.

### Wielkość zasobnika tokenów

*Wielkość zasobnika tokenów* określa ilość informacji, jaką system może w danej chwili przetworzyć. Jeśli aplikacja przesyła dane do systemu szybciej, niż ten może przesyłać dane do sieci, następuje zapełnienie buforu. Wszelkie pakiety danych przekraczające ten limit są traktowane jako spoza profilu. Wyjątek stanowią strategie usług zintegrowanych. Można wybrać opcję brak ograniczeń (do not limit), co umożliwi przyjmowanie żądań 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 do sieci. Żądana przepustowość porównywana jest z limitami szybkości i przepływu określonymi w strategii QoS. System odrzuca żądanie, jeśli spowodowałoby ono przekroczenie jego limitów. Limit szybkości tokenów używany jest jedynie do kontroli dostępu w ramach strategii usług zintegrowanych. Wartość limitu może wynosić od 10 kb/s do 1 Gb/s. Można również ustawić wartość brak ograniczeń (do not limit). Przy ustawieniu brak ograniczeń jedynym ograniczeniem szybkości będą możliwości sprzętu.

**Wskazówka:** Aby określić właściwe limity, można skorzystać z monitora. W tym celu należy utworzyć strategię, w której zagregowany limit szybkości tokenów jest na tyle duży, aby można było obsłużyć większość ruchu danych w sieci. 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

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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

Podczas korzystania z kreatorów należy ustawić ograniczenia wydajności odpowiadające indywidualnym wymaganiom obsługi sieci.

## Usługi zintegrowane wykorzystujące znakowanie usług DiffServ

W tym temacie opisano korzystanie ze znakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu pakietów wysyłanych w środowisku mieszanym.

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 jakość usługi.

Aby nieco złagodzić ten problem, w strategii usług zintegrowanych można skorzystać z oznakowania stosowanego w usługach DiffServ. Jeśli dane o określonej strategii docierają do routera nieobsługującego protokołu RSVP, nadal zachowują pewien priorytet. Dodawane znakowanie nazywa się *zachowaniem w ramach segmentu sieci* (per-hop behavior).



## Brak sygnalizacji

Oprócz oznakowania można używać także funkcji braku sygnalizacji (no signal). Gdy ta funkcja jest wybrana, dostępne są wersje funkcji API bez sygnalizacji, które pozwalają tworzyć aplikacje ładujące reguły RSVP w systemie operacyjnym. Aplikacja wymaga obsługi protokołu RSVP tylko po stronie serwera połączenia TCP/IP. 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 System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz **Konfiguracja**.
3. Rozwiń **Strategie połączeń wychodzących** → **Właściwości usług zintegrowanych**.
4. Kliknij prawym przyciskiem myszy nazwę odpowiedniej strategii usług zintegrowanych i wybierz opcję **Właściwości** (Properties). 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.

"Usługi zintegrowane" na stronie 6

Drugim z dostępnych typów strategii pasma połączeń wychodzących jest strategia usług zintegrowanych. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API usługi QoS.

## Strategia akceptowania ruchu przychodzącego

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

Strategia ruchu przychodzącego służy do ograniczania ruchu danych związanych z próbami połączenia z systemem. Dostęp można ograniczać na podstawie klienta, nazwy URI, aplikacji lub lokalnego interfejsu systemu. Można ponadto poprawić wydajność systemu, określając dla ruchu przychodzącego klasę usług. Do definiowania tej strategii służy Kreator akceptacji nowych połączeń przychodzących (Inbound Admission wizard) w programie System i Navigator.

Poniżej przedstawiono trzy komponenty strategii ruchu przychodzącego, które wymagają dodatkowych informacji. 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 zawierają tematy "Zasób URI", "Szybkość połączeń" na stronie 12 i "Wagi kolejek priorytetowych" na stronie 12.

### Zasób URI

Strategii 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 nazw URI umożliwia kontrolowanie dostępu przy użyciu informacji z poziomu aplikacji w celu ograniczenia liczby akceptowanych przez serwer żądań dostępu do nazwy URI. Rozwiązanie to jest również w branży znane pod nazwą kontroli połączeń na podstawie nagłówków. Wykorzystuje ono nazwy URI do określenia priorytetów żądań.

W strategiach wykorzystujących nazwy URI sprawdzane są nie tylko nagłówki pakietów, ale także ich zawartość. Sprawdzona zawartość stanowi nazwę URI. W przypadku systemu operacyjnego i5/OS można stosować względne nazwy URI, na przykład /produkty/ubrania).

## Względna nazwa URI

Względna nazwa URI jest w rzeczywistości podzbiorem bezwzględnej nazwy URI (przypominającej bezwzględny adres 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:

- W przypadku korzystania z nazw 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.
- Do nazwy URI automatycznie dodawany jest niejawny znak wieloznaczny. Na przykład nazwa `/software` obejmuje całą zawartość katalogu `software`.
- Podczas definiowania nazw URI nie należy używać znaku `*`. Ten znak nie jest poprawny.
- Informacje o nazwach URI można wykorzystywać w strategiach ruchu przychodzącego lub w strategii usług DiffServ (ruchu wychodzącego).

Przed skonfigurowaniem strategii połączeń przychodzących korzystającej z nazw URI należy się upewnić, że port aplikacji przypisany do nazwy URI jest taki sam, jak port określony w dyrektywie Listen akceleratora pamięci podręcznej (Fast Response Cache Accelerator - FRCA) w konfiguracji serwera WWW Apache. Informacje na temat sposobu zmiany lub wyświetlenia portu serwera HTTP zawiera temat Zarządzanie adresami i portami serwera HTTP opartego na serwerze Apache.

## Szybkość połączeń

Podczas tworzenia strategii akceptowania ruchu przychodzącego trzeba wybrać klasę usług. Klasa usług określa szybkości połączeń, co umożliwia kontrolowanie dostępu w celu ograniczenia liczby połączeń akceptowanych przez system.

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 średniej i limit porcji. Obie te wartości można ustawić za pomocą kreatorów programu System i Navigator. Kiedy żądanie połączenia przychodzącego dociera do systemu, 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. W programie System i Navigator można podczas uzupełniania strategii skorzystać z pomocy, aby uzyskać podobne informacje.

## 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 są obsługiwane w porządku zgodnym z priorytetem kolejki (wysoki, średni, niski lub najlepszy możliwy). 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 Najlepszy możliwy (5). Wśród zaakceptowanych połączeń będzie:

- 50% połączeń o wysokim priorytecie

- 30% połączeń o średnim priorytecie
- 15% połączeń o niskim priorytecie
- 5% połączeń o najlepszym możliwym priorytecie

### 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

Ustawienia szybkości połączeń i porcji połączeń to limity szybkości. Limity takie umożliwiają ograniczanie połączeń przychodzących do systemu. Limity szybkości ustawia się dla klasy 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 grupowania ruchu danych. Podział na grupy i ich priorytet określa administrator, za resztę obsługi odpowiada sprzęt.

Pierwszym etapem realizacji usługi 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

Usługa QoS określa charakterystykę ruchu w ramach segmentu sieci na podstawie sugerowanych punktów kodowych. Routery i przełączniki na podstawie punktów kodowych wyznaczają priorytet ruchu danych. System nie może używać takich punktów kodowych, ponieważ nie funkcjonuje on 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 dla uzyskania oczekiwanych wyników jest utrzymanie spójności znakowania. Punkty kodowe są kluczowym elementem procesu rozróżniania poszczególnych klas ruchu danych.

### Pomiar ruchu

Usługa 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. Na podstawie informacji opisujących klasę usług system ustala, czy należy odrzucać pakiety UDP i zmniejszać okno zapełnienia TCP, czy też kształtować lub ponownie znakować pakiety spoza profilu.

Porzucanie pakietów UDP lub zmniejszenie okna zapełnienia TCP: jeśli wybrane zostanie odrzucanie i dopasowywanie pakietów spoza profilu, pakiety UDP będą odrzucane. Okno zapełnienia TCP zostanie natomiast zmniejszone, tak aby szybkość transmisji była zgodna z szybkością zasobnika tokenów. Następuje zmniejszenie liczby pakietów, które mogą być wysyłane do sieci w określonym czasie, a tym samym ograniczenie zapełnienia ruchu w sieci.

Opóźnienie (kształtowanie): jeśli zostanie wybrane opóźnianie pakietów spoza profilu, zostaną one zmodyfikowane w celu uzyskania zgodności z zadaną charakterystyką obsługi.

Ponowne zaznaczenie punktem kodowym DiffServ: jeśli pakiety spoza profilu zostaną wybrane do ponownego oznakowania za pomocą punktu kodowego, zostanie im przypisany nowy punkt kodowy. 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 systemem realizowanym za pomocą różnych strategii akceptowania ruchu przychodzącego można nadawać różne priorytety. Pozwala to na określenie kolejności obsługiwanego nawiązanych połączeń przez system. Możliwe wartości priorytetu to: wysoki, średni, niski i najlepszy możliwy.

#### **Pojęcia pokrewne**

“Usługi zintegrowane wykorzystujące znakowanie usług DiffServ” na stronie 10

W tym temacie opisano korzystanie ze znakowania usług DiffServ w strategii usług zintegrowanych w celu utrzymania priorytetu pakietów wysyłanych w środowisku mieszanym.

“Strategia akceptowania ruchu przychodzącego” na stronie 11

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

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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 usłudze QoS charakterystykę w ramach segmentu sieci określa się za pomocą sugerowanych punktów kodowych.

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

W usłudze QoS charakterystykę w ramach segmentu sieci określa się za pomocą sugerowanych punktów kodowych.

W kreatorze klasy usług należy określić stosowaną w strategii charakterystykę w ramach segmentu sieci. 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 pożądanego wyniku. 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 strategie testowe, uruchomić monitor i na podstawie obserwowanych wyników odpowiednio dostosować ustawienia.

W poniższej tabeli przedstawione są zalecane punkty kodowe, oparte na standardach branżowych. 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. Sugerowane punkty kodowe: przyspieszone przekazywanie*

<b>Przyspieszone przekazywanie</b>
101110

**Uwaga:** Przyspieszone przekazywanie wiąże się zwykle 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. Sugerowane punkty kodowe: selektor klasy*

<b>Selektor klasy</b>
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 w ramach segmentu sieci, z których każda ma trzy poziomy odrzucania: niski, średni i wysoki. Poziomy odrzucania określa prawdopodobieństwo odrzucania 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 odrzucania pakietów jest najniższe w obrębie danej klasy.

*Tabela 3. Sugerowane 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

Tabela 3. Sugerowane punkty kodowe: zapewnione przekazywanie (kontynuacja)

<b>Zapewnione przekazywanie</b>
Zapewnione przekazywanie, Klasa 4, Średni - 100100
Zapewnione przekazywanie, Klasa 4, Wysoki - 100110

### Pojęcia pokrewne

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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

Ustawienia szybkości połączeń i porcji połączeń to limity szybkości. Limity takie umożliwiają ograniczanie połączeń przychodzących do systemu. Limity szybkości ustawia się dla klasy usług używanej wraz ze strategiami akceptowania ruchu przychodzącego.

### Porcje połączeń

Od wielkości porcji połączeń zależy pojemność buforu przechowującego porcje połączeń (jednoczesne żądania połączenia). Porcje połączeń mogą napływać do serwera w tempie przekraczającym możliwości serwera lub założenia administracyjne. 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 systemu poprzez nazwę URI. System odrzuca żądania, których obsłużenie spowodowałoby przekroczenie określonych wcześniej limitów. Limit szybkości średniej połączeń określa liczbę połączeń na sekundę.

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

Aby zamiast określonej kolekcji danych przeglądać dane zbierane przez monitor w czasie rzeczywistym, 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 żadaniami połączeń przychodzącymi do sieci.

“Scenariusz: monitorowanie bieżących statystyk sieci” na stronie 46

Podczas korzystania z kreatorów należy ustawić ograniczenia wydajności odpowiadające indywidualnym wymaganiom obsługi sieci.

## Interfejsy API jakości usługi (QoS)

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazd qtoq, API sendmsg() i API monitorowania.

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 podczas pracy z monitorem QoS:

- “Funkcje API dotyczące usług zintegrowanych” na stronie 17

- “Funkcje API dotyczące usług DiffServ”
- “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 zapewnia obsługę danych określoną w rezerwacji.

Protokół RSVP jest prosty z tego względu, że rezerwacje dokonywane są 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. Ponieważ sam system nie zawiera aplikacji obsługujących protokół RSVP, odpowiednie aplikacje należy przygotować we własnym zakresie, korzystając z funkcji API RAPI lub funkcji API gniazd QoS qtoq. Pozwoli to aplikacjom korzystać z protokołu RSVP. Szczegółowe wyjaśnienia dotyczące stosowanych modeli, ich działania i obsługi komunikatów można znaleźć w wielu dostępnych źródłach. Potrzebna jest gruntowna znajomość protokołu RSVP i dokumentu RFC 2205.

### Funkcje API gniazd qtoq

Wprowadzenie obsługi protokołu RSVP w systemie jest łatwiejsze przy użyciu funkcji API gniazd QoS 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 “bez sygnalizacji” (no-signal) funkcji API umożliwiają utworzenie:

- aplikacji ładującej do systemu 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.

Przykłady typowych wywołań funkcji API QoS dla aplikacji lub protokołu opartego na gniazdach QoS qtoq z połączeniem lub bez połączenia można znaleźć odpowiednio w sekcjach Komunikacja za pomocą funkcji API QoS w trybie z nawiązaniem połączenia lub 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 definiowany jest konkretny token aplikacji. Podczas tworzenia strategii usług DiffServ można (opcjonalnie) podać parametry aplikacji (token i priorytet). Parametry te są używane podczas definiowania zaawansowanych strategii, więc jeśli nie są one potrzebne, można je pominąć. Należy jednak pamiętać, że routery i inne systemy w sieci nadal 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 (token i priorytet), które administrator QoS powinien podać 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 systemu: 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 dostarczonym przez aplikację wychodzącą. Aplikacja przekazuje 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 przekazuje 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 będzie nadal otrzymywał priorytet nadany całej strategii.

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

## **Funkcje API dotyczące monitorowania**

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

- Funkcja *QgyOpenListQoSMonitorData* (Otwieranie listy danych monitora QoS) zbiera informacje dotyczące 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 dotyczących usług QoS.
- Funkcja *QtoqListSavedQoSMonitorData* (Wykaz 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 QoS do późniejszego wykorzystania.
- Funkcja *QtoqStartQoSMonitor* (Uruchomienie monitora QoS) zbiera informacje dotyczące usług QoS.

### **Pojęcia pokrewne**

“Usługi zintegrowane” na stronie 6

Drugim z dostępnych typów strategii pasma połączeń wychodzących jest strategia usług zintegrowanych. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API usługi QoS.

“Funkcje sterujące ruchem danych” na stronie 8

Funkcje sterujące ruchem danych stosowane są tylko w usługach zintegrowanych i nie są specyficzne dla produktów System i.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 39

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

“Sprzęt i oprogramowanie sieciowe” na stronie 50

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

### **Odsyłacze pokrewne**

Funkcje API protokołu RSVP

“Konfigurowanie usługi QoS za pomocą kreatorów” na stronie 52

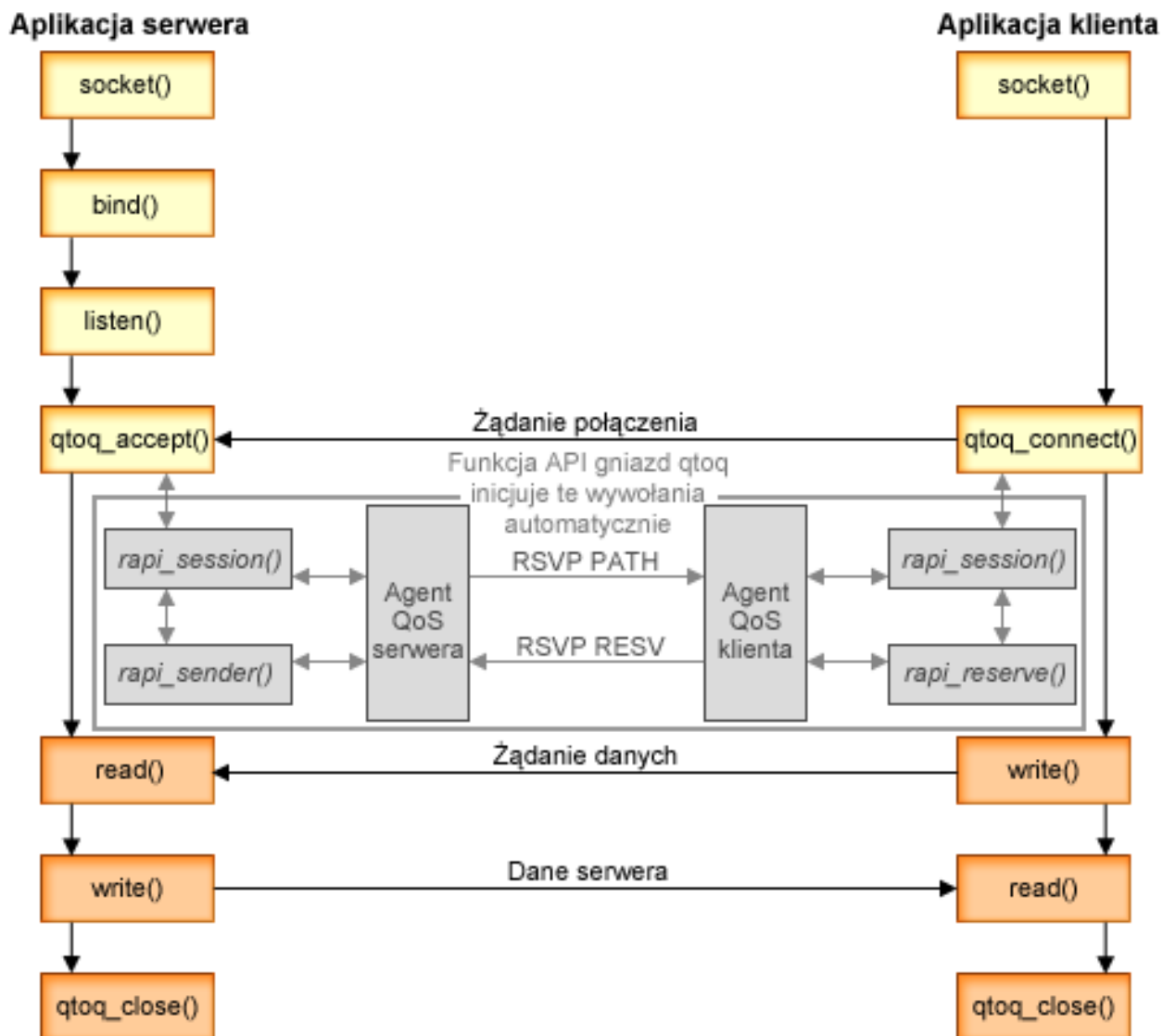
Do konfigurowania strategii jakości usługi (QoS) należy używać kreatorów QoS dostępnych w programie System i Navigator.



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

Przykłady serwera i klienta przedstawione w tym temacie pokazują działanie funkcji API gniazd QoS qtoq, które stworzono z myślą o przepływie wywołań opartym na połączeniach.

Wywołanie funkcji API QoS w celu uruchomienia komunikacji RSVP z nawiązaniem połączenia powoduje również zainicjowanie pewnych innych funkcji. Funkcje te umożliwiają agentom usługi QoS po stronie klienta i serwera skonfigurowanie obsługi protokołu RSVP dla potrzeb transmisji, która ma nastąpić.



**Przebieg zdarzeń podczas pracy z funkcjami 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(), aby pobrać deskryptor gniazda.
2. Aplikacja wywołuje funkcję listen(), aby określić typy połączeń, na które będzie oczekiwać.
3. Aplikacja wywołuje funkcję qtoq\_accept(), aby rozpocząć oczekiwanie na żądanie połączenia od klienta.

4. Interfejs API wywołuje funkcję `rapi_session()`. Jeśli jej wykonanie zakończy się powodzeniem, przypisywany jest identyfikator sesji QoS.
5. Interfejs API wywołuje standardową funkcję `accept()`, aby rozpocząć oczekiwanie na żądanie połączenia od klienta.
6. Po odebraniu zgłoszenia uruchamia się sterowanie dostępem dla żądanej reguły. Reguła ta jest przesyłana do stosu TCP/IP. Jeśli reguła jest poprawna, do aplikacji wywołującej zwracane są wyniki i identyfikator sesji.
7. Aplikacje serwera i klienta przeprowadzają wymagane transmisje danych.
8. Aplikacja wywołuje funkcję `qtoq_close()`, aby zamknąć gniazdo i usunąć regułę z pamięci.
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()`, aby pobrać deskryptor gniazda.
2. Aplikacja wywołuje funkcję `listen()`, aby określić typy połączeń, na które będzie oczekiwać.
3. Aplikacja wywołuje funkcję `qtoq_accept()`, aby rozpocząć oczekiwanie na żądanie połączenia od klienta.
4. Po nadejściu żądania połączenia wywoływana jest funkcja `rapi_session()`, która nawiązuje dla tego połączenia nową sesję z serwerem QoS i pobiera identyfikator sesji QoS, zwracany następnie wywołującemu.
5. Wywoływana jest funkcja `rapi_sender()` powodująca wysłanie komunikatu PATH z serwera QoS i informująca serwer, że od klienta nadejdzie komunikat RESV.
6. Wywoływana jest funkcja `rapi_getfd()`, która pobiera deskryptor używany następnie przez aplikacje do oczekiwania 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 komunikatu serwer 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()`, aby pobrać deskryptor gniazda.
2. Aplikacja wywołuje funkcję `qtoq_connect()`, aby poinformować aplikację serwera o żądaniu nawiązania połączenia.
3. Funkcja `qtoq_connect()` wywołuje z kolei funkcję `rapi_session()`, umożliwiającą nawiązanie sesji z serwerem QoS dla tego połączenia.
4. Serwer QoS będzie oczekiwał komendy PATH w danym połączeniu.
5. Wywoływana jest funkcja `rapi_getfd()`, która pobiera deskryptor używany następnie przez aplikacje do oczekiwania na komunikaty QoS.
6. Wywoływana jest funkcja `connect()`. Wynik wywołania funkcji `connect()` i deskryptor QoS są zwracane do 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 żądanie nie jest poprawne z punktu widzenia klienta, nie wymaga bowiem od niego żadnej odpowiedzi.

### **Odsyłacze pokrewne**

qtoq\_accept() - funkcja API przyjęcia połączenia przez gniazdo QoS

qtoq\_close() - funkcja API zamknięcia połączenia przez gniazdo QoS

rapi\_session() - utworzenie sesji RAPI

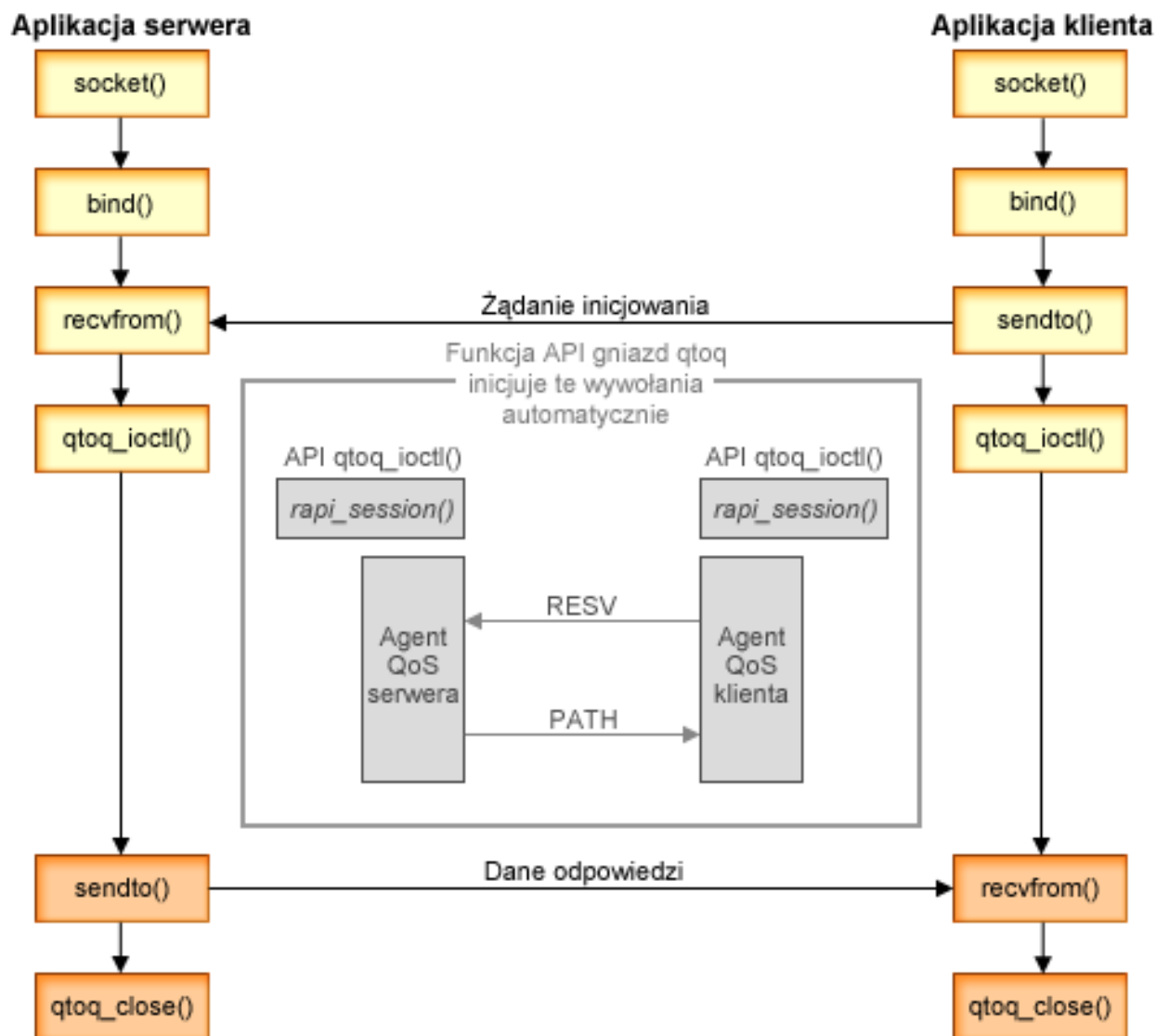
rapi\_sender() - identyfikacja nadawcy RAPI

rapi\_getfd() - pobranie deskryptora do obserwacji

qtoq\_connect() - funkcja API nawiązania połączenia przez gniazdo QoS

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

Wywołanie funkcji API obsługi QoS w celu uruchomienia komunikacji RSVP bez nawiązywania połączenia powoduje również zainicjowanie pewnych innych funkcji. Funkcje te umożliwiają agentom usługi QoS po stronie klienta i serwera skonfigurowanie obsługi protokołu RSVP dla potrzeb transmisji, która ma nastąpić między klientem a serwerem.



**Przebieg zdarzeń przy użyciu funkcji API 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 `qtoq_ioctl()` wysyła do serwera QoS komunikat z informacją, że należy uruchomić kontrolę dostępu dla żądanej reguły.
2. Jeśli regułę można zaakceptować, wywoływana jest funkcja, która do serwera QoS wysyła komunikat powodujący pobranie reguły.
3. Serwer QoS zwraca do wywołującego status informujący o powodzeniu lub niepowodzeniu żądania.
4. Gdy aplikacja kończy korzystanie z połączenia, wywołuje funkcję `qtoq_close()` w celu jego zamknięcia.
5. Serwer QoS usuwa regułę z menedżera QoS, usuwa sesję QoS i wykonuje wszelkie inne potrzebne operacje.

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

1. Funkcja `qtoq_ioctl()` wysyła do serwera QoS komunikat z żądaniem uruchomienia kontroli dostępu dla żadanego połączenia.
2. Serwer QoS wywołuje funkcję `rapi_session()`, aby zażądać nawiązania sesji dla wybranej reguły i pobrać identyfikator sesji QoS, który zostanie zwrócony do wywołującego.
3. Wywoływana jest funkcja `rapi_sender()` w celu wysłania do klienta komunikatu PATH.
4. Następnie wywoływana jest funkcja `rapi_getfd()`, która zwraca deskryptor pliku używany do czekania na zdarzenia QoS.
5. Serwer QoS zwraca do wywołującego 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 operacje.

### Po stronie klienta

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

1. Funkcja `qtoq_ioctl()` wywołuje funkcję `rapi_session()`, aby zgłosić żądanie utworzenia sesji dla połączenia. Funkcja `rapi_session()` zgłasza żądanie kontroli dostępu dla połączenia. 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. Następnie wywoływana jest funkcja `rapi_getfd()`, która zwraca deskryptor pliku używany do czekania na zdarzenia QoS.
3. Funkcja `qtoq_ioctl()` zwraca do wywołującego deskryptor oczekiwania i identyfikator 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 żądanie nie jest poprawne z punktu widzenia klienta, nie wymaga bowiem od niego żadnej odpowiedzi.

### Odsyłacze pokrewne

`qtoq_close()` - funkcja API zamknięcia połączenia przez gniazdo QoS

`rapi_session()` - utworzenie sesji RAPI

`rapi_sender()` - identyfikacja nadawcy RAPI

`rapi_getfd()` - pobranie deskryptora do obserwacji

`qtoq_ioctl()` - funkcja API ustawiania opcji sterowania gniazd QoS

## 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()` umożliwia przekazywanie danych klasyfikacyjnych 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 usługi QoS uzyskany za pośrednictwem danych klasyfikacyjnych z tego komunikatu będzie ważny dla wszystkich następnych komunikatów wysyłanych do momentu następnego wywołania funkcji `sendmsg()` z przekazaniem danych klasyfikacyjnych. Zasięg na poziomie komunikatu wskazuje, że przypisany poziom usługi QoS powinien być 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 pierwotnej 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. Podany łańcuch może zawierać zarówno wielkie, jak i małe znaki i będzie używany do celów porównawczych dokładnie w podanym 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 TCP/IP w formacie ASCII i dzięki temu nie ma potrzeby konwersji tokenu zdefiniowanego w aplikacji przy każdym żądaniu zgłoszonym przez funkcję `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 Najlepszy możliwy.
- `ip_qos_appl_token_len`: długość tokenu podanego w polu `ip_qos_appl_token`.
- `ip_qos_appl_token`: pole wirtualne, występujące 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

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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

Ruch w sieci jest w przypadku usług DiffServ identyfikowany według klas. 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 tym temacie opisano konfigurowanie protokołu LDAP (Lightweight Directory Access Protocol) i związane z nim pojęcia, jak również schemat usługi QoS.

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

### **Jak korzystać z 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 systemie lokalnym**

Zapisywanie strategii QoS na systemie 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 duplikowanie konfiguracji w innych systemach. Wystarczy skopiować zbiór z jednego systemu do drugiego. Ponieważ nie ma podziału na maszyny podstawowe i dodatkowe, każdą strategię można dostosować do potrzeb konkretnego systemu.

### **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 System i Navigator można skonfigurować serwer katalogów używany ze strategią QoS.

#### **Pojęcia pokrewne**

IBM Tivoli Directory Server for i5/OS (LDAP)

“Konfigurowanie serwera katalogów” na stronie 53

Konfiguracje strategii QoS można eksportować na serwer katalogów LDAP (Lightweight Directory Access Protocol), co ułatwia zarządzanie rozwiązaniem QoS.

### **Słowa kluczowe**

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

Słowa kluczowe są opcjonalne i można je pominąć.

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 system podstawowy.

Do identyfikacji danych konfiguracyjnych tworzonych w systemach podstawowych używane są słowa kluczowe. Chociaż słowa kluczowe tworzone są w systemie podstawowym, faktycznie korzysta się z nich w systemach dodatkowych. Umożliwiają one systemom dodatkowym pobieranie i używanie 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 System i Navigator, należy skorzystać z pomocy dotyczącej zadania QoS.

#### **Pojęcia pokrewne**

“Nazwa wyróżniająca”

Aby zarządzać częścią katalogu, należy użyć nazwy wyróżniającej lub (jeśli zostanie wybrane takie rozwiązanie) słowa kluczowego.

“Konfigurowanie serwera katalogów” na stronie 53

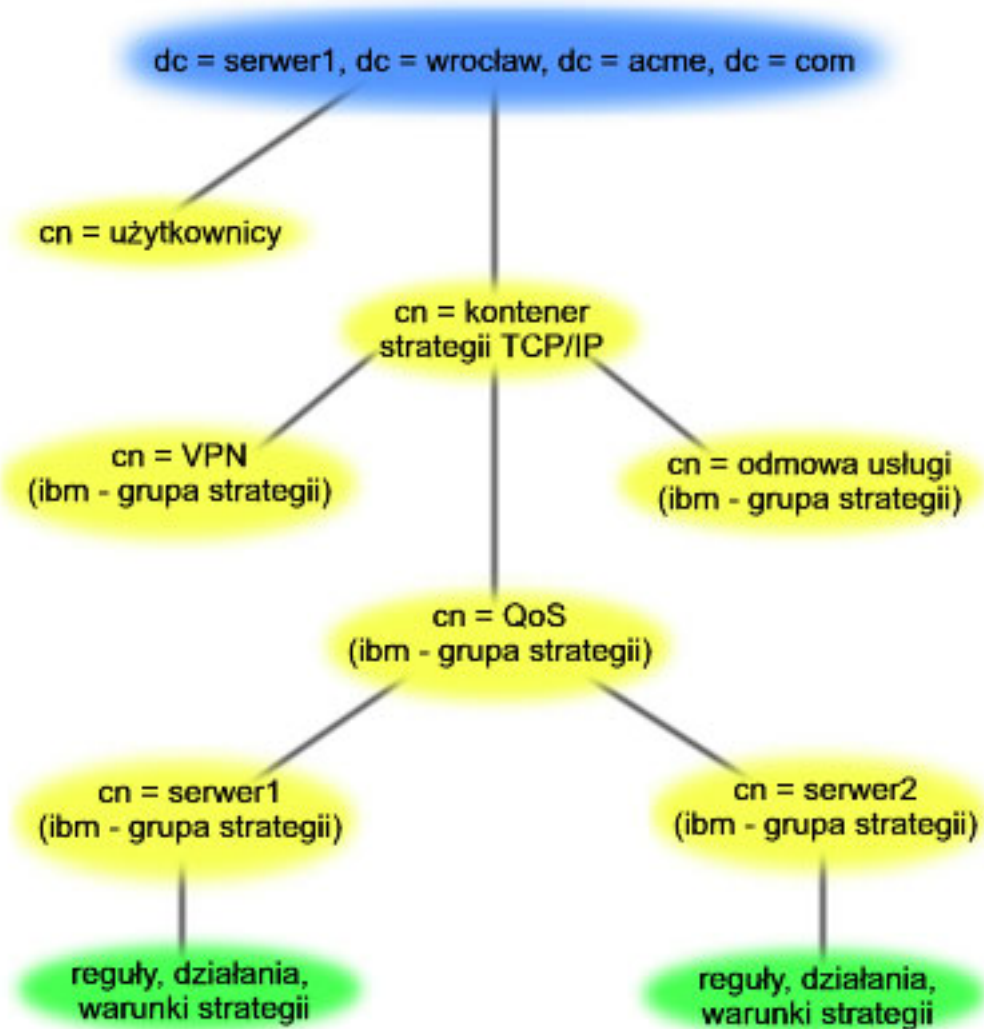
Konfiguracje strategii QoS można eksportować na serwer katalogów LDAP (Lightweight Directory Access Protocol), co ułatwia zarządzanie rozwiązaniem QoS.

### **Nazwa wyróżniająca**

Aby zarządzać częścią katalogu, należy użyć nazwy wyróżniającej lub (jeśli zostanie wybrane takie rozwiązanie) słowa kluczowego.

Nazwę wyróżniająca 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, na przykład 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 25

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 na serwer katalogów LDAP (Lightweight Directory Access Protocol), co ułatwia zarządzanie rozwiązaniem QoS.

#### Odsyłacze pokrewne

“Informacje pokrewne dotyczące usługi QoS” na stronie 67

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego.

Wszystkie pliki PDF można wyświetlić lub wydrukować.

---

## Scenariusze: strategie QoS

Podane tu scenariusze użycia strategii QoS pomagają zrozumieć przeznaczenie usługi QoS oraz poznać zasady tworzenia strategii i klas usług.

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 w systemie” na stronie 64

W tym temacie 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 usługi.

### Odsyłacze pokrewne

“Monitorowanie usługi QoS” na stronie 57

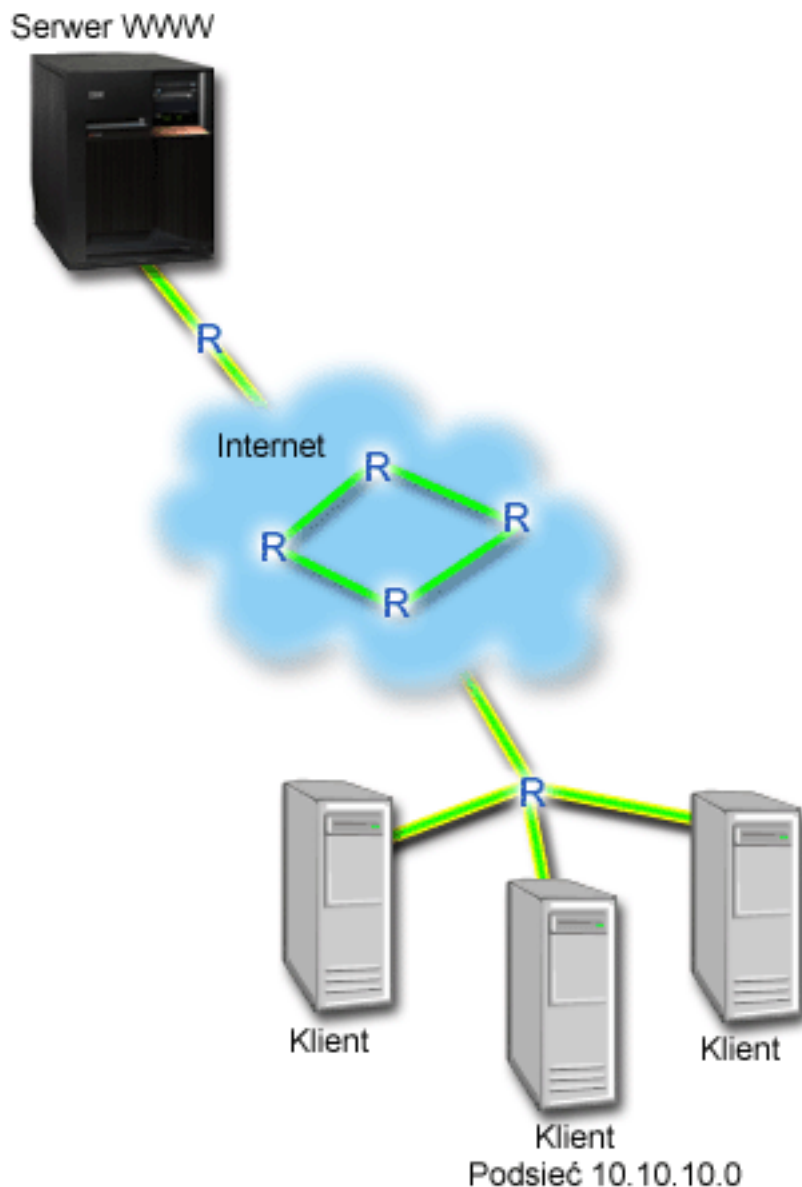
Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## 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

- Zawarta z dostawcą usług internetowych (ISP) umowa dotycząca poziomu usług pozwala zapewnić przypisywanie strategiom wymaganych priorytetów. Utworzenie strategii QoS w systemie pozwala ustawiać odpowiedni priorytet ruchu sieciowego w całej sieci. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może nawet być podstawą do negocjowania z dostawcą określonych poziomów i szybkości usług.

- Aby możliwe było korzystanie ze strategii usług DiffServ, wszystkie routery na ścieżce sieciowej muszą obsługiwać usługi DiffServ. Większość routerów nie obsługuje usług DiffServ.

## Konfiguracja

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

### Pojęcia pokrewne

“Umowa dotycząca poziomu usług” na stronie 49

Temat ten ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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 usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## Szczegóły scenariusza: tworzenie strategii usług DiffServ

W tym temacie przedstawiono informacje dotyczące tworzenia strategii usług DiffServ w systemie.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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 zostały utworzone klienty, należy anulować ich wybór i upewnić się, że wybrane są tylko klienty odpowiednie dla danej strategii.
8. Na stronie Żądanie serwera danych, sprawdź czy wybrane są opcje **Dowolny token** i **Wszystkie priorytety**, a następnie 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 Nowa klasa usług (New Class of Service).
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 jest używana wyłącznie w przypadku 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 systemy w sieci. Podczas wybierania wartości można korzystać z dostępnej w interfejsie 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** (Finish) 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** (Next), 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.

## Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS

W tym temacie przedstawiono informacje na temat uruchamiania lub aktualizowania serwera QoS.

W oknie konfiguracji serwera QoS wybierz opcję **Serwer** → **Uruchom** (Server > Start) lub **Serwer** → **Aktualizuj** (Server > Update).

## Szczegóły scenariusza: sprawdzanie poprawnego działania strategii

Korzystając z monitora należy sprawdzić, czy strategia działa tak, jak została skonfigurowana.

1. W oknie konfiguracji QoS wybierz opcję **Serwer** → **Monitor** (Server > Monitor). Zostanie wyświetlone okno Monitor QoS (QoS Monitor).
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).

Istotna jest również wartość wprowadzona w polu **Ograniczenie średniej szybkości** (Average Rate Limit). W razie przekroczenia tej wartości kolejne napływające pakiety będą odrzucane przez serwer. W konsekwencji nastąpi zwiększenie liczby bitów odpowiadających pakietom spoza profilu. Oznacza to, że strategia działa tak, jak została skonfigurowana. Temat "Monitorowanie usługi QoS" na stronie 57 zawiera opis wszystkich pól w oknie monitora.

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

## Szczegóły scenariusza: zmiana właściwości

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby osiągnąć oczekiwane wyniki.

Aby zmienić dowolną z wartości zdefiniowanych w ramach strategii, należy wykonać 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 (Properties), które zawiera wartości sterujące ogólną strategią.
2. Podaj 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 Właściwości QoS (QoS Properties), zawierające wartości sterujące sposobem zarządzania ruchem danych.
4. Podaj odpowiednie wartości.
5. W oknie Konfiguracja serwera usług QoS wybierz opcje **Serwer** → **Aktualizuj**, aby zaakceptować zmiany.

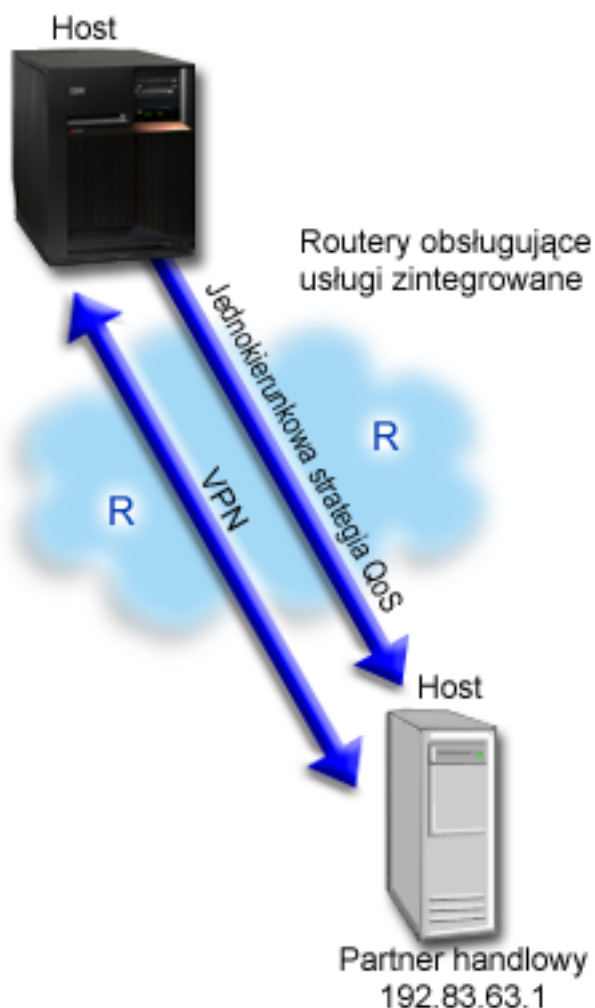
## Scenariusz: bezpieczny i przewidywalny ruch danych (sieć VPN i jakość usług)

W sieci VPN także można tworzyć strategie QoS.

### Sytuacja

Pewna firma i jej partner handlowy znajdują się w tej samej sieci VPN. Zamierzają połączyć funkcje sieci VPN i QoS, aby uzyskać bezpieczeństwo 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 lub wideo należy ustalić poziom usługi 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

Korzystając jednocześnie z sieci VPN i usługi QoS można zapewnić nie tylko bezpieczeństwo, ale i odpowiedni priorytet połączenia. 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 niewrażliwym znaczeniu.

## Wymagania wstępne i założenia

- Zawarta z dostawcą usług internetowych (ISP) umowa dotycząca poziomu usług pozwala zapewnić przypisywanie strategiom wymaganych priorytetów. Utworzenie strategii QoS w systemie pozwala ustawiać odpowiedni priorytet ruchu sieciowego w całej sieci. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może nawet być podstawą do negocjowania z dostawcą określonych poziomów i szybkości usług. Skorzystaj z odsyłacza do informacji na temat umowy dotyczącej poziomu usług, aby uzyskać więcej informacji.
- Aby możliwe było korzystanie ze strategii usług DiffServ, wszystkie routery na ścieżce sieciowej muszą obsługiwać usługi DiffServ. Większość routerów obsługuje obecnie usługi DiffServ.

## Konfiguracja

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

### Pojęcia pokrewne

“Umowa dotycząca poziomu usług” na stronie 49

Temat ten ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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 usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

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

W tym temacie przedstawione są informacje na temat konfigurowania połączenia host-host w sieci VPN.

Podczas konfigurowania sieci VPN przydatne mogą być informacje zawarte w temacie Scenariusz: podstawowe połączenie pomiędzy firmami.

## Szczegóły scenariusza: tworzenie strategii usług DiffServ

W tym temacie przedstawiono informacje dotyczące tworzenia strategii usług DiffServ.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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** (Name): Klient\_VPN
  - **Adres IP** (IP Address): 192.83.63.1
  - Kliknij przycisk **OK**, aby utworzyć klienta i powrócić do kreatora usług DiffServ.Po kliknięciu przycisku **OK** nastąpi powrót do kreatora strategii. Jeśli wcześniej zostały utworzone klienty, należy je kliknąć i upewnić się, że wybrane są tylko klienty odpowiednie dla danej strategii.
8. Na stronie Żądanie serwera danych, sprawdź czy wybrane są opcje **Dowolny token** i **Wszystkie priorytety**.
9. Na stronie Aplikacje sprawdź, czy wybrane są opcje **Wszystkie porty** i **Wszystkie**.
10. Kliknij przycisk **Dalej**.
11. Na stronie Lokalny adres IP zaakceptuj wartość domyślną i kliknij przycisk **Dalej**.
12. Na stronie Klasa usług DiffServ kliknij przycisk **Nowy**, aby zdefiniować parametry wydajności. Zostanie uruchomiony kreator Nowa klasa usług (New Class of Service).
13. Przeczytaj stronę powitania i kliknij przycisk **Dalej**.
14. Na stronie Nazwa wpisz **EF\_VPN**.



15. Na stronie Typ usług wybierz opcję **Tylko wychodzące** i kliknij przycisk **Dalej**. Ta klasa usług jest używana wyłącznie w przypadku strategii ruchu wychodzącego.
16. Na stronie Oznaczanie punktem kodowym wychodzącego ruchu DiffServ (Outbound DiffServ Codepoint Marking) wybierz opcję **Klasa 3 (Class 3)**. Wydajność obsługi ruchu danych przez routery i inne systemy w sieci będzie zależeć od charakterystyki w ramach segmentu sieci. Wybierając wartości można skorzystać z dostępnej w interfejsie pomocy.
17. 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 zągęszczenia TCP** i kliknij przycisk **Dalej**.
20. Zapoznaj się ze stroną podsumowania klasy usług i kliknij przycisk **Zakończ** (Finish), 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 (Name):** PierwszaZmiana
  - **Godzina (Time of day):** wybierz opcję Aktywność o określonych godzinach (Active at specific times) i dodaj godziny od 9:00 do 17:00.
  - **Dzień tygodnia (Day of week):** wybierz opcję Aktywność w określonych dniach (Active on specific days) i podaj dni od poniedziałku do piątku.
24. Na stronie Harmonogram kliknij przycisk **Dalej**.
25. Zapoznaj się z informacjami w podsumowaniu. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. Lista wszystkich strategii utworzonych w systemie będzie wyświetlana w oknie konfiguracji serwera QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

## Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS

W tym temacie przedstawiono informacje na temat uruchamiania lub aktualizowania serwera QoS.

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

## Szczegóły scenariusza: sprawdzanie poprawnego działania strategii

Korzystając z monitora należy sprawdzić, czy strategia działa tak, jak została skonfigurowana.

1. W oknie konfiguracji serwera QoS wybierz opcje **Serwer** → **Monitorowanie** (Server > Monitor). Zostanie wyświetlone okno Monitor QoS (QoS Monitor).
2. Wybierz typ strategii Usługi DiffServ. Zostaną wyświetlone wszystkie strategie usług 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 zągęszczenia TCP umożliwiające kolejkowanie pakietów spoza profilu. W konsekwencji nastąpi zwiększenie liczby bitów spoza profilu. Różnica między strategią tu opisywaną a strategią ze scenariusza dotyczącego ograniczania ruchu danych do przeglądarki polega na tym, że pakiety są zabezpieczone za pomocą sieci VPN. Pokazano więc, że funkcji QoS można używać w sieci VPN. Temat "Monitorowanie usługi QoS" na stronie 57 zawiera opis wszystkich pól w oknie monitora.

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

## Szczegóły scenariusza: zmiana właściwości

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby osiągnąć oczekiwane wyniki.

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 Właściwości (Properties), które zawiera wartości sterujące ogólną strategią.
2. Podaj 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 Właściwości QoS (QoS Properties), zawierające wartości sterujące sposobem zarządzania ruchem danych.
4. Podaj odpowiednie wartości.
5. W oknie Konfiguracja serwera usług QoS wybierz opcje **Serwer** → **Aktualizuj**, aby zaakceptować zmiany.

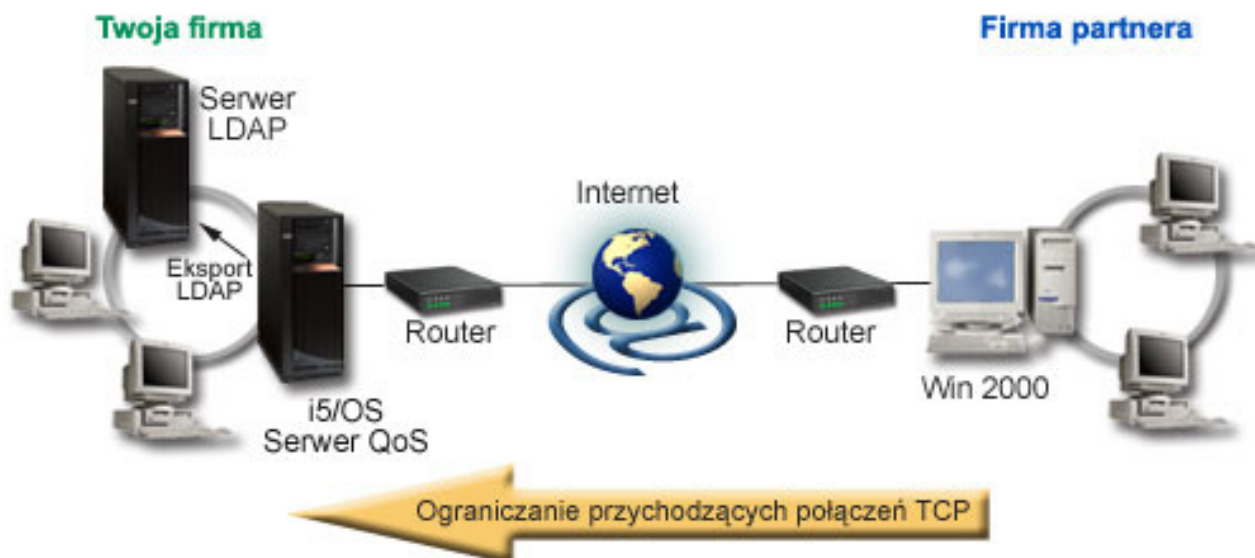
## Scenariusz: ograniczanie połączeń przychodzących

Jeśli zachodzi potrzeba kontrolowania nadsyłanych do systemu żądań połączeń, należy użyć strategii akceptowania 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. Usługa QoS umożliwia ograniczenie liczby akceptowanych połączeń przychodzących do systemu na podstawie atrybutów połączenia (na przykład adresu IP). W tym celu można zastosować strategię akceptowania ruchu przychodzącego, która będzie ograniczać liczbę akceptowanych połączeń przychodzących.

Rysunek przedstawia przykładową firmę i firmę będącą jej klientem. Strategia tu prezentowana może sterować przepływem danych tylko w jednym kierunku.



Rysunek 6. Ograniczanie przychodzących połączeń TCP

## 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 usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## Szczegóły scenariusza: tworzenie strategii akceptowania ruchu przychodzącego

W tym temacie przedstawiono informacje dotyczące tworzenia strategii akceptowania ruchu przychodzącego w systemie.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
  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 zostały utworzone klienty, należy anulować ich wybór i upewnić się, że wybrane są tylko klienty odpowiednie dla danej strategii.
8. Na stronie nazwy URI sprawdź, czy wybrana jest opcja **Dowolny URI** (Any URI) i kliknij przycisk **Dalej** (Next).
  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 Nowa klasa usług (New Class of Service).
  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** (Average connection rate): 50 na sekundę
  - **Limit porcji dla połączenia** (Connection burst limit): 50 połączeń
  - **Priorytet** (Priority): 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** (Name): PierwszaZmiana
  - **Godzina** (Time of day): wybierz opcję Aktywność o określonych godzinach (Active at specific times) i dodaj godziny od 9:00 do 17:00.
  - **Dzień tygodnia** (Day of week): wybierz opcję Aktywność w określonych dniach (Active on specific days) i podaj dni od poniedziałku do piątku.
23. Na stronie Harmonogramy kliknij przycisk **Dalej**.
24. Zapoznaj się z informacjami w podsumowaniu. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ** (Finish), aby utworzyć strategię. Lista wszystkich strategii utworzonych w systemie będzie wyświetlana w oknie konfiguracji serwera QoS. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii akceptowania ruchu przychodzącego w systemie. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

### Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS

W tym temacie przedstawiono informacje na temat uruchamiania lub aktualizowania serwera QoS.

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

### Szczegóły scenariusza: sprawdzanie poprawnego działania strategii

W tym temacie zawarto informacje o używaniu monitora do sprawdzenia, czy strategia działa tak, jak została skonfigurowana.

1. W oknie konfiguracji QoS wybierz opcje **Serwer → Monitor** (Server > Monitor). Zostanie wyświetlone okno Monitor QoS (QoS Monitor).
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).

Istotna jest również wartość wprowadzona w polu **Średnia szybkość żądań połączeń** (Average Connection Request Rate). W razie przekroczenia tej wartości kolejne napływające pakiety będą odrzucane przez serwer. W konsekwencji nastąpi zwiększenie liczby żądań odrzuconych. Oznacza to, że strategia działa tak, jak została skonfigurowana. Temat "Monitorowanie usługi QoS" na stronie 57 zawiera opis wszystkich pól w oknie monitora.

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

### Szczegóły scenariusza: zmiana właściwości

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii lub klasy usług, aby osiągnąć oczekiwane wyniki.

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 (Properties), 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 Właściwości QoS (QoS Properties), zawierające wartości sterujące sposobem zarządzania ruchem danych.
4. Podaj odpowiednie wartości.
5. W oknie Konfiguracja serwera usług QoS wybierz opcje **Serwer** → **Aktualizuj**, aby zaakceptować zmiany.

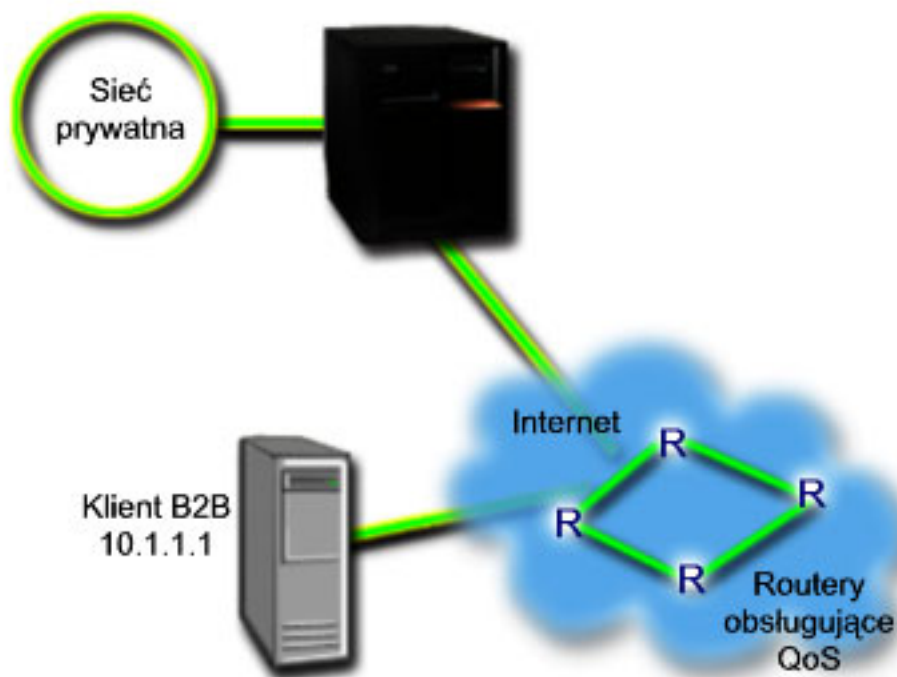
## Scenariusz: przewidywalny ruch danych firma-firma (B2B)

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

### Sytuacja

Dział sprzedaży zgłasza problemy związane z niewystarczającą szybkością transmisji danych. System operacyjny i5/OS na firmowym serwerze działa w środowisku typu firma-firma (B2B), które wymaga przewidywalnej obsługi operacji biznesowych na żądanie. 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 przeciążenia wspomaga działanie aplikacji szczególnie wrażliwych na przeciążenie sieci, dopuszczających jednak niewielkie utraty pakietów i niewielkie opóźnienia. Gdy aplikacja korzysta z usługi sterowanego przeciążenia, jej wydajność nie spadnie po zwiększeniu się obciążenia sieci. Zostanie zapewniony poziom transmisji danych niemal 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 przeciążenia.

Stosowanie strategii usług zintegrowanych wymaga też, 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**

Ponieważ sam system nie zawiera aplikacji obsługujących protokół RSVP, należy je utworzyć we własnym zakresie. 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 systemy na ścieżce sieciowej obsługujące protokół RSVP**

QoS jest rozwiązaniem dotyczącym całej sieci. Nawet jeśli nie ma pewności, czy wszystkie urządzenia sieciowe obsługują protokół RSVP, można utworzyć strategię usług zintegrowanych i zastosować znakowanie w celu nadania jej określonego priorytetu, jednak nie będzie możliwe zagwarantowanie tego priorytetu.

- **Umowa dotycząca poziomu usług**

Zawarta z dostawcą usług internetowych (ISP) umowa dotycząca poziomu usług pozwala zapewnić przypisywanie strategiom wymaganych priorytetów. Utworzenie strategii QoS w systemie pozwala ustawiać odpowiedni priorytet ruchu sieciowego w całej sieci. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może nawet być podstawą do negocjowania z dostawcą określonych poziomów i szybkości usług.

**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 przeciążenia i usługi gwarantowane.

“Usługi zintegrowane” na stronie 6

Drugim z dostępnych typów strategii pasma połączeń wychodzących jest strategia usług zintegrowanych. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API usługi QoS.

“Interfejsy API jakości usługi (QoS)” na stronie 16

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazd qtoq, API sendmsg() i API monitorowania.

“Umowa dotycząca poziomu usług” na stronie 49

Temat ten ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

### Odsyłacze pokrewne

“Monitorowanie usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## Szczegóły scenariusza: tworzenie strategii usług zintegrowanych

W tej sekcji przedstawiono informacje dotyczące tworzenia strategii usług zintegrowanych w systemie.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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 zostały utworzone klienty, należy anulować ich wybór i upewnić się, że wybrane są tylko klienty odpowiednie 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 te funkcje API nie będą wykorzystywane, aplikacja nie uzyska priorytetu ani usługi gwarantowanej. Trzeba także pamiętać, że ta strategia umożliwi aplikacjom uzyskanie priorytetu w sieci, ale go nie gwarantuje. Aby rezerwacja była zagwarantowana, konieczna jest obsługa protokołu RSVP przez wszystkie routery i systemy 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 (Name):** godziny\_szczytu
  - **Godzina (Time of day):** wybierz opcję Aktywność w określonych godzinach i dodaj godziny od 10:00 do 16:00.

- **Dzień tygodnia** (Day of week): wybierz opcję Aktywność w określonych dniach (Active on specific days) i podaj dni od poniedziałku do piątku.

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

17. Zapoznaj się z informacjami w podsumowaniu. Jeśli wszystkie parametry są odpowiednie, kliknij przycisk **Zakończ**, aby utworzyć strategię. W głównym oknie interfejsu QoS wyświetlane są wszystkie strategie utworzone w systemie. Po zakończeniu pracy z kreatorem nowa strategia pojawi się w prawym panelu.

Zakończono proces konfigurowania strategii usług zintegrowanych w systemie. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS

W tym temacie przedstawiono informacje na temat uruchamiania lub aktualizowania serwera QoS.

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

## Szczegóły scenariusza: sprawdzanie poprawnego działania strategii

W tym temacie zawarto informacje o używaniu monitora do sprawdzania, czy strategia działa tak, jak została skonfigurowana.

1. W oknie konfiguracji serwera QoS wybierz opcje **Serwer** → **Monitorowanie** (Server > Monitor). Zostanie wyświetlone okno Monitor QoS (QoS Monitor).
2. Wybierz typ strategii usług zintegrowanych. Zostaną wyświetlone wszystkie strategie usług zintegrowanych. 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. Pełen opis pól monitora można znaleźć w sekcji "Monitorowanie usługi QoS" na stronie 57.

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

## Szczegóły scenariusza: zmiana właściwości

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii, aby osiągnąć oczekiwane wyniki.

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 (Properties), które zawiera wartości sterujące ogólną strategią.
2. Podaj odpowiednie wartości.
3. W oknie Konfiguracja serwera usług QoS wybierz opcje **Serwer** → **Aktualizuj**, aby zaakceptować zmiany.

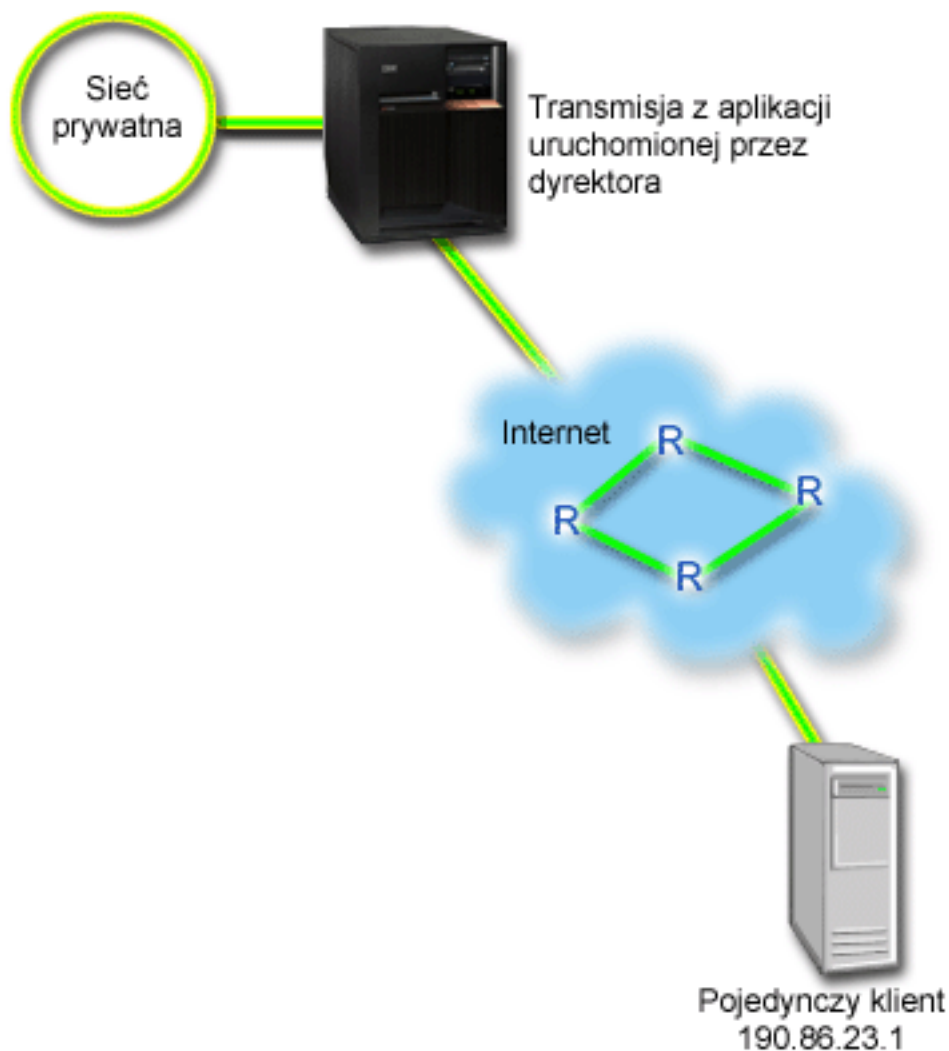
## Scenariusz: dedykowane dostarczanie (telefonii IP)

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa typy strategii usług zintegrowanych: usługi gwarantowane i usługi sterowanego przeciążenia. 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 regionu. Trzeba zagwarantować niezbędną przepustowość telefonii IP, aby nie wystąpiły żadne 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 używana przez dyrektora generalnego wymaga równej i nieprzerwanej transmisji, należy skorzystać ze strategii gwarantowanych usług zintegrowanych. Usługa gwarantowana określa maksymalne opóźnienie kolejkowania pakietów, dzięki czemu opóźnienie pakietów nie przekracza określonego czasu.

## 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**

Ponieważ sam system nie zawiera aplikacji obsługujących protokół RSVP, należy je utworzyć we własnym zakresie. W tym celu można skorzystać z funkcji API RAPI lub funkcji API gniazd QoS qtoq. Więcej informacji na ten temat zawiera temat "Interfejsy API jakości usługi (QoS)" na stronie 16, w części o funkcjach API usług zintegrowanych.

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

QoS jest rozwiązaniem dotyczącym całej sieci. Nawet jeśli nie ma pewności, czy wszystkie urządzenia sieciowe obsługują protokół RSVP, można utworzyć strategię usług zintegrowanych i zastosować znakowanie w celu nadania jej określonego priorytetu, jednak nie będzie możliwe zagwarantowanie tego priorytetu.

- **Umowa dotycząca poziomu usług**

Zawarta z dostawcą usług internetowych (ISP) umowa dotycząca poziomu usług pozwala zapewnić przypisywanie strategiom wymaganych priorytetów. Utworzenie strategii QoS w systemie pozwala ustawiać odpowiedni priorytet ruchu sieciowego w całej sieci. Priorytet ten nie jest jednak zagwarantowany, ponieważ zależy to od umowy dotyczącej poziomu usług. Wykorzystywanie strategii QoS może nawet być podstawą do negocjowania z dostawcą określonych poziomów i szybkości usług.

## 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 przeciążenia i usługi gwarantowane.

“Usługi zintegrowane” na stronie 6

Drugim z dostępnych typów strategii pasma połączeń wychodzących jest strategia usług zintegrowanych. Strategia usług zintegrowanych umożliwia aplikacjom korzystającym z protokołu IP wysyłanie żądań i rezerwację określonej przepustowości za pomocą protokołu RSVP oraz funkcji API usługi QoS.

“Umowa dotycząca poziomu usług” na stronie 49

Temat ten ma na celu zwrócenie uwagi na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

### Odsyłacze pokrewne

“Monitorowanie usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## Szczegóły scenariusza: tworzenie strategii usług zintegrowanych

W tej sekcji przedstawiono informacje dotyczące tworzenia strategii usług zintegrowanych w systemie.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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 zostały utworzone klienty, należy anulować ich wybór i upewnić się, że wybrane są tylko klienty odpowiednie 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 (Name):** jedna\_godzina
    - **Godzina (Time of day):** wybierz opcję Aktywność o określonych godzinach (Active at specific times) i dodaj godziny od 13:00 do 14:00.
    - **Dzień tygodnia (Day of week):** wybierz opcję Aktywność w określonych dniach (Active on specific days) i wybierz poniedziałek.
  16. Na stronie Harmonogram kliknij przycisk **Dalej**.
  17. Zapoznaj się z informacjami w podsumowaniu. 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 w systemie. Kolejnym etapem jest uruchomienie lub aktualizacja serwera.

## Szczegóły scenariusza: uruchomienie lub aktualizacja serwera QoS

W tym temacie przedstawiono informacje na temat uruchamiania lub aktualizowania serwera QoS.

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

## Szczegóły scenariusza: sprawdzanie poprawnego działania strategii

W tym temacie zawarto informacje o używaniu monitora do sprawdzania, czy strategia działa tak, jak została skonfigurowana.

1. W oknie konfiguracji serwera QoS wybierz opcje **Serwer** → **Monitorowanie** (Server > Monitor). Zostanie wyświetlone okno Monitor QoS (QoS Monitor).
2. Wybierz folder typu strategii usług zintegrowanych. Zostaną wyświetlone wszystkie strategie usług zintegrowanych.

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. Temat “Monitorowanie usługi QoS” na stronie 57 zawiera opis wszystkich pól w oknie monitora.

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

## Szczegóły scenariusza: zmiana właściwości

Po zapoznaniu się z wynikami monitorowania można zmienić wybrane parametry strategii, aby osiągnąć oczekiwane wyniki.

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 (Properties), które zawiera wartości sterujące ogólną strategią.
2. Podaj odpowiednie wartości.
3. W oknie Konfiguracja serwera usług QoS wybierz opcje **Serwer** → **Aktualizuj**, aby zaakceptować zmiany.

## Scenariusz: monitorowanie bieżących statystyk sieci

Podczas korzystania z kreatorów należy ustawić ograniczenia wydajności odpowiadające indywidualnym wymaganiom obsługi sieci.

### Cele

Aby można było ustalić ograniczenia, 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 system.

### Rozwiązanie

Należy utworzyć bardzo szeroką strategię usług DiffServ, która nie zawiera ograniczeń (wartości maksymalnych) i dotyczy wszystkich interfejsów i adresów IP. Za pomocą monitora QoS należy uruchomić 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 wydajności umożliwiają zagwarantowanie dostarczenia pakietów w strategiach ruchu wychodzącego, zarówno w przypadku strategii usług zintegrowanych, jak i strategii usług DiffServ.

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

Ustawienia szybkości połączeń i porcji połączeń to limity szybkości. Limity takie umożliwiają ograniczanie połączeń przychodzących do systemu. Limity szybkości ustawia się dla klasy usług używanej wraz ze strategiami akceptowania ruchu przychodzącego.

#### Odsyłacze pokrewne

“Monitorowanie usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

## Szczegóły scenariusza: otwieranie funkcji QoS w programie System i Navigator

W tym temacie przedstawiono informacje na temat otwierania funkcji QoS w programie System i Navigator.

1. W programie System i Navigator rozwiń węzły **nazwa systemu** → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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 wyświetlony kreator nowej strategii usług DiffServ.

### Szczegóły scenariusza: tworzenie strategii usług DiffServ

Ponieważ strategia ma dotyczyć większości danych napływających do sieci, można ją nazwać "sieć". Strategię należy stosować do wszystkich adresów IP, numerów portów, lokalnych adresów IP i określić, że ma być aktywna przez cały czas (jeśli odpowiada to potrzebom).

W trakcie pracy z kreatorem należy zatem użyć następujących wartości:

**Nazwa** (Name): Sieć (może to być dowolna nazwa określona przez użytkownika)  
**Klient** (Client): Wszystkie adresy IP (All IP addresses)  
**Aplikacja** (Application): Wszystkie porty (All ports)  
**Protokół** (Protocol): Wszystkie protokoły (All protocols)  
**Harmonogram** (Schedule): Wszystkie godziny (All times)

Program System i Navigator wyświetli wszystkie utworzone w systemie strategie usług DiffServ.

### Szczegóły scenariusza: kończenie tworzenia klasy usług

Podczas kończenia pracy z kreatorem należy określić charakterystykę w ramach segmentu sieci, limity wydajności i zasady obsługi danych spoza profilu. Podane wartości definiują klasę usług. Aby umożliwić obsługę jak największego ruchu, należy podać bardzo duże wartości.

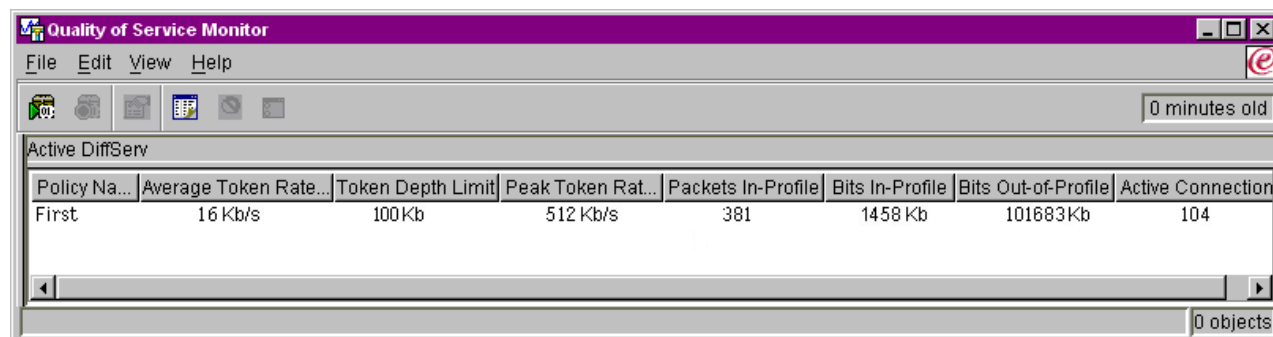
Klasa usług określa poziom wydajności ruchu danych gwarantowany przez router. Utworzoną klasę usług można nazwać "bez\_ograniczen", co będzie sygnalizować, że obsługiwany ruch otrzyma wyższy poziom usług. Program System i Navigator wyświetli wszystkie utworzone w systemie klasy usług.

### Szczegóły scenariusza: monitorowanie strategii

Korzystając z monitora można się upewnić, że ruch w sieci jest obsługiwany tak, jak zostało to skonfigurowane w strategii.

1. Wybierz określony folder strategii (usługi DiffServ, usługi zintegrowane 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.



The screenshot shows the 'Quality of Service Monitor' application window. The title bar reads 'Quality of Service Monitor'. Below the title bar is a menu bar with 'File', 'Edit', 'View', and 'Help'. There is a toolbar with several icons and a status bar on the right that says '0 minutes old'. The main area displays 'Active DiffServ' with a table of data.

Policy Na...	Average Token Rate...	Token Depth Limit	Peak Token Rat...	Packets In-Profile	Bits In-Profile	Bits Out-of-Profile	Active Connection
First	16 Kb/s	100Kb	512 Kb/s	381	1458 Kb	101683Kb	104

At the bottom right of the window, there is a status bar that says '0 objects'.

Rysunek 9. Monitorowanie QoS

Sprawdź pola, których wartości wyznaczane 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).

Istotna jest również wartość wprowadzona w polu **Limit średniej szybkości tokenów** (Average Token Rate Limit). W razie przekroczenia tej wartości kolejne napływające pakiety będą odrzucane przez serwer. W konsekwencji nastąpi

zwiększenie liczby bitów spoza profilu. Oznacza to, że strategia działa tak, jak została skonfigurowana. Aby zmienić liczbę bitów spoza profilu, należy odpowiednio dopasować limity wydajności. Temat “Monitorowanie usługi QoS” na stronie 57 zawiera opis wszystkich pól w oknie monitora.

### **Szczegóły scenariusza: zmiana wartości**

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

### **Szczegóły scenariusza: ponowne monitorowanie strategii**

Aby wyznaczyć limity optymalne w danej sieci, należy sprawdzać wyniki monitorowania i eksperymentalnie dobierać najlepsze parametry.

---

## **Planowanie wprowadzenia usługi QoS**

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.

### **Kwestie wydajności 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 w systemie” na stronie 64

W tym temacie omówiono monitor QoS umożliwiający sprawdzenie, czy strategię QoS działają zgodnie z oczekiwaniami. Monitor QoS może być przydatny w fazie planowania QoS i rozwiązywania problemów dotyczących tej usługi.

“Konfigurowanie usługi QoS” na stronie 51

Po zaplanowaniu wdrożenia usługi QoS należy utworzyć odpowiednie strategię QoS, korzystając z kreatorów dostępnych w programie System i Navigator. W tym temacie przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych 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 (a opcjonalnie również serwerów katalogów LDAP) niezbędne są następujące uprawnienia.

### **Nadawanie uprawnień do zarządzania serwerem katalogów**

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

### **Nadawanie uprawnień do uruchamiania serwera TCP/IP**

Aby nadać uprawnienia do komend STRTCPSVR i ENDTCPSVR, 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 odpowiedzialni za konfigurowanie funkcji QoS mieli uprawnienia osoby odpowiedzialnej za bezpieczeństwo. Aby nadać uprawnienia do wszystkich obiektów i uprawnienia do konfigurowania systemu, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Użytkownicy i grupy** (*nazwa systemu* > Users and Groups).
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 systemowe

Usługi QoS to integralna część systemu operacyjnego.

Muszą być spełnione następujące wymagania:

1. Zainstaluj narzędzia IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1).
2. Zainstaluj na komputerze PC program System i Navigator. Podczas instalowania oprogramowania System i Access upewnij się, że instalacja obejmuje komponent obsługi sieci (Networking). Usługa QoS jest umieszczona w pozycji Sieć - Strategie IP.

### Pojęcia pokrewne

Podstawowe informacje o programie System i Navigator

### Odsyłacze pokrewne

“Informacje pokrewne dotyczące usługi QoS” na stronie 67

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego.

Wszystkie pliki PDF można wyświetlić lub wydrukować.

## Umowa dotycząca poziomu usług

Temat ten ma na celu zwrócić uwagę na pewne ważne aspekty umów dotyczących poziomu usług (service level agreement - SLA), istotne w realizacji usługi QoS. QoS jest rozwiązaniem dotyczącym całej sieci. Aby uzyskać priorytet sieciowy poza siecią prywatną, może być konieczne zawarcie z dostawcą usług internetowych (ISP) umowy dotyczącej poziomu usług.

## Sytuacje wymagające umowy dotyczącej poziomu usług

Umowa dotycząca poziomu usług jest potrzebna tylko wtedy, gdy stosowane strategie wymagają uzyskiwania priorytetu poza siecią prywatną. Jeśli strategie ruchu wychodzącego są stosowane w celu ograniczenia szybkości ruchu danych opuszczających serwer, nie jest potrzebny gwarantowany poziom usług. W systemie można na przykład utworzyć strategię, dzięki której jedna aplikacja będzie mieć wyższy priorytet niż inna. Priorytet ten będzie uznawany przez system, ale poza systemem już niekoniecznie. Jeśli routery w sieci prywatnej zostaną skonfigurowane tak, aby

rozpoznawać znakowanie punktami kodowymi (używane w strategiach ruchu wychodzącego w celu przypisania poziomu usług), oznakowane dane będą w ramach sieci prywatnej przesyłane priorytetowo. Jednak po opuszczeniu sieci prywatnej priorytet ten nie będzie zagwarantowany. Brak umowy dotyczącej poziomu usług oznacza brak wpływu na sposób obsługi ruchu danych przez sprzęt sieciowy. Zagwarantowanie rezerwacji zasobów lub priorytetu dla klasy usług poza siecią prywatną wymaga zawarcia umowy dotyczącej poziomu usług.

## **Dlaczego potrzebna jest umowa dotycząca poziomu usług**

Strategie i rezerwacje zasobów są tak dobre jak najsłabszy element użyty w realizacji QoS. Oznacza to, że 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 dokładnie rozumieć poziom usług faktycznie zapewniany przez dostawcę. 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. Jeśli na przykład dla telefonii IP zarezerwowano przepustowość 500 kb/s, a aplikacja wymaga jedynie 20 kb/s, firma może ponosić niepotrzebne koszty bez żadnej informacji na ten temat ze strony dostawcy ISP.

**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 1

Przed rozpoczęciem pracy z usługą QoS należy poznać podstawową terminologię i pojęcia związane z jakością usługi. Zrozumienie tych pojęć pomoże określić, czy dana usługa odpowiada potrzebom.

"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 strategie QoS.

"Scenariusz: przewidywalny ruch danych firma-firma (B2B)" na stronie 39

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

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

Jeśli potrzebne jest dedykowane dostarczanie, można je zapewnić korzystając ze strategii usług zintegrowanych (IntServ). Istnieją dwa typy strategii usług zintegrowanych: usługi gwarantowane i usługi sterowanego przeciążenia. 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. Ponieważ aplikacje systemu i5/OS nie obsługują protokołu RSVP, należy o taką obsługę zadbać we własnym zakresie. Służą do tego specjalnie pisane programy korzystające z funkcji API protokołu RSVP lub funkcji API gniazd QoS qtoq. Programy takie umożliwią aplikacjom korzystanie z protokołu RSVP.

## Węzły sieci

Routery, przełączniki i używane systemy operacyjne muszą mieć funkcje umożliwiające stosowanie usługi 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

“Interfejsy API jakości usługi (QoS)” na stronie 16

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazd qtoq, API sendmsg() i API monitorowania.

“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 usługi QoS

Po zaplanowaniu wdrożenia usługi QoS należy utworzyć odpowiednie strategie QoS, korzystając z kreatorów dostępnych w programie System i Navigator. W tym temacie przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych oraz akceptowania ruchu przychodzącego.

Kreatory znacznie ułatwiają proces konfigurowania.

We wcześniej skonfigurowanych strategiach można wprowadzić zmiany, korzystając z obiektów konfiguracyjnych w programie System i Navigator. Obiekty te stanowią części składowe strategii. Pozycja QoS w programie System i Navigator zawiera foldery klientów, aplikacji, harmonogramów, strategii, klas usług, charakterystyki ruchu oraz nazw URI. Obiekty te umożliwiają utworzenie strategii. Szczegółowe informacje na temat poszczególnych obiektów zawiera przegląd zagadnień QoS dostępny w pomocy programu System i Navigator.

## Włączanie strategii QoS

Aby uaktywnić strategię, trzeba ją najpierw włączyć. Jeśli korzystano z kreatorów, system włączy strategię automatycznie. Jeśli jednak wprowadzono zmiany w strategii korzystającej z obiektów konfiguracyjnych, aktywowanie strategii wymaga dynamicznego zaktualizowania systemu. Przed włączeniem danych strategii należy sprawdzić, czy istnieją strategie nakładające się na nią. Może to być bowiem przyczyną problemów.

### Pojęcia pokrewne

“Planowanie wprowadzenia usługi QoS” 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.

Podstawowe informacje o programie System i Navigator

### Zadania pokrewne

“Definiowanie kolejności strategii QoS” na stronie 54

Jeśli zdefiniowano dwie nakładające się strategie, istotną staje się kolejność ich podania w programie System i Navigator.

## Odsyłacze pokrewne

“Zarządzanie usługą QoS” na stronie 55

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

## Konfigurowanie usługi QoS za pomocą kreatorów

Do konfigurowania strategii jakości usługi (QoS) należy używać kreatorów QoS dostępnych w programie System i Navigator.

Poniżej przedstawiono listę kreatorów i opis przeznaczenia każdego z nich:

### Kreator konfiguracji początkowej

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

### Kreator nowej strategii usług zintegrowanych

Kreator ten umożliwia utworzenie strategii usług zintegrowanych. Strategie tego typu sterują dopuszczaniem zgłoszeń RSVP, a tym samym pośrednio kontrolują przepustowość serwera. Limity wydajności zdefiniowane w strategii są używane do ustalenia, czy system jest w stanie zapewnić przepustowość żadaną przez aplikację RSVP klienta. Realizacja zdefiniowanych za pomocą tego kreatora strategii usług zintegrowanych wymaga, aby routery i aplikacje obsługiwały protokół RSVP.

**Uwaga:** Przed skonfigurowaniem strategii usług zintegrowanych należy utworzyć aplikacje umożliwiające korzystanie z protokołu RSVP.

### Kreator nowej strategii usług DiffServ

Kreator ten umożliwia zróżnicowanie obsługi ruchu danych TCP/IP i przypisanie danym priorytetów. Różnicowanie obsługi ruchu w sieci polega na tworzeniu strategii. W ramach strategii można do wychodzącego ruchu danych przypisywać poziomy usług na podstawie źródłowych/docelowych adresów IP, portów, aplikacji, a nawet klientów. Używanym aplikacjom systemu i5/OS można przydzielać poziomy usług na podstawie bardziej szczegółowych informacji o aplikacji.

### Kreator nowej klasy usług

Kreator klasy usług umożliwia definiowanie znakowania pakietów, które będzie stosowane 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 akceptacji nowych połączeń przychodzących umożliwia ograniczanie zakresu połączeń nawiązywanych z systemem. Dostęp do serwera można ograniczyć na podstawie adresu TCP/IP, aplikacji, interfejsu lokalnego lub nazwy URI. Dzięki temu administrator systemu może kontrolować dostęp określonych klientów i aplikacji serwerowych do systemu. Dodatkową korzyścią może być zwiększenie wydajności serwera.

**Uwaga:** Przed skonfigurowaniem strategii połączeń przychodzących korzystającej z nazw URI należy się upewnić, że port aplikacji przypisany do nazwy URI jest taki sam, jak port określony w dyrektywie Listen akceleratora pamięci podręcznej (Fast Response Cache Accelerator - FRCA) w konfiguracji serwera WWW Apache.

Po wybraniu typu tworzonej strategii można odpowiednią strategię skonfigurować za pomocą jednego z opisanych powyżej kreatorów.

## Korzystanie z kreatorów QoS w programie System i Navigator

Podane tu czynności pozwalają uruchamiać kreatory QoS w programie System i Navigator i używać ich do tworzenia strategii.

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

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → Sieć → Strategie IP (*nazwa systemu* > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy element **Jakość usługi** (Quality of Service), a następnie kliknij opcję **Konfiguracja** (Configuration).

**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

“Interfejsy API jakości usługi (QoS)” na stronie 16

W tym temacie przedstawiono informacje na temat protokołów i interfejsów API, jak również wymagania dotyczące routerów obsługujących protokół RSVP (ReSerVation Protocol). Dostępne interfejsy API usługi QoS to API protokołu RSVP (RAPI), API gniazdz qtoq, API sendmsg() i API monitorowania.

“Usługi DiffServ” na stronie 2

Jest to pierwszy typ strategii połączeń wychodzących, które można tworzyć w systemie operacyjnym. 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 na serwer katalogów LDAP (Lightweight Directory Access Protocol), co ułatwia zarządzanie rozwiązaniem QoS.

Zamiast konfigurować strategię QoS na wszystkich systemach, można zapisać dane konfiguracyjne na lokalnym serwerze katalogów i udostępnić je wielu systemom. Podczas pierwszej konfiguracji usługi QoS w systemie zostanie wyświetlony kreator konfiguracji początkowej. Kreator ten oferuje opcję skonfigurowania serwera katalogów.

Aby skonfigurować serwer katalogów, należy:

- znać nazwę serwera katalogów;
- wybrać nazwę wyróżniającą, która będzie odnosić się do strategii QoS;
- określić, czy połączenia z serwerem LDAP mają być zabezpieczone za pomocą protokołu SSL (Secure Sockets Layer);
- 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 w celu konfigurowania funkcji kontrolowania zabezpieczeń w systemie i5/OS.

Jeśli używany jest program System i Navigator, domyślny schemat usługi QoS jest już dostępny. Rzeczywisty plik schematu składowany jest w systemie w katalogu /QIBM/UserData/OS400/DirSrv. Jeśli jednak używany jest inny edytor niż program System i Navigator, konieczne będzie importowanie opisanego w następnej sekcji pliku w formacie LDIF (LDAP Data Interchange Format). Plik ten można importować również po wprowadzeniu zmian, jeśli chce się powrócić do oryginalnego pliku domyślnego.

## Schemat QoS

Poprawność poszczególnych typów obiektów LDAP z punktu widzenia serwera QoS określa zestaw reguł, czyli *schemat*. Schemat zawiera reguły niezbędne do poprawnego funkcjonowania usługi QoS. Jeśli używany serwer LDAP nie jest oparty na platformie System i, reguły te należy importować na serwer LDAP. Służy do tego plik w formacie LDIF (LDAP Data Interchange Format). Plik LDIF można pobrać ze strony WWW dotyczącej katalogów LDAP. Plik można znaleźć w sekcji **Kategorie** → **Strategie TCP/IP** (Categories > TCP/IP Policies) w lewym panelu.

### Pojęcia pokrewne

“Serwer katalogów” na stronie 25

Strategie można eksportować do serwera katalogów. W tym temacie opisano konfigurowanie protokołu LDAP (Lightweight Directory Access Protocol) i związane z nim pojęcia, jak również schemat usługi QoS.

“Nazwa wyróżniająca” na stronie 26

Aby zarządzać częścią katalogu, należy użyć nazwy wyróżniającej lub (jeśli zostanie wybrane takie rozwiązanie) słowa kluczowego.

IBM Tivoli Directory Server for i5/OS (LDAP)

Włączanie SSL i TLS na serwerze Directory Server

“Słowa kluczowe” na stronie 25

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

### Informacje pokrewne



IBM LDAP Directory Schema

## Definiowanie kolejności strategii QoS

Jeśli zdefiniowano dwie nakładające się strategie, istotna staje się kolejność ich podania w programie System i Navigator.

Strategie nakładają się, jeśli mają wspólny jeden z następujących parametrów: klienta, aplikację, harmonogram, lokalny adres IP, nazwę URI, dane serwera, punkt kodowy lub protokół. Strategie wyświetlane w programie System i Navigator mają postać listy uporządkowanej. 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 określić, czy strategia nakłada się na inną strategię, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy **Jakość usług**.
3. Wybierz opcję **Konfiguracja**.
4. Wybierz folder **Określone strategie** (Specific Policies).
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 usługi QoS” na stronie 51

Po zaplanowaniu wdrożenia usługi QoS należy utworzyć odpowiednie strategie QoS, korzystając z kreatorów dostępnych w programie System i Navigator. W tym temacie przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych oraz akceptowania ruchu przychodzącego.

“Kopiowanie istniejącej strategii” na stronie 56

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

“Rozwiązywanie problemów z usługą QoS” na stronie 61

Usługa QoS udostępnia wiele metod rozwiązywania problemów.

### Zadania pokrewne

“Korzystanie z pomocy dotyczącej usługi QoS w programie System i Navigator”

Aby uzyskać dostęp do pomocy dotyczącej usługi QoS, można użyć programu System i 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 i funkcji gromadzenia danych do analizy ruchu IP w systemie.

### Pojęcia pokrewne

“Konfigurowanie usługi QoS” na stronie 51

Po zaplanowaniu wdrożenia usługi QoS należy utworzyć odpowiednie strategie QoS, korzystając z kreatorów dostępnych w programie System i Navigator. W tym temacie przedstawiono sposoby tworzenia strategii usług DiffServ, usług zintegrowanych oraz akceptowania ruchu przychodzącego.

## Korzystanie z pomocy dotyczącej usługi QoS w programie System i Navigator

Aby uzyskać dostęp do pomocy dotyczącej usługi QoS, można użyć programu System i Navigator.

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy element **Jakość usługi** (Quality of Service), a następnie kliknij opcję **Konfiguracja** (Configuration).
3. Kliknij opcję **Pomoc** → **Tematy pomocy** (Help > Help topics) w pasku menu. Zostanie wyświetlone okno pomocy.

### Zadania pokrewne

“Definiowanie kolejności strategii QoS” na stronie 54

Jeśli zdefiniowano dwie nakładające się strategie, istotna staje się kolejność ich podania w programie System i Navigator.

## Składowanie strategii QoS

Strategie QoS należy składać, aby zapobiec konieczności ich ponownego tworzenia w razie wyłączenia systemu 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 zapasowych 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 odtwarzanie* zawiera instrukcje na temat odzyskiwania danych z zintegrowanego systemu plików.

### 2. Wydrukuj strategię.

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, ponieważ nie wymaga ręcznego wprowadzania danych, które istnieją już w postaci cyfrowej. Jest to prosta metoda przenoszenia danych z jednego źródła elektronicznego do innego.

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

Korzystając z produktu System i, należy zaplanować strategię składowania i odtwarzania danych.

#### Informacje pokrewne



Składowanie systemu

## Kopiowanie istniejącej strategii

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

W programie System i Navigator ta funkcja usługi QoS nosi nazwę *Nowa w oparciu o* (New based on). Aby skopiować strategię, należy skorzystać z programu System i Navigator i wyświetlić okno dialogowe usługi QoS.

Aby utworzyć kopię istniejącej strategii, należy wykonać czynności opisane w temacie pomocy **Tworzenie nowej strategii opartej na istniejącej strategii** w programie System i 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

“Definiowanie kolejności strategii QoS” na stronie 54

Jeśli zdefiniowano dwie nakładające się strategie, istotna staje się kolejność ich podania w programie System i Navigator.

## Edytowanie strategii QoS

Gdy zmieniają 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 skonfigurowanych strategiach można wprowadzić zmiany, korzystając z obiektów konfiguracyjnych w programie System i Navigator. Obiekty te stanowią części składowe strategii. Pozycja QoS w programie System i Navigator zawiera foldery klientów, aplikacji, harmonogramów, strategii, klas usług, charakterystyki ruchu oraz nazw URI. Obiekty te umożliwiają edytowanie strategii.

Aby wprowadzić zmiany w strategii za pomocą programu System i Navigator, wykonaj czynności opisane w pomocy tego programu, w sekcji Edytowanie strategii QoS.

## Monitorowanie usługi QoS

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

Monitor QoS pomaga w określeniu przyczyn powstawania przeciążeń w sieci. Przydaje się to nie tylko podczas planowania usługi 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 opcje **Server** → **Monitorowanie**. Aby monitorować jedną strategię, należy kliknąć strategię prawym przyciskiem myszy i wybrać opcję **Monitorowanie** (Monitor).

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 gromadzenia danych.

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

Jeśli wyniki monitorowania mają być zapisywane, trzeba uruchomić gromadzenie danych QoS. Monitor będzie gromadził dane do momentu zatrzymania funkcji gromadzenia. Zamknięcie okna monitora nie powoduje zatrzymania gromadzenia danych. Istnieje także możliwość zmiany właściwości, na podstawie których działa monitor podczas gromadzenia danych. W tym celu należy w oknie Monitor QoS (QoS Monitor) podświetlić pozycję **Monitor QoS** (QoS Monitor) i wybrać opcję **Plik->Właściwości** (File > Properties). Więcej informacji na ten temat zawiera pomoc elektroniczna.

Jeśli gromadzenie danych QoS jest włączone i ulegną zmianie właściwości monitora, to aby zmiany zostały uwzględnione w sposobie gromadzenia danych, należy wykonać następujące czynności:

1. Zatrzymaj gromadzenie 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 gromadzenie danych QoS.

## Monitorowanie danych wyjściowych

Dane wyjściowe monitora zależą od typu strategii, która jest monitorowana. Jak zostało to opisane w innym temacie, dostępne są następujące typy strategii: usługi DiffServ, usługi zintegrowane (kontrolowane przeciążenie), usługi zintegrowane (gwarantowane) 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 obsługiwanych, 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. Temat 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.

Tabela 4. Strategie usług DiffServ (kontynuacja)

Pole	Opis
Limit szybkości średniej tokenów	Średnia szybkość tokenów dozwolona w tej strategii dla każdego routera i systemu znajdującego się na trasie przepływu.
Limit liczby tokenów	Maksymalna wielkość buforu tokenów dozwolona w tej strategii dla każdego routera i systemu znajdującego się na trasie przepływu.
Limit szybkości szczytowej tokenów	Maksymalna szybkość tokenów dopuszczalna w danym połączeniu.
Pakiety w profilu	Liczba nadanych pakietów IP, które spełniały ograniczenia określone w strategii.
Bitów w profilu	Liczba nadanych bitów, które spełniały ograniczenia określone w strategii.
Bitów 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>• znakowanie,</li> <li>• kształtowanie,</li> <li>• odrzucanie.</li> </ul>
Bitów łącznie	Liczba bitów nadanych w danej strategii od chwili jej uruchomienia do chwili zbierania danych.
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 przeciążenie)

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

Tabela 5. Strategie usług zintegrowanych (sterowane przeciążenie)

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).



Tabela 5. Strategie usług zintegrowanych (sterowane przeciążenie) (kontynuacja)

Pole	Opis
Limit szybkości średniej tokenów	Średnia szybkość tokenów dozwolona w tej strategii dla każdego routera i systemu znajdującego się na trasie połączenia.
Limit liczby tokenów	Maksymalna wielkość buforu tokenów dozwolona w tej strategii dla każdego routera i systemu 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, które mogą być usunięte 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 (usługi gwarantowane)

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

Tabela 6. Strategie usług zintegrowanych (usługi gwarantowane)

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	Maksymalna szybkość tokenów dozwolona w tej strategii dla każdego routera i systemu znajdującego się na trasie połączenia.
Limit liczby tokenów	Maksymalna wielkość buforu tokenów dozwolona w tej strategii dla każdego routera i systemu 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.

Tabela 6. Strategie usług zintegrowanych (usługi gwarantowane) (kontynuacja)

Pole	Opis
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, które mogą być usunięte 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 systemem.
Żądania zaakceptowane	Łączna liczba żądań połączenia zaakceptowanych przez system.
Żądania odrzucone	Łączna liczba żądań połączenia odrzuconych przez system.
Limit szybkości średniej połączeń	Dozwolona średnia liczba akceptowanych przez serwer połączeń na sekundę.
Limit porcji połączeń	Maksymalna liczba połączeń akceptowanych równocześnie.
Limit szybkości szczytowej połączeń	Maksymalna szybkość, z którą system będzie 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 systemie.
Adres interfejsu	Adres IP monitorowanego interfejsu systemu.
Zakres adresów źródłowych	Zakres adresów IP klientów wysyłających żądania do systemu.
Uniform Resource Identifier (URI)	Określa nazwę URI sterowaną 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.

“Scenariusz: ograniczanie połączeń przychodzących” na stronie 36

Jeśli zachodzi potrzeba kontrolowania nadsyłanych do systemu żądań połączeń, należy użyć strategii akceptowania połączeń przychodzących.

“Scenariusz: przewidywalny ruch danych firma-firma (B2B)” na stronie 39

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

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

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

“Scenariusze: strategię QoS” na stronie 28

Podane tu scenariusze użycia strategii QoS pomagają zrozumieć przeznaczenie usługi QoS oraz poznać zasady tworzenia strategii i klas usług.

“Monitorowanie transakcji w systemie” na stronie 64

W tym temacie omówiono monitor QoS umożliwiający sprawdzenie, czy strategię QoS działają zgodnie z oczekiwaniami. Monitor QoS może być przydatny w fazie planowania QoS i rozwiązywania problemów dotyczących tej usługi.

“Scenariusz: monitorowanie bieżących statystyk sieci” na stronie 46

Podczas korzystania z kreatorów należy ustawić ograniczenia wydajności odpowiadające indywidualnym wymaganiom obsługi sieci.

---

## Rozwiązywanie problemów z usługą QoS

Usługa QoS udostępnia wiele metod rozwiązywania problemów.

### Śledzenie komunikacji

System umożliwia śledzenie komunikacji na określonym łączy, na przykład interfejsie sieci lokalnej (LAN) lub rozległej (WAN). Przeciętny użytkownik może nie rozumieć całej treści danych śledzenia. Na ich podstawie może jednak sprawdzić, czy między dwoma węzłami nastąpiła faktycznie wymiana danych.

### Włączanie usługi QoS w systemie

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

Aby sprawdzić, czy funkcja QoS jest włączona w systemie, należy wykonać następujące czynności:

1. W programie System i Navigator rozwiń węzły **nazwa systemu** → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
2. Kliknij prawym przyciskiem myszy **Jakość usług** i wybierz opcję **Konfiguracja**.
3. Po wyświetleniu interfejsu QoS kliknij prawym przyciskiem myszy element **QoS** i wybierz opcję **Właściwości** (Properties).
4. Na stronie Właściwości QoS sprawdź, czy wybrana jest opcja **Włącz QoS**.

#### Pojęcia pokrewne

Śledzenie komunikacji

#### Zadania pokrewne

“Definiowanie kolejności strategii QoS” na stronie 54

Jeśli zdefiniowano dwie nakładające się strategię, istotna staje się kolejność ich podania w programie System i Navigator.

## Kronikowanie strategii QoS

Usługa QoS obejmuje funkcję kronikowania. Kronikowanie pozwala śledzić operacje związane ze strategiami QoS, w tym dodawanie, usuwanie i modyfikowanie strategii.

Gdy funkcja kronikowania jest włączona, wszystkie operacje związane ze strategiami są zapisywane w protokole. Ułatwia to wykrywanie błędów i określanie ustawień powodujących, że strategie 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. Na podstawie kronik można utworzyć zbiór ogólny w systemie. Korzystając z danych zapisanych w kronikach można się zorientować, 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. Do włączania i wyłączania kronikowania służy program System i Navigator. W celu przeglądania kronik należy skorzystać z interfejsu wiersza komend.

Aby uruchomić lub zatrzymać kronikowanie, wykonaj następujące czynności:

1. W programie System i Navigator rozwiń węzły *nazwa systemu* → **Sieć** → **Strategie IP** (*nazwa systemu* > Network > IP Policies).
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, aby wyłączyć funkcję kronikowania.

**Uwaga:** Jeśli system był włączony 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 system lub dokonać jego aktualizacji. W obu przypadkach zostanie ponownie odczytany plik policy.conf i sprawdzony atrybut kronikowania.

## Wyświetlanie pozycji kroniki na ekranie

W tym temacie opisano sposób wyświetlania pozycji kroniki na ekranie komputera.

1. W wierszu komend wpisz komendę `DSPJRN JRN(QUSRSYS/QQOS)`.
2. Obok pozycji kroniki, która ma być wyświetlona, wybierz opcję 5.

## Przeglądanie pozycji kroniki za pośrednictwem zbioru wyjściowego

Aby przeglądać pozycje kroniki sformatowane w postaci pojedynczego folderu, należy zapoznać się ze zbiorem MODEL.OUT w katalogu QUSRSYS. Skopiowanie pozycji kroniki do zbioru wyjściowego umożliwia łatwe przeglądanie danych za pomocą narzędzi zapytań, na przykład Query/400 lub języka SQL (Structured Query Language). Można też tworzyć w językach wysokiego poziomu własne programy do przetwarzania pozycji w zbiorze wyjściowym.

Aby skopiować pozycje kroniki QoS do systemowego zbioru wyjściowego, należy wykonać następujące czynności:

1. Utwórz kopię systemowego zbioru wyjściowego QSYS/QATOQQOS w bibliotece użytkownika. Można to zrobić, korzystając z 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 użyje się komendy DSPJRN dla nieistniejącego zbioru wyjściowego, system utworzy taki zbiór, ale nie będzie on zawierał poprawnych opisów pól.

- DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTYP(MP) CMTCYCID(\*ALL) OUTPUT(\*OUTFILE) OUTFILFMT(\*TYPE4) OUTFILE(*biblioteka użytkownika/zbiór użytkownika*)
- DSPF FILE(*biblioteka użytkownika/zbiór użytkownika*)

## Protokołowanie zadań serwera QoS

Gdy wystąpią problemy ze strategiami QoS, należy przeanalizować protokoły zadań. 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 w programie System i Navigator.

Aby wyświetlić protokół zadania, należy wykonać następujące 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 zadanie podstawowe, które uruchamia wszystkie interfejsy TCP/IP. W razie wystąpienia podstawowych problemów z protokołem TCP/IP należy zanalizować protokół zadania QTCPPI.

### QTOQSRVR

Jest to zadanie podstawowe, udostępniające informacje z protokołu dotyczące 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 zbiorami komunikatów (Work with Message Files) wpisz następujące dane i naciśnij klawisz Enter:  
Zbiór komunikatów: QTCPMSG  
Biblioteka: \*LIBL
7. Aby wyświetlić wybrany zbiór komunikatu, w panelu Praca ze zbiorami komunikatów (Work with Message Files) 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. Zostanie wyświetlony szczegółowy opis komunikatu.

## Monitorowanie transakcji w systemie

W tym temacie omówiono monitor QoS umożliwiający sprawdzenie, czy strategię QoS działają zgodnie z oczekiwaniami. Monitor QoS może być przydatny w fazie planowania QoS i rozwiązywania problemów dotyczących tej usługi.

Monitor można wykorzystać do analizy ruchu danych IP obsługiwanych przez system. 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 właściwe wartości, 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. Zapoznaj się z przykładową strategią monitora, aby określić charakterystyki bieżącego ruchu w sieci.

## 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 strategię 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 połączeń przychodzących korzystającej z nazw URI należy się upewnić, że port aplikacji przypisany do nazwy URI jest taki sam, jak port określony w dyrektywie Listen akceleratora pamięci podręcznej (Fast Response Cache Accelerator - FRCA) w konfiguracji serwera WWW Apache.
- Sprawdzić harmonogram strategii. Być może analizowane wyniki dotyczą okresu, w którym strategia nie była aktywna.
- Sprawdzić, czy poprawny jest numer portu.
- Sprawdzić, czy poprawny jest adres IP.

### Pojęcia pokrewne

“Planowanie wprowadzenia usługi QoS” 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: strategię QoS” na stronie 28

Podane tu scenariusze użycia strategii QoS pomagają zrozumieć przeznaczenie usługi QoS oraz poznać zasady tworzenia strategii i klas usług.

### Odsyłacze pokrewne

“Monitorowanie usługi QoS” na stronie 57

Monitor usługi QoS można wykorzystać do analizy ruchu danych IP obsługiwanych przez system.

### Informacje pokrewne

Zarządzanie adresami i portami serwera HTTP (opartego na Apache)

## Śledzenie aplikacji TCP/IP

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

Aby uruchomić śledzenie w systemie, w wierszu komend wpisz TRCTCPAPP (komenda Śledzenie aplikacji TCP/IP - Trace TCP/IP Application).

Oto przykład wartości opcji śledzenia:

```

Aplikacja TCP/IP.....> *QOS      (TCP/IP application)
Ustawienia opcji śledzenia.....> *ON      (Trace option setting)
Maks. pamięć dla śledzenia.....> *APP      (Maximum storage for trace)
Działanie po wypełnieniu.....> *WRAP      (Trace full action)
Listy argumentów.....> 'lvl=4'      (Argument lists)
Typ śledzenia QoS.....> *ALL      (QoS trace type)
  
```

W poniższej tabeli zebrano możliwe parametry komendy śledzenia. Jeśli ustawienie nie jest widoczne w interfejsie znakowym, 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 wypełnieniu (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 wypełnieniu pamięci śledzenie zostaje zatrzymane lub rozpoczyna się zapisywanie od początku buforu. Wartością domyślną jest 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 domyślna wielkość pamięci śledzenia to 4 MB.

## Działanie po wypełnieniu

### \*WRAP

Opcja ta powoduje, że po wypełnieniu buforu pamięci dane śledzenia zapisywane są od początku buforu (zawijane). Zawijanie polega na nadpisywaniu przez system najstarszych danych w pliku, dzięki czemu możliwe jest kontynuowanie śledzenia. Jeśli opcja ta nie zostanie wybrana, po wypełnieniu buforu śledzenie zatrzymuje się.

### \*STOPTRC

Powoduje zatrzymanie zbierania danych po osiągnięciu przez system maksymalnej wielkości pliku.

## Lista argumentów

Listy argumentów określają, które poziomy błędów i jaka treść podlegają protokołowaniu. W komendzie TRCTCPAPP dopuszczalne są dwa argumenty: poziom śledzenia i zawartość. Podając poziom i zawartość śledzenia należy się upewnić, że wszystkie atrybuty są objęte tym samym cudzysłowem, 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 obiektu może na przykład wystąpić w wyniku nieoczekiwanego wyniku operacji systemowej. 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 wyłącznie operacji związanych z usługami zintegrowanymi. Należy z niej skorzystać, jeśli analiza wykaże, że problem dotyczy właśnie usług zintegrowanych.

### **Zawartość = Diffserv ('c=d')**

Opcja ta określa śledzenie wyłącznie operacji związanych z usługami DiffServ. Należy z niej skorzystać, jeśli analiza wykaże, że problem dotyczy właśnie usług DiffServ.

### **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**

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

## **Przykłady: odczytywanie danych wyjściowych śledzenia**

W tym temacie 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 najważniejszym zdarzeniem, którego należy szukać, jest ewentualne odrzucenie połączenia RSVP z powodu braku odpowiedniej strategii dla danego połączenia. 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: Znalaziono nazwę działania  
vreStnl_kraMoNICvreStnl dla przepływu[sesja=x.x.x.y:z:s, źródło=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.y]

W przypadku strategii usług DiffServ najważniejsze są komunikaty pokazujące, czy serwer załadował regułę strategii, czy też 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 5761SS1 V6R1M0 010525 TRCTCPAPP Output RS004 Date-01/11/07 Time-14:08:03 Page-6
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 pokrewne dotyczące usługi QoS

Informacje związane z kolekcją tematów o usługach QoS można znaleźć w dokumencie RFC definiującym usługi QoS, dokumentacji technicznej IBM Redbooks oraz innych kolekcjach tematów centrum informacyjnego. Wszystkie pliki PDF można wyświetlić lub wydrukować.

### Dokumenty RFC definiujące 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 typu usługi będącego elementem nagłówka pakietu IP

- **RFC 2205.**

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

- **RFC 2210.**



W dokumencie tym wyjaśniono wykorzystanie protokołu RSVP w odniesieniu do usług zintegrowanych IETF.

- **RFC 2474.**




W dokumencie tym zdefiniowano znaczenie pola usług DiffServ.

- **RFC 2475.**

W dokumencie tym przedstawiono architekturę usług DiffServ.

Aby zapoznać się z wymienionymi dokumentami RFC, skorzystaj z wyszukiwarki RFC Index  w serwisie WWW RFC Editor .

## Dokumentacja techniczna IBM (Redbooks)

- IBM i5/OS IP Networks: Dynamic  (około 16 589 KB). Opisuje sposób zaprojektowania odpornej na błędy, wydajnej sieci IP z możliwością autokonfigurowania. Poza wieloma innymi funkcjami, publikacja ta omawia zarówno teoretyczne podstawy usługi QoS, jak i zasady jej implementowania na serwerze. Można tam także znaleźć więcej przykładowych scenariuszy ze szczegółowymi instrukcjami.
- V4 TCP/IP for AS/400: 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 w systemie, 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

- IBM Tivoli Directory Server for i5/OS (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 bezpieczeństwa mogą analizować rekordy kontroli powstałe w procesie wykrywania włamań w celu zabezpieczenia sieci i5/OS przed takimi atakami.

### Odsyłacze pokrewne

“Plik PDF z informacjami dotyczącymi usługi QoS” na stronie 1

Informacje zawarte w tym temacie są także dostępne w postaci pliku PDF, który można wyświetlić i wydrukować.

---

## 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 niniejszej 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, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA 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 niniejszym dokumencie 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, Umowie Licencyjnej 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 możliwości 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/nazwiska są fikcyjne i jakiegokolwiek podobieństwo do istniejących nazw/nazwisk i adresów 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. Programy przykładowe nie zostały gruntownie przetestowane. 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.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

---

## Informacje dotyczące interfejsu programistycznego

Niniejsza publikacja dotycząca jakości usługi (QoS) 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:

AS/400  
i5/OS  
IBM  
IBM (logo)  
OS/400  
Redbooks  
System i  
Tivoli

Adobe, logo Adobe, PostScript oraz logo PostScript są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Adobe Systems Incorporated w Stanach Zjednoczonych i/lub w innych krajach.

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.





Drukowane w USA