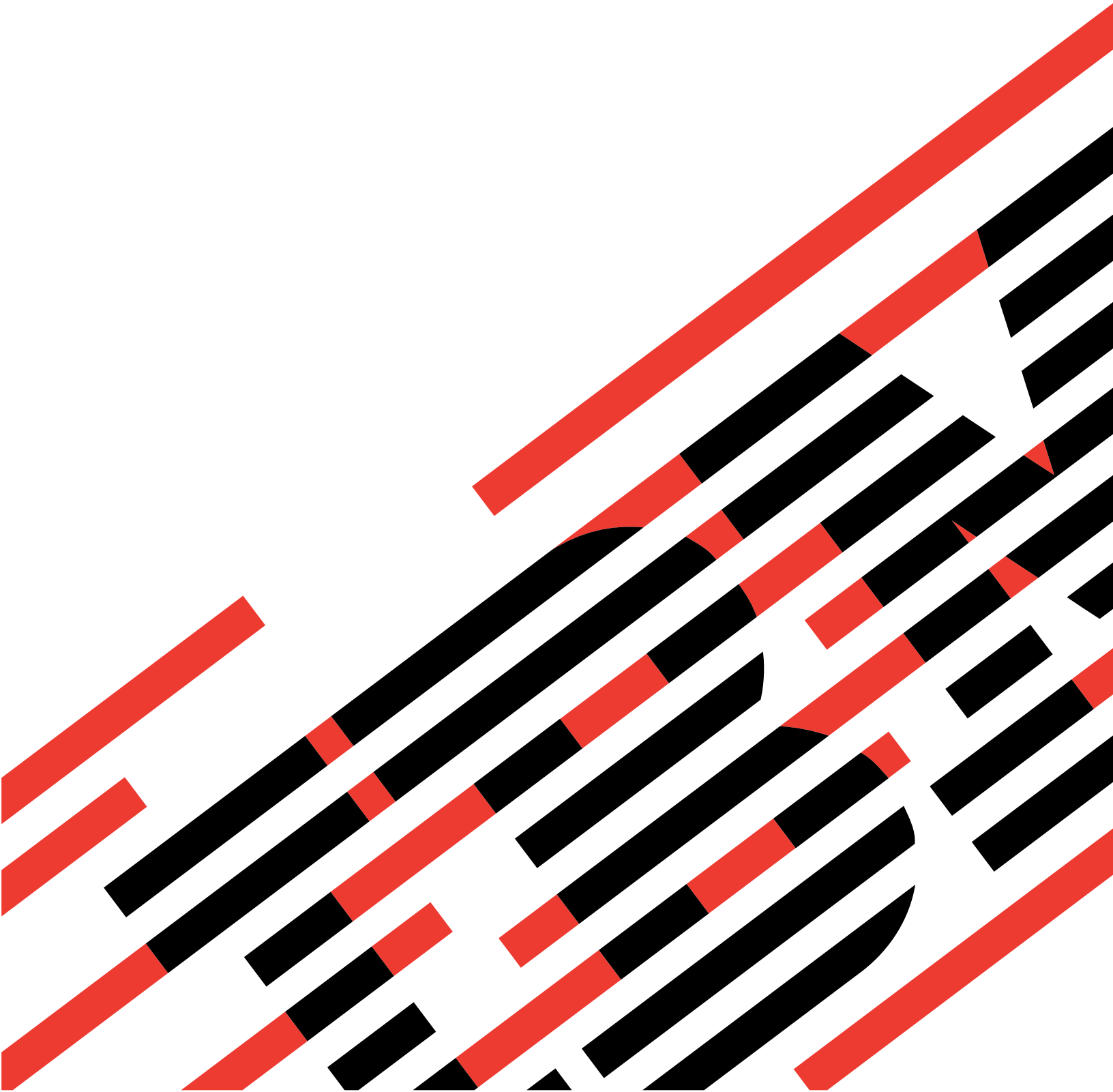
IBM

eserver

iSeries

QoS (Quality of service)



IBM

@server

iSeries

QoS (Quality of service)

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

原　典： RZAK–8000–01
iSeries
Quality of service

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2002.6

目次

Quality of service (QoS) 1
V5R2 の新機能 2
このトピックの印刷 3
QoS のシナリオ 3
QoS シナリオ: 専用送達 (IP テレフォニー) 5
QoS シナリオ: ブラウザー・トラフィックの制限 7
QoS シナリオ: インバウンド接続の制限 10
QoS シナリオ: 予測可能な B2B トラフィック 13
QoS シナリオ: 安全で予測可能な結果 (VPN と QoS) 15
QoS の概念 19
接続要求速度および URI 要求速度 19
平均接続速度およびバースト限界 21
DiffServ (差異化サービス) 21
DiffServ サービス・クラス 22
コード・ポイントおよび PHB (ホップごとの転送優先順位付け) 23
トラフィック・コンディショナー 24
ディレクトリー・サーバーの概念 25
キーワード 26
統合サービス 26
トラフィック制御機能 28
統合サービス・タイプ 29
トークン・バケットおよび帯域幅の限界 29
DiffServ マーキングを使用した統合サービス 30
RSVP プロトコルおよび QoS API 31
QoS API コネクション型機能フロー 33
QoS API コネクションレス機能フロー 35
QoS の計画 36
権限要件 36
システム要件 37
QoS ポリシーの順序付け 37
サービス・レベル・アグリーメント 38
ネットワークのハードウェアおよびソフトウェア 39
QoS の構成 39
ディレクトリー・サーバーの構成 39
ウィザードを使用した QoS の構成 40
iSeries ナビゲーターでの QoS ウィザードへのアクセス 42
QoS の管理 43
iSeries ナビゲーターの QoS ヘルプへのアクセス 43
QoS ポリシーのバックアップ 44
既存ポリシーのコピー 44
QoS のモニター 48
QoS のトラブルシューティング 49
QoS ポリシーのジャーナル処理 50
QoS サーバー・ジョブのロギング 51
サーバー・トランザクションのモニター 52
現在のネットワーク統計のモニター 52
TCP アプリケーションのトレース 55
トレース出力の読み方 57

QoS に関するその他の情報 57

Quality of service (QoS)

ネットワークのすべてのトラフィックは等しい優先順位を与えられます。クリティカルではないブラウザー・トラフィックもクリティカルなビジネス・アプリケーションと同じくらい重要と見なされます。最高経営責任者 (CEO) が、オーディオ / ビデオ・アプリケーションを使用してプレゼンテーションを行なおうとしている場合、IP パケットの優先順位が重要な問題です。プレゼンテーションの間、このアプリケーションが他のアプリケーションより優れたパフォーマンスを得られることが肝心です。

QoS を使用して、TCP/IP アプリケーションのネットワーク優先順位と帯域幅を要求することができます。マルチメディアなど、予測可能で信頼できる結果が必要なアプリケーションを送信する場合、パケットの優先順位が重要です。

ポリシー規則を計画する前に、QoS について理解しておくことが大切です。以下のリンクは、QoS をインプリメントする時に必要な情報を提供します。

V5R2 の新機能
Quality of service のネットワーキング機能および Information Center のトピックに加えられた変更をリストします。

このトピックの印刷
このトピック全部を印刷します。

QoS のシナリオ
いくつかの QoS シナリオが表示され、そこで QoS を使用する理由および使用方法を学びます。

QoS の概念
Quality of service に関して知識がない場合は、ここで基本的な QoS の概念とメカニズムを確認してください。ここでは、QoS の機能、および複数の QoS メカニズムが一体となってどう作用するか、などの概要を説明します。

QoS の計画
計画アドバイザー、および QoS を効果的に使用するために必要なネットワーク情報にリンクします。

QoS の構成
新規の DiffServ ポリシーおよび統合サービス・ポリシーを作成する時は、ここの手順に従ってください。

QoS の管理
既存のポリシーを編集する場合は、ここの手順に従ってください。ポリシーの削除、トレース、およびその他のポリシー管理技法の実際のタスクの保管場所情報が記載されています。

QoS のトラブルシューティング
このトラブルシューティング情報は、QoS の問題のデバッグにお役立てください。

QoS に関するその他の情報
他の有効な QoS ソースへのリンクが記載されています。その他にも多数のブック、Web サイト、Request For Comments (RFC)、およびホワイト・ペーパーがあります。

V5R2 の新機能

このトピックでは、バージョン 5 リリース 2 で新たに加えられた機能について説明します。このトピックの設計上の注目すべき改善点もいくつか説明します。

新機能

- **ポリシーをローカル・インターフェースに関連付ける**
  ポリシーを、iSeries (TM) の特定のローカル・インターフェースまたは一連のローカル・インターフェースに関連付けることができます。ローカル・インターフェースを指定することにより、クライアント・パケットがどのインターフェースに届くかを基に種々のポリシーを作成することができます。
- **ポリシーを複数のクライアントに関連付ける**
  ポリシーを複数のクライアントに関連付けることができます。これにより、より柔軟なポリシー定義を作成することができます。
- **インバウンド・アドミッション・ポリシー**
  サーバーにアクセスしようとする外部トラフィックを制御するためのポリシーを作成できます。 2 つの新しいウィザードにより、ネットワーク内の特定の IP アドレスまたは URI 値にアクセスしようとするトラフィックを制御することができます。上記のリンクを使用して、2 つのインバウンド・ポリシーに関する詳細を習得してください。
- **モニター情報を保管および印刷することができる**
  モニター情報を保管および印刷できるようになりました。モニター情報を保管すると、それを将来参照する時にアクセスできるようになります。モニター情報を印刷したい場合は、「HTML としてエクスポート (Export as HTML)」を指定することができます。
- **ポリシーを LDAP ディレクトリー・サーバーに保管する**
  最新の LDAP プロトコル バージョン 3 を含んだディレクトリー・サーバーに、ポリシーをエクスポートできるようになりました。ディレクトリー・サーバーを使用すると、QoS ソリューションをより簡単に管理できます。各サーバーに同じ QoS ポリシーを構成する代わりに、単一のサーバーで作成されるポリシー・データを使用できるように各サーバーを構成することができます。この場合、ポリシーはディレクトリー・サーバーに保管されます。このリンクを使用して、構成に関する詳細を参照してください。
- **スケジュール変更**
  スケジュールを時刻範囲を用いて定義します。従来は、時刻範囲は同じ日の中に設定する必要がありました。今回から、時刻範囲は任意の 24 時間枠で (2 日間にまたがった場合でも) 指定することができます。ポリシーをいつアクティブにするかを指定するために、スケジュールをポリシーに関連付けます。これにより、より柔軟なポリシー定義を作成することができます。

設計上の新しい改善点

- **QoS 計画アドバイザー**
  QoS 計画アドバイザーが更新されて、ポリシーを構成する前に提案および前提条件が示されます。 QoS 計画アドバイザーは、編成されたロケーションで複数の概念をまとめることによって計画の立案を援助します。
- **新しいインバウンド・シナリオ**
  インバウンド・ポリシーのインプリメンテーションの例を示すために、新しいシナリオが追加されました。

新規または変更情報を参照する方法

技術上の変更が加えられた箇所がわかるようにするために、以下のイメージが使用されています。

- » イメージ。新規または変更情報の始まりを示します。
- « イメージ。新規または変更情報の終わりを示します。

このリリースの新規または変更情報に関するその他の情報を見つけるには、 iSeries プログラム資料説明書 を参照してください。

このトピックの印刷

PDF 版をダウンロードし、表示するには、「Quality of service」(約 926 KB、66 ページ) を選択します。

表示用または印刷用の PDF ファイルを Netscape Navigator からワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから、「**ファイル**」をクリックする。
3. 「**名前を付けて保存**」をクリックする (IE の場合はフロッピーディスクのアイコン (名前を付けて保存) をクリックする)。
4. PDF を保存したいディレクトリーに進む。
5. 「**保存**」をクリックする。

PDF ファイルを表示したり印刷したりするためには、Adobe Acrobat Reader が必要です。これは、 Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html) からダウンロードできます。

QoS のシナリオ

Quality of service について学ぶ最善の方法の 1 つは、ネットワーク全体図の中で機能がどのように動作するかを確認することです。以下の基本例は、Quality of service ポリシーを使用する理由を示しています。
»

シナリオ: 専用送達 (IP テレフォニー)
専用送達が必要で、予約を要求したい場合は、統合サービス・ポリシーを使用します。作成する統合サービス・ポリシーには、2 つのタイプ (保証されたサービスと負荷コントロール・サービス) があります。この例では、保証されたサービスを使用します。

シナリオ: ブラウザー・トラフィックの制限
QoS を使用してトラフィック・パフォーマンスを制御できます。ネットワーク内でのアプリケーションのパフォーマンスを制限または拡張するには、DiffServ ポリシーを使用します。

シナリオ: インバウンド接続の制限
ユーザーのサーバーに対してなされるインバウンド接続要求を制御する必要がある場合には、インバウンド・アドミッション・ポリシーを使用します。

シナリオ: 予測可能な B2B トラフィック
予測可能な送達が必要で、引き続き予約を要求したい場合は、統合サービス・ポリシーも使用します。 ただし、この例では、負荷コントロール・サービスを使用します。

シナリオ: 安全で予測可能な結果 (VPN と QoS)
VPN (仮想プライベート・ネットワーク) を使用している場合でも、Quality of service ポリシーを作成できます。この例では、VPN と QoS の両方が使用されています。

«

注: IP アドレスと図は架空のものであり、例示目的でのみ使用されています。

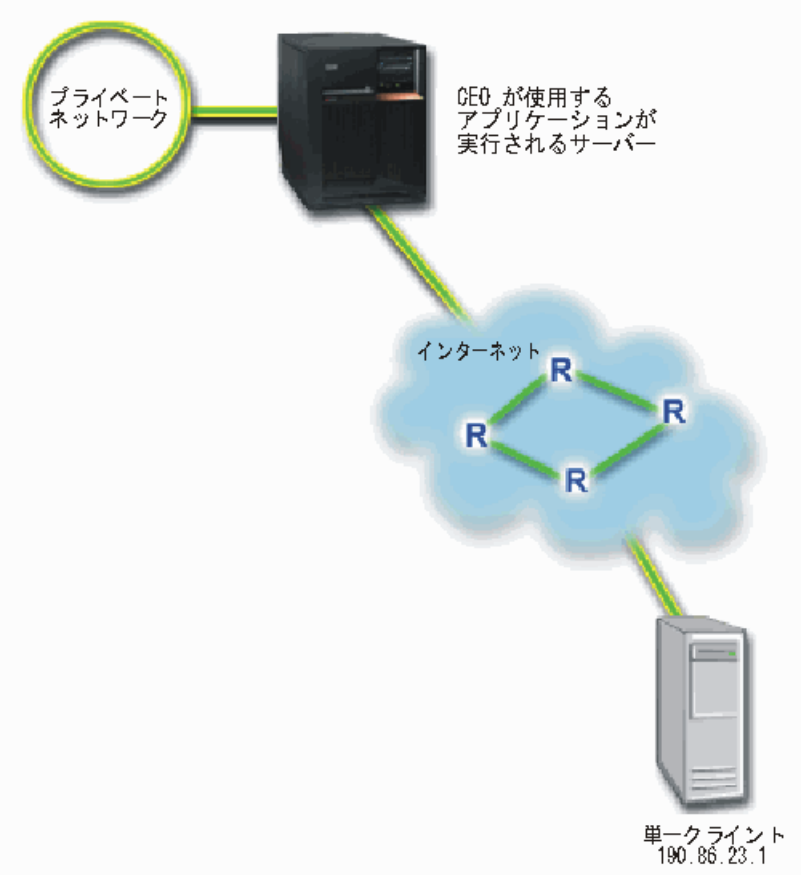
QoS シナリオ: 専用送達 (IP テレフォニー)

»

問題

会社の最高経営責任者 (CEO) は、午後 1 時～ 2 時の間、全国に設置されているクライアントにライブ・ブロードキャストを提供したいと考えています。ライブ・ブロードキャスト中に中断しないように IP テレフォニーに保証された帯域幅を用意する必要があります。このシナリオでは、アプリケーションはサーバーに常駐させます。次の図は、このシナリオでのネットワーク・セットアップを示しています。 iSeries サーバーは OS/400(R) V5R2 で稼働しています。

図 1. 統合サービス・ポリシーによって保証された CEO からクライアントへのプレゼンテーション



ソリューション

非常に機密性の高いアプリケーションには、保証された接続が必要です。 CEO が使用しているアプリケーションは、スムーズで中断されない転送を必要とするので、保証された統合サービス・ポリシーを使用することに決めました。 保証されたサービスは、パケットがある特定の時間以上は遅れないように最大キューイング遅延を制御します。

この接続を保証されたものにしたいので、保証されたサービスに統合サービス・ポリシーを使用します。統合サービス・ポリシーには、RSVP 使用可能アプリケーションが必要です。 現在、ご使用のサーバーには RSVP 使用可能アプリケーションがないため、ユーザー自身の RSVP 使用可能アプリケーションを作成する必要があります。ユーザー自身のアプリケーションを作成するには、 Resource Reservation Setup Protocol (RAPI) API または qtoq QoS ソケット API を使用してください。

統合サービス・ポリシーを使用する場合、トラフィック・パス沿いにあるルーターも RSVP 使用可能でなくてはなりません。 詳細は、統合サービスの概念に関するセクションを参照してください。

構成

1. iSeries ナビゲーターで QoS を開きます。
    1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
    2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
    3. 「**アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)**」を展開します。
    4. 「**IntServ**」を右クリックし、「**新規ポリシー (New Policy)**」を選択します。「新規 IntServ ポリシー (New IntServ policy)」ウィザードが表示されます。
2. 統合サービス・ポリシーを作成します。

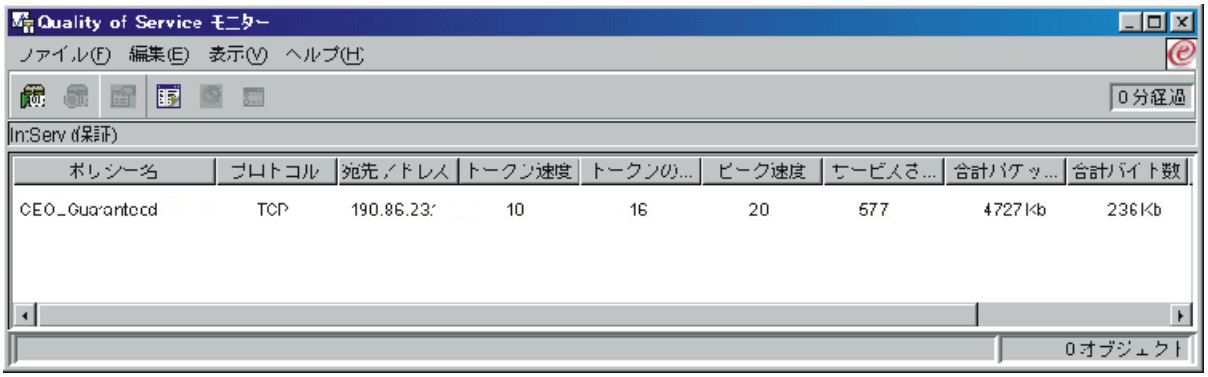
    まず最初に、新規統合サービス・ポリシーのウィザードを実行します。最高経営責任者 (CEO) から発信されるトラフィックを保証したいので、ポリシー **CEO_guaranteed** を呼び出します。単一クライアントは、IP アドレス **190.86.23.1** で、このプレゼンテーションを受信します。このアドレスは、例示目的のみの架空の番号です。 このクライアントには **Branch1** という名前を付けます。このトラフィックは、ポート 2427 で実行されるので、このアプリケーションには **port 2427** という名前を付けます。 スケジュールには、**1:00-2:00** という名前を付けます。ウィザードでは、次の値を使用します。

    Name = CEO_guaranteed
    Client = Branch1
    Application = port 2427 (これが、IP 電話の実行に使用されているポートであれば、このように指定する)
    Local IP address = 10.5.27.1
    Protocol = TCP
    Schedule = 1:00-2:00
    Token bucket size = 16 Kilobits
    Bandwidth limit (R) = 10 Megabits per second
    Number of flows = 1

    iSeries ナビゲーターが、サーバーに作成されたすべての統合サービス・ポリシーをリストします。
3. モニターを使用して、ポリシーが作動しているかを検証します。
    1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
    2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター**」を選択します。

    下記の図は、結果を説明する注記が含まれているモニター出力のダイアログです。

図 2. Quality of service モニター



最も注目する必要のあるフィールドは、トラフィックからデータを取得する測定フィールドです。 それには、合計ビット数、準拠ビット数、準拠パケット数などの各フィールドがあります。非準拠ビット数は、この統合サービス・ポリシーの要件を満たすために他のトラフィックを遅らせるか、または廃棄することを示します。 すべてのモニター・フィールドについては、『モニター』のセクションを参照してください。

4. 調整する必要がある値をすべて変更します。

   このポリシーに関するモニター結果を表示した後、前にウィザードで設定した値を変更することができます。

   1. モニターをクローズします。
   2. 前に作成したポリシー名を右マウス・ボタンでクリックします。
   3. 「**プロパティー**」を選択すると、「IntServ_Guaranteed のプロパティー」ダイアログが表示されます。
   4. トラフィック・フローを制御する値を変更するには、「**フロー制御**」タブを選択します。図からわかるように、ここでもスケジュール、クライアント、アプリケーション、およびトラフィック管理を編集できます。

«

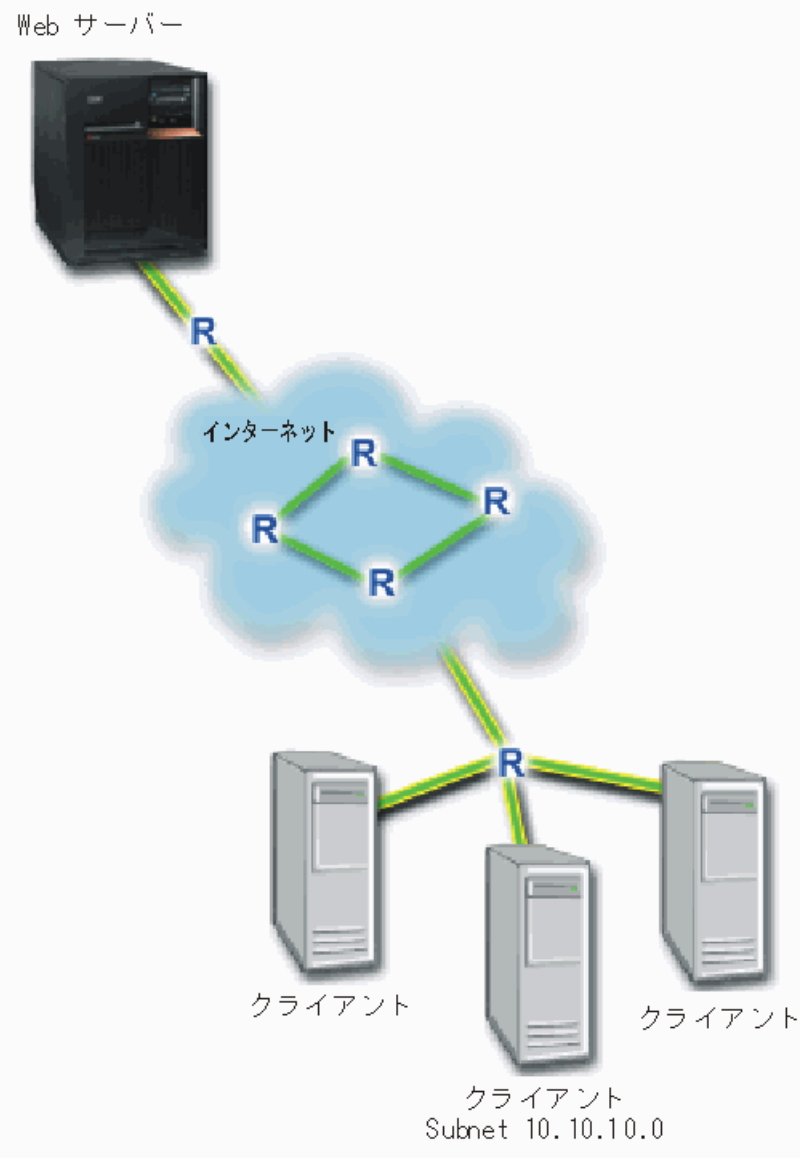
QoS シナリオ: ブラウザー・トラフィックの制限

»

問題

会社は、毎週金曜日にユーザー向け業務設計 (UCD) グループからのブラウザー・トラフィックのレベルが高くなることを経験しています。このトラフィックは、毎週金曜日に会計アプリケーションの良好なパフォーマンスを必要とする、会計部門の妨げとなっています。そこで、UCD グループからのブラウザー・トラフィックを制限することに決めます。次の図は、このシナリオでのネットワーク・セットアップを示しています。 iSeries サーバーは OS/400(R) V5R2 で稼働しています。

図 3. クライアントへのブラウザー・トラフィックを制限している Web サーバー



ソリューション

ネットワークの外側のブラウザー・トラフィックを制限するために、DiffServ ポリシーを作成することができます。 DiffServ ポリシーはトラフィックをクラスに分割します。 このポリシーの中のすべてのトラフィックにコード・ポイントが割り当てられます。このコード・ポイントはルーターに、トラフィックの処理方法を知らせます。このシナリオでは、ネットワークでのブラウザー・トラフィックの優先順位付けに影響を与えられるように、このポリシーには低いコード・ポイント値が割り当てられます。

構成

1. iSeries ナビゲーターで QoS を開きます。
    1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
    2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
    3. 「**アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)**」を展開します。

4. 「**DiffServ**」を右クリックして、「**新規ポリシー (New Policy)**」を選択します。「新規 DiffServ ポリシー (New DiffServ policy)」ウィザードが表示されます。

2. DiffServ ポリシーを作成します。

   ユーザー向け業務設計 (UCD) グループへのブラウザー・トラフィックを制限したいので、ポリシー **UCD** を呼び出します。クライアントは、サブネット・アドレス **10.10.10.0** を使用します。このアドレスは、例示目的のみの架空の番号です。 Web トラフィックは、通常はポート 80 で実行されるので、このアプリケーションには **port 80** という名前を付けます。 輻輳 (ふくそう) が発生するのは、金曜日だけなので、ポリシーには午前 9:00 ～ 午後 5:00 の スケジュールを適用できます。 これには、 **Friday9-5** という名前を付けます。ウィザードでは、次の設定値を使用します。

   Name = UCD (任意の名前を割り当てられる)
   Client = Subnet 10.10.10.0
   Application = port 80 (HTTP トラフィック用の割り当て済みポート)
   Protocol = TCP
   Schedule = Fridays9-5

   続行すると自動的に表示される「サービス・クラス」ウィザードから残りのポリシー情報を入力します。

   Token bucket size = 8 Kilobits
   Average rate limit = 10 Megabits per second
   Peak rate limit = 20 Megabits per second
   Out-of-profile traffic overflow handling = Drop packets (再送される)

   iSeries ナビゲーターが、サーバーに作成されたすべての DiffServ ポリシーをリストします。ウィザードを終了すると、右側ペインにポリシーが表示されます。

3. 新規のサービス・クラスを完成させます。

   ウィザードを進んで行くと、PHB (ホップごとの転送優先順位付け)、パフォーマンス制限、およびアウト・オブ・プロファイル・トラフィックの処理を割り当てるように指示されます。これは、サービス・クラスの中で定義されます。

   実際は、サービス・クラスがこのトラフィックがルーターから受け取るパフォーマンス・レベルを決定します。このトラフィックがより低いサービスを受けることを示すように、サービス・クラスに **Bronze** という名前を付けます。 iSeries ナビゲーターが、サーバーに定義されたすべてのサービス・クラスをリストします。

   Class of service name = Bronze

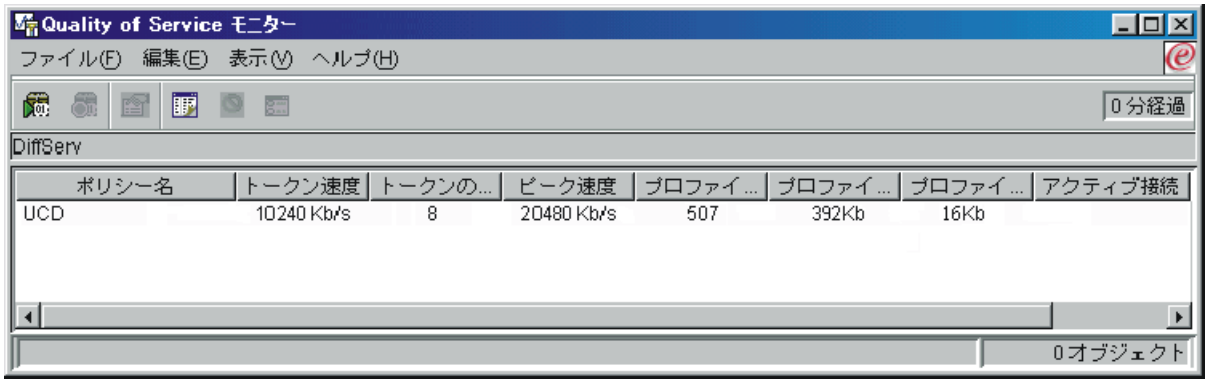
4. モニターを使用して、ポリシーが作動しているかを検証します。

   ポリシーが、ポリシーの中で構成したとおりに動作しているかを検証にするには、モニターを利用します。

   1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
   2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター**」を選択します。

   下記の図は、結果を説明する注記が含まれているモニター出力のダイアログです。

図 4. Quality of service モニター



最も注目する必要のあるフィールドは、トラフィックからデータを取得するフィールドです。 合計ビット数、イン・プロファイル・ビット数およびイン・プロファイル・パケット数の各フィールドを必ずチェックしてください。アウト・オブ・プロファイル・ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。 DiffServ ポリシーの中のアウト・オブ・プロファイルの数は、廃棄されるビット数を表します。イン・プロファイル・パケット数は、(そのパケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたビット数を示します。

平均速度制限のフィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、サーバーはそれらのパケットの廃棄を開始します。その結果、アウト・オブ・プロファイル・ビット数が増加します。これは、ポリシーが、構成したとおりに動作していることを表しています。すべてのモニター・フィールドについては、『モニター』のセクションを参照してください。

5. このポリシーに適用されない値を変更します。

   ポリシーで作成した値のどれでも変更することができます。

   1. モニターをクローズします。
   2. 左側ペインの「サービス・クラス」を選択します。
   3. 右側ペインで、前に作成したサービス・クラス名を右マウス・ボタンでクリックします。
   4. 「**プロパティー**」を選択します。トラフィックの制御値が表示された「CoS のプロパティー」ダイアログが現れます。該当の値を変更してください。

«

QoS シナリオ: インバウンド接続の制限

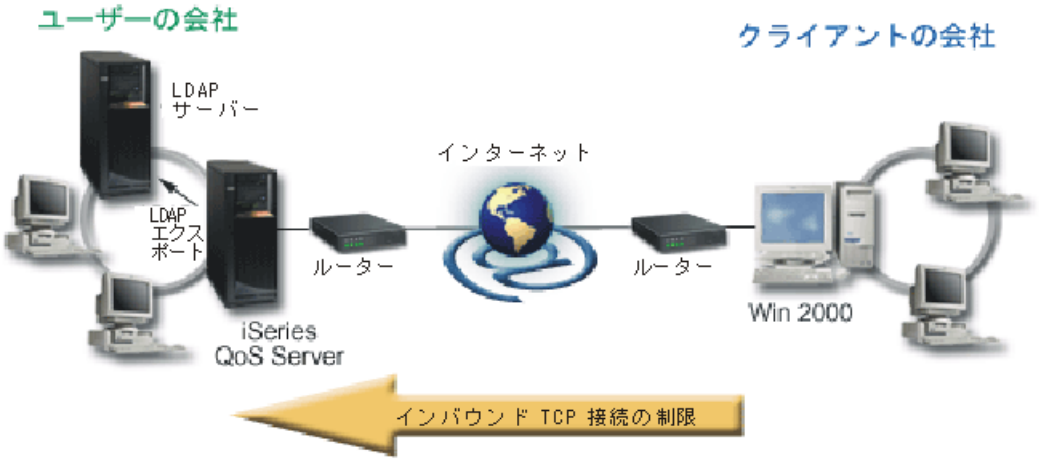
»

問題

Web サーバーのリソースが、ネットワーク内のクライアント要求によって負荷がかかりすぎています。ローカル・インターフェース 10.1.1.1 上の Web サーバー (10.1.1.4) への着信 HTTP トラフィックを減らすように求められています。 QoS は、サーバーに対する接続属性 (たとえば、IP アドレス) に基づいて、受け入れられるインバウンド接続試行を制限するのに役立ちます。そのために、受け入れられるインバウンド接続の数を制限するインバウンド・アドミッション・ポリシーをインプリメントすることに決めました。

次の図は、ユーザーの会社とクライアントの会社を示したものです。この QoS ポリシーでは、一方向のトラフィックの流れしか制御することができません。

図 5. インバウンド TCP 接続の制限



前提条件:

- iSeries V5R2 が稼働中であること
- LDAP サーバーが構成済みで、稼働中であること

ソリューション

インバウンド・ポリシーを構成する場合は、ローカル・インターフェースまたは特定のアプリケーションのどちらに対してトラフィックを制限するのか、および特定のクライアントからのトラフィックを制限するか否かを決める必要があります。この場合、クライアントの会社からローカル・インターフェース 10.1.1.1 上のポート 80 (HTTP プロトコル) への接続試行を制限するポリシーを作成する必要があります。この制限を IP アドレスによって定義するので、接続速度ポリシーを作成する必要があります。インバウンド・アドミッション・ポリシーには 2 つのタイプ (接続速度とサーバー要求 (URI)) があります。 URI ポリシーは、特定の相対 URI 名 (相対 URL に類似している) またはシステム上のすべての URL にアクセスしようとする接続を制限します。 URI ポリシーの詳細については、『インバウンド・アドミッション・ポリシー』を参照してください。

この接続速度ポリシーを作成し、前記のシナリオを完了させるには、iSeries ナビゲーターを開いて、QoS 機能に進みます。

構成

1. iSeries ナビゲーターで QoS を開きます。
    1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
    2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
    3. 「**インバウンド・アドミッション・ポリシー (Inbound admission policies)**」を展開します。
    4. 「**接続速度 (Connection rate)**」を右マウス・ボタンでクリックし、「**新規ポリシー (New Policy)**」を選択します。

2. 「接続速度ポリシー」ウィザードを完了します。

   2 番目のステップとして、新規接続速度ポリシーのウィザードを実行します。クライアントの会社 (Their_Company) からのトラフィックを制限したいので、ポリシー **Restrict_TheirCompany** を呼び出します。クライアント (Their_Company) からローカル IP アドレス 10.1.1.1 に対してなされる要求を制限する必要があります。このアドレスは、例示目的のみの架空の番号です。このトラフィックは、ポート 80 で実行されるので、このアプリケーションには **port 80** という名前を付けます。 スケジュールには、**Weekdays(9-5)** という名前を付けます。ウィザードでは、次の値を使用します。

   Name = Restrict_TheirCompany
   Client = Their_Company
   Application = port 80
   Local IP address = 10.1.1.1
   Schedule = Weekdays (9-5)
   Average connection rate = 100 per second
   Connection burst rate = 5 connections
   Priority = Medium

   iSeries ナビゲーターが、サーバーに作成されたすべての接続速度ポリシーをリストします。

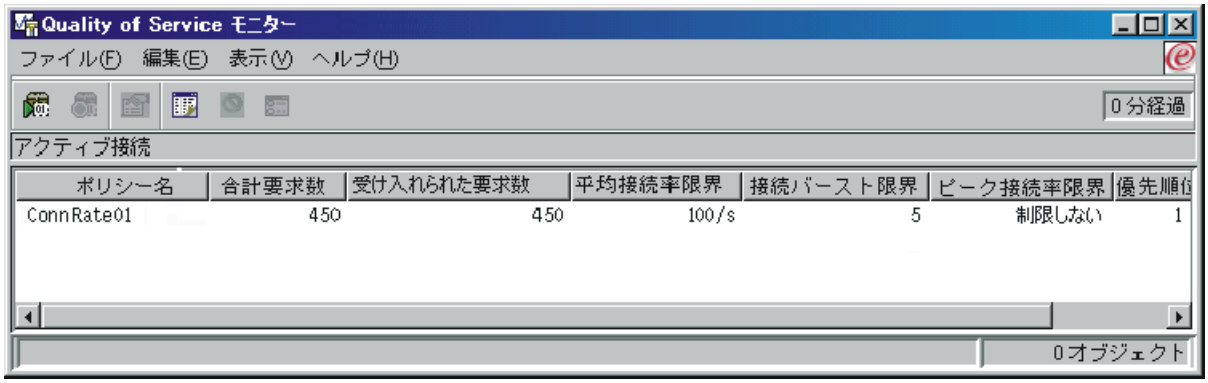
3. 必要とする結果を確実に表示するために、このポリシーに含まれているトラフィックをモニターします。

   ポリシーが構成したとおりに動作していることを検証にするには、モニターを利用します。

   1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
   2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター (Monitor)**」を選択します。

   下記の図は、結果を説明する注記が含まれているモニター出力です。

図 6. Quality of service モニター



   すべての測定値フィールド (たとえば、受け入れ済み要求の数、却下済み要求の数、要求の総数、接続速度など) を必ず検査してください。却下済み要求の数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。受け入れ済み要求の数は、(そのパケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたビット数を示します。

平均接続要求速度のフィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、サーバーはそれらのパケットの廃棄を開始します。その結果、却下済み要求の数が増加します。これは、ポリシーが、構成したとおりに動作していることを表しています。すべてのモニター・フィールドについては、『モニター』のセクションを参照してください。

4. 値を変更する必要がある場合は、プロパティーのパネルで値を変更します。

   モニターをクローズします。Restrict_TheirCompany ポリシーを**右マウス・ボタンでクリック**して、**「プロパティー」**を選択します。これらのパネルにより、ポリシーのプロパティーを編集することができます。図からわかるように、ここでもスケジュール、クライアント、アプリケーション、およびトラフィック管理を編集できます。

«

QoS シナリオ: 予測可能な B2B トラフィック

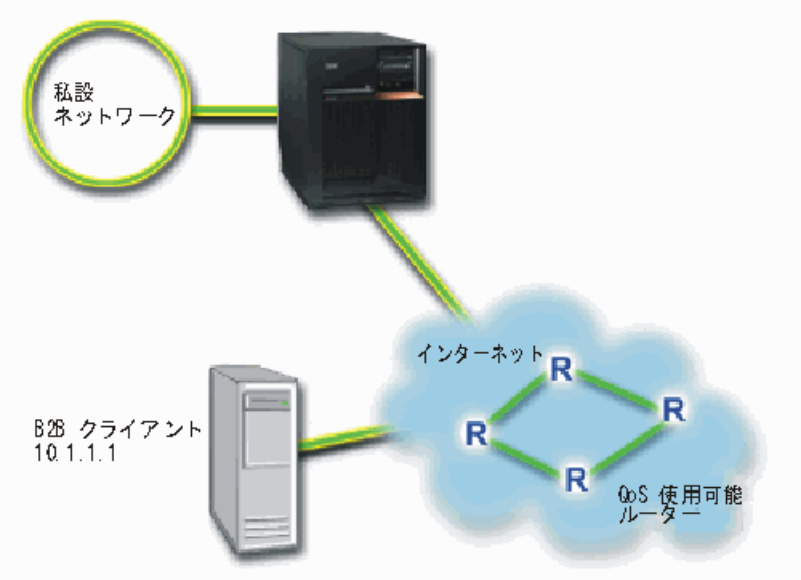
»

問題

販売部門から、ネットワーク・トラフィックが希望どおり機能していないという問題が報告されています。会社の iSeries サーバーは、予測可能な e-business サービスを必要とする企業間 (B2B) 環境に置かれています。お客様に予測可能なトランザクションを提供する必要があります。販売課の 1 日で最も忙しい時間帯 (午前 10 ～ 午後 4) に受注アプリケーション用としてより高い Quality of service をその販売課に提供したいと考えています。

下記の図では、販売チームはプライベート・ネットワーク内に存在します。 B2B クライアントへのトラフィック・パスには RSVP 使用可能ルーターが設置されています。それぞれの R は、トラフィック・パス沿いのルーターを表しています。

図 7. RSVP 使用可能ルーターを使用した B2B クライアントへの統合サービス・ポリシー



ソリューション

負荷コントロール・サービスは、混雑したネットワークによる影響を大きく受けるけれども少量の脱落や遅延を許容するアプリケーションをサポートします。アプリケーションが負荷コントロール・サービスを使用する場合、そのパフォーマンスはネットワーク負荷が増えても低下しません。トラフィックには、負荷が少ない状況のネットワークの正常なトラフィックが受けられるサービスと似たサービスが提供されます。この特定のアプリケーションは、少量の遅延を許容するので、負荷コントロール・サービスを利用する統合サービス・ポリシーを使用することに決めました。

統合サービス・ポリシーには、RSVP 使用可能アプリケーションが必要です。 現在、ご使用のサーバーには RSVP 使用可能アプリケーションがないため、ユーザー自身の RSVP 使用可能アプリケーションを作成する必要があります。ユーザー自身のアプリケーションを作成するには、 Resource Reservation Setup Protocol (RAPI) API または qtoq QoS ソケット API を使用してください。

統合サービス・ポリシーを使用する場合、トラフィック・パス沿いにあるルーターも RSVP 使用可能でなくてはなりません。 詳細は、統合サービスの概念に関するセクションを参照してください。

構成

1. iSeries ナビゲーターで QoS を開きます。
    1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
    2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
    3. 「**アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)**」を展開します。
    4. 「**IntServ**」を右マウス・ボタンでクリックし、「**新規ポリシー (New Policy)**」を選択します。「新規 IntServ ポリシー (New IntServ policy)」ウィザードが表示されます。
2. 新規の統合サービス・ポリシーを作成します。

    お客様に予測可能なトラフィックを提供したいので、ポリシー **B2B_CL** を呼び出します。単一クライアントは、IP アドレス **10.1.1.1** で、このプレゼンテーションを受信します。このアドレスは、例示目的のみの架空の番号です。 このトラフィックは、7000 ～ 8000 の間の様々なポートで実行されるので、このアプリケーションには **port 7000-8000** という名前を付けます。午前 10 時～午後 4 時の間にこのプレゼンテーションが行なわれるので、スケジュールには **Primetime** という名前を付けました。ウィザードでは、次の設定値を使用します。

    Name = B2B_CL
    Client =10.1.1.1
    Application = port 7000-8000
    Protocol = TCP
    Schedule = Primetime
    Token bucket size (b) = 8 Kilobits
    Token rate limit = 25 Megabits per second
    Token bucket size (r) = 75 Kilobits
    Number of flows = 5

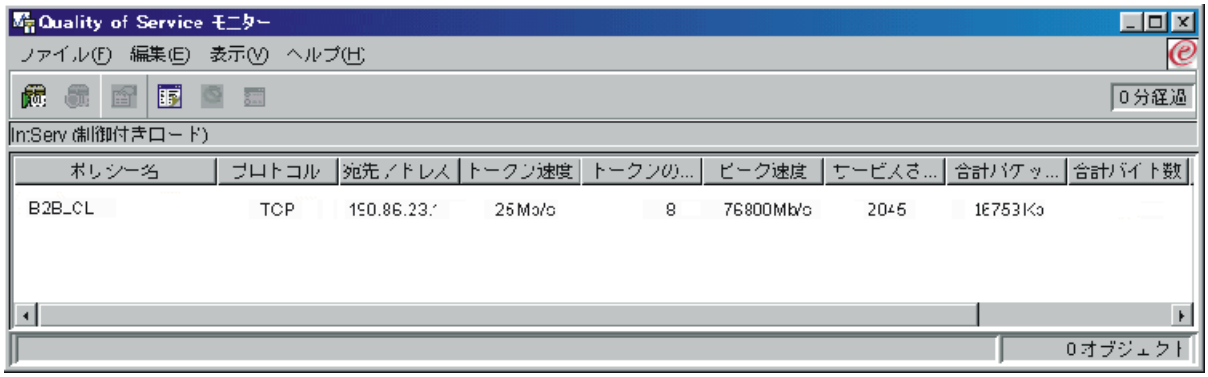
    iSeries ナビゲーターが、サーバーに作成されたすべての統合サービス・ポリシーをリストします。
3. モニターを使用して、ポリシーが作動しているかを検証します。

    ポリシーが正確に動作していることを検証にするには、モニターを利用します。

1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター (Monitor)**」を選択します。

下記の図は、結果を説明する注記が含まれているモニター出力のダイアログです。

図 8. Quality of service モニター



最も注目する必要のあるフィールドは、トラフィックからデータを取得するフィールドです。 合計ビット数、準拠ビット数、および準拠パケット数の各フィールドを必ずチェックしてください。非準拠ビット数は、この統合サービス・ポリシーの要件を満たすために他のトラフィックを遅らせるか、または除去されることを示します。 モニター・フィールドの詳細は、モニターのセクションを参照してください。

4. このポリシー内で調整する必要がある値を変更します。

このポリシーを作成した後、前にウィザードで作成した値を変更することができます。

1. モニターをクローズします。
2. 前に作成したポリシー名を右マウス・ボタンでクリックします。
3. 「**プロパティー**」を選択すると、「B2B_CL のプロパティー」ダイアログが表示されます。
4. トラフィック・フローを制御する値を変更するには、「**フロー制御**」タブを選択します。

図からわかるように、ここでもスケジュール、クライアント、アプリケーション、およびトラフィック管理を編集できます。

«

QoS シナリオ: 安全で予測可能な結果 (VPN と QoS)

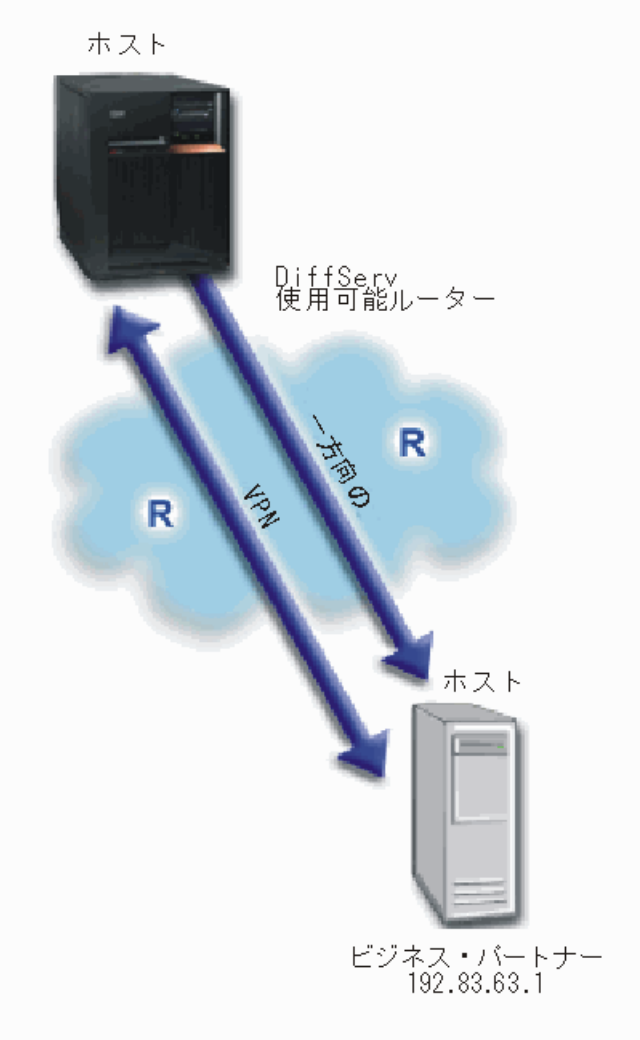
»

問題

VPN を介して接続しているビジネス・パートナーがおり、主幹業務データのセキュリティーと予測可能な e-business フローを実現できるように VPN と QoS を結合したいと考えています。 QoS 構成は、一方向にのみ送信されます。よって、オーディオ/ビデオ・アプリケーションがある場合は、接続の両端でそのアプリケーション用に QoS を設定する必要があります。

図は、ホスト間 VPN 接続されているサーバーとクライアントを表しています。それぞれの R は、ルーターのパスに存在する DiffServ 使用可能ルーターを表します。図からわかるように、QoS ポリシーは一方向にのみ流れます。

図 9. QoS DiffServ ポリシーを使用したホスト間 VPN 接続



ソリューション

保護だけでなく、この接続の優先順位も確立するために、VPN と QoS を使用します。最初に、ホスト間 VPN 接続をセットアップする必要があります。 ホスト間 VPN 接続の例は、VPN を構成する時に役立つので参照してください。 VPN 接続の保護を確立したら、QoS ポリシーをセットアップすることができます。 DiffServ ポリシーを作成できます。ネットワークでの主幹業務トラフィックの優先順位付けに影響を与えられるように、このポリシーには高優先転送コード・ポイント値が割り当てられます。

構成

1. ホスト間 VPN 接続をセットアップします。ホスト間 VPN 接続の例は、VPN を構成するときに役立つので参照してください。

2. iSeries ナビゲーターで QoS を開きます。
   1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
   2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
   3. 「**アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)**」を展開します。
   4. 「**DiffServ**」を右マウス・ボタンでクリックして、「**新規ポリシー (New Policy)**」を選択します。「新規 DiffServ ポリシー (New DiffServ policy)」ウィザードが表示されます。

3. DiffServ ポリシーを作成します。

   B2B アプリケーションのためのパフォーマンスを上げたいので、ポリシー **B2B** を呼び出します。クライアントは、単一のアドレス **192.83.63.1** をもっています。このアドレスは、例示目的のみの架空の番号です。 B2B トラフィックはどのポートでも使用できるので、アプリケーションに **All ports** という名前を付けます。輻輳 (ふくそう) が発生するのは、午前 9:00 ～ 午後 5:00 の間のみなので、ポリシーに 午前 9:00 ～ 午後 5:00 スケジュールを適用できます。これには **Firstshift** という名前を付けます。ウィザードでは、次の設定値を使用します。

   Name = B2B
   Client = VPNClient
   Application = All port
   Protocol = All
   Schedule = Firstshift

   続行すると自動的に表示される「サービス・クラス (Class of service)」ウィザードから残りのポリシー情報を入力します。

   Token bucket size = 8 Kilobits
   Average rate limit = 90 Megabits per second
   Peak rate limit = Do not limit
   Out-of-profile traffic overflow handling = Drop packets (再送される)

   iSeries ナビゲーターが、サーバーに作成されたすべての DiffServ ポリシーをリストします。

4. 新規のサービス・クラスを完成させます。

   ウィザードを進むと、サービス・クラスを割り当てるように指示されます。サービス・クラス (COS) は、パフォーマンス制限、コード・ポイント、およびアウト・オブ・プロファイル処理特性を割り当てます。このポリシーでは、優先順位の高い優先転送コード・ポイントを割り当てます。優先転送コード・ポイントを適用したいので、この値を選択した理由を覚えておくためにサービス・クラスに **EF_VPN** という名前を付けます。

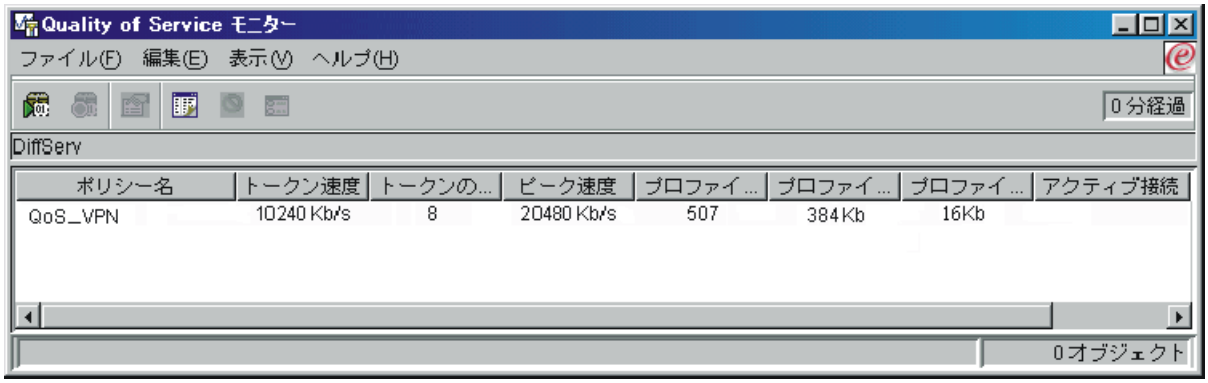
   Class of service = EF_VPN

5. モニターを使用して、ポリシーが作動しているかを検証します。

   ポリシーが構成したとおりに動作していることを検証にするには、モニターを利用します。
   1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
   2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター**」を選択します。

   下記の図は、結果を説明する注記が含まれているモニター出力です。

図 10. Quality of service モニター



例 1 と同様に、最も注目する必要のあるフィールドは、トラフィックからデータを取得するフィールドです。それには、合計ビット数、準拠ビット数、準拠パケット数などの各フィールドがあります。非準拠ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。準拠パケット数は、このポリシーによって制御されるパケット数を示します。平均速度制限のフィールドにどのような値を割り当てるかが、非常に重要です。パケットがこの制限値を超えると、サーバーはそれらのパケットの廃棄を開始します。その結果、非準拠ビット数が増加します。このポリシーが例 1 と異なる点は、パケットが VPN プロトコルを使用して保護されていることです。図からわかるように、QoS は VPN 接続において機能します。すべてのモニター・フィールドについては、『 モニター』のセクションを参照してください。

6. このポリシー内で調整する必要がある値をすべて変更します。

   サービス・クラスは、作成した後に編集することもできます。

   1. モニターをクローズします。
   2. 左側ペインの「**サービス・クラス**」を選択します。
   3. 右側ペインで、前に作成したサービス・クラス名を右マウス・ボタンでクリックします。
   4. 「**プロパティー**」を選択します。トラフィックの制御値が表示された「CoS のプロパティー」ダイアログが現れます。該当の値を変更してください。

«

QoS の概念

»

Quality of service (QoS) の用語の説明は複数の資料に記載されているので、このトピックでは、特に iSeries サーバーに適用される基本についてのみ触れます。

Quality of service のインプリメンテーションの最も重要な部分の 1 つは、サーバー自体です。以下で説明する概念を理解するだけではなく、それらの概念のインプリメンテーションにおいてサーバーが果たす役割をも認識する必要があります。 iSeries サーバーは、クライアントまたはサーバーとしてのみ機能します。ルーターの役割は果たせません。この後、概念についてより詳しく学び、Quality of service の計画を開始する際、このことを考慮に入れる必要があります。

QoS をインプリメントするには、トラフィックのポリシーを作成します。ポリシーは、アクションが指定されている 1 セットのルールです。ポリシーは、基本的には、(指定した) クライアント、アプリケーショ

ン、およびスケジュールが特定のサービスを受けることを指示します。結局、4 つのポリシー・タイプをインプリメントすることができます。ポリシーは、最初に、2 つのカテゴリー (アウトバウンド帯域幅およびインバウンド・アドミッション) に分かれます。アウトバウンド帯域幅ポリシー内では、 2 つのサービス・タイプ (統合サービス (IntServ) ポリシーまたは DiffServ ポリシー) を作成することができます。 インバウンド・アドミッション・ポリシー内では、2 つのサービス・タイプ (新規接続要求速度ポリシーおよび新規 URI 要求速度ポリシー) を作成することができます。

インバウンドは、外側の送信元からネットワークに着信する接続要求を制御するポリシーを指しています。アウトバウンドは、ネットワークから発信されるトラフィックを制限するか、あるいは利点を役立てるポリシーを指しています。どちらのポリシーを使用するべきかを判断するためには、QoS を使用する理由を評価してください。どのような状況が、各ポリシー・タイプに適しているかを、以下の概念の説明で調べてください。

詳しくは、以下のリンクをご利用ください。

DiffServ
これは、サーバーで作成できるアウトバウンド帯域幅ポリシーの第 1 のタイプです。 DiffServ は、トラフィックをクラスに分割するQoS の部分です。ネットワークで Quality of service をインプリメントするには、ネットワーク・トラフィックの分類方法と様々なクラスの処理方法を決定する必要があります。 その後、DiffServ ポリシーで使用するサービス・クラスを作成することができます。

DiffServ サービス・クラス
ここでは、サービス・クラスを構成する部分について説明します。 DiffServ ポリシーを作成する時、サービス・クラスも作成する必要があります。

統合サービス
作成できるアウトバウンド帯域幅ポリシーの第 2 のタイプは、統合サービス・ポリシーです。 統合サービスによって、IP アプリケーションには、RSVP プロトコルを使用して帯域幅を要求し予約することができます。統合サービス・ポリシーでは、RSVP プロトコルを使用してエンドツーエンド接続を保証します。これは、指定できる最高水準のサービスですが、最も複雑なサービスでもあります。統合サービス・ポリシーを作成する時、2 つのサービス・クラス (保証されたサービスまたは負荷コントロール・サービス) のうち 1 つを指定します。

DiffServ マーキングを使用した統合サービス
このタイプのポリシーは、通常は統合サービス・ポリシーが混合ネットワーク環境を通る場合に使用します。混合ネットワーク環境には、RSVP 使用可能なネットワーク・ノードと RSVP 使用不可のネットワーク・ノードが混在しています。

RSVP および QoS API
ここでは、統合サービスの予約を行うときに使用するプロトコルおよび API について説明します。また、ルーターを RSVP 使用可能にする方法も説明します。

接続速度
このタイプのインバウンド・ポリシーは、ネットワークに入る許可 (IP アドレスによる) を要求するトラフィックを制御するためのものです。インバウンド・アドミッション・ポリシーには 2 つのタイプ (接続速度と URI) があります。このトピックでは、両方のタイプのインバウンド・ポリシーについて説明します。

URI
このタイプのインバウンド・ポリシーは、ネットワークに入る許可 (URI による) を要求するトラフィックを制御するためのものです。インバウンド・アドミッション・ポリシーには 2 つのタイプ (接続速度と URI) があります。このトピックでは、両方のタイプのインバウンド・ポリシーについて説明します。

ディレクトリー・サーバー
QoS ポリシーが、ディレクトリー・サーバーにエクスポートされるようになりました。ディレクトリー・サーバー、LDAP の概念、および構成、ならびに QoS スキーマを使用する場合の利点を調べるには、このトピックを表示してください。

QoS のインプリメンテーションを試みる前に、Quality of service について詳しく研究し、Quality of service がニーズを満たすことを確認してください。その他の情報源が必要な場合は、『QoS に関するその他の情報』のページを参照してください。 «

接続要求速度および URI 要求速度

» インバウンド・ポリシーは、サーバーに接続しようとするトラフィックを制御するためのものです。インバウンド制御を定義および構成できるようにする 2 つのタイプのポリシー (URI ポリシーと接続速度ポリシー) があります。この 2 つのポリシー・タイプについて以下で説明します。

URI 要求速度ポリシー

URI 要求速度ポリシーは、サーバーを過負荷から保護するのに役立つソリューションの一部です。このタイプのポリシーは、サーバーにより受け入れられる URI 要求を制限するために、アプリケーション・レベル情報を基にして、アドミッション制御を適用します。業界では、これは優先順位を設定するために URI を使用するヘッダー・ベースの*接続要求制御* とも呼ばれています。

接続速度ポリシーとは異なり、URI ポリシーはパケット・ヘッダーだけではなく内容も調べるので、URI ポリシーはさらに多くの制御ができます。調べる内容には、URI 名またはその他のアプリケーション固有情報を含めることができます。iSeries の場合、相対 URI 名はポリシーを定義するために使用されます。たとえば、**/products/clothing** のようにします。以下の例では、相対 URI について説明しています。

相対 URI

相対 URI は、実際には絶対 URI のサブセットです (旧絶対 URL と類似)。
http://www.ibm.com/software の例について考慮してみます。**http://www.ibm.com/software** セグメントは、絶対 URI と見なされます。**/software** セグメントは、相対 URI です。すべての相対 URI 値は、1 個のスラッシュ (**/**) で始まっていなければなりません。以下は、有効な相対 URI の例です。

- /market/grocery#D5
- /software
- /market/grocery?q=green

注: デフォルト・プロトコル、ホスト名、およびポートは、すべて HTTP サーバーから継承されます。また、URI を指定する時には暗黙のワイルドカードがあります。たとえば **/software** は、ソフトウェア・ディレクトリー内のすべてを含んでいます。

URI ポリシーはネットワークに入っているトラフィック要求を制御するので、インバウンド・ポリシーと見なされます。このインバウンド制御の一部として、URI 要求がポリシーにより受け入れられた後で処理される優先順位を指定することができます。ポリシーを優先順位付けすることにより、接続ごとに構成されている優先順位を基にして待ち行列中の接続要求を実際に優先順位付けします。

接続速度ポリシー

接続速度ポリシーも、サーバーを過負荷から保護するのに役立つソリューションの一部です。このタイプのポリシーは、サーバーにより受け入れられる接続を制限するために、接続レベル情報を基にして、アドミッション制御を適用します。業界では、*TCP SYN ポリシング* とも呼ばれています。

接続速度ポリシングは、作成されるポリシーに定義されている、秒当たりの平均接続数および瞬間最大接続数を基にして新規着信接続の受け入れまたは否認を制限します。これらの接続限界は、iSeries ナビゲーターでウィザードが入力するためのプロンプトを出す、平均速度およびバースト限界から成り立っています。着信接続要求がサーバーに到着すると、サーバーはパケット・ヘッダー情報を分析して、このトラフィックがポリシー内で定義されているかどうかを判別します。システムは、この情報を接続制限プロファイルと対比して検査します。このポリシーがポリシー限界内である場合は、待ち行列に入れられます。ポリシーと一致しないパケットは破棄されます。

URI ポリシーと同様に、接続速度ポリシーはネットワークに入っているトラフィックの接続速度を制御するので、インバウンド・ポリシーと見なされます。このインバウンド制御の一部として、接続がポリシーにより受け入れられた後で処理される優先順位を指定することができます。ポリシーを優先順位付けすることにより、接続ごとに構成されている優先順位を基にして待ち行列中の接続要求を実際に優先順位付けします。

URI ポリシーと接続速度ポリシーの両方では、ポリシーごとに定義されるトラフィック用に接続速度およびバースト限界を設定する必要があります。これらの速度限界は、サーバーに入力しようとするインバウン

ド接続を制限するのに役立ちます。平均接続速度は、サーバー内で許可された受け入れ済み URI 要求の、新規に確立された接続または速度の限界を指定します。 «

平均接続速度およびバースト限界

» 接続速度およびバースト限界は、どちらも速度限界として知られています。これらの速度限界は、サーバーに入力しようとするインバウンド接続を制限するのに役立ちます。速度限界は、インバウンド・アドミッション・ポリシー (URI と接続速度の両方) 内に設定されます。

接続バースト限界

バースト限界サイズにより、接続のバーストを保持するバッファー容量が決定されます。接続バーストは、サーバーが処理できるより速い速度で、あるいは許可したい速度より速い速度でサーバーに入力します。バースト内の接続数が、設定した接続バースト速度を超えた場合には、それ以上の接続は廃棄されます。

平均接続速度

平均接続速度は、サーバー内で許可された受け入れ済み URI 要求の、新規に確立された接続または速度の限界を指定します。要求によりサーバーが設定した限界を超えた場合には、サーバーはその要求を否認します。平均接続要求限界は、毎秒ごとの接続で測られます。

ヒント: 設定する限界を決めるために、モニターを実行することができます。参照用に、サーバー上のほとんどのデータ移動の収集に役立つサンプル・ポリシーを見るために、現行ネットワーク統計のモニターを参照してください。これらの結果を使用して、適切な限界を設定することができます。 «

DiffServ (差異化サービス)

DiffServ はトラフィックをクラスに分割します。ネットワークで Quality of service をインプリメントするには、ネットワーク・トラフィックの分類方法と様々なクラスの処理方法を決定する必要があります。

サーバーは、IP ヘッダー内のビットを使用して、IP パケットのサービス・レベルを識別します。ルーターとスイッチは、IP ヘッダーの TOS フィールドの PHB (ホップごとの転送優先順位付け) 情報に基づいてリソースを割り振ります。 TOS フィールドは、Request For Comment (RFC) 1349 と OS/400(R) V5R1 で再定義されました。 PHB は、パケットがネットワーク・ノードで受け取る転送動作です。 PHB は、コード・ポイントとよばれる 16 進値で表されます。サーバーまたはネットワークの他の部分 (ルーターなど) のいずれかの場所で、パケットのマーキングを行なえます。パケットが要求されたサービスを保持するためには、すべてのネットワーク・ノードが DiffServ 使用可能でなくてはなりません。つまり、ネットワーク装置が PHB を実施できなくてはなりません。 PHB 処理を実施するには、ネットワーク・ノードは、待ち行列スケジューリングおよびアウトバウンド優先順位管理を利用できなくてはなりません。 DiffServ 使用可能であるということはどういう状態を意味するのかについては、『トラフィック・コンディショナー』を参照してください。

パケットが、DiffServ 使用可能ではないルーターまたはスイッチを通過すると、そのパケットはサービス・レベルを失います。その結果、パケットは依然として処理可能ですが、予期しない送達が行なわれる場合があります。 iSeries サーバーでは、標準の PHB コード・ポイントを使用するか、独自のクラスを定義できます。私設ネットワークの外側での使用を目的とした、独自のコード・ポイントの作成はお勧めしません。

統合サービスとは異なり、DiffServ トラフィックの場合、予約またはフローごとの処理は必要ありません。同じクラスに分類されたすべてのトラフィックは、同等に扱われます。

DiffServ は、サーバーに入ってくるトラフィックまたはサーバーから送り出されるトラフィックの制御にも使用されます。つまり、iSeries サーバーは本当の意味で DiffServ を利用してパフォーマンスを制限するのです。重要度の低いアプリケーションを制限することで、主幹業務のアプリケーションを最初に私設ネットワークから送り出すことが可能になります。ポリシーを作成する時、サーバーで様々な制限を設定するよう

に指示されます。 パフォーマンス制限には、トークン・バケット・サイズ、ピーク速度制限、平均速度制限などがあります。 iSeries ナビゲーターの QoS 機能内のヘルプ・トピックに、これらの制限に関する詳しい情報が載っています。

以上の説明から、DiffServ を使用してトラフィックをグループ化するための詳しい知識を得られた思います。割り当てるコード・ポイントがわからない場合は、『コード・ポイントおよび PHB (ホップごとの転送優先順位付け)』で確認してください。 それでもなお、どのコード・ポイントを使用したらよいかがわからない場合は、実際に使用してみてください。テスト・ポリシーを作成し、これらのポリシーをモニターし、必要に応じて調整してください。

DiffServ サービス・クラス

DiffServ のセクションでは、DiffServ 機能がどのようにトラフィックをクラス分けするかを説明しました。このクラス分けのほとんどは装置で行なわれますが、トラフィックのクラス分け方法とトラフィックが受け取る優先順位は、ユーザーが制御します。

QoS をインプリメントする際、まず最初にポリシーを定義します。ポリシーで、だれが、なにを、どこで、いつ、といった詳細を決定します。次にサービス・クラスをポリシーに割り当てます。サービス・クラスは個別に定義するので、ポリシーが再利用できます。サービス・クラスは、PHB (ホップごとの転送優先順位付け)、トラフィック制限、およびサービス・クラスでのアウト・オブ・プロファイル処理から構成されます。

PHB (ホップごとの転送優先順位付け)
Quality of service は、推奨されるコード・ポイントを使用して、トラフィックに PHB を割り当てます。ルーターとスイッチは、これらのコード・ポイントを使用してトラフィックに優先順位レベルを与えます。ご使用のサーバーは、ルーターとして動作していないので、これらのコード・ポイントを使用できません。ご使用のネットワークのニーズに基づいて、どのコード・ポイントを使用するかを決定する必要があります。自分の環境にとって、どのアプリケーションが最も重要か、およびどのポリシーに高い優先順位を割り当てる必要があるかを考える必要があります。 最も重要なことは、マーキングと一貫性があることです。それによって、期待した結果が得られます。これらのコード・ポイントは、トラフィックの様々なクラスを区別する上でキーとなります。

パフォーマンス制限
Quality of service は、パフォーマンス制限を利用してネットワークを通るトラフィックを制限します。パフォーマンス制限を設けるには、トークン・バケット・サイズ、ピーク速度制限、および平均速度制限を設定します。これらの特定の値の詳細については、トークン・バケットおよび帯域幅の制限を参照してください。

アウト・オブ・プロファイル処理
サービス・クラスの最後の部分は、アウト・オブ・プロファイル処理です。上記のパフォーマンス制限を割り当てるとき、トラフィックを制限する値を設定します。トラフィックが制限値を超えると、そのパケットはアウト・オブ・プロファイルと見なされます。サーバーは、サービス・クラス内のこの情報から、アウト・オブ・プロファイル・パケットを廃棄するか、シェーピングするか、または再送するかを判断します。アウト・オブ・プロファイル・パケットを廃棄すると決定すると、それらのパケットは、指定された時間が経過した後に再送されます。アウト・オブ・プロファイル・パケットを遅らせると、これらのパケットは、定義された処理特性に従うようにシェーピングされます。
DiffServ コード・ポイント (DSCP) でアウト・オブ・プロファイル・パケットに再度マーキングすると、それらのパケットには新規のコード・ポイントが割り当てられます。ウィザードでこの処理指示を割り当てる時、「ヘルプ」をクリックして詳しい情報をご確認ください。

コード・ポイントおよび PHB (ホップごとの転送優先順位付け)

Quality of service は、以下の推奨されるコード・ポイントを使用して、トラフィックに PHB を割り当てます。 ご使用のネットワークのニーズに基づいて、どのコード・ポイントを使用するかを決定する必要があります。 どのコード・ポイント・スキームを自分の環境で使用するかを決定できるのは、自分のみです。自分の環境にとって、どのアプリケーションが最も重要か、およびどのポリシーに高い優先順位を割り当てる必要があるかを考える必要があります。最も重要なことは、マーキングと一貫性があることです。それによって、期待した結果が得られます。

この表には、推奨されるコード・ポイントが記載されています。独自の PHB を作成することもできます。

優先転送 (23See)	クラス・セレクター (23See)	保証転送 (23See)
101110	クラス 0 - 000000	保証転送、クラス 1、低 - 001010
	クラス 1 - 001000	保証転送、クラス 1、中 - 001100
	クラス 2 - 010000	保証転送、クラス 1、高 - 001110
	クラス 3 - 011000	保証転送、クラス 2、低 - 010010
	クラス 4 - 100000	保証転送、クラス 2、中 - 010100
	クラス 5 - 101000	保証転送、クラス 2、高 - 010110
	クラス 6 - 110000	保証転送、クラス 3、低 - 011010
	クラス 7 - 111000	保証転送、クラス 3、中 - 011100
		保証転送、クラス 3、高 - 011110
		保証転送、クラス 4、低 - 100010
		保証転送、クラス 4、中 - 100100
		保証転送、クラス 4、高 - 100110

優先転送

優先転送は、DiffServ PHB のタイプの 1 つです。優先転送は、主にネットワークでの保証されたサービスの提供に使用されます。優先転送は、ネットワークにまたがって帯域幅を保証することで、脱落およびジッターの少ないエンドツーエンド・サービスをトラフィックに提供します。パケットが送信される前に予約が行なわれます。主な目的は、遅延を防ぎ、パケットを適時に送信することです。

注: 優先転送処理は通常はコストが高いので、この PHB (ホップごとの転送優先順位付け) の常用はお勧めしません。

クラス・セレクター

クラス・セレクター・コード・ポイントは、DiffServ のもう 1 つのタイプです。クラスは 7 つあります。クラス 0 はパケットに最低優先順位を与え、クラス 7 はパケットに、クラス・セレクターのコード・ポイント値の範囲内で最高の優先順位を与えます。ほとんどのルーターはすでに似たようなコード・ポイントを使用しているので、これは PHB の最も共通したグループです。

保証転送

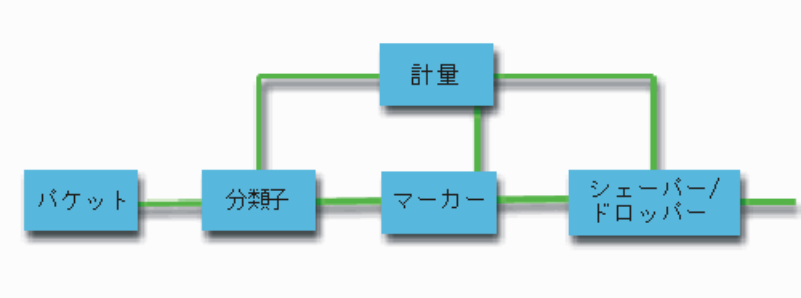
保証転送は、4 つの PHB クラスにわかれており、各クラスに廃棄優先順位 (低、中、高) があります。廃棄優先順位によって、パケットの廃棄の可能性が決まります。各クラスに独自の帯域幅仕様があります。「クラス 1、高」の場合、ポリシーには最低優先順位が与えられ、「クラス 4、低」の場合はポリシーに最高優先順位が与えられます。 廃棄レベルが「低」ということは、このポリシーの中のパケットは、この特定のクラス・レベルで廃棄される可能性が最も低いという意味です。

トラフィック・コンディショナー

QoS ポリシーを使用するネットワーク装置は、QoS を認識するものでなくてはなりません。つまり、ルーターやスイッチなどのネットワーク装置には、分類子、計量、マーカー、シェーパー、およびドロッパー機能が装備されている必要があります。これらの機能をトラフィック・コンディショナー と呼びます。ネットワーク装置にすべてのトラフィック・コンディショナーが装備されていると、その装置は QoS を認識すると見なされます。

次の図は、トラフィック・コンディショナーの作用を論理的に表したものです。

図 11. トラフィック・コンディショナー



各トラフィック・コンディショナーについて、詳しく説明します。

分類子
パケット分類子は、パケットの IP ヘッダーの内容に基づいてトラフィック・ストリームの中からパケットを選択します。 iSeries サーバーは、2 つのタイプの分類子を定義しています。 BA (動作集合) は、排他的に DiffServ コード・ポイントに基づいてパケットを分類します。 MF (複数フィールド) 分類子は、ヘッダー・フィールド (ソース・アドレス、宛先アドレス、DiffServ フィールド、プロトコル ID、ソース・ポート、宛先ポート番号など) のうちの 1 つ以上のフィールドの組み合わせの値に基づいてパケットを選択します。

計量
トラフィック計量機能は、分類子によって転送されている IP パケットがトラフィックの IP ヘッダー・プロファイルに対応しているかどうかを判定します。 IP ヘッダー内の情報は、このトラフィックの QoS ポリシーの中に設定した値によって決定します。計量機能は、アクションを起動するために情報を他の調整機能に渡します。アクションは、(それがイン・プロファイルか、アウト・オブ・プロファイルかに関係なく) それぞれのパケットごとに起動されます。

マーカー
パケット・マーカーは、DiffServ (DS) フィールドを設定します。このマーカーは、DiffServ コード・ポイント設定を取り出し、それをバイトに変換します。マーカーは、単一のコード・ポイントか、または PHB の選択に使用するコード・ポイント・セットへのすべてのパケットにマーキングを行なうように構成することができます。

シェーパー
シェーパーは、トラフィック・ストリームをトラフィック・プロファイルに準拠させるためにそのトラフィック・ストリーム内のいくつかのパケットまたはすべてのパケットを遅らせます。シェーパーのバッファー・サイズは限られているので、遅延パケットを保持するためのスペースがないとパケットが廃棄される場合があります。

ドロッパー
ドロッパーは、トラフィック・ストリーム内のいくつかのパケットまたはすべてのパケットを廃棄します。これは、ストリームをトラフィック・プロファイルに準拠させるために行なわれます。

ディレクトリー・サーバーの概念

» QoS ポリシー構成は、LDAP ディレクトリー・サーバーに保管されます。最新の LDAP プロトコル・バージョン 3 で LDAP サーバーを使用しなければなりません。

ディレクトリー・サーバーを使用する場合の利点

ディレクトリー・サーバーを使用すると、QoS ソリューションを管理するのが容易になります。すべてのサーバーで QoS ポリシーを構成する代わりに、1 つのローカル・ディレクトリー・サーバーで構成データを保管して、多くのシステムで共用することができます。ただし、データの共用は不要です。 QoS でディレクトリー・サーバーを使用する方法として、その他に 2 つの方法があります。

1. データは引き続き、構成、保管され、1 システムでのみ使用することができます。
2. また、構成データは、別のシステムのデータを保持するディレクトリー・サーバーに置くことができますが、それらの別のシステム間では必ずしも共用されるわけではありません。これによって、単一ロケーションを使用して幾つかのシステムのデータをバックアップおよび保管することができます。

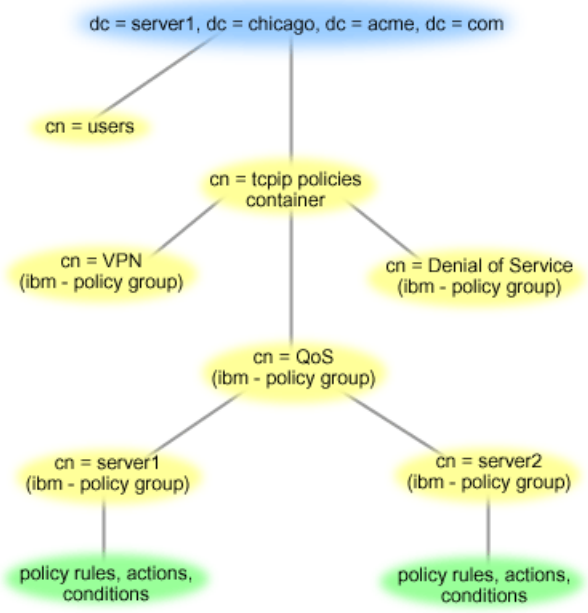
LDAP リソース

QoS を使用する前に、LDAP の概念およびディレクトリー構造について理解しておくことが必要です。iSeries Information Center のディレクトリー・サービス (LDAP) のトピックの中の LDAP に関する基本事項を検討してください。

QoS ツリー構造

ディレクトリーの一部を管理したい場合は、**識別名 (DN)** または (選択した場合) キーワードを参照してください。ディレクトリー・サーバーを構成する時に、DN を指定します。DN は通常、項目自体の名前、ならびにディレクトリー内のその項目より上のオブジェクト (逆の順序で) から構成されます。サーバーは、DN より下にあるディレクトリーのすべてのオブジェクトにアクセスすることができます。たとえば、LDAP サーバーが下記のディレクトリー構造を含んでいるものとします。

図 12. QoS ディレクトリー構造の例



一番上の Server1 (dc=server1,dc=chicago,dc=acme,dc=com) は、ディレクトリー・サーバーが常駐するサーバーです。その他のサーバー (たとえば、cn=QoS または cn=tcpip policies) には、QoS の各サーバーが常駐します。そのため、cn=server1 では、デフォルトの DN は cn=server1,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com になります。cn=server2 では、デフォルトの DN は cn=server2,cn=QoS,cn=tcpip policies,dc=server1,dc=chicago,dc=acme,dc=com になります。

ディレクトリーを管理する場合は、適切なサーバーを cn または dc などの DN に変更することが重要です。 DN のストリングは通常、スクロールしなくては表示できないほど長くなるので、 DN を編集するときには特に注意が必要です。 iSeries ナビゲーターの Quality of service 機能でディレクトリー・サーバーを構成する方法については、『ディレクトリー・サーバーの構成』を参照してください。

いくつかの代替 LDAP リソースについては、『QoS に関するその他の情報』を参照してください。 «

キーワード

»

ディレクトリー・サーバーを構成する場合は、キーワードを各 QoS 構成に関連付けるか否かを決める必要があります。キーワード・フィールドはオプショナルであり、無視することができます。以下の説明は、キーワードの概念およびキーワードを使用する必要性を理解するのに役立ちます。

「新規 Quality of Service 構成」ウィザードを使用して、ディレクトリー・サーバーを構成します。構成するサーバーが基本ディレクトリー・サーバーか 2 次システムかを指定します。すべての QoS ポリシーを維持できるサーバーが、1 次システムとして知られています。

1 次システムによって作成された構成を識別するのに、キーワードを使用します。キーワードは、1 次システムで作成されますが、実際には、2 次システムのためのものです。キーワードによって、2 次システムは、1 次システムで作成された構成をロードおよび使用することができます。以下の記述では、各システムでキーワードを使用する方法について説明されています。

キーワードと 1 次システム
キーワードは、1 次システムによって作成および維持される QoS 構成と関連付けられます。これらは、2 次システムが 1 次システムで作成された構成を識別できるよう使用されます。

キーワードと 2 次システム
2 次システムは、キーワードを使用して構成を検索します。2 次システムは、1 次システムによって作成された構成をロードおよび使用します。2 次システムを構成する時に、特定のキーワードを選択することができます。選択したキーワードによっては、2 次システムはその選択したキーワードと関連した構成をロードします。これによって、2 次システムは複数の 1 次システムによって作成された複数の構成をロードすることができます。

iSeries ナビゲーターでディレクトリー・サーバーの構成を開始する場合は、具体的な説明のある QoS タスク・ヘルプを使用してください。 «

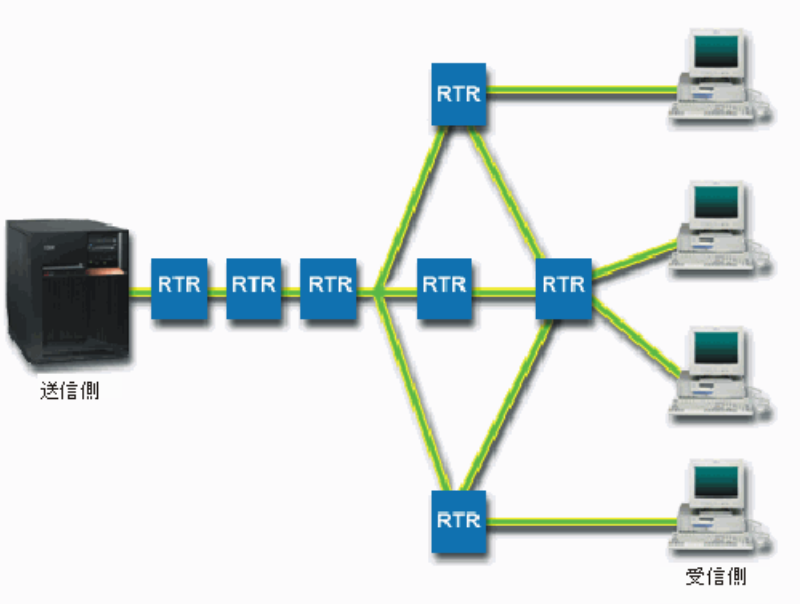
統合サービス

統合サービスは、トラフィック送達時間および特定のトラフィックの特別な処理命令を処理します。統合サービス・ポリシーは、データ転送を保証する手段としてはまだ比較的費用のかかる方法なので、統合サービス・ポリシーについては慎重であることが大切です。ただし、リソースのオーバープロビジョン (バンド幅過供給) は、統合サービスよりもさらに費用がかかる場合があります。

» 統合サービスは、データを送信する前に特定のポリシー用にリソースを予約します。データ転送の前にルーターに信号が送られ、ネットワークが実際にポリシーに基づいて (エンドツーエンド) データ転送に同意し管理します。**ポリシー**とは、アクションを指定する規則のセットです。ポリシーは、基本的にはアドミッション制御リストです。帯域幅要求は、クライアントからの予約に入ります。パスの中のすべてのルーターが要求側クライアントからの要件を応諾する場合は、その要求はサーバーおよび IntServ ポリシーに届きます。要求が、ポリシーで定義された限度内にある場合は、QoS サーバーは RSVP 接続を許可し、アプリケーションの帯域幅を無視します。リソースの予約は、Resource Reservation Protocol (RSVP) と RAPI または qtoq QoS ソケット API (あるいはその両方) を使用して行います。詳細については、RSVP プロトコルおよび QoS API を参照してください。 «

トラフィックが通過する各ノードには、RSVP プロトコルを使用する能力が備わっている必要があります。ルーターは、パケット・スケジューラー、パケット分類子およびアドミッション制御というトラフィック制御機能を通じて Quality of service を提供します。このトラフィック制御を実行する能力があることを、頻繁に RSVP 使用可能であるといいます。つまり、統合サービス・ポリシーをインプリメントする場合の最も重要な課題は、ネットワークでリソースを制御可能および予測可能になることです。予測可能な結果を得るためには、ネットワークのすべてのノードが RSVP 使用可能になる必要があります。たとえば、トラフィックは、どのパスに RSVP 認識ルーターがあるかに基づいてではなく、リソースに基づいて経路指定されます。 RSVP を認識しないルーターを使用すると、予測不可能なパフォーマンス上の問題が発生する場合があります。接続は続行されますが、アプリケーションが要求するパフォーマンスは、そのルーターによって保証されません。次の図は、統合サービス機能が論理的にどのように動作するかを示しています。

図 13. クライアントとサーバーの間の RSVP パス



サーバー上の RSVP 使用可能アプリケーションが、クライアントからの接続要求を検出します。それに応じて、サーバーのアプリケーションはクライアントに対して PATH コマンドを発行します。このコマンドは RAPI API または qtoq QoS ソケット API を使用して発行します。このコマンドにはルーター IP アドレス情報が入っています。 PATH コマンドには、サーバー上の使用可能なリソースとパスに存在するルーターの情報、およびサーバーとクライアントの間の経路情報が含まれます。次に、クライアント上の RSVP 使用可能アプリケーションは、ネットワーク・リソースが割り振られたことをサーバーに知らせるためにネットワーク・パスを介して RESV コマンドを戻します。このコマンドは、PATH コマンドからのルーター情報に基づいて予約を行います。サーバーとパスに存在するすべてのルーターが、RSVP 接続用にリソース

を予約します。サーバーが RESV コマンドを受け付けると、アプリケーションはクライアントへのデータ送信を開始します。データは、予約と同じ経路で送信されます。これは、ポリシーの実施を成功させるためには、この予約を実行するルーター能力がいかに重要であるかを示しています。

統合サービスは、HTTP のように、短期間の RSVP 接続には向きません。ただし、もちろんこれは自由裁量です。ご自分のネットワークにとって、なにが最善かを判断してください。どの領域とアプリケーションにパフォーマンスの問題があり、Quality of service が必要かを考えてください。統合サービス・ポリシーで使用するどのアプリケーションも、RSVP プロトコルを使用できなくてはなりません。現在、ご使用のサーバーには RSVP 使用可能アプリケーションがないため、 RSVP を使用できるアプリケーションを作成する必要があります。詳細は、『RSVP』セクションを参照してください。

パケットが到着し、ネットワークから出ようとすると、サーバーは、パケットを送信するためのリソースがあるかどうかを判断します。この受け入れは、トークン・バケット内のスペース量によって決まります。トークン・バケット内の受け入れ用のスペース (ビット数)、帯域幅制限、トークン速度制限、およびサーバーで許可する最大接続数は、手動で設定します。これらの値はパフォーマンス制限値と呼ばれます。着信パケットによってバケットの制限値を超過するようだと、そのパケットは非準拠バケットと見なされます。サーバーでの非準拠トラフィックの処理方法は、いくつかあります。サーバーは、非準拠パケットを遅延、シェーピング、再送、または廃棄することができます。パケットがサーバーの制限内に収まるようだと、そのパケットはプロファイルに準拠しているので送信されます。統合サービスでは、各接続には独自のトークン・バケットが与えられます。 DiffServ では、サブネット全体またはある範囲のクライアントがトークン・バケットを共用します。

トラフィック制御機能

トラフィック制御機能は、統合サービス・ポリシーにのみ適用されます。予測可能な結果を得るためには、トラフィック・パスに RSVP 使用可能ハードウェアを設置する必要があります。ルーターには、RSVP プロトコルを使用するためのある特定のトラフィック制御機能が必要です。この、あるトラフィック制御機能がある状態を、頻繁に RSVP 使用可能である、または QoS 使用可能である、といいます。サーバーの役割はクライアントまたはサーバーのいずれかであることを覚えておいてください。現時点では、サーバーをルーターとして使用することはできません。

トラフィック制御機能には、次のものがあります。

パケット・スケジューラー
パケット・スケジューラーは、IP ヘッダー内の情報に基づいて転送されるパケットを管理します。パケット・スケジューラーにより、パケットは、ポリシーの中に設定したパラメーターに従って送達されます。スケジューラーは、パケットがキューイングされるポイントにインプリメントされます。

パケット分類子
パケット分類子は、IP フローのどのパケットが IP ヘッダー情報に基づいてある特定のサービス・レベルを受けるかを識別します。それぞれの着信パケットは、分類子によって特定のクラスにマップされます。同じクラスに分類されたすべてのパケットは、同じ処理を受けます。このサービス・レベルは、ポリシーの中に設定した情報に基づきます。

アドミッション制御
アドミッション制御には、ルーターが、新規フロー用に要求された QoS を受け入れる十分な経路指定リソースがあるかどうかを判断する時に使用する、決定アルゴリズムが組み込まれています。十分なリソースがないと、新規のフローは拒否されます。フローが受け入れられると、ルーターは、要求された QoS を予約するためにパケット分類子とスケジューラーを割り当てます。アドミッション制御は、予約パス沿いに存在する各ルーターで行われます。

ここでは、分類子とスケジューラーのすべてを説明しているわけではありません。他の情報源が『QoS に関するその他の情報』のページに記載されていますので、参照してください。

統合サービス・タイプ

» 統合サービスには、負荷コントロール・サービスと保証されたサービスの 2 つのタイプがあります。

負荷コントロール・サービス

負荷コントロール・サービスは、混雑したネットワークによる影響を大きく受けるアプリケーション (たとえば、リアルタイム・アプリケーション) をサポートします。このようなアプリケーションは、少量の脱落や遅延も許容しなければなりません。アプリケーションが負荷コントロール・サービスを使用する場合、そのパフォーマンスはネットワーク負荷が増えても低下しません。トラフィックには、負荷が少ない状況でのネットワークの正常なトラフィックが受けられるサービスと似たサービスが提供されます。

ルーターは、負荷コントロール・サービスが十分な帯域幅およびパケット処理リソースを確実に受け取るようにする必要があります。このためには、ルーターは、統合サービスをサポートする QoS 使用可能でなければなりません。ルーターの仕様をチェックして、トラフィック制御機能を通じて Quality of service を提供するかどうかを調べる必要があります。トラフィック制御は、次の要素、すなわち、パケット・スケジューラー、パケット分類子、およびアドミッション制御から構成されます。

保証されたサービス

保証されたサービスは、パケットが指定の送達時間内で確実に到着するようにします。保証されたサービスを必要とするアプリケーションには、ストリーミング・テクノロジーを使用するビデオおよびオーディオのブロードキャスト・システムが含まれます。保証されたサービスは、パケットがある特定の時間以上は遅れないように最大キューイング遅延を制御します。パケットのパス沿いにあるルーターはすべて、送達を保証するための RSVP 機能を備えていなければなりません。トークン・バケット制限および帯域幅制限を割り当てると、保証されたサービスを定義することになります。 «

トークン・バケットおよび帯域幅の限界

» トークン・バケット限界と帯域幅限界はともにパフォーマンス制限として知られています。これらのパフォーマンス制限は、アウトバウンド帯域幅ポリシー (統合サービスおよび DiffServ の両方) 内でパケットのデリバリーの保証に役立ちます。

トークン・バケット・サイズ

トークン・バケット・サイズにより、データのバーストを保持するバッファー容量が決定されます。バースト・データは、アプリケーションが、終了できる速度より速い速度でサーバーに入力する情報です。アプリケーションが十分なバースト・データをサーバーに素早く送信した場合には、バッファーが満杯になります。アプリケーションが、サーバーを終了するより遅く情報を送信した場合には、バッファーは空になります。データがサーバーに入力されるのと同じ速度でサーバーから離れると、トークン・バケット・サイズは変更されないままです。バッファーが満杯になると、QoS は追加データ・パケットをプロファイル規定外として取り扱います。このポリシーで、QoS がプロファイル規定外トラフィックを処理する方法を決定することができます。

トークン速度限界

速度 (帯域幅) 限界は、長期データ転送速度またはネットワーク内に許容されるビット/秒の数を指定します。サーバーから RSVP を要求しているクライアントは、帯域幅 (フロー限界) の特定量を尋ねてきます。QoS ポリシーは要求された帯域幅を調べ、それとこのポリシーの速度およびフロー限界を比較します。この要求によりサーバーがその限界を超えると、サーバーはその要求を否認します。トークン速度限界は、統合サービス (IntServ) ポリシー内のアドミッション制御のみに使用されます。これは、Kb/s で計測されます。この値は、10 Kb/s ～ 1Gb/s の間で変動してかまいません。

平均速度限界または帯域幅限界は、ユーザーがインターフェース全体を使用し尽くしてしまうことがないように、ピーク速度限界またはピーク帯域幅限界より低くなければなりません。たとえば、36 Kb/s 以下を使用するモデムがあったとすると、平均速度限界をインターフェース全体は使用されないような値に設定することが必要になります。

ヒント: 設定する限界を決めるために、モニターを実行することができます。ネットワーク上のほとんどのデータ・トラフィックを収集するのに集約トークン速度限界が十分に大きいポリシーを作成します。 次に、このポリシーでデータ収集を開始します。ご使用のアプリケーションおよびネットワークが現在使用する合計速度を収集する 1 つの方法として、『現行ネットワーク統計のモニター』の例を参照してください。これらの結果を使用して、限界を適切に削減することができます。

詳細については、『DiffServ サービス・クラス』および『統合サービス』のトピックを参照してください。
«

DiffServ マーキングを使用した統合サービス

混合環境がある場合、このポリシーが最も頻繁に使用されます。統合サービス予約をサポートせずに、DiffServ をサポートする様々なルーターを統合サービス予約が通過する場合、混合環境が生じます。トラフィックは、様々な異なるドメイン、サービス・レベル・アグリーメント、およびさまざまな権限を持つ設備を通過するので、常に希望のサービスを得られるとは限りません。

この潜在的な問題を減少させるために、DiffServ マーキングを統合サービス・ポリシーに付加することができます。ポリシーが、RSVP プロトコルを使用できないルーターを通っても、ポリシーはいくらかの優先順位を保持します。追加するマーキングは、PHB (ホップごとの転送優先順位付け) といいます。 »

非シグナル方式

マーキングの使用に加えて、上記のように、新しい「非シグナル」機能を使用することもできます。「非シグナル方式」は、統合サービス・ポリシー内に指定します。統合サービス・ポリシーの「**プロパティー**」パネルで「非シグナル方式」を指定してください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. **「アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)」—>「IntServ」**を展開します。
4. 前に作成したポリシー名を右マウス・ボタンでクリックし、「**プロパティー**」を選択すると、「IntServ プロパティー」ダイアログが表示されます。
5. 「**トラフィック管理**」タブを選択して、シグナル通知を使用不可または使用可能にします。図からわかるように、ここでもスケジュール、クライアント、アプリケーション、およびトラフィック管理を編集できます。

API の「非シグナル方式」バージョンを選択した場合は、サーバー上に RSVP 規則がロードされるようにするアプリケーションを作成できるようになります。この場合、TCP/IP 会話のサーバー側アプリケーションを RSVP 使用可能にするだけで済みます。 RSVP シグナル方式は、クライアント・サイドのために自動的に実行されます。これにより、クライアント・サイドが RSVP プロトコルを使用できない場合でも、アプリケーションの RSVP 接続が可能になります。 «

詳細については、『DiffServ サービス・クラス』および『統合サービス』の各トピックを参照してください。

RSVP プロトコルおよび QoS API

»

Resource Reservation Protocol (RSVP) は、RAPI API または qtoq QoS ソケットAPI と共に統合サービスの予約を行います。トラフィックが通過する各ノードは、RSVP プロトコルを使用する能力をもっていなくてはなりません。 この統合サービス・ポリシーを実行する能力があることを、頻繁に RSVP 使用可能であるといいます。 RSVP プロトコルの使用に必要なルーター機能の詳細については、『トラフィック制御機能』を参照してください。

RSVP プロトコルは、トラフィックのパスに存在するすべてのネットワーク・ノードでの RSVP 予約の作成に使用されます。 RSVP プロトコルは、要求されたサービスをポリシーに提供する期間中、この予約を保持します。予約は、この対話でデータが必要とする処理と帯域幅を定義します。各ネットワーク・ノードは、予約で定義されているデータ処理を実行することに同意します。

RSVP は単純なプロトコルであり、予約は (受信側から) 一方向でのみ行われます。オーディオ/ビデオ会議などのより複雑な接続の場合は、送信側のそれぞれが受信側でもあります。この場合、それぞれの側で 2 つの RSVP セッションをセットアップする必要があります。

RSVP 使用可能ルーターに加えて、統合サービスを使用するためには RSVP 使用可能アプリケーションも必要です。この時点では、iSeries サーバーに RSVP 使用可能アプリケーションはないので、RAPI API またはqtoq QoS ソケット API を使用して RSVP 使用可能アプリケーションを作成する必要があります。これらの API により、アプリケーションは RSVP プロトコルを使用できるようになります。詳しい説明が必要な場合は、これらの API モデル、その動作およびメッセージングに関する多数の情報源がありますので、それらを参照してください。 RSVP プロトコルおよびインターネット RFC 2205 の内容についての理解を深める必要があります。

qtoq ソケット API

qtoq QoS ソケット API を使用して、iSeries システム上で RSVP プロトコルを使用するのに必要な作業を単純化できるようになりました。 qtoq ソケット API は RAPI API を呼び出して、より複雑なタスクの一部を実行します。 qtoq ソケット API は、RAPI API ほど柔軟ではありませんが、少ない負荷で同じ機能を提供します。 API の「非シグナル方式」バージョンにより、下記のアプリケーションを作成することができます。

- サーバー上に RSVP 規則をロードするアプリケーション。
- TCP/IP 会話のサーバー側アプリケーションを RSVP 使用可能にするだけのアプリケーション。

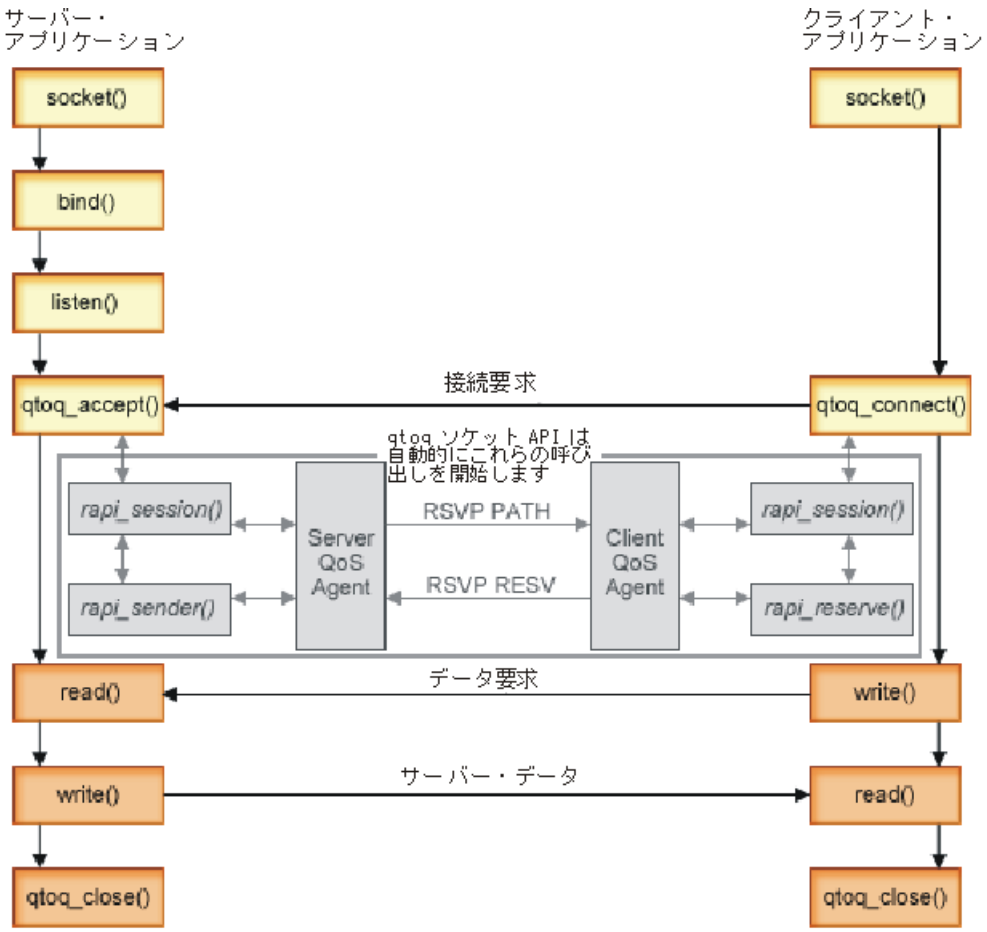
RSVP シグナル方式は、クライアント・サイドのために自動的に実行されます。

コネクション型またはコネクションレスの qtoq QoS ソケットを使用するアプリケーション/プロトコルの典型的な QoS API フローについては、『QoS API コネクション型機能フロー』のページ、または『QoS API コネクションレス機能フロー』のページを参照してください。 «

QoS API コネクション型機能フロー

» 次の図は、TCP などのコネクション型プロトコル用の QoS 使用可能 API qtoq ソケット機能のクライアント/サーバー関係を示したものです。

RSVP の始動を要求するコネクション型フローのために、QoS 使用可能 API 機能が呼び出されると、その他の機能も開始されます。これらの追加の機能により、クライアントおよびサーバー上の QoS エージェントは、クライアントとサーバーとの間のデータ・フローのための RSVP プロトコルをセットアップします。



イベントの qtoq フロー: 次のソケット呼び出し手順では、上図について説明しています。また、コネクション型設計でのサーバー・アプリケーションとクライアント・アプリケーション間の関係についても説明しています。これらは基本ソケット API を修正したものです。

サーバー・サイド

「非シグナル方式」とマーク付けされた規則に関するqtoq_accept()

1. アプリケーションは socket() 機能を呼び出し、ソケット記述子を取得します。
2. アプリケーションは listen() を呼び出し、どの接続を待つのかを示します。
3. アプリケーションは qtoq_accept()を呼び出し、クライアントからの接続要求を待ちます。
4. API は rapi_session() API を呼び出します。その呼び出しが成功した場合は、QoS セッション ID が割り当てられます。
5. API は標準 accept() 機能を呼び出し、クライアントの接続要求を待ちます。
6. 接続要求が受信されると、要求された規則に関してアドミッション制御が行われます。この規則は TCP/IP スタックに送られ、それが有効である場合は、その結果とセッション ID と一緒に呼び出し側アプリケーションに戻されます。
7. サーバーとクライアントのアプリケーションは、要求されたデータ転送を実行します。
8. アプリケーションは qtoq_close() 機能を呼び出し、ソケットをクローズして規則をアンロードします。

9. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他の終結処理をすべて実行します。

通常の RSVP シグナル方式による qtoq_accept()

1. アプリケーションは socket() 機能を呼び出し、ソケット記述子を取得します。
2. アプリケーションは listen() を呼び出し、どの接続を待つのかを示します。
3. アプリケーションは qtoq_accept()を呼び出し、クライアントからの接続要求を待ちます。
4. 接続要求が届くと、rapi_session() API が呼び出されます。この API が、この接続に関する QoS サーバーとのセッションを作成し、呼び出し元に戻されることになる QoS セッション ID を取得します。
5. QoS サーバーからの PATH メッセージを伝え、クライアントからの RESV メッセージが必要であることを QoS サーバーに通知するために、 rapi_sender() API が呼び出されます。
6. rapi_getfd() API が呼び出され、 QoS イベント・メッセージを待つためにアプリケーションが使用する記述子を取得します。
7. 受け入れ記述子および QoS 記述子は、アプリケーションに戻されます。
8. QoS サーバーは、RESV メッセージが受信されるのを待ちます。メッセージが受信されると、QoS サーバーは、QoS マネージャーを使用して適切な規則をロードし、アプリケーションにメッセージを送信します (アプリケーションが qtoq_accept() API 呼び出しに関する通知を要求した場合)。
9. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
10. アプリケーションは、この接続の完了時に qtoq_close() を呼び出します。
11. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる終結処理をすべて実行します。

クライアント・サイド

通常の RSVP シグナル方式による qtoq_connect()

1. アプリケーションは socket() 機能を呼び出し、ソケット記述子を取得します。
2. アプリケーションは qtoq_connect() 機能を呼び出し、接続を望んでいることをサーバー・アプリケーションに通知します。
3. qtoq_connect() 機能は、この接続に関する QoS サーバーとのセッションを作成するために、rapi_session() API を呼び出します。
4. QoS サーバーは、要求された接続からの PATH コマンドを待つためにプライム状態になります。
5. rapi_getfd() API が呼び出され、 QoS メッセージを待つためにアプリケーションが使用する QoS 記述子を取得します。
6. connect() 機能が呼び出されます。connect() の結果および QoS 記述子は、アプリケーションに戻されます。
7. QoS サーバーは、PATH メッセージが受信されるのを待ちます。メッセージが受信されると、QoS サーバーは、アプリケーション・サーバー・マシン上の QoS サーバーに対する RESV メッセージで応答します。
8. アプリケーションが通知を要求した場合は、QoS サーバーは、QoS 記述子を使用してアプリケーションに通知を送ります。
9. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
10. アプリケーションは、この接続の完了時に qtoq_close() を呼び出します。
11. QoS サーバーは QoS セッションをクローズし、必要な終結処理をすべて実行します。

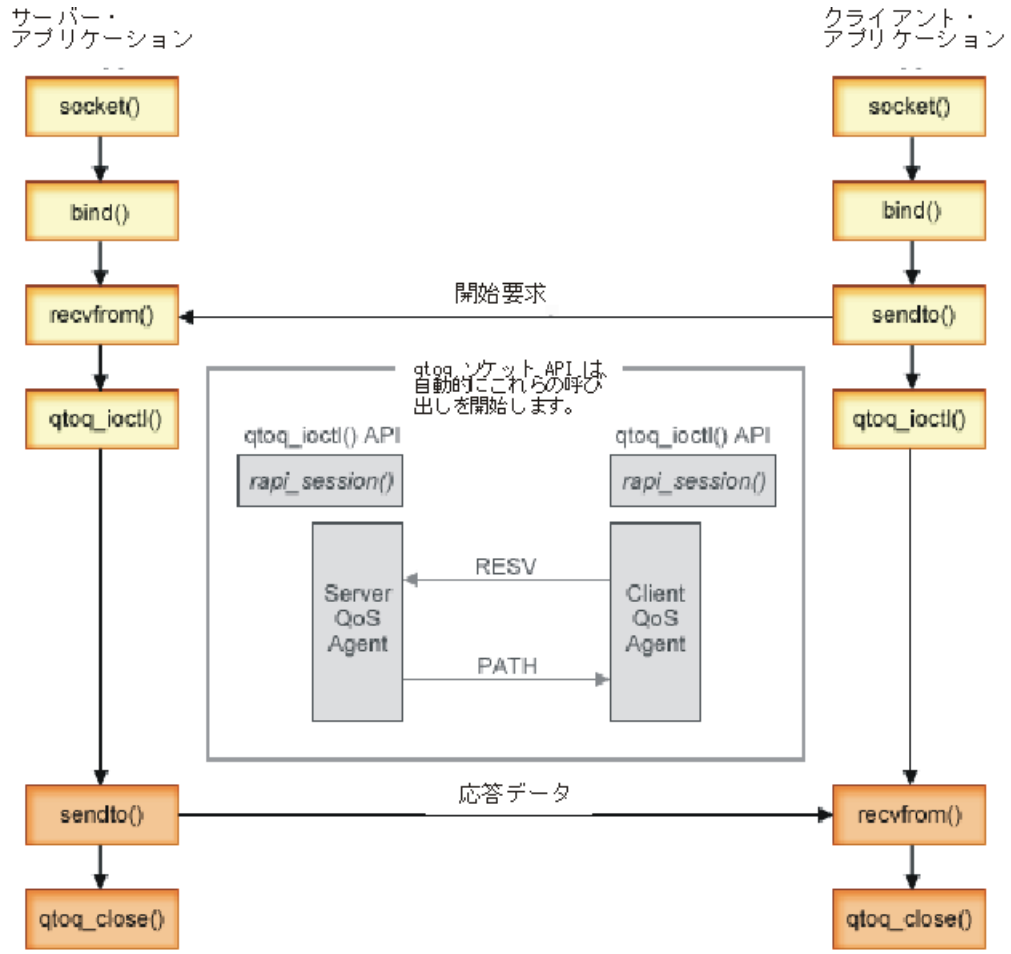
「非シグナル方式」とマーク付けされた規則に関する qtoq_connect()

この要求はクライアント・サイドでは無効です。この場合はクライアントからの応答が不要であるためです。 «

QoS API コネクションレス機能フロー

» 下記のサーバーおよびクライアントの例は、コネクションレス・フローに関する qtoq QoS ソケット API を示したものです。

QoS 使用可能 API 機能が、RSVP を開始するように要求するコネクションレス・フローのために呼び出されると、その他の機能も開始されます。これらの追加の機能により、クライアントおよびサーバー上の QoS エージェントは、クライアントとサーバーとの間のデータ・フローのための RSVP プロトコルをセットアップします。



イベントの qtoq フロー: 次のソケット呼び出し手順では、上図について説明しています。また、コネクションレス設計でのサーバー・アプリケーションとクライアント・アプリケーション間の関係についても説明しています。これらは基本ソケット API を修正したものです。

サーバー・サイド

「非シグナル方式」とマーク付けされた規則に関する qtoq_ioctl()

1. 要求された規則に関してアドミッション制御を実行するように求めるメッセージを QoS サーバーに送信します。
2. この規則が受け入れ可能な場合は、規則がロードされるように要求するQoS サーバーへのメッセージを送信する機能を呼び出します。
3. この要求の成否を示す状況を呼び出し元に戻します。
4. アプリケーションが接続の使用を完了した時点で、アプリケーションは接続をクローズするために qtoq_close() 機能を呼び出します。
5. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる他の終結処理をすべて実行します。

通常の RSVP シグナル方式による qtoq_ioctl()

1. 要求された接続に関してアドミッション制御を要求するメッセージを QoS サーバーに送信します。
2. rapi_session() を呼び出して、その規則に応じてセッションをセットアップするように要求し、呼び出し元に戻される QoS セッション ID を取得します。
3. rapi_sender() を呼び出して、 PATH メッセージをクライアントに伝えます。
4. rapi_getfd() を呼び出して、QoS のイベントを待つためにファイル記述子を取得します。
5. 記述子 select()、QoS セッション ID、および状況を呼び出し元に戻します。
6. QoS サーバーは、RESV メッセージの受信時に規則をロードします。
7. アプリケーションは、この接続の完了時に qtoq_close() を実行します。
8. QoS サーバーは、その規則を QoS マネージャーから削除し、QoS セッションを削除し、さらに必要とされる終結処理をすべて実行します。

クライアント・サイド

通常の RSVP シグナル方式による qtoq_ioctl()

1. rapi_session() を呼び出して、セッションをこの接続に応じてセットアップするように要求します。rapi_session() 機能は、この接続に関するアドミッション制御を要求します。この接続がクライアント・サイドで拒否されるのは、クライアント用に構成済みの規則が存在し、その規則がこの時点で活動状態ではない場合だけです。この機能は、渡される QoS セッション ID をアプリケーションに戻します。
2. rapi_getfd() を呼び出して、QoS のイベントを待つためにファイル記述子を取得します。
3. qtoq_ioctl() は呼び出し元に戻り、記述子および セッション ID を待ちます。
4. QoS サーバーは、PATH メッセージが受信されるのを待ちます。 PATH メッセージが受信されると、QoS サーバーは、RESV メッセージで応答してから、セッション記述子を使用してアプリケーションにイベントが生じたことをシグナル通知します。
5. QoS サーバーは、確立されたセッションへの最新表示の提供を継続します。
6. クライアント・コードは、この接続の完了時に qtoq_close() を呼び出します。

「非シグナル方式」とマーク付けされた規則に関する qtoq_ioctl()

この要求はクライアント・サイドでは無効です。この場合はクライアントからの応答が不要であるためです。 «

QoS の計画

» Quality of service をインプリメントする時の最も重要なステップは、計画にあります。希望どおりの結果を得るためには、ネットワーク装置とモニター・ネットワーク・トラフィックを確認する必要があります。『QoS 計画アドバイザー』に、計画フェーズでご自分で確認する必要のある基本的な質問事項が記載されています。アドバイザーに加えて、QoS をインプリメントする前に次のサブトピックも考慮してください。

権限要件
QoS およびディレクトリー・サーバーを正常に構成するために必要なすべての権限がリストされています。

システム要件
QoS を正常に機能させるために必要なすべての要件がリストされています。

QoS ポリシーの順序付け
ファイル内でのポリシーの記載順序が、それらのポリシーの処理順序です。これは DiffServ ポリシーおよび接続速度ポリシーにのみ適用されます。

サービス・レベル・アグリーメント (SLA)
SLA は、QoS の重要な部分です。 QoS 計画の一部として SLA について理解し、ネットワーク・プロバイダーと共に SLA をセットアップする必要があります。

ネットワークのハードウェアおよびソフトウェア
Quality of service は、最も弱いリンクの能力程度に合わせて機能します。ネットワーク内部の装置とネットワーク外部の他の装置の能力は、QoS の結果に非常に大きく影響します。

ネットワーク・パフォーマンス
QoS とは、つまりネットワーク・パフォーマンスを意味します。 QoS の採用を考える主な理由は、すでにネットワーク輻輳 (ふくそう) とパケット・ロスを経験しているから、という場合がほとんどです。ポリシーをインプリメントする前に、QoS モニターを使用して IP トラフィックの現在のパフォーマンス・レベルを検証することができます。このモニター結果から、どこで輻輳 (ふくそう) が発生しているかを判断できます。 『QoS のトラブルシューティング』の『サーバー・トランザクションのモニター』トピックを参照してください。

QoS 計画アドバイザー
Quality of service をインプリメントする前に、ここに記載されている基本的な質問事項を熟考してください。ご使用のアプリケーションの能力に基づく推奨ポリシーが示された計画ワークシートが表示されます。

«

権限要件

» Quality of service ポリシーには、ネットワークに関する機密情報が含まれることがあります。したがって、QoS 管理権限は、必要な場合にのみ付与する必要があります。 QoS ポリシーまたは LDAP ディレクトリー・サーバーを構成するためには、下記の権限が必要になります。 QoS ポリシーは LDAP ディレクトリー・サーバーに保管されるので、両方の権限が必要です。

ディレクトリー・サーバーの管理に必要な権限の付与
QoS 管理者には、*ALLOBJ 権限と *IOSYSCFG 権限が必要です。代替権限については、『ディレクトリー・サーバーの構成』を参照してください。

TCP/IP サーバーを始動する権限の付与
STRTCPSVR および ENDTCPSVR コマンドに対するオブジェクト権限を付与するには、以下のステップにしたがってください。

1. **STRTCPSVR**: コマンド行で GRTOBJAUT OBJ (QSYS/STRTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) を入力し、ADMINPROFILE に対する管理者のプロファイルの名前を置き換えて、**「Enter」**キーを押します。
2. **ENDTCPSVR**: コマンド行で GRTOBJAUT OBJ (QSYS/ENDTCPSVR) OBJTYPE (*CMD) USER (ADMINPROFILE) AUT (*USE) を入力し、ADMINPROFILE に対する管理者のプロファイルの名前を置き換えて、**「Enter」**キーを押します。

全オブジェクト許可およびシステム構成権限の付与

QoS を構成するユーザーはセキュリティー担当者アクセス権を持つことをお勧めします。全オブジェクト許可およびシステム構成権限を付与するには、以下のステップにしたがってください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ユーザーおよびグループ (Users and Groups)」**の順に展開します。
2. **「すべてのユーザー」**をダブルクリックします。
3. 管理者のユーザー・プロファイルを右クリックして、**「プロパティー」**を選択します。
4. 「プロパティー」ダイアログで、**「機能」**をクリックします。
5. 「機能」ページで、**「全オブジェクト許可」**および**「システム構成」**を選択します。
6. **「OK」**をクリックして、「機能」ページをクローズします。
7. **「OK」**をクリックして、「プロパティー」ダイアログをクローズします。

«

システム要件

Quality of service (QoS) は、オペレーティング・システムの統合された部分です。 QoS を構成して開始するには、事前に OS/400(R) の V5R1 またはそれ以降のバージョンがインストールされていなければなりません。その他に、次の処理を完了させておく必要があります。

1. TCP/IP 接続ユーティリティー (57*xx*-TC1) をインストールします。
2. PC に iSeries ナビゲーターをインストールします。クライアント・アクセスのインストール時に、必ず「ネットワーク」セクションをインストールしてください。 Quality of service は、「ネットワーク」の中の「IP ポリシー」下にあります。

注: TCP/IP、ネットワーキング、または IP アドレスに関する詳しい情報が必要な場合は、 『QoS に関するその他の情報』の中の『TCP/IP Tutorial and Technical Overview』および『V4 TCP/IP for AS/400(R): More Cool Things Than Ever』を参照してください。

QoS ポリシーの順序付け

» 重複する 2 つの DiffServ ポリシーまたは重複する 2 つの接続速度ポリシーがある場合は、iSeries ナビゲーターの画面に表示されたポリシーの物理的な順序が常に重要です。重複ポリシーとは、同じクライアント、アプリケーション、スケジュール、またはプロトコルを使用する 2 つのポリシーです。ポリシーは、iSeries ナビゲーター画面で番号付きリスト形式で表示されます。ポリシーの優先順位は、このリストのポリシーの順序に依存します。あるポリシーの優先順位を別のポリシーより高くしたい場合、その優先順位が高い方のポリシーがリストでは先に表示されなくてはなりません。

あるポリシーが別のポリシーと重複しているかどうかを判断するには、次の手順に従ってください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—> 「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックします。

3. 「**構成**」を選択します。
4. 特定の「ポリシー」フォルダーを選択します。
5. 関連した重複ポリシーがあるポリシーの名前を右マウス・ボタンでクリックします。重複したポリシーの場合、重複を示すアイコンが前にあります。
6. 「**重複の表示 (Show Overlap)**」を選択します。 重複パネルが表示されます。

画面上のポリシー順序の変更は、次の方法で行います。

- ポリシーを強調表示して、画面の上矢印および下矢印を使用してポリシー順序を変更します。
- ポリシー名を右マウス・ボタン・クリックし、「**上に移動 (Move up)**」または「**下に移動 (Move down)**」を選択します。
- QoS サーバーを更新します。ツールバーの「サーバー更新」ボタンを使用するか、または詳細について『QoS タスク・ヘルプ』を参照してください。

«

サービス・レベル・アグリーメント

このセクションは、サービス・レベル・アグリーメント (SLA) に関する教育的情報の提供を目的とはしていませんが、Quality of service のインプリメンテーションに影響を与える可能性のある、SLA のいくつかの重要な局面を指摘しています。ポリシーと予約は、最も弱いリンクの能力の程度に合わせて機能します。つまり、クライアントとサーバーの間に存在する、あるノードが、DiffServ または統合サービスのトピックで説明されているトラフィック処理特性のいずれかを実行できない場合、ポリシーは希望どおりに処理されません。 SLA によって十分なリソースが使用可能でないと、最高のポリシーであってもネットワークの輻輳 (ふくそう) 問題を解決できません。

これは、ISP 間の合意にもかかわります。複数のドメインにわたり、すべての ISP は Quality of service 要求のサポートに合意していなくてはなりません。相互運用性が問題を引き起こす可能性もあります。

必ず、実際に受けているサービス・レベルを確認してください。トラフィック調整アグリーメントは、特にトラフィックの処理方法 (廃棄、マーキング、シェーピング、または再送) に関する合意です。 Quality of service を提供する主な理由は、待ち時間、ジッター、帯域幅、パケット・ロス、可用性、およびスループットにかかわっています。サービス・アグリーメントは、ポリシーに、そのポリシーが要求するものを提供できなくてはなりません。現在、必要な量のサービスを受けているかを確認してください。受けていない場合は、リソースを無駄にしている可能性があります。たとえば、IP 電話用に 500 kbps の予約を要求しても、アプリケーションは 20kbps しか必要としない場合、ISP からは通知がなくても余分な料金を支払っている可能性があります。

ネットワークのハードウェアおよびソフトウェア

ネットワーク内部の装置とネットワーク外部の他の装置の能力は、QoS の結果に非常に大きく影響します。

アプリケーション
統合サービス・ポリシーには、RSVP 使用可能アプリケーションが必要です。 iSeries アプリケーションは、現在 RSVP 使用可能ではないので、iSeries アプリケーションが RSVP プロトコルを使用できるようにする必要があります。このためには、Resource Reservation Setup Protocol (RSVP) API または qtoq QoS ソケット API を利用して特別なプログラムを作成する必要があります。 このプログラムによって、アプリケーションは RSVP を使用できるようになります。詳細については、『RSVP プロトコルおよび QoS API』を参照してください。

ネットワーク・ノード
ルーター、スイッチ、さらにはご使用のサーバーにいたるまで、Quality of service を使用する能力をもっている必要があります。 DiffServ ポリシーを使用するには、装置が DiffServ 使用可能でなくてはなりません。つまり、ネットワーク・ノードには、IP パケットの分類、計量、マーキング、シェーピングおよび廃棄を行う能力が必要です。トラフィック・コンディショナー (分類、計量、マーキング、シェーピングおよび廃棄) に関する詳細は、『トラフィック・コンディショナー』トピックを参照してください。

統合サービス・ポリシーを使用するには、装置が RSVP 使用可能でなくてはなりません。つまり、ネットワーク・ノードが RSVP プロトコルもサポートできなくてはなりません。 RSVP プロトコルに関する詳細は、『RSVP』トピックを参照してください。

QoS の構成

実際には、iSeries ナビゲーター内のウィザードを使用して QoS ポリシーを作成します。これらのウィザードから出される指示に従うことで、構成をスムーズに行なうことができます。

» ポリシーを構成した後は、iSeries ナビゲーターの構成オブジェクトを使用してポリシー構成を編集することができます。構成オブジェクトは、ポリシーを構成している様々な部分のことです。 iSeries ナビゲーターで Quality of service を開くと、クライアント、アプリケーション、スケジュール、ポリシー、サービス・クラス、PHB (ホップごとの転送優先順位付け)、および URI のラベルが付いたフォルダーがあります。これらのオブジェクトを使用してポリシーを作成できます。これらのオブジェクトの詳細は、iSeriesナビゲーターの Quality of service 概要のヘルプを参照してください。

ディレクトリー・サーバーの構成
QoS 内でディレクトリー・サーバーを構成する方法については、このトピックを参照してください。

ウィザードを使用した QoS の構成
QoS ウィザードへのアクセス方法については、このトピックを参照してください。 «

QoS の使用可能化
ポリシーを有効にするには、その前にそのポリシーを使用可能にする必要があります。 ウィザードを使用すると、サーバーは自動的にポリシーを使用可能にします。構成オブジェクトを使用してポリシーを変更した場合、ポリシーを活動状態にするにはサーバーを動的に更新する必要があります。ポリシーを使用可能にする前に、問題の原因となる重複ポリシーがないかを確認してください。詳細は、『QoS ポリシーの順序付け』を参照してください。

ディレクトリー・サーバーの構成

» QoS ポリシー構成は、LDAP ディレクトリー・サーバーに保管されます。これによって、QoS ソリューションを管理するのが容易になります。すべてのサーバーで QoS ポリシーを構成する代わりに、1 つのローカル・ディレクトリー・サーバーで構成データを保管して、たくさんのシステムで共用することができま

す。サーバー上に Quality of service を最初に構成するときに、「初期構成 (Initial Configuration)」ウィザードが表示されます。このウィザードは、ディレクトリー・サーバーを構成するようにプロンプトを出します。

ディレクトリー・サーバーを構成するためには、下記の情報を決定するかまたは認識しておく必要があります。

- ディレクトリー・サーバー名
- QoS ポリシーを参照するための識別名 (DN) を決定する
- LDAP ディレクトリー・サーバーを用いた SSL セキュリティーを使用するか否かを決定する
- ディレクトリー・サーバー上でのポリシーの検索を改善するためにキーワードを使用するか否かを決定する

注: 現在、Kerberos を、QoS サーバーがディレクトリーにアクセスするために使用する認証メソッドとして構成することはできません。

LDAP ディレクトリー・サーバーを管理するには、下記のいずれかの権限セットを保持する必要があります。

- *ALLOBJ 権限と *IOSYSCFG 権限
- *JOBCTL 権限と TCP/IP 終了 (ENDTCP)、TCP/IP 開始 (STRTCP)、TCP/IP サーバー開始 (STRTCPSVR)、TCP/IP サーバー終了 (ENDTCPSVR) の各コマンドに対するオブジェクト権限
- OS/400(R) セキュリティー監査を構成するための *AUDIT 権限

iSeries ナビゲーターを使用している場合は、デフォルトの QoS スキーマにアクセスできます。ただし、iSeries ナビゲーター以外のエディターを使用している場合は、以下で説明する LDIF ファイルをインポートする必要があります。編集後に、元のデフォルト・ファイルを再ロードしたい場合にも、LDIF ファイルをインポートすることができます。

QoS スキーマ

スキーマと呼ばれる規則セットは、どのタイプの LDAP オブジェクトが QoS サーバーに対して有効であるかを指定するためのものです。 V5R2 iSeries サーバー上のスキーマには、QoS に必要な規則が含まれています。ただし、使用する LDAP サーバーが iSeries サーバーでない場合は、これらの規則を LDAP サーバーにインポートする必要があります。このインポートは LDIF (LDAP データ交換形式) ファイルを使用して行われます。LDIF ファイルをダウンロードするには、 iSeries LDAP Web ページ を使用してください。このファイルを見つけるには、左側ペインで**「カテゴリー (Categories)」—> 「TCP/IP ポリシー」**の順に展開します。

LDIF ファイルの編集

IBM(R) SecureWay(R) Directory Management Tool (DMT) を使用して、LDAP サーバー用にスキーマ・ファイルを編集することができます。 DMT 用の setup.exe ファイルを PC に FTP でファイル転送することもできます。 setup.exe ファイルは、 `/qibm/proddata/os400/dirsrv/UserTools/Windows` からサーバーにダウンロードしてください。元の QoS スキーマは、iSeries LDAP Web ページから入手することができます。 QoS スキーマの例については、『LDAP の概念』を参照してください。スキーマ・ファイルは、`/QIBM/UserData/OS400/DirSrv` からサーバーにダウンロードされます。 «

ウィザードを使用した QoS の構成

» Quality of service ポリシーを構成するには、iSeries ナビゲーターの中の QoS ウィザードを使用する必要があります。各種ウィザードとその機能について説明します。

初期構成 (Initial Configuration) ウィザード
このウィザードでは、システム固有の構成およびディレクトリー・サーバー情報をセットアップすることができます。

新規 IntServ ポリシー (New IntServ Policy) ウィザード
新規 IntServ ポリシー・ウィザードでは、統合サービス・ポリシーを作成することができます。このポリシーは、RSVP 要求を承認または否認し、間接的にサーバーの帯域幅を制御します。ポリシー・パフォーマンスの制限 (ユーザーが設定する) により、サーバーがクライアントの RSVP アプリケーションから取り入れられる要求された帯域幅を処理できるかどうかが決まります。このウィザードで作成された統合サービス・ポリシーをインプリメントするには、RSVP 作動可能ルーターおよびアプリケーションが必要です。

> **注:** 統合サービス・ポリシーをセットアップする前に、RSVP プロトコルを使用するためのユーザー自身のアプリケーションを作成する必要があります。詳細については、『RSVP プロトコルおよび QoS API』を参照してください。

新規 DiffServ ポリシー (New DiffServ Policy) ウィザード
このウィザードでは、TCP/IP トラフィックを差異化し、優先順位を TCP/IP トラフィックに割り当てることができます。 ポリシーを作成することでトラフィックを差異化できるようになります。ポリシー内では、アプリケーションおよびポートに優先順位を割り当て、このポリシーをアクティブにする時期を指定することができます。

新規 DiffServ サービス・クラス (New DiffServ class of service) ウィザード
ネットワーク内のルーターおよびスイッチで使用されるパケット・マーキングを設定するには、この DiffServ サービス・クラス・ウィザードを利用します。このウィザードでは、ネットワークを出るトラフィックにパフォーマンス制限も割り当てます。 DiffServ ポリシーのサービス・クラスを使用します。

新規接続速度 (New Connection rate) ウィザード
「インバウンド接続速度」ウィザードを使用して、サーバーに対して行われる接続を制限します。アクセスは、TCP/IP アドレス、アプリケーション、またはローカル・インターフェースにより制限することができます。これにより、システム管理者は、特定のクライアントからのユーザーのサーバーへのアクセス、またはサーバー・アプリケーションまたはインターフェースへのアクセスを制御することができます。さらに、サーバーのパフォーマンスを向上させることができます。

新規 URI (New URI) ウィザード
「インバウンド URI」ウィザードを使用して、サーバーに対して行われる接続を制限します。アクセスは、URI、アプリケーション、または iSeries サーバー上のローカル・インターフェースにより制限することができます。これにより、システム管理者は、サーバー上の特定の URI、アプリケーション、またはインターフェースへのアクセスを制御することができます。さらに、サーバーのパフォーマンスを向上させることができます。

> **注:** URI 要求速度ポリシーを設定する前に、以下のステップを実行する必要があります。

1. `WRKHTTPCFG` - Apache Web サーバー・インスタンスを変更する。 Fast Response Cache Accelerator (FRCA) オプションを指定した Listen ディレクティブを使用してポートを使用可能にします。
2. `STRTCPSVR SERVER(*HTTP) HTTPSRV` (インスタンスの名前)。
3. iSeries ナビゲーターの QoS を使用して URI ポリシーを作成または変更する。 URI ポリシーで定義されているアプリケーション・ポートが Apache Web サーバー・インスタンスで定義されている FRCA「Listen ディレクティブ」と合致していることを確認します。
4. `STRTCPSVR SERVER(*QOS)`。

新規 URI ポリシーで割り当てられているアプリケーション・ポートは、Apache Web サーバー構成で FRCA 用に使用できる「Listen」ディレクティブと合致する必要があります。このポート値が一致しない場合は、QoS URI ポリシーは期待通りには機能しません。 URI 要求速度ポリシーについては、『接続要求速度および URI 要求速度』を参照してください。

作成するポリシーのタイプを決めた後で、上記の適切なウィザードでポリシーを構成することができます。ポリシーの構成を開始するには、『iSeries ナビゲーターでの QoS ウィザードへのアクセス』を参照してください。 «

iSeries ナビゲーターでの QoS ウィザードへのアクセス

»

QoS ウィザードにアクセスし、新規ポリシーを作成するには、次の手順に従ってください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
   注: 下記の場合には、「初期構成 (Initial Configuration)」ウィザードが表示されます。
   - サーバーを新規リリースにアップグレードしようとしている場合。情報を保管するディレクトリー・サーバーを構成することが必要になります。この変換時には、データは破損しません。
   - これが、このシステムで初めて QoS グラフィカル・ユーザー・インターフェース (GUI) を使用しようとしている場合。
   - 以前の任意の構成情報を手動で除去し、やり直したい場合。これは QoS インターフェースがすでにオープンされている場合にのみ生じます。
3. **初期構成 (Initial Configuration) ウィザード**を完了させます。「初期構成 (Initial Configuration)」ウィザードが表示されない場合は、ステップ 4 に進みます。
4. 「**ポリシー (Policies)**」を選択します。「**IntServ**」、「**DiffServ**」、「**接続速度 (Connection rate)**」、または「**サーバー要求 —> URI**」のいずれかを右マウス・ボタンでクリックします。
5. 「**新規ポリシー (New Policy)**」を選択します。

«

QoS の管理

QoS ポリシーを活動状態にして稼働させてみると、更新が必要となる場合があります。次の方法でポリシーを管理できます。

iSeries ナビゲーターの QoS タスク・ヘルプへのアクセス
本書では、iSeries ナビゲーターの QoS タスク・ヘルプを頻繁に参照します。このヘルプへのアクセス手順がわからない方は、ここで確認してください。

QoS ポリシーのバックアップ
ポリシーのバックアップをとって、ファイルの消失を防ぐことができます。

既存ポリシーのコピー
作成したいポリシーに似ている既存のポリシーをコピーできます。

ポリシーの動的更新
サーバーの稼働中にポリシーを動的に更新することができます。段階的説明については、 iSeries ナビゲーターの『QoS タスク・ヘルプ』の中の「*QoS サーバーの更新*」を参照してください。

QoS ポリシーの編集
既存のポリシーのパラメーターを変更できます。

QoS 構成プロパティーの編集
Quality of service 構成のプロパティーを変更することができます。このプロパティーには、ディレクトリー・サーバーの構成、ジャーナル処理、およびサーバーの自動的開始に関する設定値が含まれています。段階的な説明については、 iSeries ナビゲーターの『QoS タスク・ヘルプ』の中の「*QoS プロパティーの編集*」を参照してください。

QoS ポリシーの使用可能化
ポリシーを有効にするには、その前にそのポリシーを使用可能にする必要があります。ポリシーを使用可能にする前に、エラーがないかをご自身でチェックしてください。たとえば、ポリシーの順序が正確かを確認してください。ポリシー順序の詳細については、『QoS ポリシーの順序付け』を参照してください。また、段階的説明については、 iSeries ナビゲーターの『QoS タスク・ヘルプ』の中の「*QoS ポリシーの使用可能化*」を参照してください。

QoS ポリシーのモニター
ポリシーを管理する際、QoS モニターを分析して、ポリシーが希望どおり作動しているかを検証することができます。

QoS ポリシーの表示
重複ポリシーを表示して、希望しない結果がどこで発生する可能性があるかを判断できます。問題の原因となりうる、目で確認可能なポリシー間のあらゆる重複をチェックすることができます。活動化やテストの前だけではなく、印刷やバックアップの前にも重複を確認できます。これは、テストの前にエラーを最小化または除去するのに有効です。重複ポリシーの表示方法については、『QoS ポリシーの順序付け』を参照してください。

iSeries ナビゲーターの QoS ヘルプへのアクセス

» Quality of service ヘルプにアクセスするには、次のように iSeries ナビゲーターを使用してください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. メニュー・バーで「**ヘルプ」—>「ヘルプ・トピック**」を選択します。画面にタスク・ヘルプ・ウィンドウが表示されます。

«

QoS ポリシーのバックアップ

» 構成ファイルのバックアップをとることをお勧めします。ポリシーはローカルに保管され、かつディレクトリー・サーバーにも保管されます。特に、次の統合ファイル・システム・ディレクトリーのバックアップをとってください。すなわち、IBM/USRDATA/OS400/QOS/ETC、IBM/USRDATA/OS400/QOS/TEMP、および IBM/USRDATA/OS400/QOS/USR です。QoS サーバーに関するディレクトリー・サーバー公表エージェントのバックアップもとる必要があります。この公表エージェントには、ディレクトリー・サーバー名、QoS サーバーの識別名(DN)、ディレクトリー・サーバーへのアクセスに使用されるポート、および認証情報が含まれています。構成ファイルの破損時には、バックアップ・ファイルによって、スクラッチからポリシーを再作成するのに要する時間と作業量を節約することができます。破損ファイルの簡単な置き換えに利用できる一般的なヒントを、次に示します。

1. **統合ファイル・システムのバックアップおよび回復プログラムを利用する。**
   この後に出てくる、バックアップと回復に関する資料へのリンクを利用してください。
2. **ポリシーを印刷しておく。**
   印刷出力を、最も安全だと考えられる場所に保管し、必要に応じてその情報を再入力します。
3. **情報をディスクにコピーする。**
   コピーは、情報が電子的に存在するという点で、手作業で情報を再入力しなければならない印刷出力よりも利点があります。コピーは、1 つのオンライン・ソースから別のオンライン・ソースに情報をトランスポートする直接的な手段です。

   注: iSeries サーバーは、情報をフロッピー・ディスクではなくシステム・ディスクにコピーします。ルール・ファイルは、QIBM/UserData/OS400/QOS/ETC の中、ならびにユーザーが構成したディレクトリー・サーバーの識別名の中にあります (PC 上ではない)。システム・ディスクに保管されているデータを保護するためのバックアップ手段として、ディスク保護という方法を使用できます。

iSeries サーバーを使用する場合、バックアップおよび回復の方針を計画する必要があります。詳細については、バックアップおよび回復の手引き でご確認ください。 «

既存ポリシーのコピー

互いに非常に似ているポリシーがある場合があります。スクラッチからすべてのポリシーを作成するのではなく、元のポリシーのコピーを作成し、元のポリシーとは異なるポリシーのセクションを編集することもできます。 iSeries ナビゲーターで、この QoS 機能は「既存に基づく新規作成 (*New based on*)」と呼ばれています。 ポリシーのコピーを行うことができる QoS ダイアログにアクセスするには、 iSeries ナビゲーターを使用する必要があります。

既存ポリシーのコピーを作成するには、iSeries ナビゲーター・ヘルプの『**既存ポリシーを基にして新規ポリシーを作成する (Creating a new policy based on an existing policy)**』の中の手順に従ってください。

ポリシーを有効にするには、その前に、QoS サーバーを始動するかまたは『サーバーの動的更新』を実行して、そのポリシーを使用可能にする必要があります。ポリシーを使用可能にする前に、問題の原因となる重複ポリシーがないかを確認してください。詳細は、『QoS ポリシーの順序付け』を参照してください。

QoS のモニター

» モニターを利用して、サーバーで IP トラフィックを分析することができます。これは、ネットワーク内のどこで輻輳 (ふくそう) が発生しているかを判断するのに役立ちます。 QoS モニターは QoS の計画

時に役立つだけでなく、トラブルシューティング・ツールとして役立てることもできます。 QoS モニターを使用することで、必要に応じてポリシーを調整できるようにネットワークをモニターし続けることができます。

QoS モニターの実行方法については、iSeries ナビゲーターの QoS ヘルプの指示を参照してください。

注: QoS データ収集をオンにし、QoS 構成に変更を加える計画がある場合は、下記のステップを実行して、モニターが正確なデータを確実に収集するようにする必要があります。

1. QoS データ収集を停止する。
2. 構成変更を行う。
3. QoS サーバーを再始動/更新する。
4. QoS データ収集を開始する。

モニター出力

受け取る出力情報は、モニターしているポリシーのタイプによって異なります。ポリシー・タイプには、DiffServ、IntServ (負荷コントロール・サービス)、IntServ (保証されたサービス)、接続速度、および URI があります。評価するフィールドは、このポリシー・タイプによります。最も注意するべき値は、測定値です。次のフィールドは、与えられた定義ではなく測定された値です。すなわち、受け入れ済み要求、アクティブ接続、接続サービス、接続速度、却下された要求、イン・プロファイル・パケット数、イン・プロファイル・ビット数、非準拠ビット数、アウト・オブ・プロファイル・ビット数、合計ビット数、合計パケット数、および合計要求数です。

上記の測定フィールドの情報を確認することで、ネットワーク・トラフィックがどのくらいポリシーに合致しているかということがわかります。ポリシー・タイプごとのモニター出力フィールドの詳細については、以下の例を参照してください。 QoS ポリシーと一緒にモニターを使用する方法の例については、『QoS のシナリオ』のいずれかを参照してください。

- DiffServ ポリシー (45See)
- 統合サービス (負荷コントロール・サービス) ポリシー (46See)
- 統合サービス (保証されたサービス) ポリシー (47See)
- URI ポリシー (48See)
- 接続速度ポリシー (48See)

DiffServ ポリシー

フィールド	説明
ポリシー名 (Policy name)	このポリシーに割り当てた名前。
プロトコル (Protocol)	UDP、TCP、または ALL
平均トークン速度限界 (Average token rate limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する平均トークン速度。
トークンの深さの限界 (Token depth limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界 (Peak token rate limit)	この接続で許可される最大速度。
イン・プロファイル・パケット数 (Packets in-profile)	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
イン・プロファイル・ビット数 (Bits in-profile)	このポリシーのパラメーター値内に収まる、送信ビット数。

アウト・オブ・プロファイル・ビット数 (Bits out-of-profile)	このポリシーのパラメーター値を超えた、送信ビット数。
ビット・レート (Bits rate)	この接続で許可されるビットの測定数値。
アクティブ接続 (Active connections)	アクティブな接続の合計数。
トラフィック・プロファイル (Traffic profile)	アウト・オブ・プロファイル・パケットに使用されるパケット調整のタイプ。フォーマットでは、次の調整方法を指定できます。 • Re-marking (再マーキング) • Shaping (シェーピング) • Dropping (廃棄)
合計ビット数 (Bits total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって使用された送信ビット数。
イン・プロファイル・コード・ポイント (Codepoint in-profile)	パケットに新規のコード・ポイントが付いている場合、IP パケットがこのポリシーのパラメーター値内に収まっていると、それらの IP パケットはこのコード・ポイントを使用します。
アウト・オブ・プロファイル・コード・ポイント (Codepoint out-of-profile)	パケットに新規のコード・ポイントが付いている場合、IP パケットがポリシーのパラメーター値を超えていると、それらの IP パケットはこのコード・ポイントを使用します。
宛先アドレス範囲 (Destination address range)	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
合計パケット数 (Packet total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって送信されたパケット数。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

統合サービス (負荷コントロール・サービス) ポリシー

フィールド	説明
ポリシー名 (Policy name)	このポリシーに割り当てた名前。
プロトコル (Protocol)	UDP または TCP。
宛先アドレス (Destination address)	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
平均トークン速度限界 (Average token rate limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する平均トークン速度。
トークンの深さの限界 (Token depth limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界 (Peak token rate limit)	この接続で許可される最大速度。
合計パケット数 (Packet total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって送信されたパケット数。
非準拠ビット数 (Bits non-conformant)	このポリシーのパラメーター値を超えた、送信ビット数。
合計ビット数 (Bits total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって使用された送信ビット数。
ビット・レート (Bit rate)	この接続で許可されるビットの測定数値。

準拠ビット数 (Bits conformant)	このポリシーのパラメーター値内に収まる、送信ビット数。
最大パケット・サイズ (Maximum packet size)	このポリシーによって制御される最大許容パケット・サイズ。
最小ポリス単位 (Minimum policed unit)	トークン・バケットから除去される最小ビット数。 たとえば、最小ポリス単位が 100 ビットの場合、100 ビット未満パケットも 100 ビットとして除去されます。
準拠パケット数 (Packets conformant)	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

統合サービス (保証されたサービス) ポリシー

フィールド	説明
ポリシー名 (Policy name)	このポリシーに割り当てた名前。
プロトコル (Protocol)	UDP または TCP。
宛先アドレス (Destination address)	パケットの (このポリシーによって制御される) 宛先ポイントを判断するアドレス範囲。
平均トークン速度限界 (Average token rate limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する最大トークン速度。
トークンの深さの限界 (Token depth limit)	接続パスに存在する各ルーターおよびサーバーにおいて、このポリシーが許可する最大トークン・バッファー・サイズ。
ピーク・トークン速度限界 (Peak token rate limit)	この接続で許可される最大速度。
合計パケット数 (Packet total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって送信されたパケット数。
合計ビット数 (Bits total)	このポリシーが始動されてからモニター・コレクションまでの間に、ポリシーによって使用された送信ビット数。
非準拠ビット数 (Bits non-conformant)	このポリシーのパラメーター値を超えた、送信ビット数。
保証速度 (Guaranteed rate)	保証された速度 (ビット/秒)。
準拠ビット数 (Bits conformant)	このポリシーのパラメーター値内に収まる、送信ビット数。
最大パケット・サイズ (Maximum packet size)	このポリシーによって制御される最大許容パケット・サイズ。
最小ポリス単位 (Minimum policed units)	トークン・バケットから除去される最小ビット数。 たとえば、最小ポリス単位が 100 ビットの場合、100 ビット未満パケットも 100 ビットとして除去されます。
準拠パケット数 (Packets conformant)	このポリシーのパラメーター値内に収まる、送信 IP パケット数。
遊び期間 (Slack term)	希望の遅延と実際の遅延の差 (秒)。
送信元ポート範囲 (Source port range)	このポリシーによって制御されるアプリケーションを判別する、送信元ポートの範囲。

接続速度ポリシー

フィールド	説明
ポリシー名 (Policy name)	このポリシーに割り当てた名前。
接続速度	受け入れられる接続要求の数 (毎秒)。
合計要求数 (Total requests)	このサーバーに対して行われる接続要求の合計数。
受け入れ済み要求 (Accepted requests)	このサーバーが受け入れた接続要求の合計数。
却下された要求 (Dropped requests)	このサーバーによって却下された接続要求の合計数。
平均接続速度限界 (Average connection rate limit)	許可される新規接続要求の平均許容数 (毎秒)。
接続バースト限界 (Connection burst limit)	並行して受け入れられた新規接続要求の最大数。
ピーク接続速度限界 (Peak connection rate limit)	サーバーがネットワークからの接続を受け入れる最大許容速度。
優先順位 (Priority)	QoS マネージャーにロードされる各規則に割り当てられる優先順位。
キュー優先順位 (Queue Priority)	listen キューに入れられる着信接続に割り当てられる優先順位。
宛先ポート範囲 (Destination port range)	サーバー上でトラフィックの宛先となるポート範囲またはポート。
インターフェース・アドレス (Interface address)	モニターされるシステム・インターフェースの IP アドレス。
送信元アドレス範囲 (Source address range)	サーバーに要求を送信するクライアントの IP アドレス範囲。

サーバー要求 - URI ポリシー

フィールド	説明
ポリシー名 (Policy name)	このポリシーに割り当てた名前。
要求速度 (Request rate)	受信される要求の数 (毎秒)。
合計要求数 (Total Requests)	ターゲット・サーバーが受信した要求の合計数。
受け入れ済み要求 (Accepted requests)	受け入れられた要求の合計数。
却下された要求 (Dropped requests)	却下された要求の合計数。
URI	ポリシングされる URI の ID。
平均要求速度限界 (Average request rate limit)	許可される新規要求の平均許容数 (毎秒)。
要求バースト限界 (Request burst limit)	並行して受け入れられる新規要求の最大数。
ピーク要求バースト限界 (Peak request burst limit)	サーバーがネットワークからの要求を受け入れる最大許容速度。
キュー優先順位 (Queue pitrity)	listen キューに入れられる着信接続に割り当てられる優先順位。
宛先ポート (Destination port)	サーバー上でトラフィックの宛先となるポート。
インターフェース・アドレス (Interface address)	モニターされるシステム・インターフェースの IP アドレス。

«

QoS のトラブルシューティング

ここでは、QoS の問題のトラブルシューティングに関するアドバイスを提供します。

通信トレース
サーバーからは、ローカル・エリア・ネットワーク (LAN) または広域ネットワーク (WAN) インターフェースなどの通信回線上のデータを収集するための通信トレースが提供されます。 ユーザーは、一般的にトレース・データの内容全体を理解していない場合があります。 しかし、本書の読者であれば、トレース項目から 2 つの地点間のデータ交換が実際に行われたかどうかを判断できます。 詳細については、「TCP/IP のトラブルシューティング」のトピックの中の『通信トレース』を参照してください。

サーバー上の QoS の使用可能化
QoS サーバーが始動しない場合に最初に調べるものは、 CHGTCP コマンドを使用した IPQOSENB の値です。初めてポリシーを構成する場合は、「初期構成 (Initial configuration)」ウィザードがサーバー上の QoS を自動的に使用可能にします。この値が何らかの理由で変更された場合は、サーバーは始動しません。コマンド行インターフェースで、CHGTCPA IPQOSENB(*YES) を入力してください。

QoS ポリシーのジャーナル処理
Quality of service には、ジャーナル処理機能が組み込まれています。サーバーで追加、除去または変更された IP ポリシーのロギングにジャーナル処理を利用できます。ジャーナル処理により、デバッグ、ポリシーのスポット・チェック、およびポリシーが希望どおり機能しているかどうかの検証を行なうことができます。

QoS ポリシーのロギング
サーバーで問題が発生した場合は、ジョブ・ログを分析できます。

サーバー・トランザクションのモニター
QoS 問題の検出と訂正には、まずは QoS モニターを使用してください。 QoS モニターは QoS パフォーマンス情報を記録します。ユーザーは、その情報を確認することができます。

TCP アプリケーションのトレース
数レベルのサーバー・アクションをログに記録するには、トレース・コマンドを利用してください。これは、QoS ポリシー問題の判断に役立ちます。

QoS ポリシーの順序付け
ファイル内のポリシーの順序は、Quality of service のインプリメンテーションを成功させる上で非常に重要な要素です。

QoS ポリシーのジャーナル処理

QoS にはジャーナル処理機能が組み込まれています。ジャーナル処理機能を利用して、いつポリシーが追加、除去、または変更されたかなど QoS ポリシーのアクションを追跡できます。ジャーナル処理機能をオンに設定している間は、ポリシー・アクションのログが作成されます。このログは、ポリシーが期待どおり動作していない個所をデバッグしたりスポット・チェックするのに役立ちます。たとえば、午前 9 時～午後 4 時の間はポリシーが実行されるように設定したとします。そして、ジャーナル・ログをチェックして、ポリシーが実際に午前 9 時に追加され、午後 4 時に除去されたかを確認することができます。

ジャーナル処理がオンに設定されていると、ポリシーが追加、除去または変更されるたびにジャーナル項目が生成されます。このジャーナルから、iSeries サーバー上に一般ファイルを作成します。これにより、システムのジャーナルに記録された情報からシステムの使用状況を判断することができます。これは、ポリシーの様々な局面の変更を決定する時に役立ちます。

ジャーナル処理する内容は慎重に選択してください。ジャーナル処理は、システム・リソースに多大な負担を与えます。ジャーナル処理の開始または停止には、iSeries ナビゲーターを使用します。ジャーナル・ログを表示するには、文字ベースのインターフェースを使用してください。

ジャーナル処理の開始または停止は、次の手順で行ってください。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. 「**QoS**」を右マウス・ボタン・クリックし、「**プロパティー**」を選択します。
4. ジャーナル処理をオンにするには、「**ジャーナル処理の実行 (Run Journaling)**」ボックスを選択します。
5. ジャーナル処理をオフにするには、「**ジャーナル処理の実行 (Run Journaling)**」ボックスを選択解除します。

重要: 上記の手順を終了する前にすでにサーバーが始動している場合は、サーバーを停止して再始動する必要があります。ジャーナル処理をオンにしたら、2 つの方法のうちのいずれかを使用してジャーナル処理をアクティブにします。ジャーナル処理をアクティブにする方法の 1 つは、サーバーを停止して再始動することで、もう 1 つの方法はサーバーを更新することです。いずれかの方法を実行すると、サーバーが policy.conf ファイルの再読み取りをして、ジャーナル処理属性を探します。

モニターでのジャーナル項目の確認

これらのジャーナル項目を画面に表示するには、次のことを行ってください。

1. iSeries サーバーのコマンド・プロンプトで、 DSPJRN JRN(QUSRSYS/QQOS) コマンドを入力します。表示したいジャーナル項目に関して「**オプション 5 (Option 5)**」を選択します。

出力ファイルでのジャーナル項目の確認

1 つのフォルダーにフォーマット設定されたジャーナル項目を見たい場合は、QUSRSYS ディレクトリー内の MODEL.OUT ファイルを見てください。ジャーナル項目を出力ファイルにコピーすれば、Query/400 や SQL などの Query ユーティリティーを利用して簡単にジャーナル項目を確認できます。出力ファイル内の項目を処理する独自の HLL プログラムを作成することもできます。

QoS ジャーナル項目をシステムが提供する出力ファイルにコピーするには、次の手順で行ってください。

1. ユーザー・ライブラリーの中に、システム提供の出力ファイル QSYS/QATOQQOS のコピーを作成します。このコピーは、複製オブジェクト作成 (CRTDUPOBJ) コマンドで作成できます。以下は、CRTDUPOBJ コマンドの例です。

   ```
   CRTDUPOBJ OBJ(QADSPJR4) FROMLIB(Qsys) OBJTYPE(*FILE) TOLIB(userlib) NEWOBj(userfile)
   ```

2. ジャーナル表示 (DSPJRN) コマンドを使用して、QUSRSYS/QQOS ジャーナルから、前のステップで作成した出力ファイルに項目をコピーします。 DSPJRN を存在しない出力ファイルにコピーしようとすると、システムでファイルが作成されますが、このファイルには適切なフィールド記述が含まれていません。

   a. DSPJRN JRN(QUSRSYS/QQOS) JRNCDE((M)) ENTTYP(MP) CMTCYCID(*ALL) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4) OUTFILE(userlib/userfile)

   b. DSPF FILE(userlib/userfile)

QoS サーバー・ジョブのロギング

QoS ポリシーに問題が発生した場合は、常に iSeries サーバーのジョブ・ログを分析する必要があります。ジョブ・ログには、エラー・メッセージおよび QoS に関連するその他の情報が入っています。

QoS ジョブ QTOQSRVR だけを、サブシステム QSYSWRK で実行することができます。 iSeries ナビゲーターで古い QoS サーバー・ジョブ・ログと現在の QoS サーバー・ジョブ・ログを見ることができます。

ログの表示は、次の手順で行います。

1. 「**ネットワーク**」を展開し、「**IP ポリシー**」をクリックします。
2. 「**Quality of Service**」を右マウス・ボタンでクリックします。
3. 「**診断ツール**」—>「**QoS サーバー・ログ**」を選択します。

ジョブに関する作業を行うウィンドウが開きます。

最も重要なジョブ名、およびそのジョブの用途の簡単な説明を、次に挙げます。

QTCP
このジョブは、すべての TCP/IP インターフェースを始動する基本ジョブです。 TCP/IP に基本的な問題がある場合、通常は QTCPIP ジョブ・ログを分析してください。

QTOQSRVR
このジョブは、QoS のみのログ情報を提供する基本 QoS ジョブです。 (作業スプール・ファイル) WRKSPLF QTCP を実行して、QTOQSRVR ログを探してください。

作業スプール・ファイルを検査してエラーを探すには、下記のタスクを実行してください。

1. コマンド行インターフェースで、**WRKSPLF QTCP**と入力し、Enter キーを押します。
2. 「すべてのスプール・ファイルの処理 (Work with All Spool Files)」ウィンドウが表示されます。「ユーザー・データ (User Data)」欄で、QoS サーバーに具体的に関係しているエラーを検出するために QTOQSRVR を探します。
3. 表示したい回線に関する「**オプション 5 (Option 5)**」を選択します。この情報を読み通して、問題について説明しているメッセージ ID (たとえば TCP920C) を記録します。
4. **F3** キーを 2 回押してメインメニューに戻ります。
5. コマンド行インターフェースで、 **WRKMSGF** と入力し、**Enter** キーを押します。
6. 「メッセージ・ファイルの処理 (Work with Message File)」画面で、下記の情報を入力し、**Enter** キーを押します。
   Message File: QTCPMSG
   Library: *LIBL
7. 「メッセージ・ファイルの処理 (Work with Message File)」画面で、確認したいメッセージ・ファイルを表示するために「**オプション 5**」を選択し、**Enter** キーを押します。
8. 「メッセージ記述の表示 」画面で、下記の情報を入力します。
   Position to: (上記の番号 3 からの メッセージ ID (たとえば TCP920C) を入力し、Enter キーを押します。)
9. 希望するメッセージ ID に関して「**オプション 5 (Option 5)**」を選択し、**Enter** キーを押します。
10. 「メッセージの詳細の選択 (Select message details)」画面で、 30 (前記のすべて (All of the Above)) を選択し、**Enter** キーを押します。
11. メッセージの詳細記述が表示されます。

サーバー・トランザクションのモニター

QoS モニターは、QoS の計画フェーズとトラブルシューティング・フェーズで役に立ちます。

モニターを利用して、サーバーで IP トラフィックを分析できます。 これによって、ネットワーク内のどこで輻輳 (ふくそう) が発生しているかを判断できます。 QoS モニターを使用することで、必要に応じてポリシーを調整できるようにネットワークをモニターし続けることができます。

パフォーマンスの計画と保守

QoS のインプリメンテーションの最も難しい部分の 1 つは、ポリシーでどのようなパフォーマンス制限を設定するかの判断です。 1 つ 1 つのネットワークは異なるので、特定の勧告はありません。ご自身のポリシーにとって適切な値を判断するために、業務固有のポリシーを開始する前にモニターを使用することができます。

現在のネットワーク・トラフィックの動作を確認するためには、計量を選択しないで DiffServ ポリシーを作成してみてください。このポリシーを使用可能にして、モニターを始動します。このモニターの結果を利用して、特定のニーズに合うようにポリシーを調整することができます。現在のトラフィックの動作を確認するための『モニター・ポリシーの例』を参照してください。

パフォーマンス上の問題のトラブルシューティング

問題のトラブルシューティングにもモニターを利用できます。モニター出力を利用して、ポリシーに割り当てたパラメーターが順守されているかを判断できます。モニター出力の例を参照したい方は、『QoS のシナリオ』か、または『QoS のモニター』に記載されているすべてのモニター・フィールドのリストを参照してください。

現在のネットワーク統計のモニター

»

問題

ウィザード内で、パフォーマンス制限を設定するように求められます。これらは、このこれらの値は、個々のネットワーク要件に基づいたものであるため制限値を設定することはお勧めできません。この制限値を設定するためには、現在のネットワーク・パフォーマンスについてよく理解しておく必要があります。
Quality of service ポリシーの構成を試みているということは、現在のネットワーク要件について十分に認識しているものと想定されます。正確な速度限界 (たとえば、トークン・バケット速度) を判断する場合に、どの速度限界を設定すべきかをより良く判断できるように、サーバー上のすべてのトラフィックをモニターすることができます。

ソリューション

制限値 (最大値ではない) を含まず、かつすべてのインターフェースおよびすべての IP アドレスに適用される、許容範囲の広い DiffServ ポリシーを作成してください。 QoS モニターを使用して、このポリシーに関するデータを記録します。

ステップ 1: iSeries ナビゲーターで QoS を開きます。

1. iSeries ナビゲーターで、ユーザーのサーバー —> **「ネットワーク」—>「IP ポリシー」**の順に展開します。
2. 「**Quality of Service**」を右マウス・ボタンでクリックし、「**構成**」を選択します。
3. 「**アウトバウンド帯域幅ポリシー (Outbound bandwidth policies)**」を展開します。
4. 「**DiffServ**」を右マウス・ボタンでクリックし、「**新規ポリシー (New Policy)**」を選択します。「新規 DiffServ ポリシー (New DiffServ policy)」ウィザードが表示されます。

ステップ 2: DiffServ ポリシーを作成します。
ネットワークに入るほとんどのトラフィックを収集するのに、ポリシー **Network** を呼び出します。 すべての IP アドレス、すべてのポート、すべてのローカル IP アドレス、およびすべての時刻 (適宜) を使用します。ウィザードでは、次の設定値を使用します。

Name = Network (任意の名前を割り当てられる)
Client = All IP addresses
Application = All ports
Protocol = All protocols
Schedule = All times

iSeries ナビゲーターが、サーバーに作成されたすべての DiffServ ポリシーをリストします。

ステップ 3: 新規のサービス・クラスを完成させます。
ウィザードを進んで行くと、PHB (ホップごとの転送優先順位付け)、パフォーマンス制限、およびアウト・オブ・プロファイル・トラフィックの処理を割り当てるように指示されます。これは、サービス・クラスの中で定義されます。可能な限り多くのトラフィック・フローを許容するための特に大きな値を選択します。

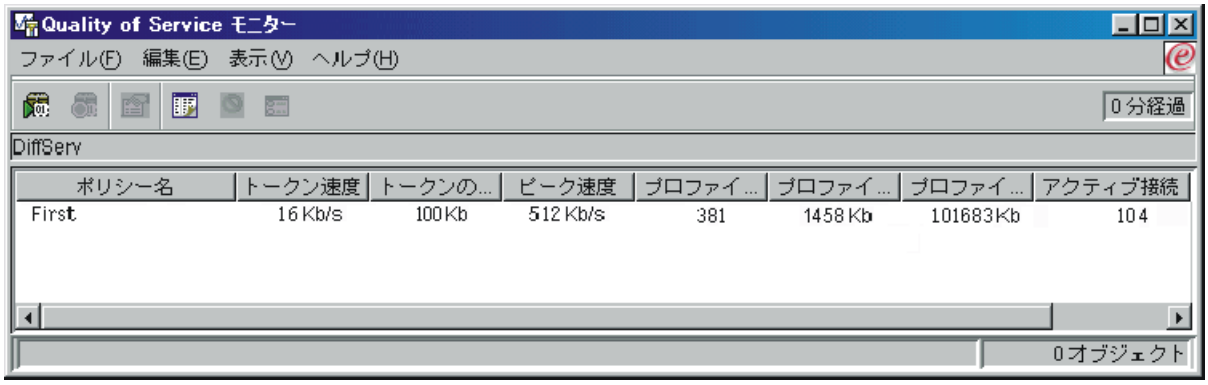
実際は、サービス・クラスが、このトラフィックがルーターから受け取るパフォーマンス・レベルを決定します。このトラフィックがより高いサービスを受けることを示すように、サービス・クラスに **Unlimited** という名前を付けます。 iSeries ナビゲーターが、サーバーに定義されたすべてのサービス・クラスをリストします。

ステップ 4: ポリシーをモニターします。
トラフィックが、ポリシーの中で構成したとおりに動作しているかを検証にするには、モニターを利用します。

1. 特定のポリシー・フォルダー (DiffServ、IntServ、サーバー要求—>URI、または接続速度) を選択します。
2. モニターしたいポリシーを右マウス・ボタンでクリックして、「**モニター**」を選択します。

次のリストは、上記で設定したポリシーに関して考えられるモニター出力を示したものです。

図 14. Quality of service モニター



トラフィックからデータを取得するフィールドを探してください。合計ビット数、イン・プロファイル・ビット数、イン・プロファイル・パケット数、およびアウト・オブ・プロファイル・ビット数の各フィールドを必ずチェックしてください。アウト・オブ・プロファイル・ビット数は、トラフィックが、構成されたポリシー値を超えた場合に示されます。 DiffServ ポリシーの中のアウト・オブ・プロファイルの数は、廃棄

されるバイト数を表します。イン・プロファイル・パケット数は、(そのパケットが発信してから現在のモニター出力に至るまでの間) このポリシーによって制御されたバイト数を示します。

平均トークン速度制限のフィールドにどのような値を割り当てるかということも重要です。パケットがこの制限値を超えると、サーバーはそれらのパケットの廃棄を開始します。 その結果、アウト・オブ・プロファイル・ビット数が増加します。これは、ポリシーが、構成したとおりに動作していることを表しています。アウト・オブ・プロファイル・ビット数を変更するには、パフォーマンス制限を調整する必要があります。すべてのモニター・フィールドについては、『モニター』のセクションを参照してください。

ステップ 5: 必要に応じて値を変更します。
モニターした後で、以前に選択した値のどれでも変更することができます。このポリシーで作成したサービス・クラス名を右マウス・ボタン・クリックします。 「**プロパティー**」を選択すると、トラフィックの制御値が表示された「CoS のプロパティー」ダイアログが現れます。

ステップ 6: ポリシーを再度モニターします。
表示された結果を見てから、「推測とチェック」方式を使用して、ネットワークのニーズに合う最適の制限を見つけます。 «

TCP アプリケーションのトレース

トレース機能に関する作業を行う場合および現在のトレース・バッファーを確認する場合は、QoS トレースを使用します。サーバーでトレースを実行するには、TRCTCPAPP と入力します。次に、トレース選択の入力例を挙げます。

```
TCP/IP application...........> *QOS
Trace option setting.........> *ON
Maximum storage for trace....> *APP
Trace full action............> *WRAP
Argument lists...............> 'lvl=4'
QoS trace type...............> *ALL
```

次の表は、トレースで使用可能なパラメーターを示しています。設定値が文字ベースのインターフェースに表示されない場合は、コマンドに設定値を入力する必要があります。たとえば、TRCTCPAPP APP(*QOS) MAXSTG(1000) TRCFULL(*STOPTRC) ARGLIST('l=4 c=i') と入力します。

設定	オプション
TCP/IP アプリケーション (TCP/IP application)	QOS
トレース・オプション設定 (Trace option setting)	*ON、*OFF、*END、*CHK
トレース用最大記憶域 (Maximum storage for trace) (55See) (MAXSTG)	1 ～ 16000、*APP
トレース満杯時のアクション (Trace full action) (55See) (TRCFULL)	*WRAP、*STOPTRC
引き数リスト (Argument list) (55See) (ARGLIST)	レベル: 'lvl=1'、'lvl=2'、'lvl=3'、'lvl=4' 内容: 'c=a'、'c=i'、'c=d'、'c=m'、'c=r'、'c=s'
QoS トレース・タイプ (QoS trace type)	*ALL

トレース出力の解釈方法に関するヘルプが必要な場合は、『トレース出力の読み方』を参照してください。トレース出力ページには、出力の意味の解釈に役立つ注記付きの出力例が含まれています。

トレース用最大記憶域 (Maximum storage for trace)

1 ～ 16000
トレース・データ用の最大記憶域サイズです。トレースは、このサイズに達すると停止するか、または折り返します。デフォルト・サイズは 4 MB です。デフォルト・サイズを指定する場合は、*APP を選択します。

***APP**
デフォルト・オプションです。アプリケーションに、デフォルトのトレース・サイズを使用するように指示します。 QoS サーバーのデフォルトのトレース・サイズは 4 MB です。

トレース満杯時のアクション (Trace full action)

***WRAP**
トレースが最大ディスク・スペース・サイズ (トレース・バッファー・サイズ) に達すると、トレース情報を折り返します。折り返しにより、ファイル内の最も古い情報が上書きされ、トレース情報の記録が継続されます。折り返しを選択しない場合、ディスクが満杯になるとトレース操作は停止します。

***STOPTRC**
システムが最大ディスク・スペースに達すると、情報の収集は停止します。

引き数リスト (Argument lists)

ログに記録するエラー・レベルおよび内容を指定します。TRCTCPAPP コマンドで使用できる引き数は 2 つ (トレース・レベルとトレース内容) あります。トレース・レベルとトレース内容を指定する場合は、すべての属性が一組の単一引用符内に収まるようにしてください。たとえば、TRCTCPAPP 'l=1 c=a' のように指定します。

注: ログ・レベルは包括的です。つまり、あるログ・レベルを選択すると、その前のすべてのログ・レベルも選択されます。たとえば、レベル 3 を選択すると、レベル 1 とレベル 2 も自動的に選択されます。 **トレース・レベル**

レベル 1: システム・エラー (SYSERR)
システム操作において発生したエラーをログに記録します。このエラーが発生した場合、QoS サーバーの稼働を継続することはできません。たとえば、システム・メモリーが不足している場合、システムが TCP/IP と通信できない場合などに、システム・エラーは発生します。

レベル 2: オブジェクト間のエラー (OBJERR)
QoS サーバー・コード内で発生したエラーをログに記録します。たとえば、あるサーバー操作を実行して予期しない結果が生じた場合などに、オブジェクト・エラーが発生することがあります。これは、通常はサービスに報告しなければならない深刻な状態です。

レベル 3: 特定のイベント (EVENT)
行われたすべての QoS 操作をログに記録します。たとえば、イベント・ログにはコマンドと要求が記録されます。結果は、QoS ジャーナル処理機能の結果に似ています。

レベル 4: メッセージのトレース (TRACE)
QoS サーバーとの間で転送されているすべてのデータをトレースします。たとえば、問題のデバッグに役立つと思われるあらゆる情報のロギングに、このハイレベル・トレースを利用できます。このトレースの情報は、問題の発生個所および問題の再生成方法を判断する時に役立ちます。

トレース内容

注: 内容タイプを 1 つだけ指定してください。トレースする内容を指定しないと、(デフォルトにより) すべての内容がトレースされます。

Content = All ('c=a')
QoS サーバーの全機能をトレースします。これはデフォルト値です。この内容タイプは、最初に問題を探すために使用します。

Content = Intserv ('c=i')
IntServ 操作のみをトレースします。問題が IntServ に関連していると判断した場合に、この内容タイプを使用します。

Content = Diffserv ('c=d')
DiffServ 操作のみをトレースします。問題が DiffServ に関連していると判断した場合に、この内容タイプを使用します。

Content = Monitor ('c=m')
モニター操作のみをトレースします。

Content = Rate ('c=r')
インバウンド接続速度イベントをトレースします。

Content = Server ('c=s')
モニター操作を除くすべてをトレースします。この内容タイプが役立つのは、モニター・トレースが、トレース出力を不必要に雑然とさせる可能性がある多量の情報を生成するからです。

TRCTCPAPP コマンドの詳細については、「CL コマンド」のトピックの中の TRCTCPAPP (TCP/IP アプリケーションのトレース)コマンド記述 を参照してください。

トレース出力の読み方
ここでは、トレース出力の解読方法のすべてを説明しているわけではありませんが、トレース情報の中で検出する必要のる重要なキー・イベントを取り上げて説明します。

統合サービス・ポリシーの場合、検出する必要のある最も重要なイベントは、RSVP 接続が拒否された原因は、その接続に関するポリシーが見つからなかったことか否か、ということです。次に、正常に接続した場合のメッセージの例を挙げます。

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Found action name vreStnl_kraMoNlCvreStnl for
flow[sess=x.x.x.x:y:z:s, source=x.x.x.x:y]
```

統合サービスの接続が失敗した場合のメッセージの例を、次に示します。

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unable to find action name for flow
[sess=x.x.x.x:y]
```

DiffServ ポリシーの場合、最も重要なメッセージは、サーバーがポリシー規則をロードしたかどうか、もしくはポリシー構成ファイルでエラーが発生したかどうかを示しているメッセージです。

例:

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

ポリシー構成ファイル内のタグが間違っていることを示すメッセージが戻される場合もあります。以下にメッセージの例を挙げます。

```
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unknown attribute %s in ServicePolicy-Ignoring.
12/15 11:36:14 [336,80] TRCE :.......rpapi_getPolicyData: Unknown attribute %s in Priority
Mapping-Ignoring.
```

注: % 符号は、認識されないタグを表す変数です。

QoS に関するその他の情報

業界には、他にも Quality of service に関する多数の情報源があります。 QoS の一般情報については、最新の RFC、ホワイト・ペーパー、Redbooks(TM)、およびその他の情報源でご確認ください。いくつかの情報源をご紹介します。

IBM 以外の情報源

RFC 1349
この RFC は、IP パケット・ヘッダー内の TOS フィールドの新規定義について説明しています。

RFC 2205
この RFC は、Resource ReSerVation Protocol (RSVP) に関するものです。

RFC 2210
この RFC は、IETF 統合サービスにおける RSVP の使用に関するものです。

RFC 2474
この RFC は、DiffServ フィールド (DS フィールド) の定義に関するものです。

RFC 2475
この RFC は、DiffServ のアーキテクチャーに関するものです。

IBM(R) Redbooks

TCP/IP More Cool Things than Ever
この資料には、構成例を用いて一般的なソリューションを具体的に説明するサンプル・シナリオが記載されています。この資料の中の情報は、iSeries サーバー上の TCP/IP の計画、インストール、調整、構成、およびトラブルシューティングに役立ちます。この資料ではまだ Quality of service について具体的に取り上げてはいませんが、LDAP ディレクトリー・サーバーについて詳しく説明しています。

TCP/IP Tutorial and Technical Overview
この資料には、プロトコルおよびアプリケーションの一連の TCP/IP プロトコルの概要ならびに参照するものを示してあります。第 22 章の *Part 3. Advanced concepts and new technologies* の中で Quality of service について説明しています。

iSeries Information Center の関連トピック

iSeries ディレクトリー・サービス (LDAP)
ディレクトリー・サーバーの基本概念、構成、管理、およびトラブルシューティングについては、このトピックを参照してください。「ディレクトリー・サービス」のトピックには、ディレクトリー・サーバーを構成するための追加のリソースも記載されています。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12