

IBM

@server

iSeries

TCP/IP トラブルシューティング

バージョン 5





@server

iSeries

TCP/IP トラブルシューティング

バージョン 5

© Copyright International Business Machines Corporation 1997, 2002. All rights reserved.

© Copyright IBM Japan 2002

目次

第 1 章 TCP/IP トラブルシューティング	1
V5R2 の新機能	1
トピックの印刷	2
第 2 章 TCP/IP の一般的な問題	3
最初の TCP/IP 問題分析	3
原因リスト A	4
IPv6 での解決方法	5
原因リスト B	7
原因リスト C	8
原因リスト D	10
原因リスト E	11
PING コマンドに関する考慮事項	11
ドメイン名のホスト名への連結	11
一般的なエラー・メッセージ	12
ジョブ・ログおよびメッセージ待ち行列の処理	12
第 3 章 特定のアプリケーションの問題	15
第 4 章 通信トレース	17
通信トレースの計画	17
通信トレースの実行	18
通信トレースの開始	18
通信トレースの終了	19
通信トレースのダンプ	19
通信トレースの印刷	20
通信トレースの内容の表示	21
通信トレースを読む	21
通信トレースの追加機能	23
第 5 章 TCP/IP 構成ファイル	25
第 6 章 プロダクト活動記録ログ	27

第 1 章 TCP/IP トラブルシューティング

TCP/IP 機能がうまく動作しないのはなぜでしょうか。堅固なネットワークを設計し、すべての指示事項に従いましたが、それでも問題が発生します。このトピックで問題を解決してください。

このサイトは、TCP/IP に関する問題の答えを発見するための出発点です。あなたが直面しているのが接続に関する一般的な問題であれば、すぐに答えが見つかるでしょう。あるいは、深い調査を必要とするもっとローカルな問題の場合もあるでしょう。問題を解決するために、以下のトラブルシューティング・ツールを役立ててください。

V5R2 の新機能

このトピックでは、TCP/IP のトラブルシューティングを行うための新しい方法や変更された方法について説明します。

トピックの印刷

このトピックでは、TCP/IP トラブルシューティング資料の Portable Document Format (PDF) 版を印刷またはダウンロードする方法を説明します。

TCP/IP の一般的な問題

このトピックは、TCP/IP 接続を検証するのに役立ちます。質問・回答形式に従って問題を正確に突き止め、解決策へのリンクを提供します。

特定のアプリケーションの問題

FTP や DNS のような特定のアプリケーションに問題があることがわかっている場合は、このトピックから、その特定のアプリケーションに関する解決策のリンクを利用してください。

通信トレース

このトピックでは、通信トレースを収集するための手順を解説します。トレースを使えば、エラーを識別することができ、問題解決の第一歩となります。トレース情報はユーザーが独自に利用することもできますが、IBM® 担当員がトラブルシューティングの援助をする際、担当員にトレース情報を提供することもできます。

TCP/IP 構成ファイル

このトピックは、TCP/IP 構成ファイルをコピーする方法を説明します。IBM 担当員の援助を受けることにした場合、これらのコピーを IBM に提供する必要があります。

プロダクト活動記録ログ

このトピックでは、問題分析のためにプロダクト活動記録ログを利用する方法について説明します。

V5R2 の新機能


バージョン 5 リリース 2 の TCP/IP トラブルシューティング・トピックの新規項目には以下のものが含まれます。

- **TCP/IP の一般的な問題**

インターネット・プロトコル・バージョン 6 (IPv6) に関連した問題のトラブルシューティングの方法を説明します。

- **通信トレース**

CL コマンドを使用して通信トレースを行う方法を説明します。このトラブルシューティング・ツールを使用すると、通信回線上のデータをトレースして問題の原因を突き止めることができます。

新機能あるいはこのリリースでの変更内容についての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。

トピックの印刷

この文章の PDF 版を参照用または印刷用にダウンロードし、表示することができます。PDF 版をダウンロードし、表示するには、TCP/IP トラブルシューティング (約 527 KB、36 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 ファイルを開く (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。

Adobe Acrobat Reader のダウンロード

PDF ファイルを表示したり印刷したりするには、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。

第 2 章 TCP/IP の一般的な問題

このトピックでは、いくつかのトラブルシューティング手法を紹介します。これらの手法を使用すると、一般的な問題を判別して、TCP/IP 接続を検証することができます。すでに TCP/IP 接続の検証が終わっている場合、または、特定のアプリケーションに問題があることが判明している場合には、『特定のアプリケーションの問題』に進んでください。

最初の TCP/IP 問題分析

ここには、問題の原因究明に役立つ一連の指示および質問があります。

PING コマンドに関する考慮事項

この情報は、PING コマンドについてより良く理解し、操作方法に習熟するうえで役立ちます。

ジョブ・ログおよびメッセージ待ち行列の処理

このトピックは、TCP/IP トラブルシューティングのもう 1 つの方法を紹介します。

最初の TCP/IP 問題分析

以下の質問と答えは、問題分析を行って、問題と解決策を識別するうえで役立ちます。表示される原因リストのリンク先へ移動して、トラブルシューティングの次の段階に進んでください。

1. PING コマンドを、ローカル・ネットワークのホストに対して実行してください。結果は正常でしたか？
 - a. はい。項目 2 に進んでください。
 - b. いいえ。『原因リスト A』に進みます。
2. PING コマンドを、リモート・システムに対して実行してください。結果は正常でしたか？
 - a. はい。項目 3 に進みます。
 - b. いいえ。『原因リスト B』に進みます。
3. QSYSWRK サブシステム内の必要なすべての TCP/IP ジョブを検査してください。すべてのジョブがありますか？
 - a. はい。項目 4 に進みます。
 - b. いいえ。『原因リスト C』に進みます。
4. NETSTAT を使用して、インターフェースが活動状態にあるかどうかを検査します。インターフェースは活動状態ですか？
 - a. はい。項目 5 に進みます。
 - b. いいえ。『原因リスト D』に進みます。
5. TELNET または FTP を使用して、TCP/IP 経路が正しく構成されているかどうかを検査します。さらに、NETSTAT を使用して、接続が確立されているかどうかを検査します。接続は確立されていますか？
 - a. はい。アプリケーションを開始してください。
 - b. いいえ。『原因リスト E』に進みます。

原因リスト A

リモート・システム (遠隔システム) で ICMP 応答が使用不可になっている場合があることに注意してください。ICMP 応答が使用不可になっていると、たとえ接続が確立されていても、リモート・システムから応答を受け取ることができません。これが問題の原因と考えられる場合には、他のシステムとの接続、および他のシステム間の接続を検査して、障害の可能性が最も高いと考えられる場所を特定してください。

1. TCP/IP がシステムで活動化されていることを検査します。

TCP/IP スタックが活動状態になっていることを確認するには、以下のステップを実行してください。

- a. STRTCP コマンドを入力します。活動状態になっている場合は、メッセージ TCP1A04「TCP/IP が現在活動中」を受信するはずですが、TCP/IP が活動状態になっていない場合は、STRTCP コマンドを入力して、サーバー上で TCP/IP を活動化してください。TCP/IP の始動の際、エラーが発生しなかったことを確認してください。
- b. IPv6 を使用している場合は、特に IPv6 に関連したトラブルシューティング手法を説明している、『IPv6 での解決方法』を参照してください。そうでない場合には、次の項目に進んでください。

2. ご使用のサーバー TCP/IP ソフトウェアを検査します。

サーバー上では、ホスト名 LOOPBACK および *LOOPBACK の回線記述値を持つインターフェースが、TCP/IP ソフトウェアを検査するために予約されています。LOOPBACK ホスト名を指定した場合は、どの物理回線にもデータは送信されません。これを利用して、TCP/IP ソフトウェアが当該システムで正常に作動しているかどうかを迅速に判定することができます。

TCP/IP ソフトウェアを検査するには、次のようにします。

- a. ローカル・ホスト・テーブルに、LOOPBACK ホスト名の項目と、127.0.0.1 のインターネット・アドレスがあることを確認します。
- b. LOOPBACK ホストに関連したインターフェースが活動状態になっていることを確認します。LOOPBACK インターフェースに関連したインターネット・アドレスは、通常、127.0.0.1 です。LOOPBACK ホスト名の IP アドレスをもつインターフェースが *LOOPBACK の回線記述で構成されていることを確認します。次のコマンドを使用します。

```
NETSTAT OPTION(*IFC)
```

すると、LOOPBACK インターフェースの状況が表示されます。表示画面で活動状態になっていない場合は、オプション 9 を使用して活動化してください。

- c. LOOPBACK ホストのインターフェースが活動状態になっていることを確認したら、次のように入力します。

```
PING RMTSYS(LOOPBACK)
```

ループバックのホストを使用すると、次のことが可能になります。

- 物理回線またはネットワークに接続しなくても、FTP、TELNET、LPR、ユーザー作成のアプリケーション・プログラムをテストする。
- TCP/IP ソフトウェアが正しくインストールされていること、および正しく作動していることを検査する。

PING コマンドを使用して他のローカル定義 IP アドレスとの接続を検査することによっても、同様のテストを行えます。

- d. ソフトウェアおよびハードウェア (アダプター、ネットワーク接続) をテストするには、ネットワーク上の外部ホストのインターネット・アドレスを次のように指定します。

```
PING RMTSYS('nnn.nnn.nnn.nnn')
```

- e. システム名またはそのインターネット・アドレスを指定してネットワークへのシステムの接続を検査しても、成功しない場合は、該当のインターフェースに関連した回線記述のソース・サービス・アクセス点 (SSAP) をチェックしてください。X'AA' を SSAP (ソース・サービス・アクセス点) リストの項目として指定しなければなりません。新規の回線記述を作成する際に SSAP パラメーターをデフォルトの値の *SYSGEN のままにしておいた場合は、上記の項目がデフォルトの値として組み込まれます。既存の回線記述がある場合は、回線記述の変更コマンドを使用してこれらの値をリストに追加してください。

回線記述のすべてのタイプが TCP/IP の SSAP を持っているとは限らないので、このインターフェースに関連した回線記述のソース・サービス・アクセス点 (SSAP) リストをチェックしてください。

- f. 回線記述の項目をすべて検査してください。特に、このインターフェースの最大伝送単位 (MTU) がフレーム・サイズ以上であることを確認してください。
- g. リモート・システム (遠隔システム) が正常に応答しない場合は、システム、ネットワーク、外部ホスト、またはネットワーク内のブリッジが使用不能か、あるいは作動していないことが考えられます。また、応答不良の原因として、リモート・システムで ICMP 応答が使用不可になっている可能性も考えられます。リモート・システムがファイアウォールとして作動し、ICMP 要求に応答しないよう構成されている場合に、このことが起こり得ます。他のシステムとの接続、および他のシステム間の接続を検査して、この障害の可能性が最も高いと考えられる場所を特定してください。
- h. ローカル・インターフェース構成が正しいことを確認します。
- i. TCP/IP インターフェース (LOOPBACK を含む) が活動化しない場合、または TCP/IP を終了も開始もできない場合は、以下の 2 つの経路指定項目が QSYSWRK サブシステム記述内に構成されていることを確認してください。これらの項目が存在しない場合または正しくない場合は、それらの追加または訂正を行ってから、要求を再度試行してください。

```
ADDRTGE  SBSDB(QSYS/QSYSWRK) +
          SEQNBR(2505) +
          CMPVAL(TCPIP) +
          PGM(QSYS/QTOCTCPIP) +
          CLS(QSYS/QSYSCLS20) +
          MAXACT(*NOMAX) +
          POOLID(1)
```

```
ADDRTGE  SBSDB(QSYS/QSYSWRK) +
          SEQNBR(2506) +
          CMPVAL(TCPEND) +
          PGM(QSYS/QTOCETCT) +
          CLS(QSYS/QSYSCLS20) +
          MAXACT(*NOMAX) +
          POOLID(1)
```

『最初の TCP/IP 問題分析』に戻って、トラブルシューティングを続けてください。

IPv6 での解決方法

IPv6 通信に問題がある場合には、以下の手法でネットワークのトラブルシューティングをしてみてください。

1. IPv6 スタックが実行されていることを確認します。
 - a. ループバック・インターフェースが構成されていて、活動状態であることを確認します。ループバック・インターフェースの状況を検査するには、以下のステップを実行してください。
 - 1) iSeries™ ナビゲーターで、ユーザー・サーバー → 「ネットワーク」 → 「TCP/IP 構成」 → 「IPv6」 → 「インターフェース」の順に展開します。
 - 2) 右側のペインで、ループバック・インターフェースを探します。IPv6 ループバック・アドレスの IP アドレスは ::1 で、回線名は Loopback 6 です。リストにループバック・インターフェー

- スが表示されない場合には、「IPv6 構成 (IPv6 Configuration)」ウィザードを使用してループバック・インターフェースを構成する必要があります。
- b. ループバック・アドレス (::1) を PING します。サーバーは IPv6 パケットを自分自身に送信し、そのことにより IPv6 スタックが作動していることを確認します。PING ユーティリティを使用してスタックの試験をするには、以下のステップを実行してください。
 - 1) iSeries ナビゲーターで、ユーザー・サーバー → 「ネットワーク」の順に展開します。
 - 2) 「TCP/IP 構成」を右マウス・ボタン・クリックし、「ユーティリティ」をクリックし、「PING」をクリックします。
2. IPv6 スタックが実行されていることを確認したら、IPv6 回線が構成されており、活動状態であることを確認します。この回線は、イーサネット回線あるいは構成されたトンネル回線のいずれかになります。
- サーバー上で構成された回線状況を検査するには、以下のステップを実行してください。
- a. iSeries ナビゲーターで、ユーザー・サーバー → 「ネットワーク」 → 「TCP/IP 構成」 → 「回線」の順に展開します。
 - b. 右側のペインで、IPv6 のために構成されている回線を探し、状況欄にチェックマークを付けます。リストにその回線が表示されない場合には、「IPv6 構成 (IPv6 Configuration)」ウィザードを使用して IPv6 のための回線を構成する必要があります。IPv6 用の回線の構成についての説明は、『IPv6 の構成』を参照してください。リストにその回線が表示されており、「ロードされていません (Not loaded)」の状況になっている場合、その回線は構成されているものの、IPv6 スタック構成にロードされていません。文字ベースのインターフェースで、回線記述処理 (WRKLIND) コマンドを使用して、その回線の問題を診断します。
3. 少なくとも 2 つの IPv6 インターフェースが活動状態であることを確認します。つまり、ローカル・インターフェースと PING の送信先のインターフェースの 2 つです。
- IPv6 インターフェースの状況を検査するには、以下のステップを実行してください。
- a. iSeries ナビゲーターで、ユーザー・サーバー → 「ネットワーク」 → 「TCP/IP 構成」 → 「IPv6」 → 「インターフェース」の順に展開します。
 - b. 右側のペインで、ローカル・インターフェースに関連した IP アドレスを探し、インターフェースの状況にチェックマークを付けます。
 - c. インターフェースが「非活動 (Inactive)」になっている場合、インターフェースを活動化する必要があります。インターフェースを活動化するには、IP アドレスを右マウス・ボタン・クリックして、「開始」を選択します。
 - d. これらのステップを繰り返して、リモート・インターフェースの状況を検査します。
4. IPv6 アドレスへの PING が正常に実行されなかった場合は、両方のインターフェースのアドレス状態を確認します。インターフェースのアドレス状態は、両方とも「優先 (Preferred)」でなければなりません。宛先あるいは送信元インターフェースのいずれかが優先の状態でない場合には、検査のために他のインターフェースを選択するか、あるいは使用中のインターフェースを正しい状況およびアドレス状態に変更します。
- 送信元インターフェースのアドレス状態を確認あるいは変更するには、以下のステップを実行してください。
- a. iSeries ナビゲーターで、ユーザー・サーバー → 「ネットワーク」 → 「TCP/IP 構成」 → 「IPv6」 → 「インターフェース」の順に展開します。
 - b. 右側のペインで、そのインターフェースに関連した IP アドレスを右マウス・ボタン・クリックし、「プロパティ」を選択し、「オプション」ページを選択します。このダイアログでは、インターフェースの優先継続時間あるいは有効継続時間を指定することができます。

- 1 c. これらのステップを繰り返して、宛先のインターフェース・アドレスの状態を検査します。

原因リスト B

VFYTCPCNN または PING コマンドがローカル・システムに対して正常に実行された場合、システムと、通信したいシステムとの間の接続可能性を検査する必要があります。前と同じように、PING コマンドを実行しますが、今度は遠隔ホストのインターネット・アドレスを指定してください。『一般的なエラー・メッセージ』をご覧ください。リモート・システム、または中間ファイアウォールで、ICMP 応答が使用不可になっている場合があることに注意してください。ICMP 応答が使用不可になっていると、たとえ接続が確立されていても、リモート・システムから応答を受け取ることができません。これが問題の原因と考えられる場合には、他のシステムとの接続、および他のシステム間の接続を検査して、障害の可能性が最も高いと考えられる場所を特定してください。

1. 遠隔インターネット・アドレスを使用した接続を正常に検証できるものの、リモート・システム名を使用した接続を正常に検証できない場合には、名前またはアドレスがホスト・テーブル内で正しくありません。遠隔ネーム・サーバーが使用不能になっている可能性もあります。
2. システムが遠隔ネーム・サーバーを使用する場合、それぞれの遠隔ネーム・サーバーに到達できることを確認してください。この確認は、PING コマンドを使用し、遠隔ネーム・サーバーのインターネット・アドレスを指定することによって行います。
3. PING コマンドの追加パラメーターを使用すると、パケット長さ、パケット送信数、応答への待機時間を指定することができます。この待機時間のデフォルトの値は 1 秒間ですが、これでもほとんどのネットワークでリモート・システムが応答するのに十分です。しかしリモート・システムが遠く離れていたり、ネットワークが使用中のことが多かたりする場合は、待機時間パラメーターを長くすることでよい結果が得られます。

パラメーター値は、デフォルトの値のままにしておくことをお勧めします。パラメーター値を変更すると、長いパケット長と短い待機時間とが組み合わせられ、ネットワークが応答を送受信する時間が不十分となり、タイムアウトが起きることがありますので、注意してください。応答の送受信に必要な十分な時間がネットワークに与えられていないと、システムと実際に接続しているにもかかわらず、接続していないように見えることがあります。

4. リモート・システムが正常に応答しない場合は、システム、ネットワーク、ゲートウェイ、ルーター・プログラム、またはネットワーク内のブリッジが使用不能か、あるいは作動していないことが考えられます。応答不良の原因として、リモート・システム、または中間ファイアウォールで ICMP 応答が使用不可になっている可能性も考えられます。他のシステムとの接続、および他のシステム間の接続を検査して、この障害の可能性が最も高いと考えられる場所を特定してください。
5. インターフェースをイーサネット・タイプの回線記述に構成し、そのインターフェースを検査するために PING コマンドを使用したときにリモート・システムが応答できなかった場合は、イーサネット回線記述に、正しいイーサネット規格が指定されていること、または *ALL が指定されていることを確認してください。
6. ネットワーク内のどのシステムからも応答が得られないということは、経路のどこかに障害が起きていることを示しています。問題のネットワークにつながるゲートウェイへの接続を検査してください。接続できなかった場合は、異常のある場所が見つかるまで、接続できなかったリモート・システムから戻りながら作業をやり直してください。
7. パケットは、送信を保証しない下位レベルのプロトコルを使用して送信されます。エコー要求が失われる可能性があるため、複数のコマンドをもってしても経路中のあるポイントを越えることができなかったときまで、ネットワークまたはゲートウェイに障害が起きているとは想定しないでください。

リモート・ネットワークのホストへの PING コマンドが失敗する場合は、その同じネットワークに対して経路追跡 (TRACEROUTE) コマンドを使用してください。経路追跡ユーティリティは、個々の PING 要

求が行うのと同じ接続テストのほとんどを行うことができます。経路追跡を使用すれば、そのすべてを 1 つのステップで実行することができます。経路追跡は、リモート宛先への経路のそれぞれのホップをテストし、中間ルーターに問題があるか、あるいはリモート・ネットワークに問題があるかを示します。

- | TRACEROUTE RMTSYS('x.x.x.x') と入力します。リモート・システムは、IP アドレス、またはリモート・システム名 ('xxxx.xxx.com') など) で指定できます。経路追跡ユーティリティーは、IPv4 アドレス・フォーマット ('x.x.x.x') と IPv6 アドレス・フォーマット ('x:x:x:x:x:x:x:x') の両方を受け入れます。

iSeries ナビゲーターから経路追跡を実行することも可能です。経路追跡を開始するには、以下のステップを実行してください。

1. iSeries ナビゲーターで、ユーザー・サーバー → 「ネットワーク」の順に展開します。
2. 「TCP/IP の構成」を右クリックして、「ユーティリティー」 → 「Trace Route」を選択します。

『最初の TCP/IP 問題分析』に戻って、トラブルシューティングを続けてください。

原因リスト C

1. サーバー QSYSWRK サブシステム (ローカルまたはリモート) で、必要なすべてのジョブを検査してください。少なくとも QTCPIP ジョブがなければなりません。QTCPIP ジョブは、TCP/IP 開始インターフェースおよび終了インターフェースを制御します。また、9 ページの図 1 に示すように、使用するアプリケーションにはそれぞれに少なくとも 1 つのジョブがなければなりません。これらのジョブは、FTP、LPD、TELNET ジョブのサブシステム・ジョブと同一となるようには命名されていないことがあります。すべての FTP ジョブは、QTFTP で始まります。すべての LPD ジョブは、QTLPD で始まります。すべての TELNET ジョブの名前は QVTELNET および QTVDEVICE になります。FTP、LPD、TELNET サーバー・ジョブが、複数存在する場合があります。すべての SMTP ジョブは、QSMTP で始まります。SMTP は、QSYSWRK サブシステム内で最大 4 つのジョブを、QSNADS サブシステム内で最大 2 つのジョブを活動化することができます。すべての SNMP ジョブは、QTMSNMP で始まります。SNMP は、QSYSWRK サブシステム内で 3 つのジョブ (QTMSNMP、QTMSNMPCRV、QSNMPSA) を活動化できます。

これらのジョブを表示するには、活動ジョブの処理 (WRKACTJOB) コマンドを使用します。WRKACTJOB SBS(QSYSWRK) と入力してください。

2. すべてのジョブが存在しない場合は、ENDTCP OPTION(*IMMED) コマンドを使用して TCP/IP 処理を終了します。それらのジョブに関連したジョブ・ログをすべて調べてください。
3. すべてのジョブ記述オブジェクトについて、ジョブ記述のメッセージ記録レベルを 4 0 *SECLVL に変更します。メッセージ記録レベルの詳細については、『ジョブ・ログおよびメッセージ待ち行列の処理』を参照してください。
4. STRTCP コマンドを使用して TCP/IP 処理を再度開始します。
5. すべてのジョブが活動状態にあることを確認します。
6. 必要なジョブが活動状態にない場合は、ジョブ・ログを検査します。

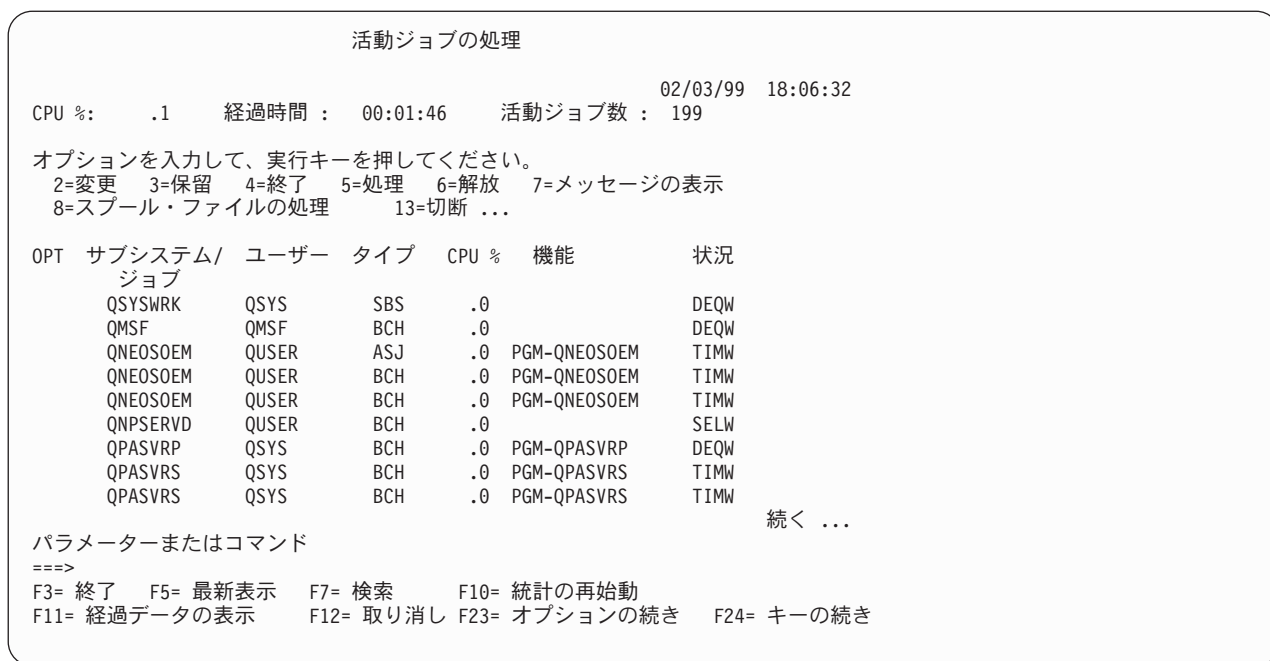


図1. 「活動ジョブの処理」画面 - 画面 1



図2. 「活動ジョブの処理」画面 - 画面 2

『最初の TCP/IP 問題分析』に戻って、トラブルシューティングを続けてください。

原因リスト D

サーバーのネットワーク状況 (NETSTAT) 機能を使って、TCP/IP インターフェース状況、TCP/IP 経路構成情報、およびローカル・システムの TCP/IP 接続状況を表示することができます。それには、WRKTCPSTS コマンドまたは NETSTAT コマンドのいずれかを使用します。

1. ネットワーク状況の機能を使用する前に、STRTCP コマンドを使用して TCP/IP を開始します。「TCP/IP ネットワーク状況の処理」メニューが表示されますが、オプションは、TCP/IP が開始するまで利用できません。
2. 「TCP/IP インターフェース状況の処理」画面で、活動状態のインターフェースの開始や、非活動状態のインターフェースの終了を試みると、それに対応したエラー・メッセージが送信されます。非活動状態のインターフェースがインターフェース開始オプションを実行しても活動状態にならない場合は、インターフェース、回線、または回線構成に問題がある可能性があります。QSYSWRK サブシステム内の QTCPIP ジョブのジョブ・ログを参照して、インターフェースの活動化時に何のエラーが発生した可能性があるかを調べてください。状況を判別するには、QSYSOPR メッセージ待ち行列とヒストリー・ログ QHT (DSPLOG) を調べるのも有益な方法です。
3. 回線記述に問題があるかどうかを判別するには、WRKCFGSTS *LIN と入力します。
4. 「TCP/IP ネットワーク状況の処理」画面でオプション 3 を選択して表示した「TCP/IP 接続状況の処理」画面で、各サーバーに少なくとも 1 つの受動 listen 接続が表示されることを確認してください。以下のアプリケーションをサポートしているサーバー、およびネットワーク上のその他の関係するサーバーの接続状況を検査する必要があります。

SNMP

TELNET

バージョン 4 リリース 4 では、TELNET に加えて、SSL TELNET もサポートされています。SSL TELNET はデフォルトで listen ポート 992 を反映し、従来の TELNET はポート 23 を使用します。SSL TELNET を使用可能にしたままで従来の TELNET サーバーを使用不可にするには、TELNET listen ポートを制限するとよいでしょう。

FTP

SMTP (構成されている場合)

POP

LPD

REXEC

HTTP (構成されている場合)

受動 listen 接続は、遠隔アドレス・フィールドと遠隔ポート・フィールド内では、アスタリスクが付いています。これらの接続を終了することはお勧めできません。リモート・システムは、関連した受動 listen 接続が終了してしまうと、SNMP、FTP、TELNET を使用することも、ローカル・システムへ SMTP メールを送信することも、または LPR を使用してローカル・システムへスプール・ファイルを送信することもできなくなります。これらを再開するには、次のようにします。すなわち、ENDTCPSVR と STRTCPSVR のコマンドを使用して、その際、終了、開始したいサーバーを指定して、全部のサーバーをいったん終了し、次に開始します。

5. 使用するアプリケーションに関連したポートが制限されていないことを確認してください。現行のポートの制限を表示するには、「TCP/IP の構成」メニューから、オプション 4 (TCP/IP ポート制限の処理) を使用します。

『最初の TCP/IP 問題分析』に戻って、トラブルシューティングを続けてください。

原因リスト E

構成データを検査します。すべての検査が終了したら、『特定のアプリケーションの問題』に進んで、ご使用の特定のアプリケーションを選択してトラブルシューティングの次の段階に進んでください。

PING コマンドに関する考慮事項

以下では、PING コマンドについてより詳しく解説します。

ドメイン名のホスト名への連結

ここでは、サーバーがドメイン名をホスト名へ連結する方法を示します。

一般的なエラー・メッセージ

最も一般的なエラー条件をいくつか例示します。

ドメイン名のホスト名への連結

以下の例では、ドメイン名の最後にピリオドが付いていない場合に、サーバーがローカル・ドメイン名を検索リストとして使用し、ドメイン名をホスト名に連結する様子を示します。

サーバー名が `SYSNAM01.A400SSC.DFW.COMPANY.COM`、接続検査対象のシステムの正式名が `SYSNAM02.DFW.COMPANY.COM` であるとします。ローカル・ホスト・テーブルには、`SYSNAM02` というホスト名はありません。

`PING SYSNAM02.DFW.COMPANY.COM` と入力した場合、サーバーは `SYSNAM02.DFW.COMPANY.COM` をリモート・ネーム・サーバーに送ります。

`PING SYSNAM02` と入力した場合、サーバーは最初に `SYSNAM02.A400SSC.DFW.COMPANY.COM` をリモート・ネーム・サーバーに送ります。続いて、`SYSNAM02.DFW.COMPANY.COM` を送ります。これが見付からない場合、最終的に `SYSNAM02.COMPANY.COM` を送信します。つまり、iSeries TCP/IP はローカル・ドメイン名のそれぞれの部分をホスト名へ連結します。

`PING SYSNAM02.` と入力した場合、遠隔ネーム・サーバーは、ホストが不明であると報告します。遠隔ネーム・サーバーが `SYSNAM02` を識別しない理由は、検索リストが連結されないまま、サーバーが遠隔ネーム・サーバーへ `SYSNAM02` という名前を送信するためです。この名前と上記の名前との違いは、名前の最後にピリオドが付いているかないかだけです。

一般的なエラー・メッセージ

PING コマンドを使用してネットワーク内の別のホストとの接続を検査する場合、TCP/IP はエラー・メッセージを出すことができます。以下の表を使用して一般的なエラー・メッセージを識別し、問題解決のためにすべきことを判別してください。

エラー・メッセージ	対処方法
TCP/IP サービスが使用できません。	<ul style="list-style-type: none"> • TCP/IP がまだ開始していないか、または開始がまだ完了していません。TCP/IP が活動状態にあるかどうかを判別するには、NETSTAT コマンドを使用します。 • 一部のジョブが QSYSWRK サブシステム内でまだ開始していない可能性があります。QSYSWRK サブシステムとその関連したジョブが活動状態にあるかどうかを判別するには、活動ジョブの処理 (WRKACTJOB) コマンドを使用します。活動状態になっていない場合、ジョブ・ログまたはシステム・デフォルトの出力待ち行列を見て、次のようなメッセージがないかどうか調べてください。
遠隔ホスト・システムとの接続を確立できません。	構成したインターフェース、その関連した回線記述、および TCP/IP 経路をチェックしてください。
リモート・システムに到達できません。	TCP/IP は要求された宛先への経路を検出できませんでした。NETSTAT オプション 2 をチェックして、*DFTRROUTE またはそれと同等のネットワーク経路が構成されて活動状態になっていることを確認してください。
遠隔ホストの VFYTCPCNN への応答は、接続検査 1 で 10 秒以内にありませんでした。	<ul style="list-style-type: none"> • 構成は正しいはずなのに、リモート・システムからの返答が得られません。遠隔ホストからシステムへ到達できることを確認してください。リモート・システムの操作員を呼び出し、当該システムへの接続を検査するように依頼してください。 • ホスト・テーブルと遠隔ネーム・サーバー (名前サーバーを使用している場合) 上で、両方のシステムをチェックしてください。また、TCP/IP インターフェース、および経路をチェックしてください。遠隔ネーム・サーバーが何らかの理由でサービスを提供できない可能性があります。 • イーサネット回線を使用している場合は、正しいイーサネット規格または *ALL を指定していることを確認してください。
VFYTCPCNN: ホスト xxxxxx が不明です。ここで、xxxxxx はホスト名です。	ホスト・テーブルとネーム・サーバーのいずれを使用しても、ホスト名を IP アドレスとして解決できませんでした。ローカル・ホスト・テーブルまたは遠隔ネーム・サーバー (名前サーバーを使用している場合) 上で、遠隔ホストの項目をチェックしてください。

ジョブ・ログおよびメッセージ待ち行列の処理

TCP/IP には、いくつかのジョブ記述が同梱されています。

ジョブ記述は、QSYS ライブラリーまたは QTCP ライブラリーの中に格納されます。一般的に、出荷時のメッセージ記録レベルは 4、メッセージ記録重大度は 0、メッセージ記録テキスト値は *NOLIST です。出荷時のこれらの値は、ジョブ開始メッセージとジョブ終了メッセージしか入っていないジョブ・ログが作成されてしまうのを防ぐためです。

TCP/IP の作動に問題がある場合に最初に行うべきことの 1 つは、問題のあるアプリケーションのジョブ記述のメッセージ記録レベルを変更して、メッセージ記録テキスト値 *SECLVL にすることです。メッセージ記録レベルを変更すると、そのアプリケーションのジョブ・ログが生成されます。変更を反映させるには、サーバーをいったん終了してから再始動しなければなりません。ジョブを即時に変更したい場合は、CHGJOB コマンドを使用して活動ジョブのメッセージ・ロギング・レベルを変更しなければなりません。

特定のアプリケーションのジョブ記述のメッセージ・ロギング・レベルを変更する場合は、以下の例を参照してください。

- FTP サーバーに問題がある場合は、次の CL コマンドを入力することによって QTMFTPS ジョブ記述を変更します。

```
CHGJOB JOB(QTCP/QTMFTPS) LOG(4 0 *SECLVL)
```

- SMTP に問題がある場合は、次の CL コマンドを入力することによって、QTMSMTPS ジョブ記述を変更します。

```
CHGJOB JOB(QTCP/QTMSMTPS) LOG(4 0 *SECLVL)
```

QTMSMTPS ジョブ記述だけでなく、次の CL コマンドを入力することによって、QSNADS サブシステムのジョブ記述の記録レベルを変更することも考慮する必要がある場合があります。

```
CHGJOB JOB(QGPL/QSNADS) LOG(4 0 *SECLVL)
```

第 3 章 特定のアプリケーションの問題

TCP/IP で実行している特定のアプリケーションに問題があることが判明したら、以下の中からご使用のアプリケーションを選んで、トラブルシューティングの詳細情報に進んでください。それぞれのリンクをたどると、TCP/IP トラブルシューティングのサイトから出て、選択したアプリケーションに関する新しいサイトに移ります。

ドメイン・ネーム・システム・サーバー (DNS)

このトピックには問題分析フローチャートがあり、DNS の問題を解消するためのデバッグ方針を明らかにします。

ファイル転送プロトコル (FTP)

このトピックでは FTP の問題の解決策を提案し、トラブルシューティング・ツールとしてのサーバー・ジョブ・ログを紹介します。

2 地点間プロトコル (PPP)

このトピックでは、PPP 接続に関する一般的な問題の解決策を示します。

Post Office Protocol サーバー (POP)

POP サーバーその他の E-mail アプリケーションに関するトラブルシューティングは、このトピックをご覧ください。

REXEC

このトピックにあるフローチャートを使用すると、Rexec の問題を正確に突き止めて解決策を見付けることができます。

シンプル・メール転送プロトコル (SMTP)

このトピックでは、シンプル・メール転送プロトコル (SMTP) その他の E-mail アプリケーションに関する問題の解決策を示します。

Telnet

このトピックでは、Telnet に関する一般的な問題、およびエミュレーション・タイプと SSL サーバーに関する特定の問題についての情報を提供します。さらに、問題を報告するためにどのような情報を把握する必要があるかを示します。

仮想私設ネットワーク (VPN)

トピックでは、接続、構成エラー、フィルター規則などの VPN の問題に関するトラブルシューティングの方針を示します。

第 4 章 通信トレース


通信トレース (通信追跡) を使用して、TCP/IP のトラブルシューティングをします。通信トレースとは、ローカル・エリア・ネットワーク (LAN) や広域ネットワーク (WAN) などの、通信回線上でのデータ・トレースを可能にするサービス機能です。データのトレースが終了すると、生データはストリーム・ファイルにダンプされるか、あるいはフォーマット (形式設定) されて表示あるいは印刷用のスプール・ファイルに入れられます。

通信トレースは、IPv4 と IPv6 の両方の通信のトラブルシューティングに使用できます。

以下の状況で通信トレースを使用します。

- ユーザーによる問題分析の手順では問題に関する十分な情報が得られない場合。
- プロトコル違反が問題であると疑われる場合。
- 回線ノイズが問題であると疑われる場合。
- アプリケーションがネットワークで正常に情報を伝達しているかを確認したい場合。
- ネットワーク輻輳 (ふくそう) あるいはデータ・スループットに関するパフォーマンス上の問題があるかどうかを知りたい場合。

CL コマンドを使用して通信トレースを行うためには、*SERVICE 特殊権限か、iSeries ナビゲーターを通して OS/400® のサービス・トレース機能を使用する権限が必要です。このタイプの権限の詳細について

は、iSeries 機密保護解説書  のユーザー・プロファイルに関する章を参照してください。

接続追跡 (TRCCNN) コマンドは、通信トレースに似たトレースを取得するための代替手段となるコマンドです。SSL を使用する TCP アプリケーションがある場合や IP Security を使用している場合、通信回線上を流れるデータは暗号化されます。そのため、データを見る必要がある場合に通信トレースでは役に立たないかもしれません。TRCCNN は暗号化の前および復号の後にデータをトレースします。したがって、一般の通信トレースが有効でない場合にこれを使用できます。この出力は、一般の通信トレースの出力に類似しています。パラメーターおよびこのコマンドに関連した例については、アプリケーション・プログラミング・インターフェース (API) トピックにある、TRCCNN (接続追跡) コマンドの説明を参照してください。

通信トレース機能を使用するには、以下のステップを実行してください。

通信トレースの計画

通信トレースを実行する前に必要な予備的ステップ。

通信トレースの実行

通信トレースを実行するために必要なステップ。

通信トレースの追加機能

通信トレースに関連した追加機能。

通信トレースの計画

通信トレースの処理を開始する前に、以下のステップを実行してください。

1. ライブラリー IBMLIB または出力待ち行列 IBMOUTQ をまだ作成していない場合は、以下のコマンドを指定します。

- ```

| CRTLIB LIB(IBMLIB)
| CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)

```
2. 以下のコマンドを指定して、ライブラリー **IBMLIB** をライブラリー・リストへ追加し、ジョブの出力待ち行列を出力待ち行列 **IBMOUTQ** へ変更します。
- ```

| ADDLIBLE IBMLIB
| CHGJOB * OUTQ(IBMLIB/IBMOUTQ)

```
3. **QTCPPRT** プリンター・ファイルがシステム上に存在しない場合は、次のコマンドを指定して、そのファイルを作成してください。
- ```

| CRTPRTF FILE(QTCP/QTCPPRT) DEV(*JOB)
| RPLUNPRT(*YES) SCHEDULE(*FILEEND)
| FILESEP(0) LVLCHK(*NO)
| TEXT('TCP/IP printer file')
| CHGOBJOWN OBJ(QTCP/QTCPPRT) OBJTYPE(*FILE)
| NEWOWN(QSYS)

```
4. 次のコマンドを指定して、通信トレースが入ったスプール・ファイル **QTCPPRT** をライブラリー **IBMLIB** 中の出力待ち行列 **IBMOUTQ** へ送信します。
- ```

| OVRPRTF FILE(QTCPPRT) OUTQ(IBMLIB/IBMOUTQ)
| OVRPRTF FILE(QPCSMPT) TOFILE(QTCP/QTCPPRT)

```
- プリンター・ファイルの指定変更は、ジョブの終了後は効力がなくなります。
5. **TCP/IP** インターフェースに問題がある場合は、それに関連した回線記述の名前を入手します。アプリケーションまたはネットワークに問題がある場合は、それらが使用する **TCP/IP** インターフェースに関連した回線記述の名前を入手します。 **NETSTAT *IFC** を使用して、該当のインターフェースに関連した回線記述の名前を判別します。
6. その回線がオンになっていること、その回線に関連した **TCP/IP** インターフェースが開始されていること、以上によって **TCP/IP** データがこのインターフェースと回線とを介して送受信できるようになっていることを確認してください。 **NETSTAT *IFC** を使用して、そのインターフェースが活動状態になっていることを確認してください。

次の段階：
通信トレースの実行

通信トレースの実行

通信トレースを実行するためには、文字ベースのインターフェースで **CL** コマンドを使用する必要があります。通信トレースを実行するには、以下のステップを実行してください。

1. 通信トレースの開始
2. 通信トレースの終了
3. 通信トレースのダンプ
4. 通信トレースの印刷
5. 通信トレースの内容の表示
6. 通信トレースを読む

通信トレースの開始

以下のアクションを実行することにより、指定した回線あるいはネットワーク・インターフェース記述の通信トレースが開始します。

注: ネットワーク・サーバー記述 (*NWS) のデータをトレースするために通信トレースを使用することはできなくなりました。通信トレース機能は、特定の回線 (*LIN) あるいはネットワーク・インターフェース記述 (*NWI) のいずれかのデータをトレースするために使用してください。

通信トレースを開始するには、以下のステップを実行してください。

1. コマンド行で、STRCMNTRC を指定します。
2. 「構成オブジェクト」には、TRNLIN などの回線名を指定します。
3. 「タイプ」には、リソースのタイプを指定します。 *LIN あるいは *NWI のいずれかになります。
4. 「バッファ・サイズ」には、予想されるデータ・ボリュームに合わせて十分な容量のストレージを指定します。ほとんどのプロトコルでは、8 MB のストレージがあれば十分です。10/100 イーサネットでは、16 MB から 1 GB あれば十分です。不確かな場合は、そのプロトコルに許されるストレージの最大容量を 16 MB に指定してください。
5. 1 つのリモート・インターフェースのトレースに収集されるデータを制限したい場合には、「通信追跡オプション (Communications trace options)」に *RMTIPADR を指定します。制限したくない場合には、デフォルト値を使用します。
6. 「リモート IP アドレス」には、トレース・データが収集されるリモート・インターフェースに関連した IP アドレスを指定します。

通信トレースは、次のうちの 1 つが発生するまで継続されます。

- ENDCMNTRC コマンドが実行されたとき。
- 物理的な回線の問題が原因でトレースが終了したとき。
- 「トレース満杯 (Trace full)」パラメーターに *STOPTRC が指定されていて、バッファが満杯になったとき。

次の段階:

通信トレースの終了

通信トレースの終了

トレースをフォーマットし、表示するには、まずトレースを終了する必要があります。以下のアクションを実行するとトレースが終了し、通信トレース・バッファが保管されます。

通信トレースを終了するには、以下のステップを実行してください。

1. コマンド行で、ENDCMNTRC を指定します。
2. 「構成オブジェクト」には、TRNLIN など、トレースを開始したときに指定したのと同じ回線を指定します。
3. 「タイプ」には、リソースのタイプを指定します。 *LIN あるいは *NWI のいずれかになります。

次の段階:

ストリーム・ファイルに通信トレースのダンプを取ります。これはオプションのステップであり、実行すると便利な場合もあります。通信トレースをダンプせずに生データを印刷することを望む場合には、『通信トレースの印刷』に進んでください。

通信トレースのダンプ

インターネット・プロトコル・バージョン 6 (IPv6) を使用している場合は、以下のステップに従ってトレース・データをストリーム・ファイルにダンプする必要があります。しかし、IPv4 を使用している場合、これは通信トレース・プロセスのオプションの一部となります。

データをストリーム・ファイルにダンプすることには、いくつかの利点があります。この機能を使用するかどうかを決定するときには、以下の利点を検討してください。

- 既存のトレースのデータを失わずに新しいトレースを実行できる。
- トレース・データを複数回フォーマットできる。たとえば、アプリケーションの 1 つが ASCII を使用している場合、通信トレースをまず ASCII でフォーマットする必要があるかもしれません。さらに別のアプリケーションが EBCDIC を使用している場合は、同じトレース・データを EBCDIC でフォーマットする必要があるかもしれません。トレース・データをストリーム・ファイルにダンプしておけば、柔軟に対応してこのデータを二度に渡ってフォーマットできます。
- 初期プログラム・ロード (IPL) 実行中にトレース・データを保存しておく。
- 出力を生成するためにカスタム・フォーマッターを使用できる。

通信トレースをダンプするには、以下のステップを実行してください。

1. ディレクトリーを作成します (mydir など)。ディレクトリーを作成するためには、制御言語 (CL) のトピックにある、CRTDIR (ディレクトリー作成) コマンドの説明を参照してください。
2. コマンド行で、DMPCMTRC を指定します。
3. 「構成オブジェクト」には、TRNLINE など、トレースを開始したときに指定したものと同一回線を指定します。
4. 「タイプ」には、リソースのタイプを指定します。*LIN あるいは *NWI のいずれかになります。
5. 「宛先ストリーム・ファイル (To stream file)」には、パス名を、/mydir/mytraces/trace1 のように指定します。

次の段階:

通信トレースの印刷

通信トレースの印刷

通信トレース・データは、トレースを収集した方法に応じて 2 種類の異なるソースから印刷することができます。すなわち、収集した生データから印刷する方法と、先に生データをダンプしたストリーム・ファイルから印刷する方法です。

注: ストリーム・ファイルから通信トレース・データを印刷する場合には、システムに Java™ (5722JV1) をインストールしておく必要があります。

以下のアクションを実行することにより、指定した回線あるいはネットワーク・インターフェース記述の通信トレース・データが、スプール・ファイルあるいは出力ファイルに書き込まれます。

収集した生データからの印刷:

生データをダンプしないで収集した場合には、以下のステップに従いデータを印刷します。

1. コマンド行で、PRTCMTRC を指定します。
2. 「構成オブジェクト」に TRNLINE など、トレースを開始した時に指定したものと同一回線を指定し、実行キーを押します。
3. 「タイプ」には、リソースのタイプを指定します。*LIN あるいは *NWI のいずれかになります。
4. 「文字コード (Character code)」で *EBCDIC あるいは *ASCII のいずれかを指定します。データは二度印刷する必要があります。*EBCDIC を最初に指定したら、次に*ASCII を指定します。
5. 「TCP/IP データの形式設定 (Format TCP/IP data)」で *YES を指定し、実行キーを 2 度押します。
6. ステップ 1 から 5 を、別の文字コードを指定して再度実行します。

| ストリーム・ファイルからの印刷:

| ストリーム・ファイルヘデータをダンプした場合には、以下のステップに従いデータを印刷します。

- | 1. コマンド行で、PRTCMNTRC を指定します。
- | 2. 「元ストリーム・ファイル (**From stream file**)」に /mydir/mytraces/trace1 などのパス名を指定し、
| 実行キーを押します。
- | 3. 「文字コード (**Character code**)」で *EBCDIC あるいは *ASCII を指定します。データは二度印刷する
| 必要があります。*EBCDIC を最初に指定したら、次に*ASCII を指定します。
- | 4. 「TCP/IP データの形式設定 (**Format TCP/IP data**)」で *YES を指定し、実行キーを二度押します。
- | 5. ステップ 1 から 4 を、別の文字コードを指定して再度実行します。

| 次の段階:

| 通信トレースの内容の表示

通信トレースの内容の表示

| 通信トレースの内容を表示するには、以下のステップを実行してください。

- | 1. コマンド行で、WRKOUTQ OUTQ(IBMLIB/IBMOUTQ) を指定します。
- | 2. 「出力待ち行列処理」ダイアログで、F11 (画面 2) を押して、処理したいスプール・ファイルの日付
| と時刻を見ます。画面に「続く…」が現れ、スプール・ファイルの探索を続ける必要がある場合には、
| ファイル・リストを正方向または逆方向にページ送りしてください。それ以外の場合は、次のステップ
| へ進んでください。
- | 3. 表示したいスプール・ファイルの前の「OPT」欄に 5 を指定します。最後のファイルには最新の通信
| トレースが含まれています。
- | 4. これが追跡対象の回線の通信トレースであること、および追跡開始時刻と終了時刻が正しいことを確認
| してください。

| 次の段階:

| 通信トレースを読む

通信トレースを読む

| 通信トレースは、多くの種類の情報を表示します。通信トレースの最初の部分では、トレースを開始したと
| きに指定した「構成オブジェクト」の名前などのパラメーターについて要約します。ページ送りをすると、
| 「レコード番号」および「S/R」などの項目のリストが、関連した定義とともに表示されます。これらの項
| 目は、通信トレース・データのセクションを識別するために後で使用されるタイトルを表します。トレー
| ス・データを読むときに、このリストに戻って参照すると便利です。次のイメージでは、通信トレースの前
| の情報を示しています。

```

スプール・ファイルの表示
ファイル . . . . . : QTCPPRT
制御 . . . . . :
検索 . . . . . :
ページ/行 1/1
桁 1 - 130
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9...
通信追跡 タイトル: 01/15/02 15:34:46
追跡記述
構成オブジェクト . . . . . : TRNLINE
タイプ . . . . . : 1 1= 回線, 2= ネットワーク・インターフェイス
3= ネットワーク・サーバー
オブジェクト・プロトコル . . . . . : TRN
開始日/時刻 . . . . . : 01/15/02 15:33:31.896
終了日/時刻 . . . . . : 01/15/02 15:33:40.468
収集されたバイト数 . . . . . : 9060
バッファ・サイズ . . . . . : 16384 K バイト
データの方向 . . . . . : 3 1= 送信, 2= 受信, 3= 両方
Y=YES, N=NO
バッファ満杯時に停止 . . . . . : N
追跡するバイト数
開始バイト . . . . . : *CALC 値, *CALC, *MAX
終了バイト . . . . . : *CALC 値, *CALC
追跡オプションの選択:
名前, *ALL
リモート制御装置 . . . . . : 値, *ALL
リモート MAC アドレス . . . . . : 値, *ALL
リモート SAP . . . . . : 値, *ALL
ローカル SAP . . . . . : 値, *ALL
IP 識別コード . . . . . : 値, *ALL
リモート IP アドレス
形式設定オプション:
制御装置名 . . . . . : *ALL *ALL, 名前
データの表現 . . . . . : 1 1=ASCII, 2=EBCDIC, 3=*CALC
SNA データのみの形式設定 . . . . . : N Y=YES, N=NO
RR, RNR データの形式設定 . . . . . : N Y=YES, N=NO
TCP/IP データだけの形式設定 . . . . . : Y Y=YES, N=NO
IP アドレス . . . . . : *ALL *ALL, アドレス
IP アドレス . . . . . : *ALL *ALL, アドレス
IP ポート . . . . . : *ALL *ALL, IP ポート
UI データだけの形式設定 . . . . . : N Y=YES, N=NO
MAC, SMT データだけの形式設定 . . . . . : N Y=YES, N=NO
同報通信データの形式設定 . . . . . : Y Y=YES, N=NO
通信追跡 タイトル: 01/15/02 15:34:46
レコード番号 . . . . . : 追跡バッファのレコード番号 ( 10 進数)
S/R. . . . . : S = 送信 R = 受信 M = モデム変更
データ長 . . . . . : レコード中のデータの量 ( 10 進数)
レコード状況 . . . . . : レコードの状況
レコード・タイマー . . . . . : 時刻スタンプ。通信ハードウェアに基づいて時刻
スタンプは、次のいずれかとなります。
1. 追跡が停止されたシステム時刻に基づいた
10 ミリ秒単位の時刻 (HH:MM:SS.NNNNN)
2. 10 進数で 0-6553.5 秒の範囲の 100 ミリ秒
単位の相対タイマー
データ・タイプ . . . . . : EBCDIC データ, ASCII データ, またはブランク = 不明
制御装置名 . . . . . : レコードと関連した制御装置の名前
コマンド . . . . . : コマンド/応答情報
送信数 . . . . . : 送信レコード数
受信数 . . . . . : 受信レコード数
IP-リット/最終 . . . . . : ON=OFF の場合には IP-リット, 応答の場合には最終
宛先 MAC アドレス . . . . . : 宛先の物理アドレス
ソース MAC アドレス . . . . . : ソースの物理アドレス
DSAP . . . . . : 宛先サービス・アクセス点
SSAP . . . . . : ソース・サービス・アクセス点
フレーム形式 . . . . . : LLC (論理リンク制御) または MAC (媒体
アクセス制御)
F3= 終了 F12= 取消し F19= 左 F20= 右 F24= キーの続き

```

前の情報を読んだら、通信トレースの実際の TCP/IP データまでページ送りします。タイトル行は「レコード番号」から順番に、データ・レコードの各セクションを示しています。各レコード番号はフレームを表しており、これには、送信元と受信元の IP アドレス、完全な IP データグラムの長さ、サービスのタイプ (TOS)、送信元と受信元のポート、肯定応答 (ACK) 番号などの情報が含まれます。この情報は、この iSeries 上の TCP/IP に関する問題や、関連するネットワークの問題をデバッグするのに役立ちます。

たとえば、31* のようにレコード番号の後にアスタリスク (*) がある場合、そのアスタリスクは、欠落したトレース・データを表しているという点に注意してください。このようなことは、通信トレース・レコーダがドロップしたときに発生します。通信トレース・データは、入出力プロセッサ (IOP) により収集されます。通信回線が非常に混雑している場合、IOP はすべてのネットワーク・トラフィックを優先させ、データ・バス入出力に、通信トレース情報よりも高い優先順位を与えます。そうした状況下では、IOP は通信トレース・レコードのうちの幾らかをドロップしてしまう場合があります。このことは、速度またはトラフィックの過大なネットワークを IOP が処理できないことを示している可能性があります。

通信トレースのデータが欠落している場合は、以下の選択肢を考慮してください。

- 通信回線が混雑しており、通信トレースからフレームが欠落することを単に受け入れる。
- 通信回線上のトラフィックを調査し、別の回線あるいは TCP/IP インターフェースに移動できるトラフィックがないかを判別する。

次のイメージでは、通信トレースの TCP/IP データの部分を表示しています。

```

ファイル . . . : QTCPPRT                      ページ/行 3/1
制御 . . . . . 検索                          桁 1 - 130
* . . . . . 1 . . . . . 2 . . . . . 3 . . . . . 4 . . . . . 5 . . . . . 6 . . . . . 7 . . . . . 8 . . . . . 9 . . . . . 0 . . . . . 1 . . . . . 2 . . . . . 3
通信追跡      タイトル:                      01/15/02 15:34:46                      ページ: 3
ポート       データ レコード      制御      宛先      ソース      フレーム      送信      受信      フォール/
番号 S/R   長   タイマー      装置名      MAC アドレス  MAC アドレス  形式  コマンド  数      数      最終  DSAP  SSAP
-----
1   R     45  15:33:32.26734  0000000800  0020357A53A0  40000C11CD17  LLC  UI                      OFF  AA  AA
SNAP Header: 0000000800
Frame Type:  IP DSCP: 0 Length: 40 Protocol: TCP Datagram ID: 89CB
Src Addr: 10.5.5.1 Dest Addr: 10.20.6.1 Fragment Flags: DON'T, LAST
IP Header: 4500002889CB40007406CAC7090575A109822A15
IP Options: NONE
TCP . . . : Src Port: 1710, Unassigned Dest Port: 23, TELNET
SEQ Number: 21805081 ('014CB819'X) ACK Number: 4286833 ('00416971'X)
Code Bits: ACK Window: 12525 TCP Option: NONE
TCP Header: 06AE0017014CB81900416971501030EDA2CD0000
11  R     33  15:33:33.71591  FFFFFFFF0000  8060948ACCAE  LLC  UI                      OFF  AA  AA
経路指定情報: 8240
Frame Type:  ARP Src Addr: 10.5.8.3 Dest Addr: 10.5.25.2 Operation: REQUEST
ARP Header: 00060800060400010060948ACCAE09822A9E000000000000009822ACC
31  R     33  15:33:35.98483  FFFFFFFF0000  C0000C11CD17  LLC  UI                      OFF  AA  AA
F3= 終了 F12= 取消し F19= 左 F20= 右 F24= キーの続き

```

これで通信トレース・プロセスは完了です。

『通信トレースの追加機能』に進み、トレースの削除、トレースの状況のチェック、およびストレージ・スペースの判断の方法について調べてください。

通信トレースの追加機能

以下のコマンドおよび API により、通信トレースの追加機能が提供されます。

通信トレースの削除

同じ回線で新しいトレースを開始する前に、通信トレースを削除する必要があります。トレースが終了している場合は、通信トレースを削除することができます。以下のアクションを実行することにより、指定した回線あるいはネットワーク・インターフェース記述のトレース・バッファが削除されます。

通信トレースを削除するには、以下のステップを実行してください。

1. コマンド行で、DLTCMNTRC を指定します。
2. 「構成オブジェクト」には、TRNLINE などの回線名を指定します。
3. 「タイプ」には、リソースのタイプを指定します。 *LIN あるいは *NWI のいずれかになります。

通信トレースのチェック

通信トレースが現在サーバー上に存在しているかどうかを調べることができます。通信追跡検査 (CHKCMNTRC) を使用して、特定の回線あるいはネットワーク・インターフェース記述の通信トレース状況、あるいはサーバー上に存在する特定のタイプのすべてのトレースの通信トレース状況を戻します。その状況は、メッセージの形でユーザーに戻されます。

通信トレースの状況をチェックするには、以下のステップを実行してください。

1. コマンド行で、CHKCMNTRC を指定します。
2. 「構成オブジェクト」に TRNLINE などの回線名を指定します。特定のタイプのすべてのトレースの状況をチェックしたい場合は *ALL を指定します。
3. 「タイプ」には、リソースのタイプを指定します。 *LIN あるいは *NWI のいずれかになります。

プログラマチックにストレージ・スペースをチェックする

トレースのために割り当てられた最大スペース、およびサーバー上の活動状態あるいは停止の状態にあるすべてのトレースのサイズ (バイト数単位) をプログラマチックに検査するには、通信トレースのチェック (QSCCHKCT) API を使用します。通信トレースのチェック (QSCCHKCT) API の詳細については、アプリケーション・プログラミング・インターフェース (API) のトピックを参照してください。

第 5 章 TCP/IP 構成ファイル

TCP/IP の問題を報告するときには、必ず TCP/IP 処理に使用した構成ファイルのコピーを添付してください。TCP/IP 構成ファイルのコピーを入手するには、次のようにします。

1. ライブラリー IBMLIB または出力待ち行列 IBMOUTQ をまだ作成していない場合は、以下のコマンドを入力します。

```
CRTLIB LIB(IBMLIB)
CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
```

2. 以下のコマンドを入力して、ライブラリー IBMLIB をライブラリー・リストへ追加し、ジョブの出力待ち行列を出力待ち行列 IBMOUTQ へ変更します。

```
ADDLIBLE IBMLIB
CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
```

以下のコマンドを入力して、TCP/IP 構成で使用するすべての物理ファイルのリストを入手します。

```
WRKF FILE(QUSRSYS/QATOC*) FILEATR(PF)
WRKF FILE(QUSRSYS/QATM*) FILEATR(PF)
```

各ファイルの内容をコピーするには、オプション 3 (ファイルの処理からコピー) を使用します。または、リストした各ファイルのコマンド行で以下のコマンドを入力して、各ファイルの内容を IBMOUTQ 出力待ち行列内の個別スプール・ファイルにコピーします。

```
CPYF FROMFILE(QUSRSYS/QATOCHOST) TOFILE(*PRINT)
      FROMMBR(*ALL) TOMBR(*FROMMBR)
      MBROPT(*ADD) CRTFILE(*NO) OUTFMT(*HEX)
```

第 6 章 プロダクト活動記録ログ

TCP/IP LIC コードは、プロトコル・エラーによって TCP/IP データグラムが破棄されるたびに、プロダクト活動記録ログ内に項目を作成します。

アウトバウンド TCP/IP データグラムでは、そのようなプロトコル・エラーの例として、データグラムの送信が行われるはずであった X.25 接続の確立の失敗があります。この場合、エラーはユーザーに報告され、アウトバウンド・データグラムは破棄されます。

インバウンド・データグラムの場合、次の条件の両方が一致する場合にプロダクト活動記録ログ内に項目が作成されます。

- 「ログ・プロトコル・エラー TCP/IP 属性」が *YES に設定されている。
- RFC 1122 で指定された TCP/IP プロトコル妥当性テストのいずれかでデータグラムが失敗し、その結果としてシステムによって破棄されている。(暗黙的に破棄とは、送信側のホスト装置へのエラーの報告をしないで、受信データグラムを破棄することです。) そのようなデータグラムの例として、チェックサムまたは宛先アドレスが無効のデータグラムがあります。

データグラムが上記のように破棄されると、IP データグラム見出しと TCP/UDP データグラム見出しは、プロダクト活動記録ログ項目の詳細データに記録されます。これらのプロダクト活動記録ログ項目の参照コードは 7004 です。



Printed in Japan