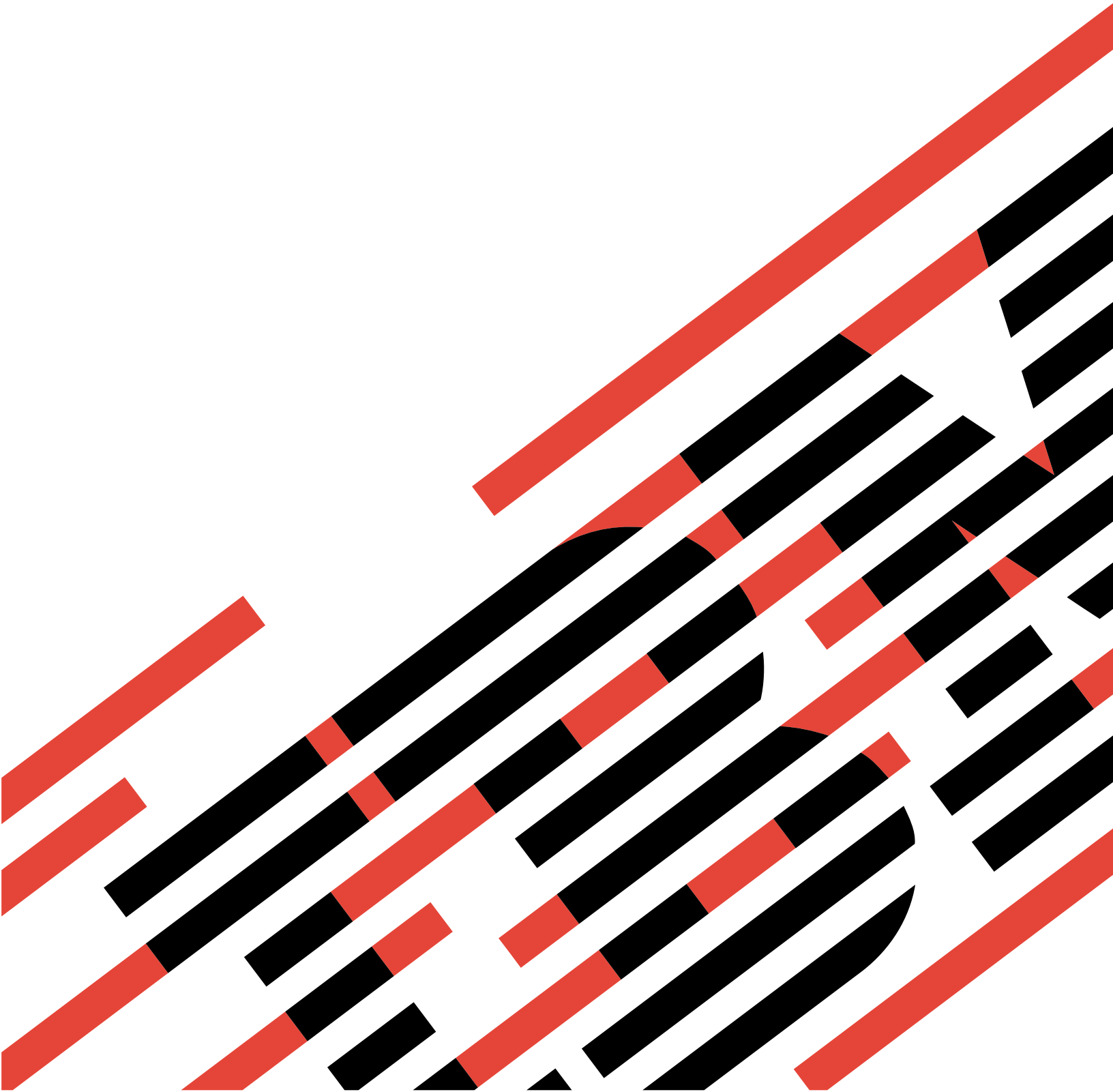
IBM

eserver

iSeries

TCP/IP 문제 해결

버전 5



IBM

@server

iSeries

TCP/IP 문제 해결

버전 5

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

목차

제 1 장 TCP/IP 문제 해결 1
V5R2에서 새로운 사항은 무엇입니까? 1
이 주제 인쇄 2

제 2 장 일반 TCP/IP 문제점 3
초기 TCP/IP 문제점 분석 3
원인 리스트 A. 4
| IPv6 솔루션 5
원인 리스트 B. 7
원인 리스트 C. 8
원인 리스트 D 10
원인 리스트 E 11
PING 명령 고려사항 11
호스트명에 정의역명 연결. 11
일반적인 오류 메세지 12
작업 기록부 및 메세지 대기행렬에 대한 작업 12

제 3 장 특정 어플리케이션 문제점 15

| **제 4 장 통신 추적** 17
| 통신 추적 계획 17
| 통신 추적 수행 18
| 통신 추적 시작 19
| 통신 추적 종료 19
| 통신 추적 덤프 20
| 통신 추적 인쇄 20
| 통신 추적의 내용 보기. 21
| 통신 추적 읽기 21
| 추가 통신 추적 기능 24

제 5 장 TCP/IP 구성 파일 25

제 6 장 제품 활동 기록부 27

© Copyright IBM Corp. 1997, 2002

제 1 장 TCP/IP 문제 해결

TCP/IP 기능을 중단시킨 원인이 무엇입니까? 완벽한 네트워크를 설계하고 모든 지침대로 처리했으나 문제가 발생할 수 있습니다. 이 주제에서는 이와 같은 문제에 대한 솔루션을 제시합니다.

이 사이트는 TCP/IP 문제에 대한 해답을 찾기 위한 중앙 자원입니다. 신속하게 알 수 있는 일반적인 연결 문제일 수도 있으며 세심한 처리를 요하는 보다 지역적인 문제점일 수도 있습니다. 아래에 문제를 해결하는 데 도움을 주는 문제 해결 툴이 나옵니다.

V5R2에서 새로운 사항은 무엇입니까?
이 주제에서 TCP/IP 문제 해결에 대해 새로운 메소드 및 변경된 메소드를 배우십시오.

이 주제 인쇄
이 주제를 참고하여 TCP/IP 문제 해결 문서의 PDF 버전을 인쇄하거나 다운로드하십시오.

일반 TCP/IP 문제점
이 주제는 TCP/IP 연결을 확인하는 것을 도와줍니다. 현재 발생한 문제점에 관해 질의 응답 형식 0을 사용하여 솔루션에 링크하십시오.

특정 어플리케이션 문제점
FTP나 DNS와 같은 특정 어플리케이션에 문제가 있는 것을 알고 있다면 이 주제를 사용하여 특정 솔루션의 해당 어플리케이션에 링크하십시오.

통신 추적
이 주제는 통신 추적을 수집하는 프로세스를 안내합니다. 추적은 오류를 분리하여 그 문제에 대한 해답을 제시합니다. 사용자 스스로 추적 정보를 사용하거나 문제 해결을 지원하는 IBM® 전문가에게 이 추적 정보를 제공할 수 있습니다.

TCP/IP 구성 파일
이 주제는 TCP/IP 구성 파일을 복사하는 방법을 알려줍니다. 전문가의 도움을 받기로 결정한 경우 이 사본을 IBM에 제공해야 합니다.

제품 활동 기록부
문제를 분석할 때 제품 활동 기록부가 어떻게 도움이 되는지에 관해 알아보려면 이 주제를 사용하십시오.

V5R2에서 새로운 사항은 무엇입니까?

버전 5 릴리스 2용 TCP/IP 문제 해결 주제의 새로운 항목에는 다음이 포함됩니다.

- **일반 TCP/IP 문제점**
  인터넷 프로토콜 버전 6(IPv6) 관련 문제점을 해결하는 방법을 제공합니다.

© Copyright IBM Corp. 1997, 2002

- **통신 추적**
  CL 명령을 사용하여 통신 추적을 수행하기 위한 지침을 제공합니다. 이 문제 해결 툴은 통신 회선상의 자료를 추적하여 문제점의 소스를 찾을 수 있도록 해줍니다.

이 릴리스의 새로운 사항이나 변경된 사항에 대한 기타 정보는 사용자 메모 를 참조하십시오.

이 주제 인쇄

PDF 버전을 보거나 다운로드하려면 TCP/IP 문제 해결(약 152KB 또는 26 페이지)을 선택하십시오.

보거나 인쇄하기 위해 워크스테이션에 PDF를 저장하려면 다음과 같이 하십시오.

1. 브라우저에서 PDF를 마우스 오른쪽 단추로 클릭하십시오(위의 링크를 마우스 오른쪽 단추로 클릭하십시오).
2. **다른 이름으로 대상 저장...**을 클릭하십시오.
3. PDF를 저장할 디렉토리로 가십시오.
4. **저장**을 클릭하십시오.

Adobe Acrobat Reader 다운로드

PDF를 보거나 인쇄하기 위해 Adobe Acrobat Reader가 필요한 경우 Adobe 웹 사이트 (www.adobe.com/prodindex/acrobat/readstep.html) 에서 사본을 다운로드할 수 있습니다.

제 2 장 일반 TCP/IP 문제점

이 주제는 여러 가지의 문제 해결 기술을 안내합니다. 이러한 기술을 사용하여 일반적인 문제점을 찾아서 TCP/IP 연결을 확인할 수 있습니다. TCP/IP 연결을 이미 확인했으며 특정 어플리케이션 내에 문제점이 있다는 것을 알고 있는 경우에는 특정 어플리케이션 문제점으로 가십시오.

초기 TCP/IP 문제점 분석
이 정보에는 문제점의 원인을 식별하는 데 도움을 주는 일련의 지침 및 질문이 나옵니다.

PING 명령 고려사항
이 정보는 PING 명령을 더 자세히 이해하는 데 도움을 주는 것으로 명령을 사용하는 방법을 알려줍니다.

작업 기록부 및 메세지 대기행렬에 대한 작업
이 주제는 TCP/IP 문제 해결을 위한 또 다른 옵션을 제공합니다.

초기 TCP/IP 문제점 분석

이 질문 및 응답들은 문제점 분석 과정을 안내하여 문제점 및 솔루션 식별을 도와줍니다. 자세한 문제 해결 정보가 나오는 원인 리스트에 링크하십시오.

1. 로컬 네트워크의 호스트에 PING 명령을 사용하십시오. 완료했습니까?
   a. 예. 항목 2를 보십시오.
   b. 아니오. 원인 리스트 A를 보십시오.
2. 리모트 시스템에 PING 명령을 사용하십시오. 완료했습니까?
   a. 예. 항목 3을 보십시오.
   b. 아니오. 원인 리스트 B를 보십시오.
3. 필요한 모든 TCP/IP 작업의 QSYSWRK 서브시스템을 확인하십시오. 모든 작업이 나옵니까?
   a. 예. 항목 4를 보십시오.
   b. 아니오. 원인 리스트 C를 보십시오.
4. NETSTS를 사용하여 인터페이스를 사용 중인지 확인하십시오. 인터페이스를 사용 중입니까?
   a. 예. 항목 5를 보십시오.
   b. 아니오. 원인 리스트 D를 보십시오.
5. TCP/IP 라우트를 TELNET이나 FTP로 올바로 구성했는지 확인하십시오. 또한 NETSTAT로 연결을 설정했는지 알아보십시오. 연결이 있습니까?
   a. 예. 어플리케이션을 시작하십시오.
   b. 아니오. 원인 리스트 E를 보십시오.

© Copyright IBM Corp. 1997, 2002

원인 리스트 A

리모트 시스템이 ICMP 응답을 작동 불가능하게 만들 수 있다는 점에 유의하십시오. ICMP 응답이 작동하지 않으면 완벽한 연결이 있더라도 리모트 시스템에서 응답을 수신하지 않습니다. 이러한 문제점이 예상되면 다른 시스템과의 연결이나 다른 시스템간의 연결을 확인하여 실패가 발생할 가능성이 많은 위치를 판별하십시오.

1. TCP/IP를 시스템에서 활성화시켰는지 확인하십시오.

   TCP/IP 스택이 활성화되었는지 확인하려면

   a. STRTCP 명령을 입력하십시오. 활성화되어 있으면 'TCP1A04, TCP/IP가 현재 활동 중입니다'라는 메세지를 수신합니다. TCP/IP가 활동 중이 아니면 STRTCP 명령을 입력하여 서버에서 TCP/IP를 활성화시킬 수 있습니다. TCP/IP가 시작하는 동안 오류가 발생하지는 않았는지 확인하십시오.

   b. IPv6을 사용하는 경우에는 IPv6 솔루션에서 특별히 IPv6에 관련된 문제 해결 기술을 참조하십시오. 그렇지 않은 경우에는 다음 항목으로 진행하십시오.

2. 서버 TCP/IP 소프트웨어를 확인하십시오.

   서버에 LOOPBACK 호스트명과 인터페이스(행 설명 값이 *LOOPBACK)가 TCP/IP 소프트웨어 확인을 위해 예약되어 있습니다. LOOPBACK 호스트명을 지정하면 물리적 회선에서 자료가 송신되지 않습니다. 이와 같이 하여 TCP/IP 소프트웨어가 시스템에서 올바로 작동하는지 신속하게 판별할 수 있습니다.

   TCP/IP 소프트웨어를 확인하려면 다음과 같이 하십시오.

   a. 로컬 호스트 표에 LOOPBACK 호스트명 및 인터넷 주소 127.0.0.1 항목이 있어야 합니다.

   b. LOOPBACK 호스트와 연관된 인터페이스가 활동 중이어야 합니다. 대개 LOOPBACK 인터페이스와 연관된 인터넷 주소는 127.0.0.1입니다. LOOPBACK 호스트명의 IP 주소를 *LOOPBACK 회선 설명으로 구성한 인터페이스가 있어야 합니다. LOOPBACK 인터페이스의 상태를 보려면 다음 명령을 사용하십시오.

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

      활동 중이 아니면 옵션 9를 사용하여 활성화하십시오.

   c. LOOPBACK 호스트의 인터페이스가 활동 중인지 확인했으면 다음을 입력하십시오.

      ```
      PING RMTSYS(LOOPBACK)
      ```

      다음은 loopback 호스트를 사용하여 할 수 있는 작업입니다.

      - 물리적 회선이나 네트워크에 접속하지 않고 FTP, TELNET, LPR 또는 사용자 작성 어플리케이션 프로그램을 테스트하십시오.
      - TCP/IP 소프트웨어를 설치했으며 올바르게 작동하는지 확인하십시오.

      로컬로 정의되어 있는 다른 IP 주소들 중 하나와의 연결을 확인하기 위해 PING 명령을 사용하여 유사한 테스트를 수행할 수 있습니다.

   d. 소프트웨어 및 하드웨어(어댑터 및 네트워크 연결)를 테스트하려면 사용자 네트워크에서 외부 호스트의 인터넷 주소를 지정하십시오.

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

e. 시스템명이나 해당 인터넷 주소를 지정하여 네트워크에서 시스템 연결을 확인할 수 없으면 인터페이스와 연관된 회선 설명의 소스 서비스 액세스점(SSAP)을 확인하십시오. X'AA'를 SSAP(소스 서비스 액세스점) 리스트에 반드시 하나의 항목으로 지정해야 합니다. 이것은 SSAP 매개변수를 해당 디폴트값인 *SYSGEN로 남겨놓고 새 회선 설명을 작성할 때 디폴트로 발생합니다. 기존의 회선 설명이 있으면 회선 설명 변경 명령을 사용하여 리스트에 이 값을 추가하십시오.

   모든 회선 유형이 TCP/IP용 SSAP를 가지는 것이 아니므로 인터페이스와 연관된 회선 설명에서 소스 서비스 액세스점(SSAP) 리스트를 확인하십시오.

f. 모든 회선 설명 항목 특히 인터페이스의 최대 전송 단위(MTU)보다 크거나 같아야 하는 프레임 크기를 확인하십시오.

g. 리모트 시스템이 응답하지 않으면 시스템, 네트워크, 외부 호스트 또는 네트워크의 브릿지를 사용할 수 없거나 작동하지 않는 것을 의미할 수 있습니다. 응답 실패는 리모트 시스템에서 ICMP 응답이 작동하지 않는다는 것을 의미할 수도 있습니다. 이것은 리모트 시스템이 방화벽의 역할을 하고 ICMP 요구에 응답하지 않도록 구성된 경우에 발생할 수 있습니다. 다른 시스템과의 연결이나 다른 시스템간의 연결을 확인하여 실패가 발생할 가능성이 많은 위치를 판별하십시오.

h. 로컬 인터페이스 구성이 올바른지 확인하십시오.

i. LOOPBACK을 포함하여 TCP/IP 인터페이스가 활성화할 수 없거나 TCP/IP를 종료하거나 시작할 수 없는 경우 다음 두 개의 라우팅 항목이 QSYSWRK 서브시스템 설명에 구성되어 있어야 합니다. 이 항목이 없거나 올바르지 않으면 이 항목을 추가하거나 정정한 후 요구를 다시 시도하십시오.

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

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

초기 TCP/IP 문제점 분석으로 돌아가서 문제 해결을 계속하십시오.

IPv6 솔루션

IPv6 통신에 문제가 있으면 다음 기술을 사용하여 네트워크의 문제를 해결해 보십시오.

1. IPv6 스택이 실행 중인지 확인하십시오.
   a. 루프백 인터페이스가 구성되어 활동 중인지 확인하십시오. 루프백 인터페이스의 상태를 검사하려면 다음 단계를 따르십시오.
      1) iSeries™ Navigator에서 **서버 --> 네트워크 --> TCP/IP 구성 --> IPv6 --> 인터페이스**를 확장하십시오.

2) 오른쪽 분할 창에서 루프백 인터페이스를 찾으십시오. IPv6 루프백 주소의 IP 주소는 ::1이며 회선 이름은 Loopback 6입니다. 목록에 루프백 인터페이스가 나타나지 않으면 **IPv6 구성** 마법사를 사용하여 루프백 인터페이스를 구성해야 합니다.

b. 루프백 주소(::1)로 ping하십시오. 서버가 자신에게 IPv6 패킷을 송신하여 IPv6 스택이 작동 중인지 확인합니다. ping 유틸리티를 사용하여 스택을 테스트하려면 다음 단계를 따르십시오.

1) iSeries Navigator에서 **서버 --> 네트워크**를 확장하십시오.

2) **TCP/IP 구성**을 마우스 오른쪽 단추로 클릭하고 **유틸리티**를 클릭한 후 **Ping**을 클릭하십시오.

2. IPv6 스택이 실행 중인지 확인한 후에는 IPv6 회선이 구성되어 활동 중인지 확인하십시오. 이 회선은 이더넷 회선이거나 구성된 터널 회선일 수 있습니다.

서버에 구성되어 있는 회선의 상태를 검사하려면 다음 단계를 따르십시오.

a. iSeries Navigator에서 **서버 --> 네트워크 --> TCP/IP 구성 --> 회선**을 확장하십시오.

b. 오른쪽 분할 창에서 IPv6용으로 구성되어야 하는 회선을 찾아 상태 열을 검사하십시오. 목록에 회선이 나타나지 않으면 **IPv6 구성** 마법사를 사용하여 IPv6용 회선을 구성해야 합니다. IPv6용 회선을 구성하는데 대한 지침은 IPv6 구성을 참조하십시오. 목록에 회선이 나타나고 **로드 안됨**이라는 상태를 표시하면 회선이 구성되었으나 IPv6 스택 구성에 로드되지 않은 것입니다. 문자 기반의 인터페이스에서 회선 설명에 대한 작업(WRKLIND) 명령을 사용하여 회선상의 문제점을 진단하십시오.

3. 최소한 두 개의 IPv6 인터페이스 즉, 로컬 인터페이스와 ping이 송신되는 인터페이스가 활동 중인지 확인하십시오.

IPv6 인터페이스의 상태를 검사하려면 다음 단계를 따르십시오.

a. iSeries Navigator에서 **서버 --> 네트워크 --> TCP/IP 구성 --> IPv6 --> 인터페이스**를 확장하십시오.

b. 오른쪽 분할 창에서 로컬 인터페이스와 연관된 IP 주소를 찾아 인터페이스 상태를 검사하십시오.

c. 인터페이스가 **비활동**인 경우에는 인터페이스를 활성화시켜야 합니다. 인터페이스를 활성화시키려면 IP 주소를 마우스 오른쪽 단추로 클릭하고 **시작**을 선택하십시오.

d. 이 단계를 반복하여 리모트 인터페이스의 상태를 검사하십시오.

4. IPv6 주소에 대한 ping이 성공하지 못하면 양 인터페이스의 주소 상태를 확인하십시오. 양 인터페이스의 주소 상태가 모두 **우선**이어야 합니다. 목표나 소스 인터페이스 중 어느 것이라도 우선 상태가 아닌 경우에는 테스트용으로 다른 인터페이스를 선택하거나 사용하는 인터페이스를 적절한 상태 및 주소 상태로 변경하십시오.

소스 인터페이스의 주소 상태를 확인하거나 변경하려면 다음 단계를 따르십시오.

a. iSeries Navigator에서 **서버 --> 네트워크 --> TCP/IP 구성 --> IPv6 --> 인터페이스**를 확장하십시오.

b. 오른쪽 분할 창에서 인터페이스와 연관된 IP 주소를 마우스 오른쪽 단추로 클릭하여 **등록 정보**를 선택하고 **옵션** 페이지를 선택하십시오. 이 대화를 사용하여 인터페이스의 우선 기간 또는 유효한 기간을 지정할 수 있습니다.

c. 이 단계를 반복하여 목표 인터페이스 주소의 상태를 검사하십시오.

원인 리스트 B

VFYTCPCNN이나 PING 명령이 로컬 시스템에서 성공적으로 이루어졌으면 사용자 시스템과 그 시스템과 통신하는 다른 시스템 사이의 연결을 확인해야 합니다. 이전에 한 것처럼 PING 명령을 실행하십시오. 그러나 이 때 리모트 호스트의 인터넷 주소를 지정하십시오. 일반적인 오류 메세지를 참조하십시오. 리모트 시스템이나 중간 방화벽이 ICMP 응답을 작동하지 않게 만들 수 있다는 점에 유의하십시오. ICMP 응답이 작동하지 않으면 완벽한 연결이 있더라도 리모트 시스템에서 응답을 수신하지 않습니다. 이러한 문제점이 예상되면 다른 시스템과의 연결이나 다른 시스템간의 연결을 확인하여 실패가 발생할 가능성이 많은 위치를 판별하십시오.

1. 리모트 시스템명이 아닌 리모트 인터넷 주소를 사용하는 연결을 확인할 수 있으면 호스트 표에서 이름이나 주소가 올바르지 않거나 리모트 이름 서버를 사용할 수 없는 것일 수 있습니다.
2. 사용자 시스템이 리모트 이름 서버를 사용하면 PING 명령을 사용하고 리모트 이름 서버의 인터넷 주소를 지정하여 각 리모트 이름 서버에 도달할 수 있는지 확인하십시오.
3. 패킷 길이, 송신할 패킷 수, 응답 대기 시간를 지정할 수 있는 PING 명령에 대한 추가 매개변수가 있습니다. 디폴트 대기 시간 1초는 리모트 시스템이 대부분의 네트워크에서 응답하기에 충분한 시간입니다. 그러나 리모트 시스템이 멀리 떨어져 있거나 네트워크를 사용 중인 경우 대기 시간 매개변수를 늘리면 성공적인 결과를 얻을 수 있습니다.

   매개변수 값은 그 디폴트 값으로 남겨놓는 것이 좋습니다. 이 값을 변경하면 큰 패킷 길이와 짧은 대기 시간의 조합이 네트워크에 응답을 전송하고 수신하기 위한 충분한 시간을 제공하지 않을 수 있으며 시간종료가 발생할 수 있다는 점에 유의하십시오. 네트워크에 응답을 전송하고 수신할 수 있는 충분한 시간을 제공하지 않으면 실제 작업시 시스템과의 연결이 이루어지지 않을 수 있습니다.
4. 리모트 시스템이 응답하지 않을 경우 시스템, 네트워크, 게이트웨이, 라우터 또는 네트워크의 브릿지를 사용할 수 없거나 작동시킬 수 없다는 것을 의미할 수 있습니다. 응답 실패는 리모트 시스템이나 중간 방화벽이 ICMP 응답을 작동하지 않게 만드는 것을 의미할 수도 있습니다. 다른 시스템과의 연결이나 다른 시스템간의 연결을 확인하여 실패가 발생할 가능성이 많은 위치를 판별하십시오.
5. 리모트 시스템이 이더넷 유형의 회선 설명에 구성된 인터페이스를 확인하기 위해 PING 명령을 사용할 때 응답 수신에 실패하면 올바른 이더넷 표준 또는 *ALL을 이더넷 회선 설명에 지정해야 합니다.
6. 네트워크의 모든 시스템이 응답을 받는 데 실패하면 경로를 따라 어딘가에서 문제가 발생한 것을 나타냅니다. 문제가 발생했을 가능성이 있는 네트워크로 이르는 게이트웨이 연결을 확인하십시오. 이 조치가 실패하면 실패 위치를 찾을 때까지 도달할 수 없는 리모트 시스템에서 역으로 다시 작업하십시오.
7. 패킷은 전달을 보장하지 않은 낮은 레벨의 프로토콜을 사용하여 송신됩니다. 에코 요구가 유실되었을 가능성이 있으므로 여러 명령들이 경로를 지나 외부로 나갈 때까지는 네트워크나 게이트웨이가 실패했다고 가정하지 마십시오.

리모트 네트워크의 호스트에 대한 PING 명령이 실패하면 같은 네트워크에 대해 라우트 추적(TRACEROUTE)명령을 사용하십시오. 라우트 추적 유틸리티는 개별 ping 요구가 할 수 있는 많은 수의 같은 연결 테스트를 수행할 수 있으나 라우트 추적은 한 단계로 모두 수행할 수 있습니다. 라우트 추적은 리모트 목적지에 대한 경로를 따라 각 홉(hop)을 테스트하며 중간 라우터나 리모트 네트워크에 문제점이 있는지를 나타냅니다.

| TRACEROUTE RMTSYS('x.x.x.x')를 입력하십시오. IP 주소를 사용하거나 예를 들어, ('xxxx.xxxx.com')
| 과 같이 리모트 시스템 이름을 사용하여 리모트 시스템을 지정할 수 있습니다. 라우트 추적 유틸리티는 IPv4
| 주소 형식('x.x.x.x') 및 IPv6 주소 형식('x:x:x:x:x:x:x:x') 모두를 승인합니다.

라우트 추적은 iSeries Navigator를 통해서도 사용할 수 있습니다. 라우트 추적을 시작하려면 다음 단계를 따르십시오.

1. iSeries Navigator에서 서버 --> **네트워크**를 확장하십시오.
2. **TCP/IP 구성**을 오른쪽 마우스 단추로 누르고 **유틸리티**를 선택한 후 **라우트 추적**을 선택하십시오.

초기 TCP/IP 문제점 분석으로 돌아가서 문제 해결을 계속하십시오.

원인 리스트 C

1. 필요한 모든 작업을 위해 서버 QSYSWRK 서브시스템을 확인하십시오(로컬 또는 리모트). 최소한 QTCPIP 작업이 있어야 합니다. QTCPIP 작업이 TCP/IP 인터페이스 시작 및 종료를 제어합니다. 또한 9 페이지의 그림 1에 나오는 것처럼 사용하려는 각 어플리케이션에 대해 최소한 하나의 작업이 있어야 합니다. 이 작업들은 FTP, LPD, TELNET 작업을 위해 서브시스템 작업과 동일하게 이름을 지정하지 못할 수 있습니다. 모든 FTP 작업은 QTFTP로 시작합니다. 모든 LPD 작업은 QTLPD로 시작합니다. 모든 TELNET 작업의 이름은 QTVTELNET 및 QTVDEVICE입니다. 둘 이상의 FTP, LPD 또는 TELNET 서버 작업을 가질 수 있습니다. 모든 SMTP 작업은 QTSMTP로 시작합니다. SMTP는 QSYSWRK 서브시스템에 최대 네 개의 활동 작업을 가지고 있으며 QSNADS 서브시스템에는 두 개의 활동 작업을 가지고 있습니다. 모든 SNMP 작업은 QTMSNMP로 시작합니다. SNMP는 QSYSWRK 서브시스템, QTMSNMP, QTMSNMPRCV 및 QSNMPSA에서 세 개의 활동 작업을 가질 수 있습니다.

   WRKACTJOB(활동 작업에 대한 작업) 명령을 사용하여 이 작업들을 표시할 수 있습니다. WRKACTJOB SBS(QSYSWRK)를 입력하십시오.
2. 그곳에 모든 작업이 없으면 ENDTCP OPTION(*IMMED) 명령을 사용하여 TCP/IP 처리를 종료하십시오. 작업과 연관된 모든 작업 기록부를 찾아보십시오.
3. 모든 작업 설명 오브젝트의 작업 설명 메세지 기록 레벨을 4 0 *SECLVL로 변경하십시오. 메세지 기록 레벨에 대한 자세한 정보는 작업 기록부 및 메세지 대기행렬에 대한 작업을 참조하십시오.
4. STRTCP 명령을 사용하여 TCP/IP 처리를 다시 시작하십시오.
5. 모든 작업이 활동 중인지 확인하십시오.
6. 해당 작업이 활동 중이 아니면 작업 기록부를 확인하십시오.

```
                활동 작업에 대한 작업            SYSNAM03

                                    02/03/99  18:06:32
CPU %:     .8     경과 시간:   02:21:32     활동 작업:   93

옵션을 입력한 후 Enter 키를 누르십시오.
  2=변경    3=보류    4=종료    5=작업 대상   6=해제   7=메세지 표시
  8=스풀 파일에 대한 작업   13=...단절

Opt 서브시스템/작업 사용자     유형   CPU %  기능             상태
     QSYSWRK        QSYS        SBS      .0                  DEQW
       QMSF         QMSF        BCH      .0                  DEQW
       QNEOSOEM     QUSER       ASJ      .0  PGM-QNEOSOEM    TIMW
       QNEOSOEM     QUSER       BCH      .0  PGM-QNEOSOEM    TIMW
       QNEOSOEM     QUSER       BCH      .0  PGM-QNEOSOEM    TIMW
       QNPSERVD     QUSER       BCH      .0                  SELW
       QPASVRP      QSYS        BCH      .0  PGM-QPASVRP     DEQW
       QPASVRS      QSYS        BCH      .0  PGM-QPASVRS     TIMW
       QPASVRS      QSYS        BCH      .0  PGM-QPASVRS     TIMW
                                                                  계속...
매개변수 또는 명령
===>
F3=나감    F5=화면정리      F7=찾기      F10=통계 재시작
F11=경과 자료 표시          F12=취소     F23=추가 옵션     F24=추가 키
```

그림 1. 활동 작업에 대한 작업 화면-화면 1

```
                활동 작업에 대한 작업            SYSNAM03
                                    02/03/99  18:06:32
CPU %:     .8     경과 시간:   02:21:32     활동 작업:   93

옵션을 입력한 후 Enter 키를 누르십시오.
  2=변경    3=보류    4=종료    5=작업 대상   6=해제   7=메세지 표시
  8=스풀 파일에 대한 작업   13=...단절

Opt 서브시스템/작업 사용자     유형   CPU %  기능             상태
       QTLPD03516   QTCP        BCH      .0                  DEQW
       QTLPD03580   QTCP        BCH      .0                  TIMW
       QTMSNMP      QTCP        BCH      .0  PGM-QTOSMAIN    DEQW
       QTMSNMPRCV   QTCP        BCH      .0  PGM-QTOSRCVR    TIMW
       QTVDEVICE    QTCP        BCH      .0  PGM-QTVDEVMG    TIMW
       QTVTELNET    QTCP        BCH      .0                  TIMW
       QZBSEVTM     QUSER       ASJ      .0  PGM-QZBSEVTM    EVTW
       QZHQSRVD     QUSER       BCH      .0                  SELW
       QZRCSRVSD    QUSER       BCH      .0                  SELW
                                                                  계속...
매개변수 또는 명령
===>
F3=나감    F5=화면정리      F7=찾기      F10=통계 재시작
F11=경과 자료 표시          F12=취소     F23=추가 옵션     F24=추가 키
```

그림 2. 활동 작업에 대한 작업 화면-화면 2

초기 TCP/IP 문제점 분석으로 돌아가서 문제 해결을 계속하십시오.

원인 리스트 D

서버의 네트워크 상태(NETSTAT) 기능을 사용하여 TCP/IP 인터페이스 상태, TCP/IP 라우트 구성 정보 및 로컬 시스템의 TCP/IP 연결 상태를 볼 수 있습니다. WRKTCPSTS 명령이나 NETSTAT 명령을 사용하십시오.

1. 네트워크 상태 기능을 사용하기 전에 STRTCP 명령을 사용하여 TCP/IP를 시작하십시오. TCP/IP 네트워크 상태에 대한 작업 메뉴가 표시되지만 TCP/IP가 시작될 때까지 옵션이 제기능을 하지 않습니다.
2. TCP/IP 인터페이스 상태에 대한 작업 화면에서 활동 인터페이스를 시작하거나 비활동 인터페이스를 종료하는 경우 해당 오류 메세지가 송신됩니다. 비활동 인터페이스가 인터페이스 시작 옵션을 사용한 후에도 활동 상태에 도달하지 않으면 인터페이스, 회선 또는 회선 구성에 문제가 있을 수 있습니다. 인터페이스를 활성화할 때 발생할 가능성이 있는 오류에 관해 알려면 QSYSWRK 서브시스템에서 QTCPIP 작업의 작업 기록부를 참조하십시오. QSYSOPR 메세지 대기행렬 및 이력 기록부인 QHT (DSPLOG)를 조사하여 상태를 판별하는데 도움을 받을 수도 있습니다.
3. 회선 설명에 문제점이 있는지 판별하려면 WRKCFGSTS *LIN을 입력하십시오.
4. TCP/IP 네트워크 상태에 대한 작업 화면에서 연결 상태에 대한 작업 화면의 옵션3에 각 서버를 위해 최소한 하나의 수동적 청취 연결이 표시되는지 확인하십시오. 이 어플리케이션들을 지원하는 서버 및 네트워크상의 기타 다른 관련된 서버에 대한 연결 상태를 확인해야 합니다.

   SNMP

   TELNET

   버전 4 릴리스 4는 Telnet외에도 SSL Telnet을 지원합니다. SSL Telnet은 디폴트로 청취 포트 992를 반영하며 기존의 Telnet에서는 포트 23을 사용합니다. Telnet 청취 포트를 제한하는 것은 SSL Telnet을 작동 가능하게 만드는 한편 기존의 Telnet 서버를 작동 불가능하게 하기 위해 권장되는 방법입니다.

   FTP

   SMTP(구성되어 있는 경우)

   POP

   LPD

   REXEC

   HPP(구성되어 있는 경우)

   수동적 청취 연결에는 *리모트 주소* 및 *리모트 포트* 필드에 별표가 있습니다. 이와 같은 연결을 종료하는 것은 바람직하지 않습니다. 연관된 수동적 청취 연결을 종료시키면 리모트 시스템이 SNMP, FTP, TELNET을 사용하거나 SMTP 메일 로컬 시스템에 송신하거나 LPR을 사용하여 스풀 파일을 로컬 시스템에 송신할 수 없습니다. ENDTCPSVR 및 STRTCPSVR 명령을 사용하여 서버를 종료한 후 종료 및 시작할 서버를 지정함으로서 재시작시킬 수 있습니다.
5. 사용하려는 어플리케이션과 연관된 포트가 제한을 받지 않아야 합니다. TCP/IP 구성 메뉴에서 옵션 4(TCP/IP 포트 제한사항에 대한 작업)를 사용하여 현재 포트 제한사항을 보십시오.

초기 TCP/IP 문제점 분석으로 돌아가서 문제 해결을 계속하십시오.

원인 리스트 E

구성 자료를 확인하십시오. 모든 것을 확인했으면 특정 어플리케이션 문제점으로 가서 문제 해결 지원에 사용중인 특정 어플리케이션을 선택하십시오.

PING 명령 고려사항

PING 명령에 대해 자세히 알려면 다음 절을 참조하십시오.

호스트명에 정의역명 연결
이 절에서는 서버가 정의역명을 호스트명에 연결하는 방법에 관해 설명합니다.

일반적인 오류 메세지
여기에는 가장 일반적인 PING 오류 상태 중 일부의 예가 나옵니다.

호스트명에 정의역명 연결

이 예에서는 정의역명의 끝에 기간을 사용하지 않을 경우 서버가 로컬 정의역명을 탐색 리스트로 사용하여 호스트명에 정의역명을 연결하는 방법을 보여줍니다.

서버명은 SYSNAM01.A400SSC.DFW.COMPANY.COM이며 완전한 이름이 SYSNAM02.DFW.COMPANY.COM인 시스템과의 연결을 확인하려고 합니다. 로컬 호스트 표에는 SYSNAM02 호스트명이 없습니다.

PING SYSNAM02.DFW.COMPANY.COM을 입력하면 서버가 이름 서버에 SYSNAM02.DFW.COMPANY.COM을 송신합니다.

PING SYSNAM02를 입력하면 서버가 먼저 리모트 이름 서버에 SYSNAM02.A400SSC.DFW.COMPANY.COM을 송신합니다. 그런 후 SYSNAM02.DFW.COMPANY.COM을 송신합니다. 이것을 찾지 못하면 마지막으로 SYSNAM02.COMPANY.COM을 송신합니다. 즉, iSeries TCP/IP가 로컬 정의역명의 각 부분을 호스트명에 연결합니다.

PING SYSNAM02.를 입력하면 리모트 이름 서버가 호스트를 알 수 없는 것으로 보고합니다. 리모트 이름 서버가 SYSNAM02를 인식하지 못하는 이유는 서버가 탐색 리스트의 해당 부분을 연결하지 않고 리모트 이름 서버에 SYSNAM02 이름을 송신하기 때문입니다. 이 이름과 이전 이름간의 유일한 차이점은 이름 끝에 마침표를 사용하는 것입니다.

일반적인 오류 메세지

PING 명령을 사용하여 네트워크에서 또 다른 호스트와의 연결을 확인할 때 TCP/IP가 오류 메세지를 발행할 수 있습니다. 이 표를 사용하여 일반적인 오류 메세지를 식별하고 문제점을 해결하기 위해 해야 할 일을 판별하십시오.

오류 메세지	해야 할 일
TCP/IP 서비스를 사용할 수 없습니다.	• TCP/IP가 아직 시작되지 않았거나 시작을 완료하지 못했습니다. TCP/IP가 활동 중인지 알려면 NETSTAT 명령을 사용하십시오. • 모든 작업이 QSYSWRK 서브시스템에서 시작되지 않을 수 있습니다. QSYSWRK 서브시스템 및 관련 작업이 활동 중인지 확인하려면 WRKACTJOB(활동 작업에 대한 작업) 명령을 사용하십시오. 활동 중이 아니면 모든 메세지의 작업 기록부 또는 시스템 디폴트 출력 대기행렬을 확인하십시오.
리모트 호스트 시스템과의 연결을 설정할 수 없습니다.	구성되어 있는 인터페이스, 관련 회선 설명 및 TCP/IP 라우트를 확인하십시오.
리모트 시스템에 도달할 수 없습니다.	TCP/IP가 요구받은 목적지에 대한 라우트를 찾을 수 없습니다. NETSTAT 옵션 2를 확인하고 *DFTROUTE 또는 이와 동등한 네트워크 라우트가 구성되어 있으며 현재 활동 중인지 확인하십시오.
리모트 호스트가 연결 검증 1을 위해 10초 내에 VFYTCPCNN에 응답하지 않았습니다.	• 구성에는 문제가 없으나 리모트 시스템에서 다시 응답을 받지 못했습니다. 리모트 호스트가 시스템에 도달할 수 있어야 합니다. 리모트 시스템 오퍼레이터에게 문의하여 사용자 시스템과의 연결을 확인하도록 요청하십시오. • 두 시스템 모두에 대해 호스트 표나 리모트 이름 서버(이름 서버를 사용 중인 경우) 그리고 TCP/IP 인터페이스와 라우트를 확인하십시오. 몇 가지 이유로 인해 사용자에게 리모트 이름 서버가 제공되지 않을 수도 있습니다. • 이더넷 회선을 사용 중이면 올바른 이더넷 표준이나 *ALL을 지정했는지 확인하십시오.
VFYTCPCNN: xxxxxx 호스트를 알 수 없습니다. 여기서 xxxxxx는 호스트명입니다.	호스트명은 호스트 표나 이름 서버를 사용하여 IP 주소로 분석할 수 없습니다. 로컬 호스트 표나 리모트 호스트 항목의 리모트 이름 서버(이름 서버를 사용 중인 경우)를 확인하십시오.

작업 기록부 및 메세지 대기행렬에 대한 작업

TCP/IP는 여러 작업 설명과 함께 제공됩니다.

작업 설명은 QSYS 또는 QTCP 라이브러리에 저장되어 있습니다. 작업 설명은 보통 메세지 기록 레벨 4, 메세지 기록 심각도 0 및 메세지 기록 텍스트 값 *NOLIS로 설정되어 제공됩니다. 이것은 작업 기록부가 작업 시작 및 작업 종료 메세지로만 작성되는 것을 방지하기 위한 것입니다.

TCP/IP 조작에 문제가 있을 때 가장 먼저 해야 할 일 중 하나는 문제가 있는 어플리케이션의 작업 설명에 대한 메세지 기록 레벨을 메세지 기록 텍스트 값 *SECLVL으로 변경하는 것입니다. 메세지 기록 레벨을 변경하면 해당 어플리케이션의 작업 기록부가 생성됩니다. 변경사항을 적용하려면 서버를 종료한 후 다시 시작해야 합니다. 즉시 작업을 변경하려면 CHGJOB 명령을 사용하여 활동 작업의 메세지 기록 레벨을 변경하십시오.

특정 어플리케이션에 대한 작업 설명의 메세지 기록 레벨을 변경하려면 다음 예를 참조하십시오.

- FTP 서버에 문제가 있으면 다음 CL 명령을 입력하여 QTMFTPS 작업 설명을 변경하십시오.

  ```
  CHGJOBD  JOBD(QTCP/QTMFTPS)  LOG(4 0 *SECLVL)
  ```

- SMTP에 문제가 있으면 다음 CL 명령을 입력하여 QTMSMTPS 작업 설명을 변경하십시오.

  ```
  CHGJOBD  JOBD(QTCP/QTMSMTPS)  LOG(4 0 *SECLVL)
  ```

QTMSMTPS 작업 설명외에 CL 명령을 입력하여 QSNADS 서브시스템 작업 설명의 기록 레벨을 변경할 것을 고려할 수도 있습니다.

```
CHGJOBD  JOBD(QGPL/QSNADS)  LOG(4 0 *SECLVL)
```

제 3 장 특정 어플리케이션 문제점

TCP/IP에서 실행 중인 특정 어플리케이션 내에 문제에 있는 것으로 결정했으면 아래의 어플리케이션을 선택하고 자세한 문제 해결 정보를 보십시오. 각 링크를 통해 일반적인 TCP/IP 문제 해결 사이트에서 나가 선택한 특정 어플리케이션에 대한 새 사이트로 갈 수 있습니다.

정의역명 시스템 서버(DNS)
문제점 분석을 위한 흐름 도표를 제공하며 DNS 문제점의 디버깅 전략을 제공합니다.

파일 전송 프로토콜(FTP)
FTP 문제점에 대한 솔루션을 제안하며 문제 해결 툴로 서버 작업 기록부에 관해 설명합니다.

지점 간 프로토콜(PPP)
공통 PPP 연결 문제점에 대한 솔루션을 제공합니다.

포스트 오피스 프로토콜 서버(POP)
POP 서버 및 기타 전자 우편 어플리케이션 문제 해결에 관해 설명합니다.

Rexec
사용자 Rexec 문제점을 중심으로 가능한 솔루션을 찾는 데 도움을 주는 흐름 도표를 제공합니다.

단순 우편 전송 프로토콜(SMTP)
단순 우편 전송 프로토콜(SMTP) 및 기타 전자 우편 어플리케이션의 문제점을 해결하는 데 필요한 몇 가지 방법을 설명합니다.

Telnet
에뮬레이션 유형 및 SSL 서버와 관련된 특정 문제점과 일반적인 Telnet 문제점에 관해 설명합니다. 또한 문제점을 보고하는 데 필요한 정보를 알아봅니다.

가상 사설망(VPN)
이 주제는 연결, 구성 오류, 필터 규칙 등과 관련된 VPN 문제점의 여러 가지 문제 해결 전략에 관해 설명합니다.

© Copyright IBM Corp. 1997, 2002

제 4 장 통신 추적

통신 추적을 사용하여 TCP/IP 문제 해결을 수행하십시오. 통신 추적은 근거리 통신망(LAN) 또는 광역 네트워크(WAN)와 같은 통신 회선에 대한 자료를 추적할 수 있는 서비스 기능입니다. 자료를 추적한 후에는 원시 자료를 스트림 파일로 덤프하거나 포맷하여 스풀 파일에 넣어 화면에 표시하거나 인쇄할 수 있습니다.

통신 추적은 IPv4 및 IPv6 통신 둘 다의 문제 해결에 사용될 수 있습니다.

다음과 같은 경우에 통신 추적을 사용하십시오.

- 문제점 분석 프로시듀어에서 문제점에 대해 충분한 정보를 제공하지 않는 경우.
- 프로토콜 위반이 문제로 의심되는 경우.
- 회선 잡음이 문제로 의심되는 경우.
- 어플리케이션에서 네트워크를 통해 정보를 정확하게 전송하고 있는지 알고 싶은 경우.
- 네트워크 혼잡이나 자료 처리량에 성능 문제가 있는지 알고 싶은 경우.

CL 명령을 사용하여 통신 추적을 수행하려면 *SERVICE 특수 권한이 있거나 iSeries Navigator를 통해 Operating System/400®의 서비스 추적 기능을 사용할 권한이 있어야 합니다. 이러한 권한 유형에 대한 자세한 정보는 iSeries 보안 참조서 에서 사용자 프로파일을 참조하십시오.

연결 추적(TRCCNN)은 통신 추적과 유사한 추적을 확보하는 대안 메소드에 대한 명령입니다. SSL을 사용하는 TCP 어플리케이션이 있거나 IP 보안을 사용하는 경우에는 통신 회선을 통해 흐르는 자료가 암호화됩니다. 자료를 봐야 하는 경우에는 통신 추적이 도움이 되지 않을 것입니다. TRCCNN은 암호화 전 및 암호 해독 후에 자료를 추적하므로 일반 통신 추적이 효과적이지 않을 때 사용될 수 있습니다. 이 명령은 일반 통신 추적 출력과 유사한 출력을 제공합니다. 이 명령과 연관된 매개변수와 예는 어플리케이션 프로그래밍 인터페이스(API) 주제에서 TRCCNN(연결 추적) 명령 설명을 참조하십시오.

통신 추적 기능을 사용하려면 다음 단계를 따르십시오.

통신 추적 계획
통신 추적을 수행하기 전에 필요한 예비 단계.

통신 추적 수행
통신 추적을 수행하기 위해 필요한 단계.

추가 통신 추적 기능
통신 추적과 연관된 추가 기능들.

통신 추적 계획

통신 추적에 대한 작업을 시작하기 전에 다음 단계를 따르십시오.

1. IBMLIB 라이브러리나 IBMOUTQ 출력 대기행렬을 아직 작성하지 않았으면 다음 명령을 입력하십시오.

© Copyright IBM Corp. 1997, 2002

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

2. 라이브러리 리스트에 IBMLIB 라이브러리를 추가하고 작업의 출력 대기행렬을 IBMOUTQ 출력 대기행렬로 변경하려면 다음 명령을 입력하십시오.

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

3. QTCPPRT 프린터 파일이 사용자 시스템에 없으면 다음 명령을 입력하여 작성하십시오.

```
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. 통신 추적이 들어 있는 QTCPPRT 스풀 파일을 IBMLIB 라이브러리의 IBMOUTQ 출력 대기행렬로 송신하려면 다음 명령을 입력하십시오.

```
OVRPRTF FILE(QTCPPRT) OUTQ(IBMLIB/IBMOUTQ)
OVRPRTF FILE(QPCSMPRT) TOFILE(QTCP/QTCPPRT)
```

   작업 종료 후에는 프린터 파일 대체가 적용되지 않습니다.

5. 문제가 있는 TCP/IP 인터페이스와 연관이 있는 회선 설명 이름이나 문제가 있는 어플리케이션 또는 네트워크가 사용하는 회선 설명 이름을 구하십시오. 인터페이스와 연관된 회선 설명의 이름을 알아보려면 NETSTAT *IFC를 사용하십시오.
6. 회선이 연결변환되어 있으며 그 회선과 연관이 있는 TCP/IP 인터페이스가 이미 시작되어 TCP/IP 자료를 인터페이스와 회선을 통해 송수신할 수 있는지 확인하십시오. 인터페이스가 활동 중인지 알아보려면 NETSTAT *IFC를 사용하십시오.

다음으로 해야 할 일:

통신 추적 수행

통신 추적 수행

통신 추적을 수행하려면 문자 기반의 인터페이스에서 CL 명령을 사용해야 합니다. 통신 추적을 수행하려면 다음 단계를 따르십시오.

1. 통신 추적 시작
2. 통신 추적 종료
3. 통신 추적 덤프
4. 통신 추적 인쇄
5. 통신 추적 내용 보기
6. 통신 추적 읽기

통신 추적 시작

이 조치는 지정된 회선이나 네트워크 인터페이스 설명에 대한 통신 추적을 시작합니다.

주: 네트워크 서버 설명(*NWS)에 대한 자료 추적에는 통신 추적이 더 이상 사용되지 않습니다. 특정 회선(*LIN) 이나 네트워크 인터페이스 설명(*NWI)에 대한 자료를 추적하는데 통신 추적 기능을 사용하십시오.

통신 추적을 시작하려면 다음 단계를 따르십시오.

1. 명령행에서 STRCMNTRC를 입력하십시오.
2. **구성 오브젝트**에서 TRNLINE과 같은 회선 이름을 지정하십시오.
3. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.
4. **버퍼 크기**에서 자료의 예상 볼륨에 대한 충분한 기억장치 양을 지정하십시오. 대부분 프로토콜의 경우 8MB 의 기억장치가 충분합니다. 10/100 이더넷의 경우에는 16MB에서 1GB 사이가 충분합니다. 확실하지 않으면 프로토콜에 허용되는 최대 기억장치 양에 16MB를 지정하십시오.
5. 한 리모트 인터페이스의 추적을 위해 수집되는 자료를 제한하고 싶으면 **통신 추적 옵션**에서 *RMTIPADR을 지정하십시오. 그렇지 않은 경우에는 디폴트 값을 사용하십시오.
6. **리모트 IP 주소**에서 추적 자료를 수집할 해당 리모트 인터페이스와 연관된 IP 주소를 지정하십시오.

다음 중 한 경우가 발생할 때까지 통신 추적이 계속됩니다.

- ENDCMNTRC 명령이 실행되는 경우.
- 물리적 회선 문제로 인해 추적이 종료되는 경우.
- **추적 가득 참** 매개변수가 *STOPTRC를 지정하고 버퍼가 가득 찬 경우.

다음으로 해야 할 일:
통신 추적 종료

통신 추적 종료

추적을 포맷하고 표시하기 위해서는 먼저 추적을 종료해야 합니다. 이 조치는 추적을 종료하지만 통신 추적 버퍼를 저장합니다.

통신 추적을 종료하려면 다음 단계를 따르십시오.

1. 명령행에서 ENDCMNTRC를 입력하십시오.
2. **구성 오브젝트**에서 TRNLINE과 같은 추적을 시작했을 때 지정한 것과 동일한 회선을 지정하십시오.
3. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.

다음으로 해야 할 일:
스트림 파일로 통신 추적 덤프. 이것은 사용자에게 유용할 수 있는 선택적 단계입니다. 덤프하지 않고 원시 자료를 인쇄하고 싶으면 통신 추적 인쇄로 가십시오.

통신 추적 덤프

인터넷 프로토콜 버전 6(IPv6)을 사용하는 경우에는 다음 단계에 따라 추적 자료를 스트림 파일로 덤프해야 합니다. 그러나 IPv4를 사용하는 경우 이 단계는 통신 추적 프로세스의 선택적 부분입니다.

자료를 스트림 파일로 덤프하면 여러가지 장점이 있습니다. 이 기능의 사용 여부를 결정할 때 이 장점들을 고려하십시오.

- 기존 추적으로부터 자료를 잃지 않으면서 새 추적을 실행할 수도 있습니다.
- 추적 자료를 여러 번 포맷할 수도 있습니다. 예를 들어, 어플리케이션 중 하나가 ASCII를 사용하는 경우에는 먼저 ASCII로 통신 추적을 포맷해야 하거나, 어플리케이션이 EBCDIC을 사용하는 경우에는 EBCDIC으로 동일한 추적 자료를 포맷해야 할 수도 있습니다. 추적 자료를 스트림 파일로 덤프하면 이 자료를 두 번 포맷할 수 있는 유연성이 제공됩니다.
- 초기 프로그램 로드(IPL)를 실행하는 동안 추적 자료를 보유할 수도 있습니다.
- 사용자 정의 포맷 프로그램을 사용하여 출력을 생성할 수도 있습니다.

통신 추적을 덤프하려면 다음 단계를 따르십시오.

1. mydir과 같은 디렉토리를 작성하십시오. 제어 언어(CL) 주제에서 CRTDIR(디렉토리 작성) 명령 설명을 참조하여 디렉토리를 작성하십시오.
2. 명령행에서 DMPCMNTRC를 입력하십시오.
3. **구성 오브젝트**에서 TRNLINE과 같은 추적을 시작했을 때 지정한 것과 동일한 회선을 지정하십시오.
4. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.
5. **파일을 스트림하려면** /mydir/mytraces/trace1과 같은 경로명을 지정하십시오.

다음으로 해야 할 일:
통신 추적 인쇄

통신 추적 인쇄

추적을 수집한 방법에 따라 두 개의 서로 다른 소스로부터 통신 추적 자료를 인쇄할 수도 있습니다. 수집한 원시 자료로부터 인쇄하거나 이전에 원시 파일을 덤프한 스트림 파일로부터 인쇄할 수도 있습니다.

주: 스트림 파일로부터 통신 추적 자료를 인쇄하기 위해서는 시스템에 Java™(5722JV1)가 설치되어 있어야 합니다.

이 조치는 지정된 회선이나 네트워크 인터페이스 설명에 대한 통신 추적 자료를 스풀 파일이나 출력 파일에 기록합니다.

수집한 원시 자료로부터 인쇄:

덤프하지 않고 원시 자료를 수집한 경우에는 다음 단계에 따라 자료를 인쇄하십시오.

1. 명령행에서 PRTCMNTRC를 입력하십시오.

2. **구성 오브젝트**에서 TRNLINE과 같은 추적을 시작했을 때 지정한 것과 동일한 회선을 지정하고 Enter를 누르십시오.
3. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.
4. **문자 코드**에서 *EBCDIC 또는 *ASCII를 지정하십시오. *EBCDIC을 지정한 후 *ASCII를 지정하여 자료를 두 번 인쇄해야 합니다.
5. **TCP/IP 자료 포맷**에서 *YES를 지정한 후 Enter를 두 번 누르십시오.
6. 1에서 5단계까지를 다시 수행하되, 다른 문자 코드를 지정하십시오.

스트림 파일로부터 인쇄:

자료를 스트림 파일로 덤프한 경우에는 다음 단계에 따라 자료를 인쇄하십시오.

1. 명령행에서 PRTCMNTRC를 입력하십시오.
2. **스트림 파일로부터**에서 /mydir/mytraces/trace1과 같은 경로명을 지정하고 Enter를 누르십시오.
3. **문자 코드**에서 *EBCDIC 또는 *ASCII를 지정하십시오. *EBCDIC을 지정한 후 *ASCII를 지정하여 자료를 두 번 인쇄해야 합니다.
4. **TCP/IP 자료 포맷**에서 *YES를 지정한 후 Enter를 두 번 누르십시오.
5. 1에서 4단계까지를 다시 수행하되, 다른 문자 코드를 지정하십시오.

다음으로 해야 할 일:
통신 추적의 내용 보기

통신 추적의 내용 보기

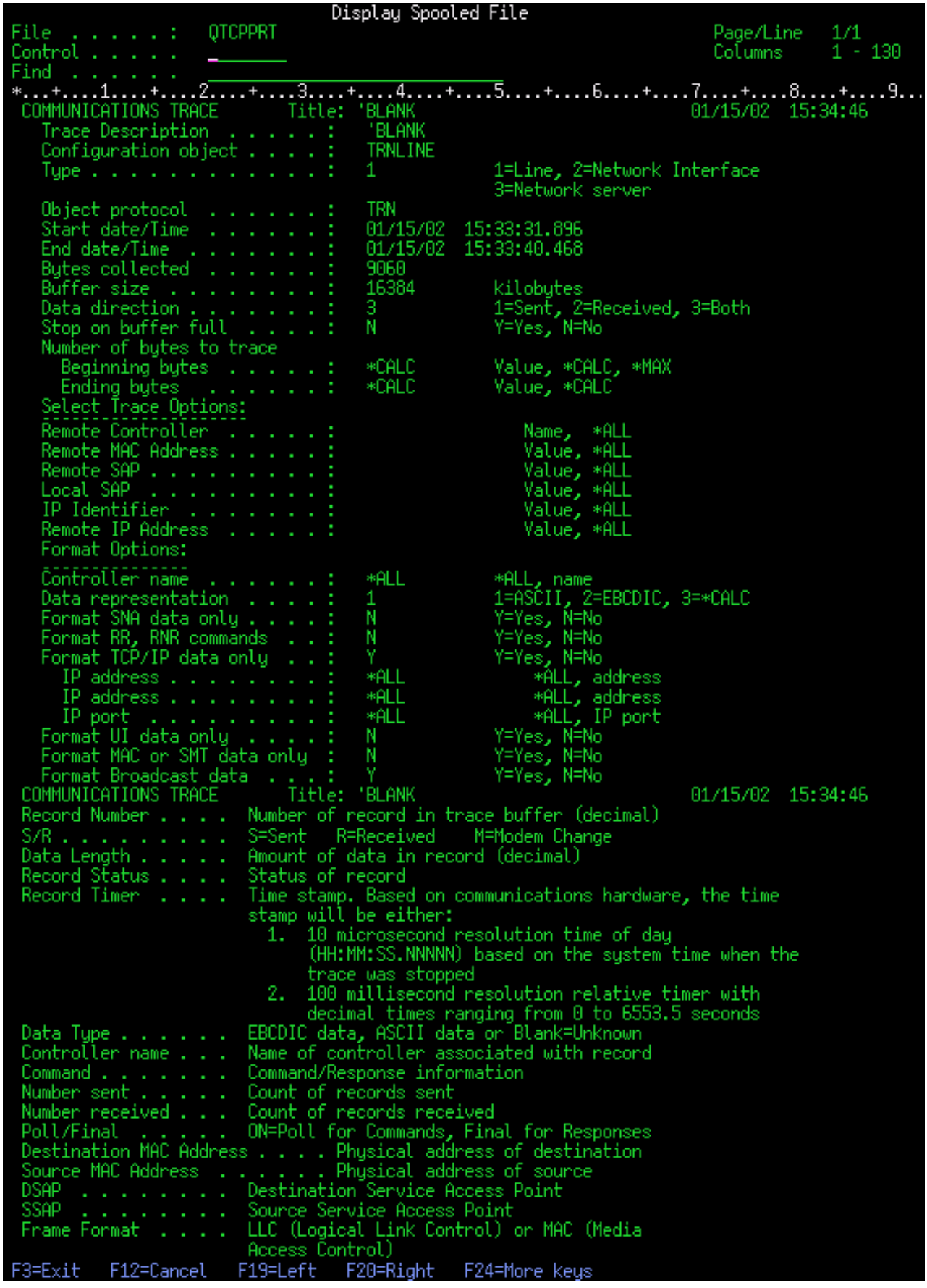
통신 추적의 내용을 보려면 다음 단계를 따르십시오.

1. 명령행에서 WRKOUTQ OUTQ(IBMLIB/IBMOUTQ)를 지정하십시오.
2. **출력 대기행렬에 대한 작업** 대화에서 F11(보기 2)을 눌러 작업하려는 스풀 파일의 날짜 및 시간을 보십시오. 표시 화면에 계속...이 나타나고 스풀 파일을 계속 탐색해야 하는 경우에는 파일 리스트 앞뒤로 페이지를 이동하십시오. 그렇지 않은 경우에는 다음 단계로 진행하십시오.
3. 표시하려는 스풀 파일 옆의 **Opt** 열에 5를 지정하십시오. 마지막 파일에는 가장 최근의 통신 추적이 들어 있습니다.
4. 이것이 추적된 회선에 대한 통신 추적이며 추적이 시작하고 종료한 시간이 정확한지 확인하십시오.

다음으로 해야 할 일:
통신 추적 읽기

통신 추적 읽기

통신 추적은 여러 유형의 정보를 표시합니다. 통신 추적의 첫 부분은 **구성 오브젝트**의 이름과 같은 추적을 시작할 때 지정한 매개변수를 요약합니다. 뒷장 키를 사용하여 연관된 정의와 함께 **레코드 번호** 및 **S/R**과 같은 항목 리스트를 찾으십시오. 이 항목들은 나중에 통신 추적 자료의 섹션을 식별하는데 사용됩니다. 추적 자료를 읽으면서 이 목록을 다시 참조하는데 유용할 것입니다. 이 이미지는 통신 추적에서 예비 정보를 보여줍니다.


Display Spooled File
File . . . . . : QTCPPRT
Page/Line 1/1
Control . . . . . _
Columns 1 - 130
Find . . . . . _
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9...
COMMUNICATIONS TRACE Title: 'BLANK 01/15/02 15:34:46
Trace Description . . . . . : 'BLANK
Configuration object . . . . : TRNLINE
Type . . . . . : 1 1=Line, 2=Network Interface
3=Network server
Object protocol . . . . . : TRN
Start date/Time . . . . . : 01/15/02 15:33:31.896
End date/Time . . . . . : 01/15/02 15:33:40.468
Bytes collected . . . . . : 9060
Buffer size . . . . . : 16384 kilobytes
Data direction . . . . . : 3 1=Sent, 2=Received, 3=Both
Stop on buffer full . . . . : N Y=Yes, N=No
Number of bytes to trace
Beginning bytes . . . . . : *CALC Value, *CALC, *MAX
Ending bytes . . . . . : *CALC Value, *CALC
Select Trace Options:
Remote Controller . . . . . : Name, *ALL
Remote MAC Address . . . . . : Value, *ALL
Remote SAP . . . . . : Value, *ALL
Local SAP . . . . . : Value, *ALL
IP Identifier . . . . . : Value, *ALL
Remote IP Address . . . . . : Value, *ALL
Format Options:
Controller name . . . . . : *ALL *ALL, name
Data representation . . . . : 1 1=ASCII, 2=EBCDIC, 3=*CALC
Format SNA data only . . . . : N Y=Yes, N=No
Format RR, RNR commands . . : N Y=Yes, N=No
Format TCP/IP data only . . : Y Y=Yes, N=No
IP address . . . . . : *ALL *ALL, address
IP address . . . . . : *ALL *ALL, address
IP port . . . . . : *ALL *ALL, IP port
Format UI data only . . . . : N Y=Yes, N=No
Format MAC or SMT data only : N Y=Yes, N=No
Format Broadcast data . . . : Y Y=Yes, N=No
COMMUNICATIONS TRACE Title: 'BLANK 01/15/02 15:34:46
Record Number . . . . Number of record in trace buffer (decimal)
S/R . . . . . S=Sent R=Received M=Modem Change
Data Length . . . . . Amount of data in record (decimal)
Record Status . . . . Status of record
Record Timer . . . . Time stamp. Based on communications hardware, the time
stamp will be either:
1. 10 microsecond resolution time of day
(HH:MM:SS.NNNNN) based on the system time when the
trace was stopped
2. 100 millisecond resolution relative timer with
decimal times ranging from 0 to 6553.5 seconds
Data Type . . . . . EBCDIC data, ASCII data or Blank=Unknown
Controller name . . . Name of controller associated with record
Command . . . . . Command/Response information
Number sent . . . . . Count of records sent
Number received . . . Count of records received
Poll/Final . . . . . ON=Poll for Commands, Final for Responses
Destination MAC Address . . . . Physical address of destination
Source MAC Address . . . . . Physical address of source
DSAP . . . . . Destination Service Access Point
SSAP . . . . . Source Service Access Point
Frame Format . . . . LLC (Logical Link Control) or MAC (Media
Access Control)
F3=Exit F12=Cancel F19=Left F20=Right F24=More keys

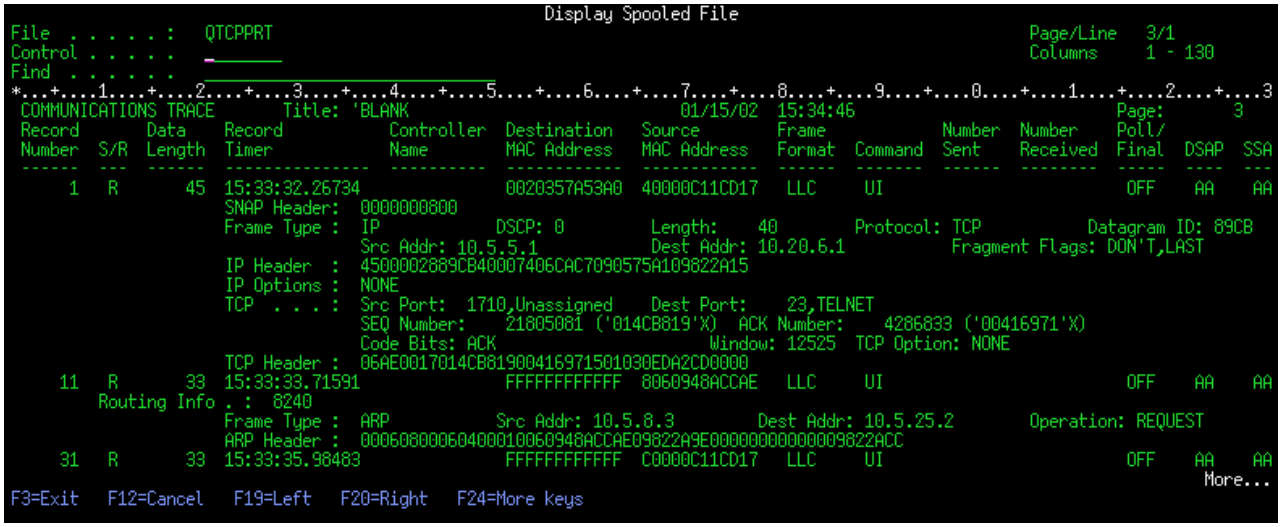
예비 정보를 읽은 후에는 통신 추적에서 실제 TCP/IP 자료 페이지로 내려가십시오. **레코드 번호**로 시작하는 제목 행은 자료 레코드의 각 섹션을 식별합니다. 각 레코드 번호는 프레임을 나타내며 소스 및 목적지 IP 주소, 완벽한 IP 데이터그램 길이, 서비스 유형(TOS), 소스 및 목적지 포트, 수신 확인(ACK) 번호와 같은 정보가 포함되어 있습니다. 이 정보를 통해 이 iSeries상의 TCP/IP나 연관된 네트워크에 있는 문제점을 디버그하는데 도움을 받을 수 있습니다.

예를 들어, 31*과 같이 레코드 번호 뒤에 별표(*)가 있는 경우 별표(*)는 누락 추적 자료를 나타내는 것임을 주목하십시오. 통신 추적 레코드가 드롭(drop)될 때 이런 현상이 일어납니다. 통신 추적 자료는 입/출력 프로세서(IOP)에 의해 수집됩니다. 통신 회선 사용량이 너무 많으면 IOP가 모든 네트워크 통신량에 우선순위를 정하며 통신 추적 정보보다 자료 경로 입/출력에 더 높은 우선순위를 부여합니다. 이러한 상황에서 IOP가 일부 통신 추적 레코드를 드롭(drop)할 수도 있습니다. 이는 IOP가 네트워크상의 과도한 속도나 통신량을 처리할 수 없음을 나타내는 것일 수도 있습니다.

통신 추적에서 자료가 누락되는 경우 다음과 같은 옵션을 고려하십시오.

- 통신 회선이 사용 중이며 통신 추적에서 해당 프레임이 누락될 것임을 인정하십시오.
- 통신 회선상의 통신량을 조사하여 다른 회선이나 TCP/IP 인터페이스로 이동될 수 있는 통신량이 있는지 판별하십시오.

이 이미지는 통신 추적의 TCP/IP 자료 부분을 보여줍니다.



통신 추적 프로세스를 완료했습니다.

추가 통신 추적 기능으로 가서 추적 삭제, 추적 상태 검사 및 기억장치 공간 판별 방법을 알아보십시오.

추가 통신 추적 기능

다음 명령 및 API는 추가 통신 추적 기능을 제공합니다.

통신 추적 삭제

동일한 회선에서 새 추적을 시작하기 전에 통신 추적을 삭제해야 합니다. 추적이 종료된 후에는 통신 추적을 삭제할 수 있습니다. 이 조치는 지정된 회선이나 네트워크 인터페이스 설명에 대한 통신 추적 버퍼를 삭제합니다.

통신 추적을 삭제하려면 다음 단계를 따르십시오.

1. 명령행에서 DLTCMNTRC를 입력하십시오.
2. **구성 오브젝트**에서 TRNLINE과 같은 회선 이름을 지정하십시오.
3. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.

통신 추적 검사

서버에 통신 추적이 현재 존재하는지 여부를 알아내고자 할 수도 있습니다. 통신 추적 검사(CHKCMNTRC)를 사용하여 특정 회선이나 네트워크 인터페이스 설명 또는 서버에 있는 특정 유형의 모든 추적에 대한 통신 추적 상태를 리턴하십시오. 메세지에 상태가 리턴됩니다.

통신 추적의 상태를 검사하려면 다음 단계를 따르십시오.

1. 명령행에서 CHKCMNTRC를 입력하십시오.
2. **구성 오브젝트**에서 TRNLINE과 같은 회선 이름을 지정하거나 특정 유형의 모든 추적 상태를 검사하려는 경우에는 *ALL을 지정하십시오.
3. **유형**에서 *LIN 또는 *NWI의 자원 유형을 지정하십시오.

프로그램으로 기억장치 공간 검사

통신 추적 검사(QSCCHKCT) API를 사용하여 추적에 할당된 최대 공간 및 서버에서 활동 중이거나 중단된 상태에 있는 모든 추적의 바이트 단위 크기를 프로그램으로 검사하십시오. 통신 추적 검사(QSCCHKCT) API에 대한 자세한 정보는 어플리케이션 프로그래밍 인터페이스(API) 주제를 참조하십시오.

제 5 장 TCP/IP 구성 파일

보고된 모든 TCP/IP 문제점에는 TCP/IP 처리에 사용되는 구성 파일의 사본을 포함시켜야 합니다. TCP/IP 구성 파일의 사본을 구하려면 다음과 같이 하십시오.

1. IBMLIB 라이브러리나 IBMOUTQ 출력 대기행렬을 작성하지 않았으면 다음 명령을 입력하십시오.

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

2. 라이브러리 리스트에 IBMLIB 라이브러리를 추가하고 작업의 출력 대기행렬을 IBMOUTQ 출력 대기행렬로 변경하려면 다음 명령을 입력하십시오.

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

   TCP/IP 구성에 사용된 모든 실제 파일의 리스트를 구하려면 다음 명령을 입력하십시오.

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

   각 파일의 내용을 복사하려면 옵션 3(대상 파일에서 복사)을 사용하거나 나열된 각 파일마다 명령행에 다음 명령을 입력하여 각 파일의 내용을 IBMOUTQ 출력 대기행렬에 있는 별도의 스풀 파일에 복사할 수 있습니다.

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

© Copyright IBM Corp. 1997, 2002

제 6 장 제품 활동 기록부

TCP/IP LIC 코드는 TCP/IP 데이터그램이 프로토콜 오류로 인해 삭제될 때마다 제품 활동 기록부에 항목을 작성합니다.

아웃바운드 TCP/IP 데이터그램에 있어서 그와 같은 프로토콜 오류의 예로는 데이터그램이 송신된 X.25 연결 설정 실패가 있습니다. 이 경우 사용자에게 오류가 보고되며 아웃바운드 데이터그램은 삭제됩니다.

다음 조건이 모두 맞으면 인바운드 데이터그램이 제품 활동 기록부에 항목을 작성합니다.

- 프로토콜 오류 TCP/IP 속성 기록이 *YES로 설정되어 있습니다.
- RFC 1122에 지정된 TCP/IP 프로토콜 유효성 확인 테스트 중 하나가 실패함으로 인해 데이터그램이 시스템에서 삭제되었습니다(**무인 삭제**는 시작한 호스트 장치에 오류를 보고하지 않고 수신 데이터그램을 삭제한다는 것을 의미합니다). 그와 같은 데이터그램의 예로는 유효하지 않은 체크섬 또는 목적지 주소가 있는 데이터그램이 있습니다.

위에서 설명한 것처럼 데이터그램이 삭제되면 IP 및 TCP/UDP 데이터그램 헤더가 제품 활동 기록부 항목의 상세 자료에 기록됩니다. 이러한 제품 활동 기록부 항목의 참조 코드는 7004입니다.

© Copyright IBM Corp. 1997, 2002

Printed in U.S.A