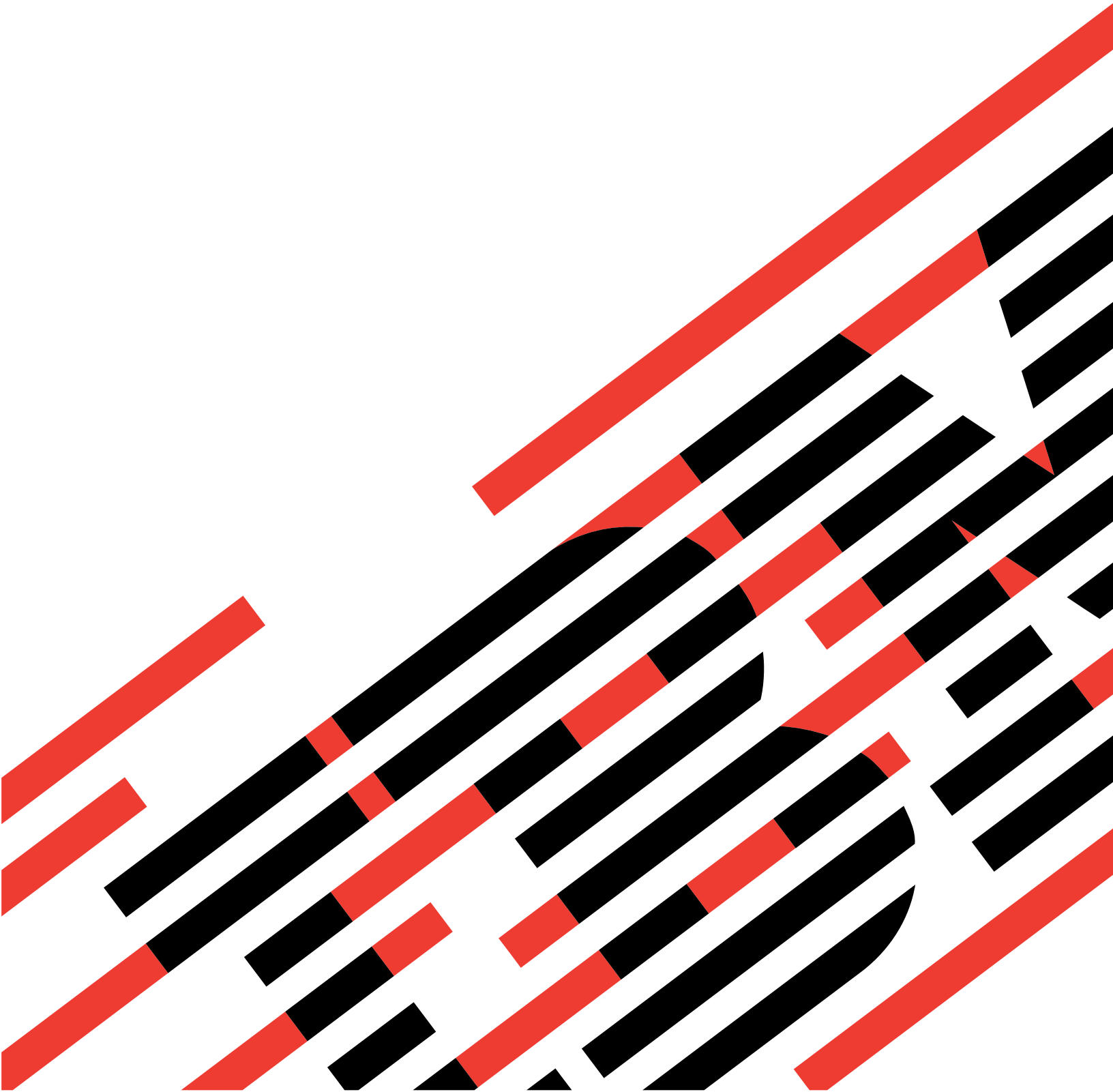
IBM

eserver

iSeries

Odstraňování problémů s TCP/IP

Verze 5



IBM

@server

iSeries

Odstraňování problémů s TCP/IP

Verze 5

Obsah

Kapitola 1. Odstraňování problémů s TCP/IP

Co brání fungování TCP/IP? Navrhli jste solidní síť a postupovali podle všech instrukcí, přesto jste se dostali do slepé uličky. Toto téma vás dovede k řešení.

Na tomto serveru jsou soustředěny prostředky k nalezení odpovědí na problémy s TCP/IP. Můžete mít obecný problém s připojitelností, který lze rychle identifikovat, nebo omezenější problém vyžadující důkladnější uvážení. K řešení problémů využijte níže uvedené nástroje.

Co je nového ve verzi V5R2?
V tomto tématu jsou uvedeny odkazy na nové a upravené metody odstraňování problémů s TCP/IP.

Tisk daného tématu
Toto téma slouží k vytisknutí nebo stažení příručky Odstraňování problémů s TCP/IP ve formátu PDF (Portable Document Format).

Obecné problémy s TCP/IP
Toto téma vám pomůže ověřit připojitelnost TCP/IP. Pomocí metody otázek a odpovědí se zaměříte na daný problém a použijete odkazy na možná řešení.

Problémy s určitými aplikacemi
Pokud víte, že se problém týká určité aplikace, například FTP nebo DNS, využijte toto téma, které obsahuje odkazy na konkrétní řešení týkající se této aplikace.

Trasování komunikace
Toto téma vás povede shromažďováním informací z trasování komunikace. Trasováním můžete izolovat chyby a najít cestu k řešení problému. Trasovací informace můžete využít sami nebo je můžete poskytnout odborníkům IBM, kteří vám při odstraňování problémů pomáhají.

Konfigurační soubory TCP/IP
V tomto tématu se naučíte, jak kopírovat konfigurační soubory TCP/IP. Tyto kopie budete muset poskytnout IBM, pokud se rozhodnete požádat o pomoc odborníka.

PAL (Product Activity Log)
V tomto tématu získáte informace o tom, jak využít PAL (Product Activity Log) k analýze problémů.

Co je nového ve verzi V5R2?

K novým položkám v tématu Odstraňování problémů s TCP/IP ve verzi V5R2 patří:

- **Obecné problémy s TCP/IP**
  V této kapitole naleznete způsoby, jak odstraňovat problémy související s protokolem Internetu verze 6 (IPv6).
- **Trasování komunikace**
  V této kapitole naleznete pokyny k provádění trasování komunikace pomocí CL příkazů. Tento nástroj k odstraňování problémů slouží ke sledování dat na komunikační lince a k lokalizaci zdroje problému.

Další informace o novinkách a změnách v této verzi najdete v dokumentu Sdělení pro uživatele  .

Tisk tohoto tématu

Chcete-li si prohlédnout nebo stáhnout PDF verzi, vyberte odkaz Odstraňování problémů s TCP/IP (asi 152 KB nebo 26 stran).

K uložení PDF souboru na vaši pracovní stanici za účelem prohlížení a tisku použijte tento postup:

1. Klepněte pravým tlačítkem myši v prohlížeči na odkaz na soubor PDF (klepněte pravým tlačítkem na výše uvedený odkaz).
2. Klepněte na **Save Target As... (Uložit cíl jako...)**.
3. Vyhledejte adresář, do kterého chcete PDF soubor uložit.
4. Klepněte na **Save** (Uložit).

Stažení aplikace Adobe Acrobat Reader

Potřebujete-li k prohlížení nebo tisku těchto souborů PDF aplikaci Adobe Acrobat Reader, můžete si její kopii stáhnout z webové stránky Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Kapitola 2. Obecné problémy s TCP/IP

V tomto tématu se postupně seznámíte s několika technikami odstraňování problémů. Tyto techniky slouží k izolování obecných problémů a ověření připojitelnosti TCP/IP. Pokud jste připojitelnost TCP/IP již ověřili a víte, že se problém týká určité aplikace, přejděte na kapitolu Problémy s určitými aplikacemi.

Počáteční analýza problémů s TCP/IP
Tato část obsahuje sérii pokynů a otázek, které vám pomohou určit příčinu problémů.

Pojednání o příkazu PING
Tyto informace slouží k lepšímu porozumění příkazu PING a jeho zvládnutí.

Práce s protokolem úlohy a frontami zpráv
Toto téma nabízí další možnost odstraňování problémů s TCP/IP.

Počáteční analýza problémů s TCP/IP

Tyto otázky a odpovědi vás povedou analýzou problémů a pomohou vám identifikovat problémy a určit řešení. K podrobnějšímu řešení problémů slouží odkazy na seznamy příčin.

1. Pomocí příkazu PING otestujte spojení s hostitelským systémem v lokální síti. Byli jste úspěšní?
   a. Ano. Přejděte na položku 2.
   b. Ne. Přejděte na Seznam příčin A.
2. Pomocí příkazu PING otestujte spojení se vzdáleným systémem. Byli jste úspěšní?
   a. Ano. Přejděte na položku 3.
   b. Ne. Přejděte na Seznam příčin B.
3. Ověřte, zda v podsystému QSYSWRK existují všechny nezbytné úlohy TCP/IP. Jsou tam všechny úlohy?
   a. Ano. Přejděte na položku 4.
   b. Ne. Přejděte na Seznam příčin C.
4. Pomocí příkazu NETSTAT ověřte, zda je rozhraní aktivní. Je rozhraní aktivní?
   a. Ano. Přejděte na položku 5.
   b. Ne. Přejděte na Seznam příčin D.
5. Pomocí TELNET nebo FTP ověřte, zda jsou přenosové cesty TCP/IP řádně nakonfigurovány. Pomocí příkazu NETSTAT také zkontrolujte, zde je vytvořeno připojení. Existuje připojení?
   a. Ano. Spusťte aplikaci.
   b. Ne. Přejděte na Seznam příčin E.

Seznam příčin A

Uvědomte si, že vzdálený systém může mít blokovány odpovědi ICMP. Pokud jsou odpovědi ICMP blokovány, odpověď vzdáleného systému nedostanete, i když máte spolehlivé spojení. Domníváte-li se, že to je ten problém, zkuste ověřit spojení s jinými systémy a mezi jinými systémy. Můžete tak určit nejpravděpodobnější místo chyby.

1. Ověřte, zda byl TCP/IP v systému aktivován.

   Chcete-li zajistit, aby byl balík TCP/IP aktivní, postupujte takto:
   a. Zadejte příkaz STRTCP. Pokud je TCP/IP aktivní, měli byste obdržet zprávu TCP1A04 (TCP/IP je v současné době aktivní). Pokud není TCP/IP aktivní, bude zadáním příkazu STRTCP aktivován TCP/IP na daném serveru. Ověřte, zda se při spuštění TCP/IP nevyskytly chyby.
   b. Používáte-li protokol IPv6, přejděte na část Řešení IPv6, kde najdete techniky odstraňování problémů související konkrétně s IPv6. Jinak pokračujte na další položce.

2. Ověřte software TCP/IP na serveru.

   K ověřování softwaru TCP/IP je na serveru vyhrazeno hostitelské jméno LOOPBACK a rozhraní s popisem linky *LOOPBACK. Zadáte-li hostitelské jméno LOOPBACK, nebudou na fyzické linky odesílána žádná data. Můžete tak rychle určit, zda software TCP/IP v systému funguje správně.

   Chcete-li ověřit software TCP/IP, postupujte takto:

   a. Zajistěte, aby lokální hostitelská tabulka obsahovala položku s hostitelským jménem LOOPBACK a internetovou adresou 127.0.0.1.

   b. Zajistěte, aby bylo aktivní rozhraní asociované s hostitelem LOOPBACK. S rozhraním LOOPBACK je obvykle asociována internetová adresa 127.0.0.1. Zajistěte, aby bylo nakonfigurováno rozhraní s IP adresou hostitelského jména LOOPBACK pomocí popisu linky *LOOPBACK. Pomocí příkazu

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

      zobrazte stav rozhraní LOOPBACK. Není-li aktivní, aktivujte je pomocí volby 9.

   c. Až ověříte, že je rozhraní hostitele LOOPBACK aktivní, napište:

      ```
      PING RMTSYS(LOOPBACK)
      ```

      Hostitel LOOPBACK umožňuje uživateli provádět tyto činnosti:

      - Testovat FTP, TELNET, LPR a uživatelské aplikační programy bez připojení k fyzické lince nebo síti.
      - Ověřit, zda je software TCP/IP nainstalován a zda správně funguje.

      Podobný test pomocí příkazu PING lze provést, chcete-li ověřit připojitelnost k některé jiné lokálně definované IP adrese.

   d. Chcete-li otestovat software a hardware (adaptér a připojení do sítě), zadejte internetovou adresu externího hostitelského systému ve vaší síti:

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

   e. Nemůžete-li úspěšně ověřit připojení systému do sítě zadáním jména systému nebo jeho internetové adresy, zkontrolujte zdrojový servisní přístupový bod (SSAP) popisu linky asociovaného s rozhraním. V seznamu SSAP (zdrojový servisní přístupový bod) musí být uvedena položka X'AA'. K tomu dojde standardně, je-li nový popis linky vytvořen s parametrem SSAP, který má předvolenou hodnotu *SYSGEN. Máte-li existující popis linky, použijte k přidání těchto hodnot do seznamu příkaz Změna popisu linky (Change Line Description).

      Některé typy popisů linky nemusejí mít SSAP pro TCP/IP, zkontrolujte proto seznam SSAP v popisu linky asociovaném s rozhraním.

   f. Ověřte všechny položky popisu linky, zejména velikost rámce, která by měla mít minimálně takovou hodnotu jako MTU (maximální přenosová jednotka) rozhraní.

   g. Pokud vzdálený systém nedokáže odpovídat, může to znamenat, že není dostupný nebo funkční systém, síť nebo komunikační můstek v síti. Selhání odpovědí může také znamenat, že ve vzdáleném systému jsou blokovány odpovědi ICMP. To může nastat, jestliže vzdálený systém funguje jako ochranná bariéra a byl nakonfigurován tak, aby neodpovídal na požadavky ICMP. Zkuste ověřit spojení s jinými systémy a mezi jinými systémy. Můžete tak určit nejpravděpodobnější místo chyby.

   h. Ověřte, zda je správně nakonfigurováno lokální rozhraní.

   i. Jestliže nelze rozhraní TCP/IP aktivovat (ani LOOPBACK) nebo nelze TCP/IP ukončit či spustit, zajistěte, aby byly v popisu podsystému QSYSWRK nakonfigurovány následující dvě směrovací položky. Pokud neexistují nebo nejsou správné, přidejte je nebo opravte a zopakujte požadavek.

      ```
      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)
```

Vraťte se k části Počáteční analýza problémů s TCP/IP a pokračujte v odstraňování problémů.

Řešení IPv6

Pokud máte problémy s komunikací IPv6, zkuste odstranit problémy se sítí pomocí těchto technik.

1. Ověřte, zda je spuštěn balík IPv6.
   a. Zajistěte, aby bylo rozhraní smyčkového testu (LOOPBACK) nakonfigurováno a bylo aktivní. Chcete-li zkontrolovat stav rozhraní smyčkového testu, proveďte následující kroky:
      1) V prostředí produktu iSeries Navigator rozbalte **Server —> Síť —> Konfigurace TCP/IP —> IPv6 —> Rozhraní**.
      2) V pravém podokně vyhledejte rozhraní smyčkového testu (LOOPBACK). IP adresa smyčkového testu (LOOPBACK) IPv6 je ::1 a jméno linky je Loopback 6. Pokud se rozhraní LOOPBACK v seznamu neobjeví, musíte je nakonfigurovat pomocí průvodce **konfigurací IPv6**.
   b. Otestujte (příkazem PING) adresu loopback (::1). Server pošle paket IPv6 sám sobě a ověří tak, zda balík IPv6 funguje. Při testování balíku IPv6 pomocí obslužného programu PING proveďte následující kroky:
      1) V prostředí produktu iSeries Navigator rozbalte **Server —> Síť**.
      2) Pravým tlačítkem myši klepněte na **Konfigurace TCP/IP**, klepněte na **Obslužné programy** a potom klepněte na **Testování spojení**.
2. Po ověření funkčnosti balíku IPv6 zajistěte, aby byla nakonfigurována a aktivní linka IPv6. Může to být linka typu Ethernet nebo nakonfigurovaná tunelová linka.

   Chcete-li zkontrolovat stav linek nakonfigurovaných na serveru, proveďte následující kroky:
   a. V prostředí produktu iSeries Navigator rozbalte **Server —> Síť —> Konfigurace TCP/IP —> Linky**.
   b. V pravém podokně vyhledejte linku, která má být nakonfigurována pro IPv6, a zkontrolujte stavový sloupec. Pokud se linka v seznamu neobjeví, musíte nakonfigurovat linku pro IPv6 pomocí průvodce **konfigurací IPv6**. Přejděte na téma Konfigurace IPv6, potřebujete-li pokyny ke konfiguraci linky pro IPv6. Pokud se linka v seznamu objeví a ukazuje stav **Nezavedeno**, je nakonfigurována, není však zavedena do konfigurace balíku IPv6. Problémy na lince můžete diagnostikovat v znakově orientovaném rozhraní pomocí příkazu WRKLIND (Práce s popisy linky).
3. Zajistěte, aby byla aktivní alespoň dvě rozhraní IPv6: lokální rozhraní a rozhraní, na které posíláte test spojení (PING).

   Chcete-li zkontrolovat stav rozhraní IPv6, proveďte následující kroky:
   a. V prostředí produktu iSeries Navigator rozbalte **Server —> Síť —> Konfigurace TCP/IP —> IPv6 —> Rozhraní**.
   b. V pravém podokně vyhledejte IP adresu asociovanou s lokálním rozhraním a zkontrolujte stav rozhraní.
   c. Pokud je rozhraní **Neaktivní**, musíte je aktivovat. Rozhraní budete aktivovat tak, že pravým tlačítkem myši klepnete na IP adresu a vyberete **Spustit**.
   d. Stejným postupem zkontrolujte stav vzdáleného rozhraní.

4. Pokud byl test spojení (příkazem PING) s adresou IPv6 neúspěšný, ověřte stav adresy obou rozhraní. Obě rozhraní by měla mít stav adresy **Preferovaná**. Jestliže cílové nebo zdrojové rozhraní není v preferovaném stavu, zvolte pro test jiná rozhraní nebo změňte stav a stav adresy používaných rozhraní na správný stav.

   Chcete-li ověřit nebo změnit stav adresy zdrojového rozhraní, proveďte následující kroky:

   a. V prostředí produktu iSeries Navigator rozbalte **Server —> Síť —> Konfigurace TCP/IP —> IPv6 —> Rozhraní**.

   b. V pravém podokně klepněte pravým tlačítkem myší na IP adresu asociovanou s rozhraním, vyberte volbu **Vlastnosti** a pak stránku **Volby**. Tento dialog umožňuje pro rozhraní zadat preferovanou nebo platnou dobu trvání.

   c. Stejným postupem zkontrolujte stav adresy cílového rozhraní.

Seznam příčin B

Jestliže byly příkazy VFYTCPCNN nebo PING vzhledem k lokálnímu systému úspěšné, měli byste ověřit možnost navázání spojení mezi vaším systémem a systémem, se kterým chcete komunikovat. Spusťte příkaz PING, jako jste to udělali předtím, tentokrát však zadejte internetovou adresu vzdáleného hostitelského systému. Informace najdete v části Běžné chybové zprávy. Uvědomte si, že vzdálený systém nebo mezilehlá ochranná bariéra mohou mít blokovány odpovědi ICMP. Pokud jsou odpovědi ICMP blokovány, odpověď vzdáleného systému nedostanete, i když máte spolehlivé spojení. Domníváte-li se, že to je ten problém, zkuste ověřit spojení s jinými systémy a mezi jinými systémy. Můžete tak určit nejpravděpodobnější místo chyby.

1. Můžete-li spojení ověřit pomocí vzdálené internetové adresy, nikoli však pomocí jména vzdáleného systému, není správné jméno nebo adresa v tabulce hostitelů nebo nejsou dostupné vzdálené servery jmen.
2. Používá-li váš systém vzdálené servery jmen, ověřte pomocí příkazu PING, ve kterém uvedete internetovou adresu vzdáleného serveru jmen, zda jsou tyto vzdálené servery jmen dosažitelné.
3. V příkazu PING lze zadat přídavné parametry, které umožňují uvést délku paketů, počet odesílaných paketů a dobu čekání na odpověď. Předvolená čekací doba 1 sekunda poskytuje vzdálenému systému ve většině sítí dostatek času k odpovědi. Pokud je však systém velmi vzdálený nebo je síť zatížená, můžete prodloužením čekací doby získat úspěšný výsledek.

   Doporučuje se ponechat předvolené hodnoty parametrů. Uvědomte si, že pokud je změníte, nemusí kombinace velké délky paketů a krátké čekací doby poskytnout síti dostatek času k přenosu a přijetí odpovědi, takže může docházet k překročení časového limitu. Nemá-li síť dostatek času k přenosu a přijetí odpovědi, může to vypadat, že se k systému nemůžete připojit, i když ve skutečnosti můžete.
4. Pokud vzdálený systém nedokáže odpovídat, může to znamenat, že není dostupný nebo funkční systém, síť, směrovač nebo můstek v síti. Selhání odpovědí může také znamenat, že ve vzdáleném systému nebo v pomocné ochranné bariéře jsou blokovány odpovědi ICMP. Zkuste ověřit spojení s jinými systémy a mezi jinými systémy. Můžete tak určit nejpravděpodobnější místo chyby.
5. Pokud se vzdálenému systému nedaří odpovídat na příkaz PING použitý k ověření rozhraní, které je nakonfigurováno na popis linky typu Ethernet, ujistěte se, zda je v popisu linky Ethernet uveden správný standard Ethernet nebo *ALL.
6. Chyby při získávání odpovědí od všech systémů v síti ukazují na to, že zádrhel je někde na cestě. Ověřte spojení s komunikační bránou vedoucí do dotyčné sítě. Pokud toto selže, postupujte zpět směrem od vzdáleného systému, kterého nemůžete dosáhnout, až najdete příčinu chyby.
7. Pakety jsou odesílány pomocí protokolu nízké úrovně, který nezaručuje doručení. Protože se může ztratit žádost o odezvu, nemůžete předpokládat, že selhala síť nebo komunikační brána, dokud se neúspěch při pokusu dostat se za určitý bod na cestě neprojeví u více příkazů.

Jestliže testování hostitelského systému ve vzdálené síti pomocí příkazu PING selže, použijte na stejnou síť příkaz pro trasování přenosové cesty (TRACEROUTE). Obslužný program pro trasování přenosové cesty může provádět mnoho stejných testů připojitelnosti jako jednotlivé příkazy PING, avšak najednou v jednom

kroku. Při trasování přenosové cesty budou testovány všechny směrovací uzly na cestě k vzdálenému cíli a bude indikováno, zda se problém týká mezilehlého směrovače nebo vzdálené sítě.

Napište TRACEROUTE RMTSYS('x.x.x.x'). Vzdálený systém můžete zadat pomocí IP adresy nebo jména vzdáleného systému; například ('xxxx.xxxx.com'). Obslužný program pro trasování přenosové cesty přijímá jak formát adresy IPv4 ('x.x.x.x'), tak formát adresy IPv6 ('x:x:x:x:x:x:x:x').

Trasování přenosové cesty je také dostupné z prostředí produktu iSeries Navigator. Chcete-li spustit trasování přenosové cesty, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator rozbalte Server —> **Síť**.
2. Pravým tlačítkem myši klepněte na **Konfigurace TCP/IP**, vyberte **Obslužné programy** a pak **Trasovat přenosovou cestu**.

Vraťte se k části Počáteční analýza problémů s TCP/IP a pokračujte v odstraňování problémů.

Seznam příčin C

1. Ověřte, zda na serveru v podsystému QSYSWRK existují všechny nezbytné úlohy (lokální nebo vzdálené). Měla by tam být alespoň úloha QTCPIP. Úloha QTCPIP řídí spouštění a ukončování rozhraní TCP/IP. Také by měla existovat alespoň jedna úloha pro každou aplikaci, kterou se pokoušíte použít, jak ukazuje Obrázek 1 na stránce 8. Tyto úlohy pravděpodobně nebudou pojmenovány shodně jako úlohy podsystému FTP, LPD a TELNET. Jména všech úloh FTP začínají QTFTP. Jména všech úloh LPD začínají QTLPD. Všechny úlohy TELNET budou pojmenovány QTVTELNET nebo QTVDEVICE. Je možné mít více než jednu úlohu serveru FTP, LPD nebo TELNET. Jména všech úloh SMTP začínají QTSMTP. V podsystému QSYSWRK jsou aktivní až čtyři úlohy SMTP, v podsystému QSNADS jsou aktivní dvě úlohy. Jména všech úloh SNMP začínají QTMSNMP. V podsystému QSYSWRK mohou být aktivní tři úlohy SNMP - QTMSNMP, QTMSNMPRCV a QSNMPSA.

   K zobrazení těchto úloh použijte příkaz WRKACTJOB (Práce s aktivními úlohami). Napište WRKACTJOB SBS(QSYSWRK).
2. Pokud neexistují všechny úlohy, ukončete pomocí příkazu ENDTCP OPTION(*IMMED) zpracování TCP/IP. Vyhledejte všechny protokoly úloh asociované s úlohami.
3. Změňte úroveň protokolování zpráv u popisů úloh pro všechny objekty popisů úloh na 4 0 *SECLVL. Podrobné informace o úrovních protokolování zpráv najdete v části Práce s protokolem úlohy a frontami zpráv.
4. Pomocí příkazu STRTCP spusťte znovu zpracování TCP/IP.
5. Ověřte, zda jsou aktivní všechny úlohy.
6. Pokud nejsou odpovídající úlohy aktivní, zkontrolujte protokoly úloh.

```
                Work with Active Jobs             SYSNAM03

                                    02/03/99  18:06:32
CPU %:     .8     Elapsed time:   02:21:32     Active jobs:   93

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect ...

Opt  Subsystem/Job  User        Type  CPU %  Function        Status
     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
                                                                More...
Parameters or command
===>
F3=Exit   F5=Refresh       F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys
```

Obrázek 1. Obrazovka Work with Active Jobs - obrazovka 1

```
                Work with Active Jobs             SYSNAM03
                                    02/03/99  18:06:32
CPU %:     .8     Elapsed time:   02:21:32     Active jobs:   93

Type options, press Enter.
  2=Change   3=Hold   4=End   5=Work with   6=Release   7=Display message
  8=Work with spooled files   13=Disconnect ...

Opt  Subsystem/Job  User        Type  CPU %  Function        Status
       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
                                                                More...
Parameters or command
===>
F3=Exit   F5=Refresh       F7=Find      F10=Restart statistics
F11=Display elapsed data   F12=Cancel   F23=More options   F24=More keys
```

Obrázek 2. Obrazovka Work with Active Jobs - obrazovka 2

Vraťte se k části Počáteční analýza problémů s TCP/IP a pokračujte v odstraňování problémů.

Seznam příčin D

Funkce pro zjištění stavu sítě (NETSTAT) na serveru umožňuje zobrazit stav rozhraní TCP/IP, informace o konfiguraci přenosové cesty TCP/IP a stav spojení TCP/IP v lokálním systému. Můžete použít buď příkaz WRKTCPSTS, nebo příkaz NETSTAT.

1. Než funkci pro zjištění stavu sítě použijete, spusťte TCP/IP pomocí příkazu STRTCP. Menu Work with TCP/IP Network Status se zobrazí, ale volby nebudou funkční, dokud nespustíte TCP/IP.

2. Pokud se na obrazovce Work with TCP/IP Interface Status pokusíte spustit aktivní rozhraní nebo ukončit neaktivní rozhraní, bude odeslána odpovídající chybová zpráva. Jestliže vyberete volbu pro spuštění neaktivního rozhraní a toto rozhraní nepřejde do aktivního stavu, mohou být problémy s rozhraním, linkou nebo konfigurací linky. Podívejte se do protokolu úlohy QTCPIP v podsystému QSYSWRK, jaké chyby se mohly při aktivaci rozhraní vyskytnout. Při určování stavu vám může pomoci také zobrazení fronty zpráv QSYSOPR a protokolu historie QHT (DSPLOG).
3. Chcete-li určit, zda problém není v popisu linky, napište WRKCFGSTS *LIN.
4. Ověřte, zda je pro každý ze serverů na obrazovce Work with TCP/IP Connection Status (volba 3 z obrazovky Work with TCP/IP Network Status) zobrazeno alespoň jedno pasivní naslouchající spojení. Stav spojení byste měli ověřit u serverů podporujících tyto aplikace a u všech souvisejících serverů v síti:

   SNMP

   TELNET

   Verze 4 vydání 4 podporuje kromě protokolu Telnet také protokol SSL Telnet. SSL Telnet standardně používá naslouchající port 992, tradiční Telnet používá port 23. Doporučeným přístupem při zablokování tradičního serveru Telnet je omezení naslouchajících portů Telnet a současné povolení protokolu SSL Telnet.

   FTP

   SMTP, je-li nakonfigurován

   POP

   LPD

   REXEC

   HTTP, je-li nakonfigurován

   Pasivní naslouchající spojení mají v polích *Remote Address* a *Remote Port* hvězdičku. Ukončení těchto spojení se nedoporučuje. Pokud by byla asociovaná pasivní naslouchající spojení ukončena, nemohly by vzdálené systémy používat protokol SNMP, FTP nebo TELNET, posílat do lokálního systému poštu SMTP nebo posílat pomocí LPR do lokálního systému soubory určené pro souběžný tisk. Tato spojení mohou být znovu spuštěna tak, že ukončíte a spustíte servery pomocí příkazů ENDTCPSVR a STRTCPSVR, ve kterých uvedete server, který má být ukončen a spuštěn.
5. Zajistěte, aby nebyly omezeny porty asociované s aplikací, kterou se pokoušíte použít. K zobrazení aktuálních omezení portů použijte volbu 4 (Work with TCP/IP port restrictions) z menu Configure TCP/IP.

Vraťte se k části Počáteční analýza problémů s TCP/IP a pokračujte v odstraňování problémů.

Seznam příčin E

Ověřte konfigurační data. Pokud je vše v pořádku, přejděte na kapitolu Problémy s určitými aplikacemi a zvolte konkrétní aplikaci, kterou používáte a se kterou potřebujete pomoci při odstraňování problémů.

Pojednání o příkazu PING

V následujících částech se dozvíte další informace o příkazu PING.

Přidání jména domény ke jménu hostitele
Tato část pojednává o tom, jak server přidává jméno domény ke jménu hostitele.

Běžné chybové zprávy
V této části jsou uvedeny příklady některých nejčastějších chybových stavů při použití příkazu PING.

Přidání jména domény ke jménu hostitele

Tento příklad ilustruje, jak server používá jméno lokální domény jako seznam hledání a přidává jména domén ke jménu hostitele, není-li na konci jména domény uvedena tečka.

Dejme tomu, že jméno vašeho serveru je SYSNAM01.A400SSC.DFW.COMPANY.COM a chcete ověřit spojení se systémem, jehož úplné jméno je SYSNAM02.DFW.COMPANY.COM. V lokální hostitelské tabulce není hostitelské jméno SYSNAM02 uvedeno.

Napíšete-li příkaz PING SYSNAM02.DFW.COMPANY.COM, server pošle vzdálenému serveru jmen SYSNAM02.DFW.COMPANY.COM.

Napíšete-li příkaz PING SYSNAM02, server pošle vzdálenému serveru jmen nejdříve SYSNAM02.A400SSC.DFW.COMPANY.COM. Potom pošle SYSNAM02.DFW.COMPANY.COM. Nebude-li toto jméno nalezeno, server nakonec pošle SYSNAM02.COMPANY.COM. Jinak řečeno, iSeries TCP/IP přidává postupně k hostitelskému jménu každou část jména lokální domény.

Napíšete-li příkaz PING SYSNAM02., vzdálený server jmen ohlásí, že hostitelský systém je neznámý. Vzdálený server jmen jméno SYSNAM02 nerozpozná, protože server mu poslal jméno SYSNAM02 bez jakékoli přidané části seznamu hledání. Jediným rozdílem mezi tímto jménem a předchozím jménem v příkazu PING je tečka na konci jména.

Běžné chybové zprávy

Použijete-li příkaz PING k ověření spojení s jiným hostitelským systémem v síti, může TCP/IP vydat chybovou zprávu. Pomocí následující tabulky můžete identifikovat běžné chybové zprávy a určit postup řešení problémů.

Chybová zpráva	Doporučený postup
No TCP/IP service available	• TCP/IP nebyl dosud spuštěn nebo nebylo spouštění dokončeno. Pomocí příkazu NETSTAT zjistěte, zda je TCP/IP aktivní. • V podsystému QSYSWRK pravděpodobně nebyly spuštěny všechny úlohy. Ověřte pomocí příkazu WRKACTJOB (Práce s aktivními úlohami), zda je aktivní podsystém QSYSWRK i související úlohy. Nejsou-li aktivní, podívejte se, zda protokol úlohy nebo předvolená výstupní fronta systému neobsahuje nějaké zprávy.
Not able to establish connection with remote host system	Zkontrolujte nakonfigurovaná rozhraní, jejich související popisy linek a přenosové cesty TCP/IP.
Cannot reach remote system	TCP/IP nemohl najít přenosovou cestu k požadovanému cíli. Vyberte v NETSTAT volbu 2 a ověřte, zda cesta *DFTROUTE nebo ekvivalentní předepsaná cesta k síti byla nakonfigurována a je aktivní.
Remote host did not respond to VFYTCPCNN within 10 seconds for connection verification 1.	• Konfigurace je pravděpodobně správná, nedostáváte však odpověď vzdáleného systému. Zajistěte, aby vzdálený hostitelský systém mohl dosáhnout váš systém. Zavolejte operátora vzdáleného systému a požádejte ho, aby ověřil spojení s vaším systémem. • Zkontrolujte hostitelské tabulky nebo vzdálený server jmen (používáte-li server jmen) v obou systémech a rozhraní i přenosové cesty TCP/IP. Vzdálený server jmen vám pravděpodobně z nějakých důvodů nemůže poskytovat služby. • Používáte-li linku Ethernet, ujistěte se, že jste zadali správný standard Ethernet nebo *ALL.
VFYTCPCNN: Unknown host, xxxxxx, kde xxxxxx je hostitelské jméno.	Hostitelské jméno nebylo možné převést na IP adresu pomocí hostitelské tabulky nebo serveru jmen. Zkontrolujte v lokální hostitelské tabulce nebo u vzdálených serverů jmen (používáte-li server jmen) položku popisující vzdálený hostitelský systém.

Práce s protokolem úlohy a frontami zpráv

TCP/IP je dodáván s několika popisy úloh.

Popisy úloh jsou uloženy v knihovně QSYS nebo QTCP. Obecně jsou dodávány s úrovní protokolování zpráv 4, závažností protokolování zpráv 0 a hodnotou textu protokolování zpráv *NOLIST. S těmito hodnotami jsou dodávány proto, aby vytvořené protokoly úloh neobsahovaly pouze zprávy o spuštění a ukončení úloh.

Máte-li problémy s činností TCP/IP, měli byste jako jednu z prvních věcí změnit úroveň protokolování zpráv u popisu úlohy pro aplikaci, se kterou máte problémy, na hodnotu textu protokolování zpráv *SECLVL. Změníte-li úroveň protokolování zpráv, bude pro danou aplikaci vygenerován protokol úlohy. K tomu, aby se změna projevila, musíte ukončit a znovu spustit server. Chcete-li změnit úlohu okamžitě, použijte ke změně úrovně protokolování zpráv aktivní úlohy příkaz CHGJOB.

Chcete-li změnit úroveň protokolování zpráv u popisu úlohy pro konkrétní aplikaci, podívejte se na tyto příklady:

- Pokud je problém se serverem FTP, změňte popis úlohy QTMFTPS napsáním tohoto CL příkazu:
  ```
  CHGJOBD  JOBD(QTCP/QTMFTPS)  LOG(4 0 *SECLVL)
  ```
- Pokud je problém se SMTP, změňte popis úlohy QTMSMTPS napsáním tohoto CL příkazu:
  ```
  CHGJOBD  JOBD(QTCP/QTMSMTPS)  LOG(4 0 *SECLVL)
  ```

  Kromě popisu úlohy QTMSMTPS byste měli uvážit změnu úrovně protokolování popisu úlohy podsystému QSNADS napsáním tohoto CL příkazu:
  ```
  CHGJOBD  JOBD(QGPL/QSNADS)  LOG(4 0 *SECLVL)
  ```

Kapitola 3. Problémy s určitými aplikacemi

Pokud jste zjistili, že se problém týká určité aplikace používající TCP/IP, zvolte níže uvedenou aplikaci a seznamte se s podrobnými informacemi o odstraňování problémů. Každý odkaz vás zavede na obecný server věnovaný odstraňování problémů s TCP/IP, odkud se dostanete na server vyhrazený zvolené aplikaci.

Server DNS (Domain Name System)
Toto téma nabízí vývojový diagram pro analýzu problémů a provede vás strategiemi odstraňování problémů s DNS.

FTP (File Transfer Protocol)
Toto téma nabízí řešení problémů s FTP a předvádí protokol úlohy serveru v roli nástroje pro odstraňování problémů.

PPP (Point-to-Point Protocol)
Toto téma nabízí řešení běžných problémů s připojením realizovaným protokolem PPP.

Server POP (Post Office Protocol)
Na toto téma přejděte, chcete-li odstraňovat problémy se serverem POP a dalšími aplikacemi elektronické pošty.

Rexec
Toto téma nabízí vývojový diagram, který vám pomůže zaměřit se na problém se serverem Rexec a najít možná řešení.

SMTP (Simple Mail Transfer Protocol)
Toto téma nabízí několik metod pro řešení problémů se serverem SMTP (Simple Mail Transfer Protocol) a dalšími aplikacemi elektronické pošty.

Telnet
Toto téma vám pomůže při řešení obecných problémů s protokolem Telnet i specifických problémů souvisejících s typem emulace a serverem SSL. Kromě toho zjistíte, které informace jsou nezbytné při nahlašování problémů.

VPN (Virtual Private Networking)
Toto téma vás provede několika strategiemi odstraňování problémů s VPN, souvisejících se spojením, chybami konfigurace, filtrovacími pravidly a podobně.

Kapitola 4. Trasování komunikace

Trasování komunikace slouží k odstraňování problémů s TCP/IP. Trasování komunikace je obslužná funkce, která umožňuje sledovat tok dat komunikační linkou, například lokální sítí (LAN) nebo dálkovou sítí (WAN). Po shromáždění trasovacích dat mohou být prvotní data vypsána do proudového souboru nebo mohou být formátována a umístěna do souboru pro souběžný tisk a potom zobrazena nebo vytištěna.

Trasování komunikace může být využito k odstraňování problémů s komunikací IPv4 i IPv6.

Trasování komunikace je vhodné použít v těchto situacích:

- Procedury analýzy problémů neposkytly o problému dostatek informací.
- Domníváte se, že problém je způsoben narušením protokolu.
- Domníváte se, že problém je způsoben šumem na lince.
- Chcete vědět, zda aplikace přenáší správně informace po síti.
- Chcete vědět, zda máte výkonnostní problémy se zahlcením sítě nebo propustností dat.

K tomu, abyste mohli pomocí CL příkazů provádět trasování komunikace, musíte mít zvláštní oprávnění *SERVICE nebo oprávnění k funkci Trasování služby licencovaného programu Operating System/400 v prostředí produktu iSeries Navigator. Další informace o tomto typu oprávnění najdete v kapitole o uživatelských profilech v příručce iSeries Security Reference .

Příkaz TRCCNN (Trace Connection) je alternativní metodou získání trasovacích informací, které se podobají trasování komunikace. Máte-li aplikace TCP používající SSL nebo používáte-li zabezpečení IP, jsou data přenášená komunikační linkou kódovaná. Potřebujete-li data zobrazit, trasování komunikace nepomůže. Příkaz TRCCNN trasuje data před jejich zakódováním a po jejich dekódování, a může být proto použit tam, kde není obecné trasování komunikace účinné. Poskytuje výstup podobný výstupu obecného trasování komunikace. Parametry a příklady vztahující se k tomuto příkladu najdete v popisu příkazu TRCCNN (Trace Connection) v tématu věnovaném rozhraním API (Application Programming Interface).

Chcete-li použít funkci trasování komunikace, proveďte následující kroky:

Plánování trasování komunikace
Dříve než můžete provést trasování komunikace, je nutné podniknout přípravné kroky.

Provedení trasování komunikace
Tato část obsahuje kroky potřebné k provedení trasování komunikace.

Další funkce trasování komunikace
Tato část popisuje další funkce vztahující se k trasování komunikace.

Plánování trasování komunikace

Dříve než zahájíte trasování komunikace, proveďte následující kroky:

1. Pokud jste nevytvořili knihovnu IBMLIB nebo výstupní frontu IBMOUTQ, zadejte tyto příkazy:
   ```
   CRTLIB LIB(IBMLIB)
   CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
   ```
2. Přidejte knihovnu IBMLIB do seznamu knihoven a změňte výstupní frontu úlohy na výstupní frontu IBMOUTQ pomocí těchto příkazů:
   ```
   ADDLIBLE IBMLIB
   CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
   ```
3. Pokud v systému neexistuje tiskový soubor QTCPPRT, vytvořte ho pomocí těchto příkazů:

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

4. Odešlete soubor pro souběžný tisk QTCPPRT obsahující informace získané trasováním komunikace do výstupní fronty IBMOUTQ v knihovně IBMLIB pomocí těchto příkazů:

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

   Přesměrování tiskového souboru přestane platit po skončení úlohy.
5. Získejte jméno popisu linky asociovaného s rozhraním TCP/IP, se kterým jsou problémy nebo které využívá aplikace či síť, se kterou jsou problémy. K určení jméno popisu linky asociovaného s rozhraním použijte příkaz NETSTAT *IFC.
6. Zajistěte, aby byla linka logicky zapnuta a aby bylo spuštěno rozhraní TCP/IP asociované s linkou, aby tak bylo možné rozhraním a linkou odesílat a přijímat data TCP/IP. K ověření toho, zda je rozhraní aktivní, použijte příkaz NETSTAT *IFC.

Další krok:
Provedení trasování komunikace.

Provedení trasování komunikace

Chcete-li provést trasování komunikace, musíte použít CL příkazy ve znakově orientovaném rozhraní. Trasování komunikace se skládá z těchto kroků:

1. Spuštění trasování komunikace.
2. Ukončení trasování komunikace.
3. Výpis výsledků trasování komunikace.
4. Tisk výsledků trasování komunikace.
5. Zobrazení obsahu výsledků trasování komunikace.
6. Čtení výsledků trasování komunikace.

Spuštění trasování komunikace

Při této akci spustíte trasování komunikace pro zadanou linku nebo popis síťového rozhraní.

Poznámka: Trasování komunikace pravděpodobně již nebude možné provést pro popis síťového serveru (*NWS). Funkci trasování komunikace použijte k trasování dat na určité lince (*LIN) nebo pro určitý popis síťového rozhraní (*NWI).

Chcete-li spustit trasování komunikace, proveďte následující kroky:

1. Na příkazové řádce zadejte příkaz STRCMNTRC.
2. V parametru **Configuration object** zadejte jméno linky, například TRNLINE.
3. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.
4. V parametru **Buffer size** zadejte dostatečné množství paměti pro předpokládaný objem dat. U většiny protokolů je 8 MB dostatečná paměť. Pro síť typu Ethernet 10/100 stačí 16 MB až 1 GB. Pokud váháte, uveďte jako maximální množství paměti povolené pro daný protokol hodnotu 16 MB.
5. V parametru **Communications trace options** zadejte *RMTIPADR, pokud chcete, aby bylo shromažďování dat omezeno na trasování jednoho vzdáleného rozhraní. Jinak použijte předvolenou hodnotu.
6. V parametru **Remote IP address** zadejte IP adresu přiřazenou vzdálenému rozhraní, pro které mají být shromažďována trasovací data.

Trasování komunikace bude probíhat, dokud nebude splněna některá z těchto podmínek:

- Bude proveden příkaz ENDCMNTRC.
- Problém s fyzickou linkou způsobí konec trasování.
- Parametr **Trace full** má hodnotu *STOPTRC a dojde k zaplnění vyrovnávací paměti.

Další krok:
Ukončení trasování komunikace.

Ukončení trasování komunikace

K tomu, abyste mohli naformátovat a zobrazit výsledky trasování, musíte nejdříve trasování ukončit. Při této akci bude trasování ukončeno a vyrovnávací paměť trasování komunikace bude uložena.

Chcete-li ukončit trasování komunikace, proveďte následující kroky:

1. Na příkazové řádce zadejte příkaz ENDCMNTRC.
2. V parametru **Configuration object** zadejte stejnou linku, kterou jste uvedli při spuštění trasování, například TRNLINE.
3. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.

Další krok:
Proveďte výpis výsledků trasování komunikace do proudového souboru. Je to volitelný krok, který může být prospěšný. Chcete-li raději prvotní data vytisknout, aniž byste prováděli jejich výpis do proudového souboru, přejděte na část Tisk výsledků trasování komunikace.

Výpis výsledků trasování komunikace

Používáte-li protokol Internetu verze 6 (IPv6), musíte níže uvedeným postupem vypsat trasovací data do proudového souboru. Pokud však používáte protokol IPv4, je tento výpis pouze volitelnou částí procesu trasování komunikace.

Výpis dat do proudového souboru přináší různé výhody. Při rozhodování, zda tuto funkci použít, uvažte tyto její výhody:

- Při spuštění nových trasování neztratíte data z již provedeného trasování.
- Trasovací data můžete formátovat vícekrát. Jestliže například jedna z aplikací používá kód ASCII, můžete výsledky trasování komunikace nejprve naformátovat do ASCII. Pokud jiná aplikace používá kód EBCDIC, můžete stejná trasovací data naformátovat do EBCDIC. Vypsáním trasovacích dat do proudového souboru získáte možnost formátovat tato data dvakrát.
- Trasovací data můžete uchovat i po spuštění IPL.
- Ke generování výstupu můžete použít uživatelský formátovací program.

Chcete-li vypsat výsledky trasování komunikace, proveďte následující kroky:

1. Vytvořte adresář, například mydir. Informace o tom, jak vytvořit adresář, najdete v popisu příkazu CRTDIR (Create Directory) v tématu popisujícím jazyk CL.
2. Na příkazové řádce zadejte příkaz DMPCMNTRC.
3. V parametru **Configuration object** zadejte stejnou linku, kterou jste uvedli při spuštění trasování, například TRNLINE.
4. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.
5. V parametru **To stream file** zadejte jméno souboru včetně cesty, například /mydir/mytraces/trace1.

Další krok:
Tisk výsledků trasování komunikace.

Tisk výsledků trasování komunikace

Data získaná trasováním komunikace můžete tisknout ze dvou různých zdrojů podle toho, jakým způsobem jste shromáždili výsledky trasování. Buďto můžete k tisku použít shromážděná prvotní data, nebo proudový soubor, do kterého jste prvotní data vypsali.

Poznámka: K tomu, abyste mohli data získaná trasováním komunikace tisknout z proudového souboru, musíte mít v systému nainstalován produkt Java (5722JV1).

Při této akci budou data získaná trasováním určité linky nebo popisu síťového rozhraní zapsána do souboru pro souběžný tisk nebo do výstupního souboru.

Tisk ze shromážděných prvotních dat:

Pokud jste prvotní data shromáždili a nevypsali je do proudového souboru, postupujte při tisku dat takto:

1. Na příkazové řádce zadejte příkaz PRTCMNTRC.
2. V parametru **Configuration object** zadejte stejnou linku, kterou jste uvedli při spuštění trasování, například TRNLINE, a stiskněte klávesu Enter.
3. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.
4. V parametru **Character code** zadejte buď *EBCDIC, nebo *ASCII. Budete-li chtít použít oba kódy, musíte data vytisknout dvakrát - poprvé zadáte *EBCDIC a potom zadáte *ASCII.
5. V parametru **Format TCP/IP data** zadejte *YES a dvakrát stiskněte klávesu Enter.
6. Zopakujte kroky 1 až 5, zadejte však jiný kód znaků.

Tisk z proudového souboru:

Pokud jste data vypsali do proudového souboru, postupujte při tisku dat takto:

1. Na příkazové řádce zadejte příkaz PRTCMNTRC.
2. V parametru **From stream file** zadejte jméno souboru včetně cesty, například /mydir/mytraces/trace1, a stiskněte klávesu Enter.
3. V parametru **Character code** zadejte buď *EBCDIC, nebo *ASCII. Budete-li chtít použít oba kódy, musíte data vytisknout dvakrát - poprvé zadáte *EBCDIC a potom zadáte *ASCII.
4. V parametru **Format TCP/IP data** zadejte *YES a dvakrát stiskněte klávesu Enter.
5. Zopakujte kroky 1 až 4, zadejte však jiný kód znaků.

Další krok:
Zobrazení obsahu výsledků trasování komunikace.

Zobrazení obsahu výsledků trasování komunikace

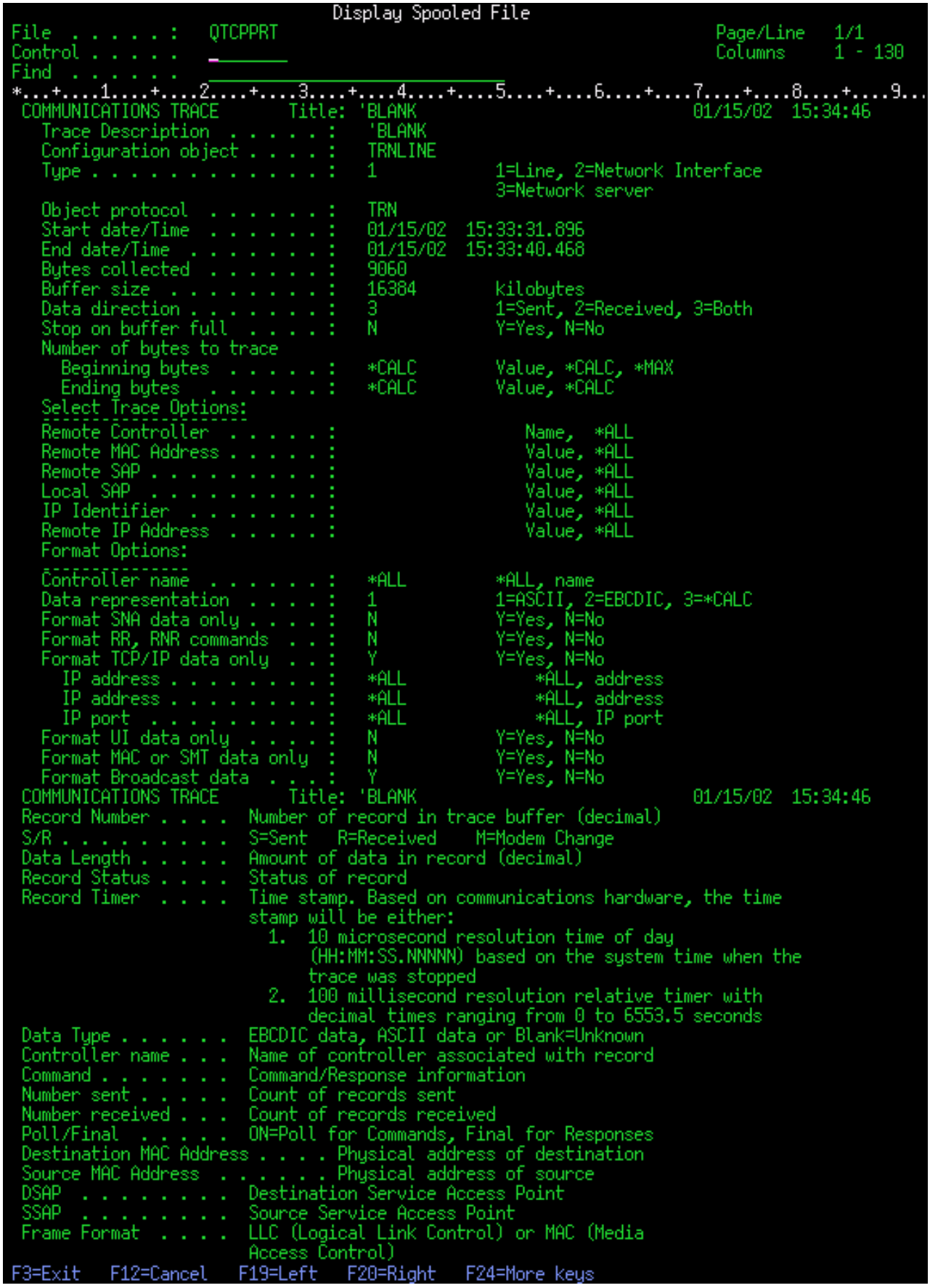
Chcete-li zobrazit výsledky trasování komunikace, proveďte následující kroky:

1. Na příkazové řádce zadejte příkaz WRKOUTQ OUTQ(IBMLIB/IBMOUTQ).
2. V dialogu **Work with Output Queue** stiskněte klávesu F11 (View 2). Zobrazíte tak datum a čas souboru pro souběžný tisk, se kterým chcete pracovat. Pokud se na obrazovce objeví More... a potřebujete pokračovat v hledání souboru pro souběžný tisk, listujte v seznamu souborů dopředu nebo dozadu. Jinak přejděte na další krok.
3. U souboru pro souběžný tisk, který chcete zobrazit, zadejte do sloupce **Opt** hodnotu 5. Nejnovější výsledky trasování komunikace jsou obsaženy v posledních souborech.
4. Ověřte, zda se jedná o výsledky trasování komunikace požadované linky a zda jsou správné časy spuštění a ukončení trasování.

Další krok:
Čtení výsledků trasování komunikace.

Čtení výsledků trasování komunikace

Výsledky trasování komunikace obsahují několik typů údajů. V první části výsledků trasování komunikace jsou shrnuty parametry, které jste zadali při spuštění trasování, například jméno konfiguračního objektu (**Configuration object**). Budete-li listovat dolů, najdete seznam položek, například **Record Number** a **S**/**R**, spolu s připojenými definicemi. Tyto položky představují nadpisy, které jsou dále použity k označení sekcí dat získaných trasováním komunikace. Při čtení trasovacích dat může být prospěšné tento seznam využívat. Následující obrázek ukazuje úvodní informace v zobrazení výsledků trasování komunikace.


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

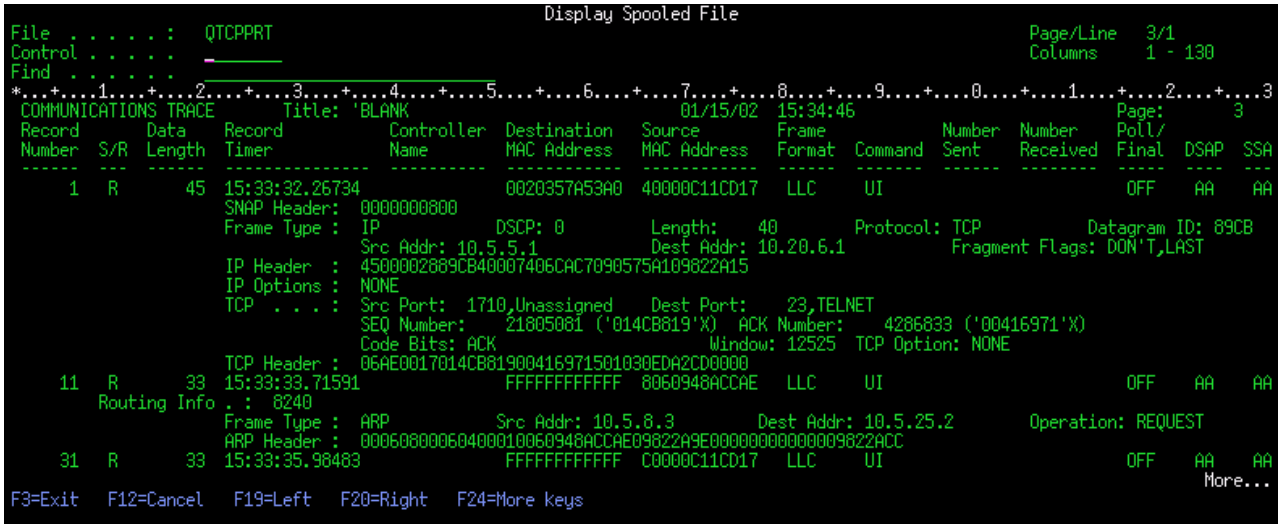
Po přečtení úvodních informací listujte ve výsledcích trasování komunikace dolů k vlastním datům TCP/IP. Jednotlivé sekce záznamů dat jsou označeny řádkou nadpisů, kde prvním nadpisem je vždy **Record Number** (číslo záznamu). Každé číslo záznamu uvádí rámec, který obsahuje takové informace, jako je zdrojová a cílová IP adresa, délka úplného IP datagramu, typ služby (TOS), zdrojový a cílový port nebo čísla ACK. Tyto informace by vám měly pomoci při odstraňování problémů, které máte s TCP/IP na tomto serveru iSeries nebo v přidružené síti.

Pokud je za číslem záznamu uvedena hvězdička (*), například 31*, znamená to, že chybějí trasovací data; to nastane, když jsou vypuštěny záznamy trasování komunikace. Data z trasování komunikace jsou shromažďována vstupním/výstupním procesorem (IOP). Pokud je komunikační linka velmi zatížena, IOP začne síťovému provozu udělovat priority a vyšší prioritu dává vstupní a výstupní cestě dat než informacím z trasování komunikace. Za těchto okolností může IOP některé ze záznamů trasování komunikace vypustit. Může to signalizovat, že IOP nedokáže zpracovat nadměrné rychlosti nebo provoz v síti.

Pokud ve výsledcích trasování komunikace chybějí data, uvažte tyto možnosti:

- Pouze vezměte na vědomí, že komunikační linka je zatížena a že ve výsledcích trasování komunikace budou chybět rámce.
- Prozkoumejte provoz na komunikační lince a snažte se zjistit, zda nelze některou část provozu převést na jinou linku nebo rozhraní TCP/IP.

Tento obrázek ukazuje datovou část výsledků trasování komunikace TCP/IP.



Proces trasování komunikace byl dokončen.

Chcete-li zjistit, jak vymazat výsledky trasování, zkontrolovat stav trasování nebo určit paměťový prostor, přejděte na část Další funkce trasování komunikace.

Další funkce trasování komunikace

Tyto příkazy a rozhraní API poskytují další funkce pro trasování komunikace.

Vymazání výsledků trasování komunikace

Dříve než spustíte na stejné lince nové trasování komunikace, musíte vymazat výsledky trasování komunikace provedené pro tuto linku. Výsledky trasování komunikace lze vymazat po ukončení trasování. Při této akci bude vymazána vyrovnávací paměť s výsledky trasování komunikace pro zadanou linku nebo popis síťového rozhraní.

Chcete-li vymazat výsledky trasování komunikace, proveďte následující kroky:

1. Na příkazové řádce zadejte příkaz DLTCMNTRC.
2. V parametru **Configuration object** zadejte jméno linky, například TRNLINE.
3. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.

Kontrola trasování komunikace

Pravděpodobně budete chtít zjistit, zda na serveru v současné době existují trasování komunikace. Chcete-li zjistit stav trasování komunikace pro určitou linku nebo popis síťového rozhraní, případně pro všechna trasování určitého typu existující na serveru, použijte příkaz CHKCMNTRC (Check Communications Trace). Stav bude vrácen ve formě zprávy.

Chcete-li zkontrolovat stav trasování komunikace, proveďte následující kroky:

1. Na příkazové řádce zadejte příkaz CHKCMNTRC.
2. V parametru **Configuration object** zadejte jméno linky, například TRNLINE, anebo zadejte *ALL, chcete-li zkontrolovat stav všech trasování určitého typu.
3. V parametru **Type** zadejte typ prostředku, a to buď *LIN, nebo *NWI.

Programová kontrola paměťového prostoru

Chcete-li programově zkontrolovat maximální prostor přidělený trasováním a velikosti (v bajtech) všech trasování v aktivním nebo zastaveném stavu na serveru, použijte rozhraní API QSCCHKCT (Check Communications Trace). Další informace o rozhraní API QSCCHKCT (Check Communications Trace) najdete v tématu věnovaném rozhraním API.

Kapitola 5. Konfigurační soubory TCP/IP

Všechny nahlašované problémy s TCP/IP by měly obsahovat kopii konfiguračních souborů používaných při činnosti TCP/IP. Chcete-li získat kopii konfiguračních souborů TCP/IP, postupujte takto:

1. Pokud jste nevytvořili knihovnu IBMLIB nebo výstupní frontu IBMOUTQ, zadejte tyto příkazy:

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

2. Přidejte knihovnu IBMLIB do seznamu knihoven a změňte výstupní frontu úlohy na výstupní frontu IBMOUTQ pomocí těchto příkazů:

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

   Získejte seznam všech fyzických souborů použitých ke konfiguraci TCP/IP pomocí těchto příkazů:

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

   Ke kopírování obsahu jednotlivých souborů můžete použít volbu 3 (Copy from the work with files). Obsah jednotlivých souborů můžete zkopírovat do samostatných souborů pro souběžný tisk ve výstupní frontě IBMOUTQ rovněž tak, že pro každý soubor v seznamu zadáte tento příkaz:

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

Kapitola 6. PAL (Product Activity Log)

Kdykoli je kvůli chybě protokolu vyřazen datagram TCP/IP, kód LIC pro TCP/IP vytvoří záznam v protokolu PAL.

Příkladem takové chyby protokolu je u odchozích datagramů TCP/IP selhání pokusu o vytvoření spojení X.25, přes které měl být datagram odeslán. V tomto případě je uživateli ohlášena chyba a odchozí datagram je vyřazen.

Příchozí datagramy způsobí vytvoření záznamu v protokolu PAL (Product Activity Log), pokud jsou splněny obě následující podmínky:

- Atribut předepisující protokolování chyb protokolu TCP/IP je nastaven na hodnotu *YES.
- Datagram nevyhoví některému z testů platnosti protokolu TCP/IP definovanému v RFC 1122, a je proto systémem vyřazen. (**Tiché vyřazení** (silently discarded) znamená, že přijatý datagram bude vyřazen, aniž by byla hostitelskému zařízení, odkud datagram pochází, ohlášena chyba.) K takovým datagramům patří například datagramy s neplatným kontrolním součtem nebo neplatnou cílovou adresou.

Pokud je datagram vyřazen výše popsaným způsobem, jsou v podrobných údajích záznamu protokolu PAL zaprotokolována záhlaví datagramů IP a TCP/UDP. Referenční kód těchto položek v protokolu PAL je 7004.

Vytištěno v Dánsku společností IBM Danmark A/S.