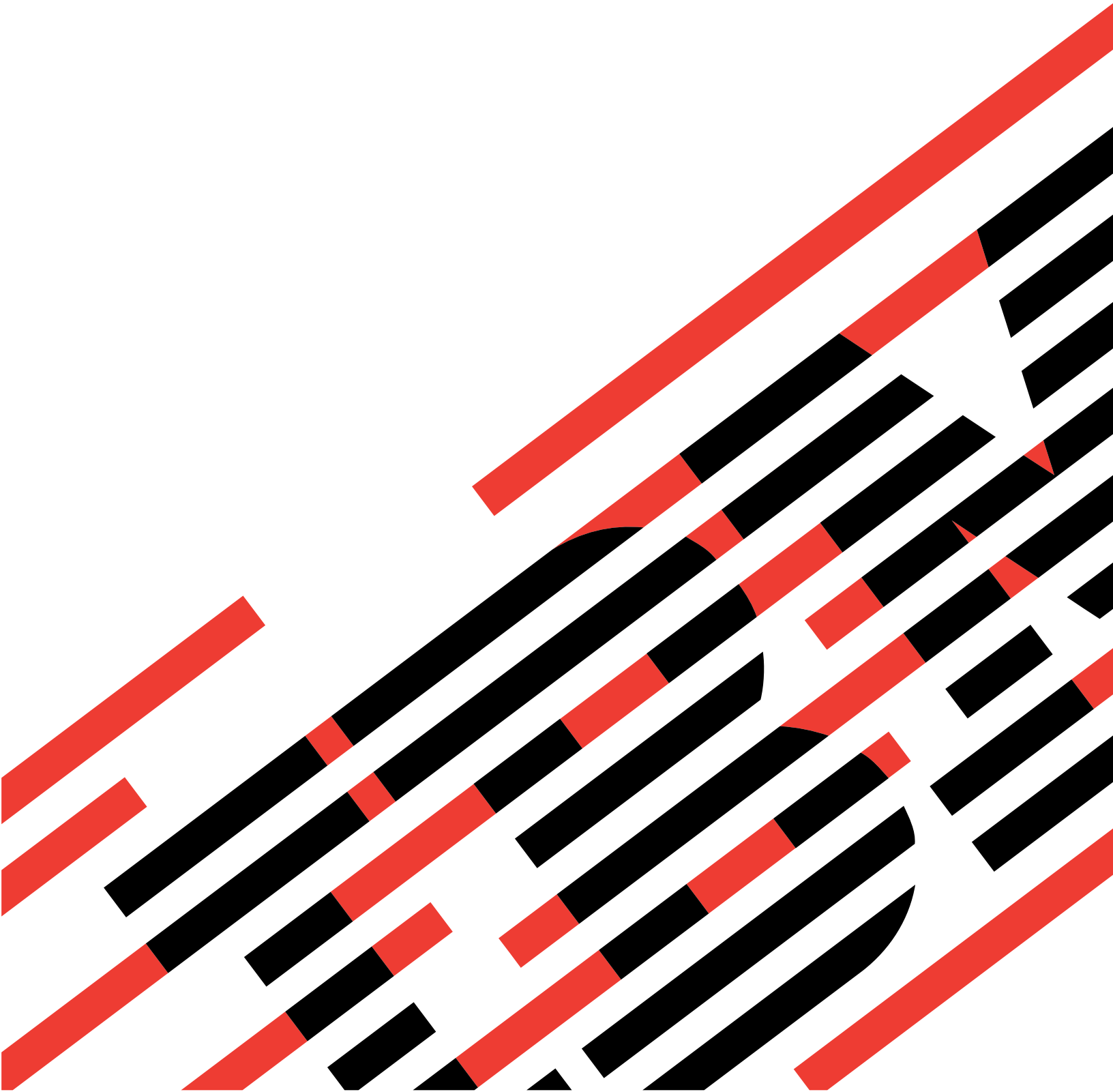
IBM

eserver

iSeries

Odstraňovanie problémov TCP/IP

Verzia 5



IBM

@server

iSeries

Odstraňovanie problémov TCP/IP

Verzia 5

Obsah

Kapitola 1. Odstraňovanie problémov TCP/IP

Čo znižuje funkčnosť vášho TCP/IP? Vytvorili ste spoľahlivú sieť a dodržali pri tom všetky inštrukcie, ale i tak ste sa dostali do slepej uličky. Táto téma vám ponúka riešenie.

Táto stránka je súhrnným zdrojom informácií pri hľadaní riešení problémov TCP/IP. Môžete mať bežný problém s pripojiteľnosťou, ktorý rozpoznáte rýchlo, alebo špecifický problém, ktorý si vyžaduje podrobnejšie posúdenie. Nižšie sú uvedené nástroje na odstraňovanie problémov, ktoré vám pomôžu váš problém vyriešiť.

Čo je nové vo verzii V5R2?
Táto téma vás naučí viac o nových spôsoboch odstraňovania problémov TCP/IP.

Vytlačte si túto tému
Táto téma vám napovie, ako stiahnuť alebo vytlačiť dokument vo formáte PDF (Portable Document Format), obsahujúci dokumentáciu k odstraňovaniu problémov TCP/IP.

Bežné problémy TCP/IP
Táto téma vám pomôže pri overovaní vašej pripojiteľnosti TCP/IP. Pomocou formulára otázok a odpovedí zamerajte svoj problém a nájdite odkaz na jeho možné riešenie.

Problémy špecifických aplikácií
Ak viete, že váš problém spočíva v konkrétnej aplikácii ako napríklad FTP alebo DNS, nájdite si v tejto téme odkaz, ktorý vedie priamo k riešeniu problémov s touto aplikáciou.

Sledovanie komunikácií
Táto téma vás sprevádza procesom zbierania údajov o sledovaní komunikácií. Sledovanie môže izolovať chyby a pootvoriť dvierka k vyriešeniu problému. Informáciu o sledovaní môžete použiť sami, alebo ju môžete poskytnúť špecialistom IBM, ktorí vám budú pomáhať pri odstraňovaní problému.

Konfiguračné súbory TCP/IP
Táto téma vám ukáže, ako skopírovať konfiguračné súbory TCP/IP. Ak sa rozhodnete využiť konzultáciu špecialistov firmy IBM, títo budú potrebovať, aby ste im kópie poskytli.

Protokol aktivity produktu
V tejto téme zistíte, ako vám pri analýze problému môže pomôcť protokol aktivity produktu.

Čo je nové vo verzii V5R2?

Medzi novinky pri odstraňovaní problémov TCP/IP V5R2 patria:

- **Bežné problémy TCP/IP**
  Zoznámte sa so spôsobmi odstraňovania problémov spojených s internetovým protokolom verzie 6 (IPv6).
- **Sledovanie komunikácií**
  Nájdite inštrukcie, ako sledovať komunikácie pomocou príkazov v jazyku CL. Tento nástroj na odstraňovanie problémov sleduje údaje na komunikačnej linke, takže môžete lokalizovať zdroj vášho problému.

Ďalšie informácie o tom, čo je nové, alebo zmenené v tomto vydaní, nájdete v téme Memo to Users  .

Vytlačte si túto tému

Ak si chcete stiahnuť, alebo prezrieť dokument vo formáte PDF, kliknite na Odstraňovanie problémov TCP/IP (približne 152 kB, 26 strán).

Ak si chcete uložiť PDF na svojej pracovnej stanici za účelom prezerania alebo tlače:

1. Vo svojom prehliadači kliknite pravým tlačidlom myši na odkaz na PDF.
2. Kliknite na **Save Target As...**.
3. Vyberte adresár, do ktorého chcete tento dokument PDF uložiť.
4. Kliknite na **Save**.

Stiahnutie programu Adobe Acrobat Reader

Ak na prezeranie alebo tlač týchto PDF potrebujete Adobe Acrobat Reader, môžete si stiahnuť kópiu z internetovej stránky Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

Kapitola 2. Bežné problémy TCP/IP

Táto téma vás sprevádza niekoľkými technikami odstraňovania problémov. S ich pomocou určíte všeobecné problémy a overíte si pripojiteľnosť TCP/IP. Ak už ste si pripojiteľnosť TCP/IP overili a viete, že váš problém spočíva priamo v konkrétnej aplikácii, choďte priamo na časť Upresnite problémy s aplikáciou.

Počiatočná analýza problému TCP/IP
Tieto informácie obsahujú sériu inštrukcií a otázok, ktoré vám pomôžu určiť príčinu vášho problému.

Úvahy o príkaze PING
Tieto informácie vám pomôžu lepšie pochopiť príkaz PING a naučiť sa ho využívať.

Práca s protokolom úlohy a frontami správ
Tu nájdete ďalšie možnosti odstraňovania problémov TCP/IP.

Počiatočná analýza problému TCP/IP

Tento systém otázok a odpovedí vás prevedie celou analýzou problému a pomôže vám rozoznať problémy a ich riešenia. Cez linky sa dostanete na zoznamy príčin, ktoré naznačujú ďalšie riešenia.

1. Na hostiteľovi v lokálnej sieti použite príkaz PING. Boli ste úspešný?
   a. Áno. Prejdite k položke 2.
   b. Nie. Prejdite na Zoznam príčin A.
2. Použite príkaz PING na vzdialenom systéme. Boli ste úspešný?
   a. Áno. Prejdite k položke 3.
   b. Nie. Prejdite na Zoznam príčin B.
3. Skontrolujte všetky potrebné úlohy TCP/IP v podsystéme QSYSWRK. Sú tam všetky úlohy?
   a. Áno. Prejdite k položke 4.
   b. Nie. Prejdite na Zoznam príčin C.
4. Použitím príkazu NETSTAT si overte, či je rozhranie aktívne. Je aktívne?
   a. Áno. Prejdite k položke 5.
   b. Nie. Prejdite na Zoznam príčin D.
5. Overte si, či sú trasy TCP/IP správne nakonfigurované na používanie aplikácií TELNET alebo FTP. Tiež sa pomocou príkazu NETSTAT presvedčte, či je vytvorené pripojenie. Existuje pripojenie?
   a. Áno. Spustite aplikáciu.
   b. Nie. Prejdite na Zoznam príčin E.

Zoznam príčin A

Uvedomte si, že vzdialený systém môže mať zakázané odpovede ICMP. Ak máte odpovedanie ICMP zakázané, nedostanete od vzdialeného systému žiadnu odpoveď, ani v prípade, že máte spoľahlivé pripojenie. Ak máte podozrenie, že toto je dôvodom problému, pokúste sa overiť si pripojenie k iným systémom a medzi nimi a pokúste sa určiť najpravdepodobnejšie umiestnenie zlyhania.

1. Overte si, či je na vašom systéme aktivované TCP/IP.

   Takto sa uistíte, či je váš zásobník TCP/IP aktívny:

   a. Zadajte príkaz STRTCP. Ak je aktívny, mali by ste obdržať správu TCP1A04, TCP/IP je práve aktívne. Ak TCP/IP aktívne nie je, zadanie príkazu STRTCP ho na vašom serveri aktivuje. Overte si, či sa počas spúšťania TCP/IP neobjavili žiadne chyby.
   b. Ak používate IPv6, prezrite si v časti Riešenia pre IPv6 techniky odstraňovania problémov určené konkrétne pre IPv6. Ak nie, pokračujte ďalšou položkou.

2. Overte si softvér TCP/IP na vašom serveri.

   Hostiteľský názov LOOPBACK a rozhranie s hodnotou popisu linky *LOOPBACK sú rezervované pre overovanie softvéru TCP/IP. Ak zadáte LOOPBACK ako hostiteľský názov, nie sú fyzickými linkami von zasielané žiadne údaje. To vám umožní rýchlo určiť, či softvér TCP/IP na vašom systéme pracuje bezchybne.

   Takto si overíte svoj softvér TCP/IP:

   a. Uistite sa, či má lokálna hostiteľská tabuľka zadanú hodnotu pre hostiteľský názov LOOPBACK a internetovú adresu 127.0.0.1.

   b. Uistite sa, či je aktívne rozhranie spojené s hostiteľom LOOPBACK. S rozhraním LOOPBACK je zvyčajne spojená internetová adresa 127.0.0.1. Uistite sa, či existuje rozhranie s IP adresou hostiteľského názvu LOOPBACK s nakonfigurovaným popisom linky *LOOPBACK. Použitím príkazu

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

      si prezriete stav rozhrania LOOPBACK. Ak nie je aktívne, aktivujte ho pomocou možnosti 9.

   c. Keď ste si overili, že je hostiteľské rozhranie LOOPBACK aktívne, napíšte:

      ```
      PING RMTSYS(LOOPBACK)
      ```

      Hostiteľ loopback umožňuje užívateľovi:

      - Testovať FTP, TELNET, LPR alebo užívateľom napísané aplikačné programy bez toho, aby bol pripojený na fyzickú linku alebo sieť.
      - Overte si, či je softvér TCP/IP nainštalovaný a či funguje bezchybne.

      Podobný test môžete vykonať, ak použitím príkazu PING overíte pripojiteľnosť k niektorému z vašich ďalších lokálne definovaných IP adries.

   d. Softvér a hardvér (pripojiteľnosť adaptéra a siete) otestujete zadaním internetovej adresy externého hostiteľa vašej siete:

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

   e. Ak neviete pripojenie vášho systému k sieti úspešne overiť zadaním vášho systémového názvu, alebo internetovej adresy, skontrolujte zdrojový prístupový bod služby (SSAP) opisu linky spojeného s rozhraním. Musí byť zadané X'AA' ako hodnota v zozname SSAP (source service access point). Táto hodnota je pri vytváraní nového opisu linky pridelená automaticky, ak je parametru SSAP ponechaná štandardná hodnota *SYSGEN. Ak máte už existujúci opis linky, použite príkaz Change Line Description a pridajte tieto hodnoty do zoznamu.

      Nie všetky typy opisov liniek musia mať SSAP pre TCP/IP, preto skontrolujte zoznam SSAP v opise linky spojeného s rozhraním.

   f. Overte všetky položky opisov liniek, najmä veľkosť rámca, ktorá by mala byť väčšia alebo rovná maximálnej jednotke vysielania (MTU) tohto rozhrania.

   g. Ak vzdialený systém neodpovedá, môže to znamenať, že je systém, sieť, externý hostiteľ alebo most v sieti je nedostupný alebo nefunkčný. Neodpovedanie môže tiež znamenať, že vzdialený systém má zakázané odpovedanie ICMP. Takýto zákaz sa môže vyskytnúť, ak vzdialený systém vystupuje ako firewall a bol nakonfigurovaný, aby na požiadavky ICMP neodpovedal. Pokúste sa overiť si pripojenie k ostatným systémom a medzi nimi navzájom a pokúste sa určiť najpravdepodobnejšie umiestnenie zlyhania.

   h. Overte si, či je správna konfigurácia lokálneho rozhrania.

   i. Ak sa rozhrania TCP/IP, vrátane LOOPBACK, neaktivujú, alebo ak nemôžete ukončiť, či spustiť TCP/IP, uistite sa, či sú nasledujúce dva smerovacie záznamy nakonfigurované v opise podsystému QSYSWRK. Ak neexistujú, alebo nie sú správne, opravte ich, alebo pridajte a skúste zopakovať svoju požiadavku.

      ```
      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)
```

Vráťte sa k časti Počiatočná analýza problému TCP/IP a pokračujte v odstraňovaní problému.

Riešenia pre IPv6

Ak máte problémy s komunikáciou IPv6, vyskúšajte na ich odstránenie tieto postupy.

1. Overte si, či je spustený zásobník IPv6.
   a. Uistite sa, či je rozhranie loopback nakonfigurované a aktívne. Nasledujúcimi krokmi skontrolujete stav rozhrania loopback:
      1) V produkte iSeries Navigator rozviňte váš **server —> Sieť —> Konfigurácia TCP/IP —> IPv6 —> Rozhrania**.
      2) V pravom paneli nájdite rozhranie loopback. Adresa IPv6 loopback má IP adresu ::1 a názov linky je Loopback 6. Ak rozhranie loopback nie je v zozname, musíte ho nakonfigurovať pomocou **Sprievodcu konfiguráciou IPv6**.
   b. Otestujte odozvu adresy loopback (::1). Server sám sebe zašle paket IPv6 paket a tým si overí, či zásobník IPv6 pracuje. Zásobník môžete otestovať pomocným programom ping, ak dodržíte tieto kroky:
      1) V produkte iSeries Navigator rozviňte váš **server —> Sieť**.
      2) Pravým tlačidlom myši kliknite na **Konfigurácia TCP/IP**, kliknite na **Pomocné programy** a na **Ping**.
2. Keď ste si overili, že je zásobník IPv6 spustený, uistite sa, či je linka IPv6 nakonfigurovaná a aktívna. Táto linka môže byť buď linka Ethernet, alebo môže byť nakonfigurovaná ako tunel.

   Stav liniek nakonfigurovaných na serveri skontrolujete takto:
   a. V produkte iSeries Navigator rozviňte váš **server —> Sieť —> Konfigurácia TCP/IP —> Linky**.
   b. V pravom paneli nájdite linku, ktorá by mala byť nakonfigurovaná na IPv6 a skontrolujte stĺpec s informáciami o stave. Ak linka nie je v zozname, musíte linku pre IPv6 nakonfigurovať pomocou **Sprievodcu konfiguráciou IPv6**. Informácie o konfigurácii linky pre IPv6 nájdete v časti Konfigurácia IPv6. Ak sa linka v zozname nachádza a jej status je **Nenatiahnutá**, znamená to, že linka je nakonfigurovaná, ale nie je natiahnutá v konfiguračnom zásobníku IPv6. Problém na linke určite použitím príkazu Work with line descriptions (WRKLIND) v znakovom rozhraní.
3. Uistite sa, či sú aktívne minimálne dve rozhrania IPv6: vaše lokálne rozhranie a rozhranie, do ktorého zasielate test odozvy.

   Stav rozhranie IPv6 skontrolujete týmito krokmi:
   a. V produkte iSeries Navigator rozviňte váš **server —> Sieť —> Konfigurácia TCP/IP —> IPv6 —> Rozhrania**.
   b. V pravom paneli nájdite IP adresu spojenú s lokálnym rozhraním a skontrolujte stav rozhrania.
   c. Ak je stav rozhrania **Neaktívne**, musíte ho aktivovať. Rozhranie aktivujete tak, že kliknete pravým tlačidlom myši na IP adresu a vyberiete **Štart**.
   d. Zopakujte tieto kroky a skontrolujte stav vzdialeného rozhrania.
4. Ak vaše testovanie odozvy adresy IPv6 nebolo úspešné, overte si stav adries oboch rozhraní. Obe rozhrania by mali mať stav rozhrania **Prednostný**. Ak nie je cieľové alebo zdrojové rozhranie v prednostnom stave, vyberte si na testovanie iné rozhrania, alebo zmeňte status používaných rozhraní na správny.

Stav adresy zdrojového rozhrania môžete overiť alebo zmeniť nasledujúcimi krokmi:

a. V produkte iSeries Navigator rozviňte váš **server —> Sieť —> Konfigurácia TCP/IP —> IPv6 —> Rozhrania**.
b. V pravom paneli kliknite pravým tlačidlom myši na IP adresu spojenú s rozhraním, vyberte **Vlastnosti** a kliknite na stránku **Možnosti**. Toto dialógové okno vám umožní zadať odporúčanú alebo platnú životnosť rozhrania.
c. Zopakujte tieto kroky a skontrolujte stav adresy cieľového rozhrania.

Zoznam príčin B

Ak boli príkazy VFYTCPCNN alebo PING na lokálnom systéme úspešné, mali by ste si overiť možnosť spojenia medzi vaším systémom a systémom, s ktorým chcete komunikovať. Spustite príkaz PING tak, ako predtým, ale tentoraz zadajte internetovú adresu vzdialeného hostiteľa. Prezrite si Bežné chybové správy. Uvedomte si, že vzdialený systém alebo prechodný firewall môžu mať zakázané odpovedanie ICMP. Ak máte odpovedanie ICMP zakázané, nedostanete od vzdialeného systému žiadnu odpoveď, ani v prípade, že máte spoľahlivé pripojenie. Ak máte podozrenie, že toto je dôvodom problému, pokúste sa overiť si pripojenie k iným systémom a medzi nimi navzájom a pokúste sa určiť, najpravdepodobnejšie umiestnenie zlyhania.

1. Ak môžete overiť pripojenie pomocou vzdialenej internetovej adresy, ale nie pomocou názvu vzdialeného systému, znamená to, že názov alebo adresa vo vašej hostiteľskej tabuľke nie je správna, alebo že nie sú dostupné vzdialené názvové servery.
2. Ak váš systém používa vzdialené názvové servery, overte si, či môžete každý z nich dosiahnuť použitím príkazu PING a zadaním jeho internetovej adresy.
3. Príkaz PING obsahuje ďalšie parametre, ktoré vám umožňujú zadať dĺžku paketu, počet paketov, ktoré majú byť odoslané a čas čakania na odpoveď. Štandardný čakací čas 1 sekunda je pre väčšinu sietí dostatočný na to, aby vzdialený systém odpovedal. Ak je však vzdialený systém ďaleko, alebo ak je sieť zaneprázdnená, môže zvýšenie parametra čakacieho času viesť k úspešnému výsledku.

   Je žiadúce, aby sa predvolené hodnoty parametrov nemenili. Uvedomte si, že ak ich zmeníte, môže kombinácia veľkej dĺžky paketov a krátkeho čakacieho času spôsobiť, že sieť nebude mať dosť času na vysielanie a prijímanie odpovedí, čo povedie k uplynutiu vyhradeného času. Ak sieť nemá dostatok času na vyslanie a prijatie odpovede, môže to vyzerať, ako by ste k systému neboli pripojení, hoci pripojení ste.
4. Ak vzdialený systém neodpovedá, môže to znamenať, že je systém, sieť, brána, smerovač alebo most v sieti nedostupný alebo nefunkčný. Neodpovedanie môže tiež znamenať, že vzdialený systém alebo prechodný firewall má zakázané odpovedanie ICMP. Pokúste sa overiť si pripojenie k ostatným systémom a medzi nimi navzájom a pokúste sa určiť najpravdepodobnejšie umiestnenie zlyhania.
5. Ak použijete príkaz PING na overenie rozhrania nakonfigurovaného na popis linky ethernetového typu a vzdialený systém neodpovedá, uistite sa, či je v popise ethernetovej linky nastavené *ALL alebo správna štandardná hodnota.
6. Ak nedostanete odpovede od žiadneho zo systémov v sieti, naznačuje to problém niekde na ceste. Overte si pripojenie k bráne vedúcej k príslušnej sieti. Ak neuspejete, prepracujte sa spätne od vzdialeného systému, ktorý nemôžete dosiahnuť, až kým nenájdete miesto zlyhania.
7. Pakety sú odosielané pomocou protokolu nízkej úrovne, ktorý nezaručuje jeho doručenie. Keďže opakovaná požiadavka sa môže stratiť, nepredpokladajte, že zlyhala sieť alebo brána, kým nezlyhá na ceste k tomu istému bodu niekoľko príkazov.

Ak zlyhá príkaz PING na hostiteľa vo vzdialenej sieti, použite na tú istú sieť príkaz na sledovanie trasy TRACEROUTE. Pomocný program na sledovanie trasy vykoná časť rovnakých testov pripojenia ako jednotlivá požiadavka testovania odozvy, ale je schopný vykonať ich všetky v jednom kroku. Tento príkaz otestuje každý skok na ceste ku vzdialenému cieľu a naznačí, či sa problém nachádza ešte pred prechodným smerovačom, alebo až v rámci vzdialenej siete.

Napíšte TRACEROUTE RMTSYS('x.x.x.x'). Vzdialený systém môžete určiť zadaním jeho IP adresy, alebo jeho názvu; napríklad, ('xxxx.xxxx.com'). Pomocný program na sledovanie trasy akceptuje tak adresu vo formáte IPv4 ('x.x.x.x'), ako aj vo formáte IPv6 ('x:x:x:x:x:x:x:x').

Sledovanie trasy je tiež prístupné cez produkt iSeries Navigator. Sledovanie trasy spustíte týmito krokmi:

1. V produkte iSeries Navigator rozviňte váš server —> **Sieť**.
2. Pravým tlačidlom myši kliknite na **Konfigurácia TCP/IP**, označte **Pomocné programy** a kliknite na **Sledovanie trasy**.

Vráťte sa k časti Počiatočná analýza problému TCP/IP a pokračujte v odstraňovaní problému.

Zoznam príčin C

1. Skontrolujte všetky potrebné úlohy (lokálne aj vzdialené) v podsystéme QSYSWRK. Mala by tam byť minimálne úloha QTCPIP. Úloha QTCPIP kontroluje spúšťanie a ukončovanie rozhraní TCP/IP. Mala by tam byť aj minimálne jedna úloha na každú aplikáciu, ktorú sa pokúšate použiť, ako to ukazujeObrázok 1 na strane 8. Je možné, že tieto úlohy nemusia byť priamo pomenované podľa FTP, LPD a TELNET úloh vášho podsystému. Všetky úlohy FTP začínajú na QTFTP. Všetky úlohy LPD začínajú na QTLPD. Všetky úlohy TELNET budú pomenované QTVTELNET a QTVDEVICE. Je možné, že bude spustená viac než jedna serverová úloha FTP, LPD alebo TELNET. Všetky úlohy SMTP začínajú na QTSMTP. SMTP má v podsystéme QSYSWRK až štyri aktívne úlohy a dve aktívne úlohy v podsystéme QSNADS. Všetky úlohy SNMP začínajú na QTMSNMP. SNMP môže mať tri aktívne úlohy v podsystéme QSYSWRK, QTMSNMP, QTMSNMPRCV a QSNMPSA.

   Zobrazte tieto úlohy príkazom Work with Active Jobs (WRKACTJOB). Napíšte WRKACTJOB SBS(QSYSWRK).
2. Ak tam nie sú všetky úlohy, ukončite proces TCP/IP pomocou príkazu ENDTCP OPTION(*IMMED). Hľadajte všetky protokoly úloh spojené s týmito úlohami.
3. Pre všetky objekty popisov úloh zmeňte úroveň protokolovania správy popisu úlohy na 4 0 *SECLVL. Detailnejšie informácie o úrovniach protokolovania správy nájdete v téme Práca s protokolom úlohy a frontami správ.
4. Príkazom STRTCP znova spustite proces TCP/IP
5. Overte si, či sú všetky úlohy aktívne.
6. Skontrolujte protokoly úloh, či príslušné úlohy nie sú aktívne.

```
                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
```

Obrázok 1. Práca s aktívnymi úlohami—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
```

Obrázok 2. Práca s aktívnymi úlohami—Obrazovka 2

Vráťte sa k časti Počiatočná analýza problému TCP/IP a pokračujte v odstraňovaní problému.

Zoznam príčin D

Funkcia network status (NETSTAT) na serveri vám umožňuje prezrieť si vo vašom lokálnom systéme stav rozhrania TCP/IP, informácie o konfigurácii smerovania TCP/IP a stav pripojenia TCP/IP. Môžete tiež použiť príkaz WRKTCPSTS, alebo príkaz NETSTAT.

1. Pred použitím funkcie network status spustite TCP/IP príkazom STRTCP. Ponuka Stavu siete displeja Práca sa s TCP/IP sa zobrazí, ale možnosti nie sú funkčné, kým nie je spustené TCP/IP.

2. Na obrazovke stavu rozhrania Práca s TCP/IP sa pri pokuse o spustenie aktívneho rozhrania alebo vypnutie neaktívneho rozhrania odošle príslušná chybová správa. Ak sa po zvolení možnosti spustiť rozhranie nedostane neaktívne rozhranie do aktívneho stavu, môže ísť o problém s rozhraním, linkou alebo konfiguráciou linky. Ak si prezriete protokol úlohy QTCPIP v podsystéme QSYSWRK, môžete v ňom zistiť, aké chyby sa mohli objaviť pri aktivovaní rozhrania. Tiež sa môžete pozrieť do frontu správ QSYSOPR a protokolu histórie QHT (DSPLOG) a pomôcť určiť stav.
3. Ak chcete určiť, či má opis linky nejaký problém, napíšte WRKCFGSTS *LIN.
4. Overte si, či je zobrazené aspoň jedno pasívne načúvajúce pripojenie pre každý zo serverov v displeji Práca so stavom pripojenia TCP/IP, možnosti 3 z displeja Práca so stavom siete TCP/IP. Mali by ste si overiť stav pripojenia serverov, ktoré podporujú tieto aplikácie, a stav akýkoľvek ďalších relevantných serverov v sieti:

   SNMP

   TELNET

   Verzia 4, vydanie 4 podporuje SSL Telnet na dôvažok k Telnetu. SSL Telnet používa štandardne načúvajúci port 992 a tradičný Telnet používa port 23. Odporúčaný prístup na vyradenie tradičného servera Telnet z prevádzky je obmedzenie počúvajúcich portov Telnet a medzitým povolenie SSL Telnet.

   FTP

   SMTP, ak je nakonfigurované

   POP

   LPD

   REXEC

   HTTP, ak je nakonfigurované

   Pasívne načúvajúce pripojenia majú v poliach *Vzdialená adresa* a *Vzdialený port* hviezdičku. Neodporúča sa ukončiť pripojenia. Ak by ste ich ukončili, nebudú môcť s nimi spojené vzdialené systémy používať SNMP, FTP a TELNET, posielať SMTP správy lokálnemu systému, ani posielať lokálnemu systému spoolové súbory pomocou LPR. Môžu byť znova spustené ukončením a spustením serverov pomocou príkazov ENDTCPSVR a STRTCPSVR, a potom určením serverov, ktoré chcete ukončiť a spustiť.
5. Uistite sa, či porty, spojené s aplikáciami, ktoré sa pokúšate použiť, nie sú zakázané. Použite voľbu 4 (obmedzenia portov v Práci s TCP/IP) v menu Konfigurácia TCP/IP a prezrite si aktuálne obmedzenia portov.

Vráťte sa k časti Počiatočná analýza problému TCP/IP a pokračujte v odstraňovaní problému.

Zoznam príčin E

Overte si konfiguračné údaje. Ak je všetko v poriadku, choďte na Problémy špecifických aplikácií a vyberte si asistenciu pri odstraňovaní problémov konkrétnej aplikácie, ktorú používate.

Úvahy o príkaze PING

Prečítajte si nasledujúce časti a zistite viac informácií o príkaze PING.

Zreťazenie názvu domény s názvom hostiteľa
Táto časť rozoberá, ako server zreťazí názov domény s názvom hostiteľa.

Bežné chybové správy
Táto časť poskytuje príklady niektorých najbežnejších chybových stavov príkazu PING.

Zreťazenie názvu domény s názvom hostiteľa

Tento príklad ilustruje, ako server používa názov lokálnej domény ako vyhľadávací zoznam a reťazí názvy domén s názvami hostiteľov, ak nie je na konci názvu domény použitá bodka.

Názov vášho servera je SYSNAM01.A400SSC.DFW.COMPANY.COM, a chcete si overiť pripojenie k systému, ktorého plný názov je SYSNAM02.DFW.COMPANY.COM. Vo svojej lokálnej hostiteľskej tabuľke nemáte hostiteľský názov SYSNAM02.

Ak napíšete PING SYSNAM02.DFW.COMPANY.COM, pošle váš server vzdialenému názvovému serveru SYSNAM02.DFW.COMPANY.COM.

Ak napíšete PING SYSNAM02, server najprv zašle vzdialenému názvovému serveru SYSNAM02.A400SSC.DFW.COMPANY.COM. Potom odošle SYSNAM02.DFW.COMPANY.COM. Ak to nebolo nájdené, zašle nakoniec SYSNAM02.COMPANY.COM. Inými slovami, iSeries TCP/IP zreťazí každú časť názvu lokálnej domény k názvu hostiteľa.

Ak napíšete PING SYSNAM02., oznámi vzdialený názvový server, že je hostiteľ neznámy. Vzdialený názvový server nerozoznal SYSNAM02, pretože server zasiela názov SYSNAM02 vzdialenému názvovému serveru bez zreťazenia akejkoľvek časti vyhľadávacieho zoznamu. Jediný rozdiel medzi týmto a predošlým názvom je použitie bodky na konci názvu.

Bežné chybové správy

Ak na overenie pripojenia k inému hostiteľovi v sieti použijete príkaz PING, mohol by vám TCP/IP vrátiť chybovú správu. Použite túto tabuľku na rozpoznanie bežných chybových správ a na určenie toho, čo máte urobiť, aby ste ten ktorý problém odstránili.

Chybové správy	Čo by ste mali robiť
Nie je dostupná žiadna služba TCP/IP	• TCP/IP ešte nebolo spustené, alebo neukončilo spúšťanie. Použitím príkazu NETSTAT zistite, či je TCP/IP aktívne. • Možno neboli spustené všetky úlohy v podsystéme QSYSWRK. Príkazom Use the Work with Active Jobs (WRKACTJOB) si overte, či je podsystém QSYSWRK a s ním spojené úlohy v aktívnom stave. Ak nie sú aktívne, hľadajte akékoľvek správy v protokole úlohy alebo v štandardnom systémovom výstupnom fronte.
Nie je možné vytvoriť pripojenie k vzdialenému hostiteľskému systému	Zmeňte svoje nakonfigurované rozhrania, s nimi spojené opisy liniek a trasy TCP/IP.
Nie je možné zastihnúť vzdialený systém	TCP/IP nemohlo nájsť cestu k požadovanému cieľu. Skontrolujte NETSTAT možnosť 2 a overte si, či bola *DFTROUTE alebo ekvivalentná sieťová trasa nakonfigurovaná a či je aktívna.
VFYTCPCNN nedostal do 10 sekúnd odpoveď od vzdialeného hostiteľa na overenie pripojenia 1.	• Vaša konfigurácia je pravdepodobne správna, ale nedostávate odpoveď od vzdialeného systému. Uistite sa, či je vzdialený hostiteľ schopný spojiť sa s vaším systémom. Zavolajte operátora vzdialeného systému a požiadajte ho, aby overil spojenie s vaším systémom. • Skontrolujte hostiteľské tabuľky alebo vzdialený názvový server (ak používate názvový server) pre oba systémy a rozhrania a trasy TCP/IP. Vzdialený názvový server nemusí byť, z nejakého dôvodu, schopný obslúžiť vás. • Ak používate linku Ethernet, uistite sa, či ste zadali správny štandard Ethernet alebo *ALL.
VFYTCPCNN: Neznámy hostiteľ xxxxxx, kde xxxxxx je názov hostiteľa.	Hostiteľský názov nemôže byť IP adresou rozlíšený, ani s použitím hostiteľskej tabuľky alebo názvového servera. Skontrolujte lokálnu hostiteľskú tabuľku alebo vzdialené názvové servery (ak používate názvový server) kvôli zadanej hodnote vzdialeného hostiteľa.

Práca s protokolom úlohy a frontami správ

TCP/IP je odoslané s niekoľkými opismi úlohy.

Opisy úloh sú uložené v knižniciach QSYS alebo QTCP. Všeobecne sú odosielané s úrovňou protokolovania správ 4, závažnosťou protokolovania správ 0 a s hodnotou textu protokolovania správ *NOLIST. S týmito hodnotami sú odosielané preto, aby sa predišlo vytvoreniu protokolov úloh, v ktorých je len správa o spustení úlohy a správa o ukončení úlohy.

Ak máte problémy s prevádzkou TCP/IP, ako prvý krok zmeňte nastavenie úrovne protokolovania správ v popise úlohy problémovej aplikácie na textovú hodnotu protokolovania správ *SECLVL. Zmena úrovne protokolovania správ vytvorí protokol úlohy pre túto aplikáciu. Aby zmena nadobudla platnosť, musíte server ukončiť a reštartovať. Ak chcete úlohu zmeniť okamžite, musíte na zmenu úrovne protokolovania správy aktívnej úlohy použiť príkaz CHGJOB.

Ak chcete zmeniť úroveň protokolovania správy v opise úlohy konkrétnej aplikácie, pozrite si nasledujúce príklady:

- Ak máte problém so serverom FTP, zmeňte opis úlohy QTMFTPS napísaním tohto príkazu v CL:
  ```
  CHGJOBD  JOBD(QTCP/QTMFTPS)  LOG(4 0 *SECLVL)
  ```
- Ak sa vyskytol problém so SMTP, zmeňte opis úlohy QTMSMTPS napísaním tohto príkazu v CL:
  ```
  CHGJOBD  JOBD(QTCP/QTMSMTPS)  LOG(4 0 *SECLVL)
  ```

  Okrem zmeny opisu úlohy QTMSMTPS sa môžete rozhodnúť zmeniť aj úroveň protokolovania opisu úlohy podsystému QSNADS a napísať tento príkaz v CL:
  ```
  CHGJOBD  JOBD(QGPL/QSNADS)  LOG(4 0 *SECLVL)
  ```

Kapitola 3. Problémy špecifických aplikácií

Ak ste zistili, že váš problém spočíva v konkrétnej aplikácii, ktorú máte spustenú na TCP/IP, vyberte si podľa nižšie uvedených aplikácií detailnejšie informácie o odstraňovaní problémov. Každý odkaz vás zavedie na novú stránku venovanú odstraňovaniu problémov konkrétnej aplikácie.

Server Domain Name System (DNS)
V tejto téme nájdete vývojový diagram s analýzou problému, ktorý vás prevedie stratégiami ladenia problémov DNS.

File Transfer Protocol (FTP)
Táto téma odporúča riešenia vašich problémov s FTP a názorne predvádza protokol serverovej úlohy ako nástroj na odstraňovanie problémov.

Point-to-Point Protocol (PPP)
Tu nájdete riešenia bežných problémov s pripojením PPP.

Server Post Office Protocol (POP)
Túto tému si prezrite, ak potrebujete odstrániť problémy so serverom POP a s inými aplikáciami elektronickej pošty.

Rexec
Tu nájdete vývojový diagram, ktorý vám pomôže zamerať sa na váš problém s aplikáciou Rexec a nájsť možné riešenia.

Simple Mail Transfer Protocol (SMTP)
Táto téma vám poskytne niekoľko spôsobov riešenia problémov Simple Mail Transfer Protocol (SMTP) a s ďalších aplikácií elektronickej pošty.

Telnet
Táto téma vám bude asistovať pri všeobecných problémoch s aplikáciou Telnet, ako aj pri konkrétnych problémoch spojených s typom emulácie a so serverom SSL. Navyše zistíte, aké informácie sú potrebné na reportovanie vášho problému.

Virtual Private Networking (VPN)
Tu vás prevedieme niekoľkými stratégiami odstraňovania problémov s VPN, spojených s pripojením, chybami konfigurácie, pravidlami filtrovania a podobne.

Kapitola 4. Sledovanie komunikácií

Pri odstraňovaní problémov TCP/IP použite sledovanie komunikácií. Sledovanie komunikácií je funkcia služby, ktorá umožňuje, aby boli sledované údaje v komunikačnej linke, napríklad v lokálnej sieti (LAN) alebo v rozšírenej sieti (WAN). Po tom, ako budú údaje odsledované, môžu byť nespracované údaje uložené do súboru toku, alebo môžu byť naformátované, uložené do spoolového súboru a zobrazené alebo vytlačené.

Sledovanie komunikácií môže byť použité pri odstraňovaní problémov s komunikáciami IPv4 aj IPv6.

Sledovanie komunikácií použite v týchto situáciách:

- Vaše procedúry analyzovania problému vám o probléme neposkytujú dostatok informácií.
- Predpokladáte, že problémom je narušenie protokolu.
- Predpokladáte, že problémom je šum na linke.
- Chcete vedieť, či vaša aplikácia správne vysiela informácie.
- Chcete vedieť, či máte problémy s prevádzkovým preťažením siete, alebo s priepustnosťou údajov.

Aby ste mohli na sledovanie komunikácií použiť príkazy CL, musíte mať špeciálne oprávnenie *SERVICE, alebo musíte mať oprávnenie na použitie funkcie Service Trace v OS/400 cez produkt iSeries Navigator. Viac informácií o tomto type oprávnenia nájdete v kapitole o profiloch užívateľov v príručke iSeries Security Reference .

Trace Connection (TRCCNN) je príkaz na spôsob sledovania podobný sledovaniu komunikácií. Ak máte aplikácie TCP, ktoré používajú SSL, alebo ak používate Bezpečnosť IP, potom údaje prenášané komunikačnou linkou sú zakódované; je možné, že vám pri prezeraní týchto údajov nebude sledovanie komunikácií nápomocné. TRCCNN sleduje údaje pred zašifrovaním a po dešifrovaní, takže môže byť použitý v prípade, keď bežné sledovanie komunikácií nie je účinné. Výsledok je podobný bežnému výstupu sledovania komunikácií. Parametre a príklady k tomuto príkazu nájdete v časti Popis príkazu TRCCNN (Trace Connection) v téme Application Programming Interfaces (API).

Ak chcete použiť funkciu sledovania komunikácií, nasledujte tieto kroky:

Plánovanie sledovania komunikácií
Predbežné kroky, ktoré je nevyhnutné vykonať skôr, než budete sledovať komunikácie.

Vykonanie sledovania komunikácií
Kroky potrebné na vykonanie sledovania komunikácií.

Ďalšie funkcie sledovania komunikácií
Viac funkcií spojených so sledovaním komunikácií.

Plánovanie sledovania komunikácií

Skôr, ako začnete pracovať so sledovaním komunikácií, vykonajte tieto kroky:

1. Ak ste nevytvorili knižnicu IBMLIB ani výstupný front IBMOUTQ, zadajte nasledujúci príkaz:
   ```
   CRTLIB LIB(IBMLIB)
   CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
   ```
2. Zadaním nasledujúceho príkazu pridajte knižnicu IBMLIB do vášho zoznamu knižníc a zmeňte výstupný front úlohy na výstupný front IBMOUTQ:
   ```
   ADDLIBLE IBMLIB
   CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
   ```
3. Ak v systéme neexistuje súbor tlačiarne QTCPPRT, vytvoríte ho zadaním nasledujúceho príkazu:

```
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. Zadaním nasledujúcich príkazov odošlete spoolový súbor QTCPPRT, obsahujúci výstup sledovania komunikácií, do výstupného frontu IBMOUTQ v knižnici IBMLIB:

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

   Keď sa úloha ukončí, nové verzie súborov tlačiarne stratia platnosť.
5. Získajte názov opisu linky spojeného s problematickým rozhraním TCP/IP, alebo s rozhraním používaným aplikáciou či sieťou, s ktorou máte problémy. Na zistenie opisu linky spojeného s týmto rozhraním použite NETSTAT *IFC.
6. Uistite sa, či je linka zapnutá a či bolo rozhranie TCP/IP spojené s touto linkou spustené, takže údaje TCP/IP sa cez toto rozhranie môžu odosielať a prijímať. Použitím NETSTAT *IFC si overte, či je toto rozhranie aktívne.

Ďalší postup:
Vykonanie sledovania komunikácií

Vykonanie sledovania komunikácií

Ak chcete vykonať sledovanie komunikácií, musíte v znakovom rozhraní použiť príkaz CL. Vykonajte tieto kroky:

1. Spustite sledovanie komunikácií
2. Ukončite sledovanie komunikácií
3. Spracujte výsledky sledovania komunikácií
4. Vytlačte výsledky sledovania komunikácií
5. Prezrite si obsah sledovania komunikácií
6. Prečítajte si výsledky sledovanie komunikácií

Spustite sledovanie komunikácií

Táto akcia spustí sledovanie komunikácií zadanej linky alebo opisu sieťového rozhrania.

Poznámka: Sledovanie komunikácií už viac nemôže byť použité na sledovanie údajov popisu sieťového servera (*NWS). Funkciu sledovania komunikácií môžete použiť buď na konkrétnu linku (*LIN), alebo na popis sieťového rozhrania (*NWI).

Sledovanie komunikácií spustíte týmito krokmi:

1. Do príkazového riadku zadajte STRCMNTRC.
2. Ako **Objekt konfigurácie** zadajte názov linky, napríklad TRNLINE.
3. Ako **Typ** zadajte typ zdroja, teda *LIN, alebo *NWI.
4. Do poľa **Veľkosť vyrovnávacej pamäte** zadajte dostatočný objem pamäte pre očakávaný objem údajov. Pre väčšinu protokolov je dostatočný objem pamäte 8 MB. Pre Ethernet 10/100 je dostatočným objemom 16 MB až 1 GB. Ak si nie ste istý, zadajte 16 MB ako maximálny objem pamäte povolený pre protokol.
5. Ak chcete zbierané údaje obmedziť na sledovanie jedného vzdialeného rozhrania, do poľa **Možnosti sledovania komunikácií** zadajte *RMTIPADR. Inak použite predvolenú hodnotu.
6. Do poľa **Vzdialená IP adresa** zadajte IP adresu spojenú so vzdialeným rozhraním, ktorého sledované údaje budú zbierané.

Sledovanie komunikácií pokračuje, až kým sa neobjaví jedna z nasledujúcich možností:

- Je spustený príkaz ENDCMNTRC.
- Problém s fyzickým pripojením spôsobí ukončenie sledovania.
- Parameter **Trace full** má hodnotu *STOPTRC a vyrovnávacia pamäť sa naplnila.

Ďalší postup:
Ukončite sledovanie komunikácií

Ukončite sledovanie komunikácií

Ak chcete formátovať a zobraziť výsledky sledovania, musíte ho najprv ukončiť. Táto akcia sledovanie ukončí, ale uloží jeho vyrovnávaciu pamäť.

Sledovanie komunikácií ukončíte týmito krokmi:

1. Do príkazového riadku zadajte ENDCMNTRC.
2. Ako **Objekt konfigurácie** zadajte rovnaký názov linky, aký ste zadali pri spustení sledovania, napríklad TRNLINE.
3. Ako **Typ** zadajte typ zdroja, teda *LIN alebo *NWI.

Ďalší postup:
Spracujte výsledky sledovania komunikácií. Toto je voliteľný krok, ktorý môže byť užitočný. Ak chcete radšej vytlačiť nespracované údaje bez toho, aby ste ich spracovali, prejdite k časti Vytlačte sledovanie komunikácií

Spracujte výsledky sledovania komunikácií

Ak používate Internet Protocol verzie 6 (IPv6), musíte nasledujúcimi krokmi spracovať sledované údaje do súboru toku; ak však používate IPv4, je to len voliteľná časť procesu sledovania komunikácií.

Spracovanie údajov do súboru toku vám ponúka niekoľko výhod. Pri rozhodovaní, či túto funkciu použijete, zvážte tieto výhody:

- Môžete spúšťať nové sledovania bez toho, aby ste stratili údaje o existujúcich sledovaniach.
- Údaje o sledovaní môžete formátovať viackrát. Ak napríklad niektorá z vašich aplikácií používa ASCII, budete potrebovať údaje zo sledovania komunikácií naformátovať v ASCII kóde; ak iná aplikácia používa EBCDIC, budete možno tieto údaje potrebovať naformátovať v EBCDIC. Spracovanie údajov o sledovaní do súboru toku zabezpečuje flexibilitu pri formátovaní týchto údajov.
- Sledovacie údaje môžete uchovať počas IPL.
- Na vytvorenie výstupu môžete použiť bežný program na úpravu formátu.

Obsah sledovania komunikácií spracujete vykonaním nasledujúcich krokov:

1. Vytvorte adresár, napríklad mydir. Ak chcete vytvoriť adresár, pozrite si popis príkazu CRTDIR (Create Directory) v téme Control Language (CL).
2. Do príkazového riadku zadajte DMPCMNTRC.
3. Ako **Objekt konfigurácie** zadajte rovnaký názov linky, aký ste zadali pri spustení sledovania, napríklad TRNLINE.
4. Ako **Typ** zadajte typ zdroja, teda *LIN, alebo *NWI.
5. **Do súboru toku** zadajte názov cesty, ako napríklad /mydir/mytraces/trace1.

Ďalší postup:
Vytlačte sledovanie komunikácií

Vytlačte sledovanie komunikácií

Údaje zo sledovania komunikácií môžete, v závislosti na spôsobe ich zbierania, vytlačiť z dvoch rôznych zdrojov. Môžete ich vytlačiť z nespracovaných údajov, ktoré ste zozbierali, alebo môžete vytlačiť súbor toku, do ktorého ste pôvodne nespracované údaje uložili.

Poznámka: Ak chcete údaje o sledovaní komunikácií tlačiť zo súboru toku, musíte mať na systéme nainštalovaný program Java (5722JV1).

Táto akcia zapíše údaje sledovania komunikácií konkrétnej linky alebo opisu sieťového rozhrania do spoolového súboru alebo do súboru výstupu.

Tlačenie z nespracovaných zozbieraných údajov:

Ak ste zozbierané údaje nespracovali, môžete ich vytlačiť podľa týchto krokov:

1. Do príkazového riadku zadajte PRTCMNTRC.
2. Ako **Objekt konfigurácie** zadajte rovnaký názov linky, aký ste zadali pri spustení sledovania, napríklad TRNLINE, a stlačte Enter.
3. Ako **Typ** zadajte typ zdroja, teda *LIN, alebo *NWI.
4. Ako **Znakový kód** zadajte *EBCDIC alebo *ASCII. Údaje by ste mali vytlačiť dva razy, raz so zadaním *EBCDIC a druhý raz so zadaním *ASCII.
5. Do poľa **Formátovať údaje TCP/IP** zadajte *YES a stlačte dva razy Enter.
6. Kroky 1 až 5 vykonajte ešte raz, ale tentoraz zadajte iný znakový kód.

Tlačenie zo súboru toku:

Ak ste v tokovom súbore vytvorili výpis údajov a chcete ich vytlačiť, vykonajte tieto kroky:

1. Do príkazového riadku zadajte PRTCMNTRC.
2. Do poľa **Zo súboru toku** zadajte názov cesty, napríklad /mydir/mytraces/trace1, a stlačte Enter.
3. Ako **Znakový kód** zadajte *EBCDIC, alebo *ASCII. Údaje by ste mali vytlačiť dva razy, raz so zadaním *EBCDIC a druhý raz so zadaním *ASCII.
4. Do poľa **Formátovať údaje TCP/IP** zadajte *YES a stlačte dva razy Enter.
5. Vykonajte kroky 1 až 4 ešte raz, ale tentoraz zadajte iný znakový kód.

Ďalší postup:
Prezrite si obsah sledovania komunikácií

Prezrite si obsah sledovania komunikácií

Obsah sledovania komunikácií si prezriete vykonaním nasledujúcich krokov:

1. Do príkazového riadku zadajte WRKOUTQ OUTQ(IBMLIB/IBMOUTQ).
2. V dialógu **Práca s výstupným frontom** stlačte F11 (Pohľad 2) a prezrite si dátum a čas spoolového súboru, s ktorým chcete pracovať. Ak sa na displeji objaví Viac... a vy potrebujete pokračovať v hľadaní spoolového súboru, posúvajte sa vpred a vzad v zozname súborov; inak prejdite na ďalší krok.
3. Do stĺpca **Opt**, vedľa spoolového súboru, ktorý chcete zobraziť, zadajte 5. Posledný súbor obsahuje najaktuálnejšie výsledky sledovania komunikácií.
4. Overte si, či ide o sledovanie komunikácie sledovanej linky a že súhlasia časy spustenia a ukončenia sledovania.

Ďalší postup:
Prečítajte si sledovanie komunikácií

Prečítajte si sledovanie komunikácií

Výsledok sledovania komunikácií zobrazuje niekoľko typov informácií. Prvá časť sumarizuje parametre, ktoré ste zadali pri spustení sledovania, napríklad názov **Objektu konfigurácie**. Nižšie nájdete zoznam položiek, napríklad **Číslo záznamu** a **S**/**R** aj s príslušnými definíciami; tieto položky reprezentujú nadpisy, ktoré sa neskôr použijú na identifikáciu častí údajov sledovania. Tento zoznam vám bude užitočný počas čítania údajov o sledovaní. Tento obrázok zobrazuje predbežné informácie sledovania komunikácií.

```
                              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
```

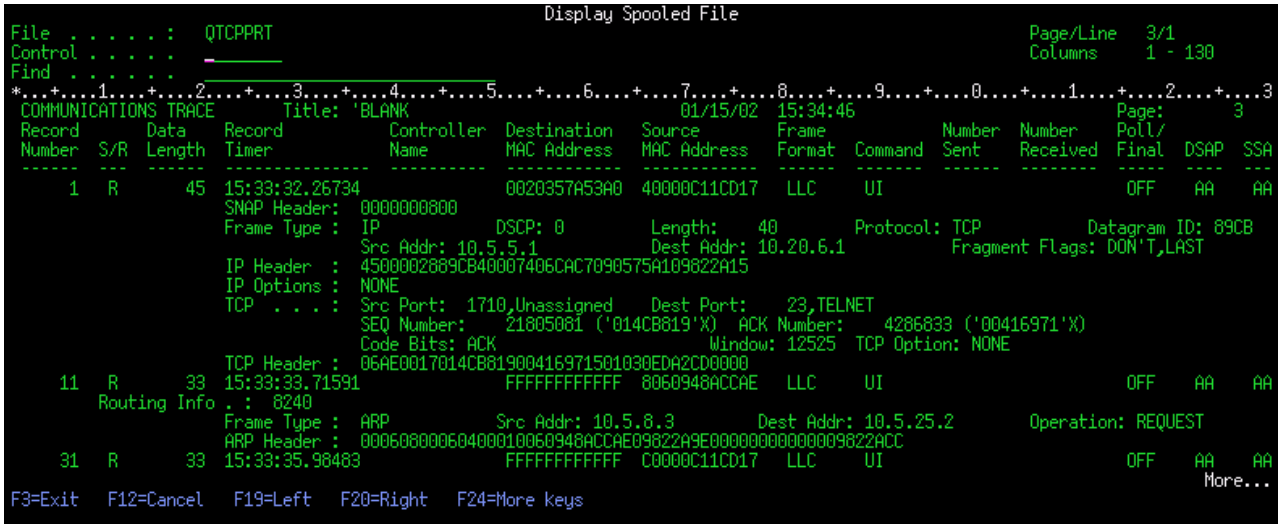
Po prečítaní úvodných informácií prejdite nižšie k aktuálnym údajom TCP/IP vo výstupe sledovania. Riadok nadpisov, začínajúci položkou **Číslo záznamu**, určuje každú časť zaznamenaných údajov. Každé Číslo záznamu predstavuje rámec a ten obsahuje informácie ako zdrojová a cieľová IP adresa, dĺžka celého IP datagramu, typ služby (TOS), zdrojový a cieľový port a čísla potvrdenia (ACK). Tieto informácie by vám mali pomôcť vyladiť problém, ktorý máte s TCP/IP na tomto serveri iSeries alebo na priradenej sieti.

Ak za číslom záznamu nájdete hviezdičku (*), napríklad 31*, uvedomte si, že hviezdička nahrádza chýbajúce údaje sledovania; toto sa stane, ak sú údaje o sledovaní komunikácií poškodené. Údaje o sledovaní komunikácií sa zbierajú procesorom I/O (IOP). Ak je komunikačná linka príliš vyťažená, IOP určí priority celej sieťovej komunikácii a vstupom a výstupom údajov priradí vyššiu prioritu, než informáciám o sledovaní komunikácií. Za týchto podmienok môže IOP stratiť niektoré zo záznamov o sledovaní komunikácií. Môže to naznačovať, že IOP nie je schopný zvládnuť nadmerné rýchlosti komunikácie v sieti.

Ak vám chýbajú niektoré údaje o sledovaní komunikácie, zvážte tieto možnosti:

- Pripustite, že vaša komunikačná linka je preťažená a že vám budú chýbať rámce zo sledovania komunikácie.
- Preskúmajte premávku na komunikačnej linke a určite, či môže byť jej časť presmerovaná do inej linky alebo rozhrania TCP/IP.

Tento obrázok zobrazuje časť údajov TCP/IP zo sledovania komunikácií.



Ukončili ste proces sledovania komunikácií.

Choďte na Ďalšie funkcie sledovania komunikácií a zistite, ako vymazať sledovanie, skontrolovať stav sledovania a určiť veľkosť pamäte.

Ďalšie funkcie sledovania komunikácií

Tieto príkazy a API poskytujú ďalšie funkcie sledovania komunikácií.

Vymazať sledovanie komunikácií

Skôr než spustíte nové sledovanie komunikácií na tej istej linke, musíte vymazať to predchádzajúce. Sledovanie komunikácií môže byť vymazané, len ak je sledovanie ukončené. Táto akcia vymaže vyrovnávaciu pamäť sledovania konkrétnej linky alebo opisu sieťového rozhrania.

Obsah sledovania komunikácií vymažete vykonaním týchto krokov:

1. Do príkazového riadku zadajte DLTCMNTRC.

2. Ako **Objekt konfigurácie** zadajte názov linky, napríklad TRNLINE.
3. Ako **Typ** zadajte typ zdroja, teda *LIN alebo *NWI.

Skontrolovať sledovanie komunikácií

Je možné, že budete potrebovať zistiť, či na vašom serveri práve prebieha nejaké sledovanie komunikácií. Použitím príkazu Check communications trace (CHKCMNTRC) zistíte stav sledovania pre konkrétnu linku a opis sieťového rozhrania, alebo pre všetky sledovania zadaného typu, ktoré na serveri prebiehajú. Výsledkom je správa o stave.

Stav sledovania komunikácií skontrolujete týmito krokmi:

1. Do príkazového riadku zadajte CHKCMNTRC.
2. Ako **Objekt konfigurácie** zadajte názov linky, napríklad TRNLINE, alebo zadajte *ALL, ak chcete skontrolovať stav všetkých sledovaní pre zadaný typ.
3. Ako **Typ** zadajte typ zdroja, teda *LIN alebo *NWI.

Kontrolujte pamäťový priestor automaticky

Použite API Check Communications Trace (QSCCHKCT) na automatické kontrolovanie maximálneho priestoru vyhradeného pre sledovanie a veľkosti všetkých aktívnych alebo pozastavených sledovaní na vašom serveri. Viac informácií o API Check Communications Trace (QSCCHKCT) nájdete v téme Application Programming Interfaces (API).

Kapitola 5. Konfiguračné súbory TCP/IP

Všetky reportované problémy TCP/IP by mali obsahovať aj kópiu konfiguračných súborov použitých pri procese TCP/IP. Kópiu konfiguračných súborov TCP/IP získate nasledovne:

1. Ak ste nevytvorili knižnicu IBMLIB ani výstupný front IBMOUTQ, zadajte nasledujúci príkaz:

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

2. Zadaním nasledujúcich príkazov pridajte knižnicu IBMLIB do vášho zoznamu knižníc a zmeňte výstupný front úlohy na výstupný front IBMOUTQ:

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

   Zadaním nasledujúcich príkazov získajte zoznam všetkých fyzických súborov použitých pri konfigurácii TCP/IP:

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

   Obsah každého zo súborov môžete nakopírovať použitím možnosti 3 (Copy from the work with files), alebo môžete v príkazovom riadku zadať nasledujúci príkaz pre každý zo súborov, a tak skopírovať ich obsah do osobitných spoolových súborov vo výstupnom fronte IBMOUTQ.

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

Kapitola 6. Protokol aktivity produktu

Kód TCP/IP LIC vytvorí záznam v protokole aktivity produktu zakaždým, keď je datagram TCP/IP vyradený z dôvodu chyby protokolu.

Pri odchádzajúcich datagramoch TCP/IP je príkladom takejto chyby protokolu zlyhanie pri vytváraní pripojenia X.25, cez ktoré mal byť tento datagram odoslaný. V takomto prípade je užívateľovi ohlásená chyba a odchádzajúci datagram je vyradený.

Prichádzajúci datagram vytvorí zápis do protokolu aktivity produktu, ak sú splnené obe tieto podmienky:

- Atribút Zaznamenať chyby protokolu TCP/IP je nastavený na *YES
- Datagram neprešiel niektorým z testov platnosti protokolu TCP/IP určených v RFC 1122, a tým spôsobil, že ho systém vyradil. (**Vyradený potichu** znamená nasledovné: Vyradiť doručený datagram bez toho, aby bola pôvodnému zariadeniu oznámená chyba.) Takýmito datagramami sú napríklad tie, ktorých kontrolné súčty alebo cieľové adresy nie sú platné.

Keď je datagram vyradený takýmto spôsobom, hlavičky datagramov IP a TCP/UDP sú zaznamenané v detailných údajoch záznamu v Protokole aktivity produktu. Takéto záznamy v Protokole aktivity produktu majú odkazový kód 7004.

Vytlačené v USA