z/OS TCP/IP PACKET TRACING

Packet trace is a diagnostic method for obtaining traces of IP packets flowing to and from a TCP/IP stack on a z/OS Communications Server host. You can use this trace to copy IP packets as they enter or leave TCP/IP (not ALCS), and then examine the contents of the copied packets.

Note that many details about (a) how to start and stop a packet trace, (b) which options may be used, and (c) how to use IPCS can be found in the IP Diagnosis Guide and in the IPCS User Guide. Those manuals are distributed on the operating system Collection CD-ROMs and are available for on-line viewing at the IBM website.

There are essentially three steps:

(I) Put the trace data into an internal TCP/IP buffer using VARY TCPIP Commands)
(II) Write the trace data out of the internal buffer using MVS TRACE CT Commands
(III) Format the trace data using IPCS.

- **BEFORE YOU START**

If needed consult your MVS system programmer.

(a) You must have the proper RACF authorization.

(b) You must know the tcpprocname (see also ISPF DA).

(c) The size of the internal TCP/IP buffer and other trace parameters must be defined in the PARMLIB member CTIEZBxx.

(d) You must store a Component Trace external writer procedure in a PROCLIB. Use a PROCLIB (See IEFPDSI) found in the PARMLIB member MSTJCLxx. (Most likely that will be SYS1.PROCLIB).

```
//TCPIPT       PROC
//IEFPROC    EXEC  PGM=ITTTRCWR
//TRCOUT01 DD DSNAME=my.tcpip.traceout,DISP=SHR
```

(e) Allocate *my.tcpip.traceout* with attributes: VB, BLKSIZE=27998, LRECL=27994, PS, and as much space as you need.

- **START / STOP PACKET PACKET TRACING AND USE IPCS TO FORMAT THE TRACE (A quick guide)**

(a) Start packet tracing

Use this vary command to start a packet trace (nb there are synonyms):

V TCPIP,tcpprocname,PKT,ON,FULL,IP=ipaddr|*,SRCP=port,**DEST=**port

1) ipaddr is the destination or source IP address (or * = all addresses).
2) When you must trace both source (SRCP) and destination (DEST) packets for a particular port, enter two PKT commands,

e.g. V TCPIP,tcpprocname,PKT,ON,FULL,IP=aa.aa.aa.aa,SRCP=8002
V TCPIP,tcpprocname,PKT,ON,FULL,IP=aa.aa.aa.aa,DEST=8002

NB. If SRCP or DEST are not specified then all source and destination ports will be traced.

There are many other options that can be specified, See the IP diagnosis guide for more details.

(b) Start and connect the external writer

To start the external writer and 'connect' it issue the following commands:

TRACE CT,WTRSTART=TCPIPT,WRAP|NOWRAP

This will start the external writer using procedure **TCPIPT** (WRAP or NOWRAP defines whether the trace should be wrapped or not).

TRACE CT,ON,COMP=SYSTCPDA,SUB=(tcpprocname)

This will start the component trace for SYSTCPDA (PKTTRACE). NB. This will result in a WTOR to which you reply:

xx,WTR=TCPIPT,END

(c) Disconnect and stop the external writer

After tracing you need to 'disconnect' and to stop the external writer as follows:-

TRACE CT,ON,COMP=SYSTCPDA,SUB=(tcpprocname)

This will disconnect the external writer and will stop the component trace resulting in a WTOR to which you reply:

xx,WTR=DISCONNECT,END

TRACE CT,WTRSTOP=TCPIPT

This will stop the external writer. This should result in this message:

AHL904I THE FOLLOWING TRACE DATASETS CONTAIN TRACE DATA
MY.TCPIP.TRACEOUT

(d) Stop TCP/IP packet tracing:

V TCPIP,tcpprocname,PKT,OFF

(e) Format the trace with IPCS

To format the packet trace do following:

Invoke IPCS
Select 1 - Standard IPCS (if needed**)**
Select 6 - Command
Issue DROPD (just in case)
Issue SETD DSN('MY.TCPIP.TRACEOUT')

Return to main IPCS menu and
Select 2 - Analysis
Select 7 - Traces
Select 1 - Component Traces
Select D - Display

In the Display panel enter the following:-

```
-------------------------------------------------------------------------------
  ------------------------------------------- CTRACE DISPLAY PARAMETERS  -------
  COMMAND ===> s

    System      ===>            (System name or blank)
    Component   ===> systcpda   (Component name (required))
    Subnames    ===>

    GMT/LOCAL   ===>                           (G or L, GMT is default)
    Start time  ===>                           (mm/dd/yy,hh:mm:ss.dddddd or
    Stop time   ===>                            mm/dd/yy,hh.mm.ss.dddddd)
    Limit       ===>           Exception ===>
    Report type ===> full      (SHort, SUmmary, Full, Tally)
    User exit   ===>           (Exit program name)
   Override source ===>
   Options         ===> packettrace

   To enter/verify required values, type any character
   Entry IDs ===>   Jobnames ===>   ASIDs ===>   OPTIONS ===>   SUBS ===>

   ENTER = update CTRACE definition.  END/PF3 = return to previous panel.
   S = start CTRACE.  R = reset all fields.
-------------------------------------------------------------------------------
```

and hit enter