The Journey through the Layers of Enterprise Extender continues
I knew it must be the firewall!

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com

Mike Riches
IBM United Kingdom
mike_riches@uk.ibm.com

Thursday Feb. 7 2013 8:00-9:00 AM
Session 12856 Golden Gate 3

Twitter @mreede
Find us on Facebook at ip.wizards@groups.facebook.com
sna.wizards@groups.facebook.com
The Problem statement

- EE between VTAM and system i (AS/400)
  - Not a new installation – had been running flawless for months
    - Nothing has changed
- CICS sessions terminate unexpectedly
  - Have to be restarted twice an hour from system i.
- Problem was documented using standard *mustgather*
  - VTAM Internal Trace to Dataspace (pre V1R13)
    - F NET,TRACE,TYPE=VTAM,DSPSIZE=5,OPT=(CIA,HPR)
  - CSDUMP
    - F NET,CSDUMP
# IPCS – Dump Analysis – TSO DNET

## DNET RTPS SWITCH(YES)

<table>
<thead>
<tr>
<th>PU NAME</th>
<th>CP NAME</th>
<th>COSNAME</th>
<th>SWITCH</th>
<th>CONGEST</th>
<th>STALL</th>
<th>SESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR018EB</td>
<td>DBNET1.BEVHVM14</td>
<td>#INTER</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>1</td>
</tr>
<tr>
<td>CNR018E9</td>
<td>DBNET1.BEVHVM14</td>
<td>#CONNECT</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>1</td>
</tr>
</tbody>
</table>

2 OF 2 MATCHING RTP PIPES DISPLAYED

## DNET RTPS CPNAME(BEVHVM14)

<table>
<thead>
<tr>
<th>PU NAME</th>
<th>CP NAME</th>
<th>COSNAME</th>
<th>SWITCH</th>
<th>CONGEST</th>
<th>STALL</th>
<th>SESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR018F1</td>
<td>DBNET1.BEVHVM14</td>
<td>CPSVCMG</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>2</td>
</tr>
<tr>
<td>CNR018EB</td>
<td>DBNET1.BEVHVM14</td>
<td>#INTER</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>1</td>
</tr>
<tr>
<td>CNR018E9</td>
<td>DBNET1.BEVHVM14</td>
<td>#CONNECT</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>1</td>
</tr>
<tr>
<td>CNR018DD</td>
<td>DBNET1.BEVHVM14</td>
<td>RSETUP</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>0</td>
</tr>
</tbody>
</table>

4 OF 4 MATCHING RTP PIPES DISPLAYED
IPCS DUMP Analysis – TSO DNET
VTAM – D NET,RTPS,SWITCH=Yes

### IPCS CLIST to issue VTAM DISPLAY commands
- Same syntax and operands like the real D NET,
- Only for static information (no APING, EEDIAG etc...)
  - Will be withdrawn in V2R1!

### D NET,RTPS,SWITCH=Yes shows 2 pipes
- Currently PATHSWITCH when CSDUMP was taken.
VTAM – D NET,RTPS,ID=cpname

- D NET,RTPS,ID=cpname shows a summary of all pipes
  - The names consist of a prefix and an incremental number
  - Name allows to recognize the sequence of activation
- There are 4 HPR pipes active
- Their activation sequence was
  
  RSETUP -> #CONNECT -> #INTER -> CPSVCMG

---

IKV0017I DNET RTPS CPNAME(BEVHVM14) of 00010

IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = RTPS
IST1695I PU_NAME CP_NAME COSNAME SWITCH CONGEST STALL SESS
.. < IST1960I CNR018F1 DBNET1.BEVHVM14 CPSVCMG NO NO NO 2
.. < IST1960I CNR018EB DBNET1.BEVHVM14 #INTER YES NO NO 1
.. < IST1960I CNR018E9 DBNET1.BEVHVM14 #CONNECT YES NO NO 1
.. < IST1960I CNR018DD DBNET1.BEVHVM14 RSETUP NO NO NO 0
IST2084I 4 OF 4 MATCHING RTP PIPES DISPLAYED
IST314I END
The VIT shows 2 HPR Pipes entering PATHSWITCH
- Reason is SHORT REQUEST RETRY LIMIT EXHAUSTED
- RPN PCB addresses: CNR018EB:13A677F8  CNR018E9:13A67018
VTAM Internal Trace – HPR Pipes to AS400

- These are the HPR pipes to the AS400
  - Notice the pattern of the remote TCIDs
    - An incremental number at offset 1
      - 006017A610 006017A613 006017A617 006017A61B
  - VTAM's TCIDs have an incremental number at offset 0
    - 24ADBC250001 24ADBC300001 24ADBC320001 24ADBC380001
VTAM Internal Trace – RSETUP Pipe I.

There are only outbound packets for this pipe
- Notice the first hop routers address changes
  - IPCONFIG MULTIPATH PERCONNECTION
- Initial TTL of z/OS is 64, local IP address 172.21.205.5
Second RSETUP pipe also shows only outbound traffic
Finally terminates with a CFAULT segment
SENSE A0020001  The RTP connection is terminating.

Remote IP address is 172.21.7.14
VTAM Internal Trace – #CONNECT Pipe

- Outbound packets get an ICMP message
  - Source IP address of ICMP packet is AS400
  - Destination unreachable, Port unreachable
  - This happens after 70 seconds of no traffic!
VTAM Internal Trace – #INTER Pipe

Outbound packets get an ICMP message
Source IP address of ICMP packet is AS400
Destination unreachable, Port unreachable
This happens after 83 seconds of no traffic!
VTAM Internal Trace – inbound packets

All packets come from the same IP address
- All EE packets come in with a TTL of 40
  - ip.id increments: 3EB3, 3EB4, ... 3ECF
- All ICMP packets arrive with a TTL of 56
  - ip.id increments: A882, A883
VTAM Internal Trace – inbound packets

- All packets come from the same IP address
- All EE packets come in with a TTL of 40
  - `ip.id` increments: 3ECF ... 3EDB
- All ICMP packets arrive with a TTL of 56
  - `ip.id` increments: A882,A883,A884 ... A889
The ip.ttl can be used to see how far a packet has travelled.

- All EE packets come in with a TTL of 40
- All ICMP packets arrive with a TTL of 56

### IP TTL - Who is sending this packet?

Initial TTL Value by Operating System

<table>
<thead>
<tr>
<th>OS</th>
<th>ICMP_TTL</th>
<th>UDP_TTL</th>
<th>TCP_TTL</th>
<th>ip.id</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>zOS</td>
<td>64 PING_REQ(255)</td>
<td>64</td>
<td>64</td>
<td>ip.id++ / stack</td>
<td></td>
</tr>
<tr>
<td>Linux 3.0</td>
<td></td>
<td>64</td>
<td></td>
<td>ip.id++ /tcp</td>
<td></td>
</tr>
<tr>
<td>Linux 2.6+</td>
<td></td>
<td>64</td>
<td>64</td>
<td>ip.id++ /tcp</td>
<td></td>
</tr>
<tr>
<td>Tandem</td>
<td></td>
<td>64</td>
<td></td>
<td>iid++</td>
<td></td>
</tr>
<tr>
<td>DataPower</td>
<td></td>
<td>195</td>
<td></td>
<td>ip.id++/tcp</td>
<td>sets SYN,ECN,CWR</td>
</tr>
<tr>
<td>Linux 2.5-</td>
<td></td>
<td>255</td>
<td>64</td>
<td>ip.id++ /tcp</td>
<td></td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td>255</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HP Printer</td>
<td></td>
<td>64</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIX</td>
<td></td>
<td>255</td>
<td>30</td>
<td>60</td>
<td>ip.id++/stack</td>
</tr>
<tr>
<td>Win</td>
<td></td>
<td>128</td>
<td>128</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>IOS</td>
<td></td>
<td>64</td>
<td>64</td>
<td>ip.id++/stack</td>
<td></td>
</tr>
</tbody>
</table>
Tune in to ICMP.fm


- ICMP packets, when closely inspected, can tell the topology
Wireshark - How far away is the sender of the ICMP messages?

1. The sender of the ICMP messages can be determined by analyzing the TTL (Time To Live) values in the packet headers.
2. The packet with TTL = 55 indicates an ICMP error, suggesting the sender is closer than the packet with TTL = 64.
3. The packet with TTL = 40 is a STATUS Request, indicating the sender is further away than the packet with TTL = 41.
4. The packet with TTL = 63 is a STATUS Request, suggesting the sender is closer than the packet with TTL = 62.

Complete your sessions evaluation online at SHARE.org/SanFranciscoEval
Wireshark – pcapng (Rel. 1.8.0 and up)
Allows you to leave comments

- Commenting on the file
- Commenting on packets in the file
The Journey through the Layers of Enterprise Extender continues
I knew it must be the firewall!

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com

Mike Riches
IBM United Kingdom
mike_riches@uk.ibm.com

Thursday Feb. 7 2013 8:00-9:00 AM
Session 12856 Golden Gate 3

Twitter @mreede
Find us on Facebook at ip.wizards@groups.facebook.com
sna.wizards@groups.facebook.com