

# 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  
Session 12856

8:00-9:00 AM  
Golden Gate 3

Twitter @mreede

Find us on Facebook at [ip.wizards@groups.facebook.com](https://www.facebook.com/ip.wizards@groups.facebook.com)  
[sna.wizards@groups.facebook.com](https://www.facebook.com/sna.wizards@groups.facebook.com)

SocialBusiness  
IBMSmartCloud



# 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

```
IKV0017I DNET RTPS SWITCH(YES) of 0000
-----
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = RTPS
IST1695I PU NAME          CP NAME          COSNAME SWITCH CONGEST STALL SESS
.. < IST1960I CNR018EB DBNET1.BEVHVM14 #INTER YES NO NO 1
.. < IST1960I CNR018E9 DBNET1.BEVHVM14 #CONNECT YES NO NO 1
IST2084I          2 OF          2 MATCHING RTP PIPES DISPLAYED
IST314I END
```

```
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
```

# IPCS DUMP Analysis – TSO DNET VTAM – D NET,RTPS,SWITCH=YES

```
IKV0017I DNET RTPS SWITCH(YES)                                of 0000
-----
IST097I DISPLAY ACCEPTED
IST350I DISPLAY TYPE = RTPS
IST1695I PU NAME          CP NAME          COSNAME SWITCH CONGEST STALL SESS
.. < IST1960I CNR018EB DBNET1.BEVHVM14    #INTER   YES     NO     NO     1
.. < IST1960I CNR018E9 DBNET1.BEVHVM14    #CONNECT YES     NO     NO     1
IST2084I          2 OF          2 MATCHING RTP PIPES DISPLAYED
IST314I END
```

- 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

```

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
  
```

- D NET,RTPS,ID=cpname shows a summary of all pipes
  - The names consists 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

# VTAM Internal Trace - PATHSWITCH

```

D9E3D7D7 3700000B 00000032 00000078 970D1318 00000000 13A677F8 15DD2010 | RTPP. ....p.....w.8...
D4E2C740 3700E4F1 F4F9F4D9 D7C3D7C3 15DD2990 970EB59C 00000000 00000000 | MSG ..U1494RPCPC....p.....
D4E2C7F2 E2E3C1D9 E3C5C440 4040C3D5 D9F0F1F8 C5C2C4C2 D5C5E3F1 4BC2C5E5 | MSG2STARTED CNR018EB:BNET1.BEV
D4E2C7F2 C8E5D4F1 F4404000 00000000 00000000 00000000 00000000 00000000 | MSG2HVM14 .....
- - - - -
D9E3D7D7 3700000B 00000032 000000F0 970D1318 00000000 13A67018 15DDA010 | RTPP. ....0p.....w....
D4E2C740 3700E4F1 F4F9F4D9 D7C3D7C3 15DDA990 970EB59C 00000000 00000000 | MSG ..U1494RPCPC...z.p.....
D4E2C7F2 E2E3C1D9 E3C5C440 4040C3D5 D9F0F1F8 C5F9C4C2 D5C5E3F1 4BC2C5E5 | MSG2STARTED CNR018E9:BNET1.BEV
D4E2C7F2 C8E5D4F1 F4404000 00000000 00000000 00000000 00000000 00000000 | MSG2HVM14 .....
- - - - -
D4E2C7E2 37000000 E2C1E9C6 F5D7D7E3 0040C7F2 C9E2E3F1 F8F1F8C9 4040D7C1 | MSGS...SAZF5PPT. G2IST1818I PA
D4E2C7F2 E3C840E2 E6C9E3C3 C840D9C5 C1E2D6D5 7A40E2C8 D6D9E340 D9C5D8E4 | MSG2TH SWITCH REASON: SHORT REQU
- - - - -
D4E2C740 3700E4F1 F4F8F8D9 C3C3C4D9 1736F148 972FDD0E 00000000 00000000 | MSG ..U1488RCCDR..1.p.....
D4E2C7F2 C9D5C1C3 E3C9E5C1 E3C9D6D5 C3D5D9F0 F1F8C4C5 D7C1E2E2 C9E5C5C4 | MSG2INACTIVATIONCNR018DEPASSIVED
D4E2C7F2 C2D5C5E3 F14BC2C5 E5C8E5D4 F1F44040 00000000 00000000 00000000 | MSG2BNET1.BEVHVM14 .....
- - - - -
D4E2C740 370000E4 E2E240D5 D6C3C3D7 17B5A910 96B8BBAC 00000000 00000000 | MSG ...USS NOCCP...z.o.....
D4E2C7F2 00160000 D4D6C4C9 C6E840E2 D5C16BC3 E2C4E4D4 D7404040 40400000 | MSG2...MODIFY SNA,CSDUMP ..

```

- The VIT shows 2 HPR Pipes entering PATHSWITCH
- Reason is SHORT REQUEST RETRY LIMIT EXHAUSTED
- RPNCB addresses: CNR018EB:13A677F8 CNR018E9:13A67018

# VTAM Internal Trace – HPR Pipes to AS400

ISTRTPPU		Remote TCID	Local TCID	APPNCOS	RPNCB	Started
CNR018DD	10	006017A6110000D0	24ADBC2400010E17	RSETUP	143E7018	ACTIVE 08:28.57
CNR018DE	20	006017A610000050	24ADBC2500010E37	RSETUP	13E9D7F8	
CNR018E9	25	006017A613000100	24ADBC3000010E4C	#CONNECT	13A67018	PASSIVE 11:01:03
CNR018EB	80	006017A6170000C8	24ADBC3200010EC9	#INTER	13A677F8	PASSIVE 11:01:03
CNR018F1	105	006017A61B0000C0	24ADBC3800010E8D	CPSVCMG	13D32D38	PASSIVE 11:11:14

- 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.

B-VAMP_MAINZ_160x62				
Options		Macros		
----- 2cIP - TRACE ANALYSIS PANEL -----				
=> CNR018DD				
Time Stamp	Description (short)	TTL	Next HOP	IP Address
11:11:22.75	ARR RPNCB:143E7018 SR(kb/s):200 SZ:143			
11:11:22.75	NLPO RPNCB:143E7018 TCID:006017A6110000D0 BSN:00000076 ARB REQ RS			
11:11:22.75	DDPR EE_NET TCID:006017A6110000D0 BSN:00000076 ARB REQ RS	64	172.021.204.001	172.21.205.5
11:11:22.79	ARR RPNCB:143E7018 SR(kb/s):200 SZ:145			
11:11:22.79	NLPO RPNCB:143E7018 TCID:006017A6110000D0 BSN:000000EC RS			
11:11:22.79	DDPR EE_NET TCID:006017A6110000D0 BSN:000000EC RS	64	172.021.204.002	172.21.205.5
11:11:27.40	NLPO RPNCB:143E7018 TCID:006017A6110000D0 BSN:00000164 STATUS:00000			
11:11:27.40	DDPR EE_NET TCID:006017A6110000D0 BSN:00000164 STATUS:00000000	64	172.021.204.002	172.21.205.5
11:11:32.10	NLPO RPNCB:143E7018 TCID:006017A6110000D0 BSN:00000164 STATUS:00000			
11:11:32.11	DDPR EE_NET TCID:006017A6110000D0 BSN:00000164 STATUS:00000000	64	172.021.230.002	172.21.205.5

- 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



# VTAM Internal Trace – RSETUP Pipe II.

Description (short)	TTL	Next HOP	IP Address	Iden	◇ IP Address (+ Port Mode)	IP Address (+ Port From	IP Address (+ Port to
ARB RPNCB:13E9D7F8 SR(kb/s):215 S2:143							
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000044F3 ARB REQ RS							
ODPK EE_NET TCID:006017A610000050 BSN:000044F3 ARB REQ RS	64	172.021.204.001	172.21.205.5	7B5E	➤	172.21.7.14(12001)	
ARB RPNCB:13E9D7F8 SR(kb/s):215 S2:145							
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:00004569 RS							
ODPK EE_NET TCID:006017A610000050 BSN:00004569 RS	64	172.021.204.002	172.21.205.5	7B65	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.204.001	172.21.205.5	7B79	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.204.002	172.21.205.5	7BA0	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.204.001	172.21.205.5	7BDF	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.230.001	172.21.205.5	7BFA	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.204.001	172.21.205.5	7C10	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.204.002	172.21.205.5	7C21	➤	172.21.7.14(12001)	
NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E							
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E	64	172.021.230.002	172.21.205.5	7C40	➤	172.21.7.14(12001)	

NLPO RPNCB:13E9D7F8 TCID:006017A610000050 BSN:000045E1 STATUS:00003F8E  
 ODPK EE\_NET TCID:006017A610000050 BSN:000045E1 CFAult Sense(A0020001)

- 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

----- 2cIP - TRACE ANALYSIS PANEL -----

> CNR018E9 #CONNECT pipe entering PATHSWITCH

Time(De)	Description (short)	TTL	IP Address	Iden	IP Address (+ Port)	Iden
018E9						
0.000	ODPK EE_MED TCID:24ADBC3000010E4C BSN:00000958 STATUS:0000084D	40	172.21.205.5		172.21.7.14(12003)	3EC1
0.001	NLPI RPNCB:13A67018 TCID:24ADBC3000010E4C BSN:00000958 STATUS:000008					
0.002	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.001	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	63DA	172.21.7.14(12003)	
70.811	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009	64	172.21.205.5	79C0	172.21.7.14(12003)	
0.000	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	56	172.21.205.5		172.21.7.14	A882
0.009	ODPK <b>ICMP/DESTUNR Port Unreachable</b>					
0.268	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.000	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	79DA	172.21.7.14(12003)	
0.001	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A885
0.496	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.000	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	7A18	172.21.7.14(12003)	
0.011	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A887
0.533	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.002	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	7A5E	172.21.7.14(12003)	
0.002	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A888
0.532	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.008	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	7A8A	172.21.7.14(12003)	
0.453	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.001	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	7ABF	172.21.7.14(12003)	
0.565	NLPO RPNCB:13A67018 TCID:006017A613000100 BSN:0000084D STATUS:000009					
0.002	ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958	64	172.21.205.5	7AF6	172.21.7.14(12003)	
0.558	<b>RTTP RPNCB:13A67018</b>					

- 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

> CNR018EB #INTER pipe enterin PATHSWITCH █ 2cIP - TRACE ANALYSIS PANEL

Time(DeI	Description (short)	TTL	IP Address	Iden	IP Address (+ Port	Iden
018EB					Mode	Mode
0.002	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CDD ARB REQ FID5	64	172.21.205.5	618A	172.21.7.14(12002)	
0.012	ODPK EE_HIG TCID:24ADBC3200010EC9 BSN:0002CBCF STATUS:00005CFB	40	172.21.205.5		172.21.7.14(12002)	3EBA
0.002	NLPI RPNCB:13A677F8 TCID:24ADBC3200010EC9 BSN:0002CBCF STATUS:00005C					
0.215	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.003	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	61A4	172.21.7.14(12002)	
0.003	ODPK EE_HIG TCID:24ADBC3200010EC9 BSN:0002CBCF STATUS:00005CFB	40	172.21.205.5		172.21.7.14(12002)	3EBB
0.002	NLPI RPNCB:13A677F8 TCID:24ADBC3200010EC9 BSN:0002CBCF STATUS:00005C					
83.444	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.000	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	79BF	172.21.7.14(12002)	
0.009	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A883
0.267	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.000	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	79D9	172.21.7.14(12002)	
0.002	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A884
0.496	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.000	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	7A17	172.21.7.14(12002)	
0.012	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A886
0.530	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.002	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	7A5D	172.21.7.14(12002)	
0.539	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.006	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	7A8B	172.21.7.14(12002)	
0.452	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.001	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	7ABE	172.21.7.14(12002)	
0.004	ODPK <b>ICMP/DESTUNR Port Unreachable</b>	56	172.21.205.5		172.21.7.14	A889
0.559	NLPO RPNCB:13A677F8 TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CB					
0.002	ODPK EE_HIG TCID:006017A6170000C8 BSN:00005CFB STATUS:0002CBCF	64	172.21.205.5	7AF5	172.21.7.14(12002)	
0.500	RTPP RPNCB:13A677F8					

- 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

2cIP - TRACE ANALYSIS PANEL

Inbound traffic from 'AS400' ■

Time(DeI	Description (short)	TTL	IP Address	IP Address (+ Port	Iden
0.006	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB3
0.041	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB4
0.006	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB5
0.061	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB6
0.006	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB7
0.064	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB8
0.005	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EB9
0.078	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EBA
0.224	ODPK EE_HIG TCID:24ADBC3200010EC9	40	172.21.205.5	172.21.7.14(12002)	3EBB
12.631	ODPK EE_MED TCID:24ADBC3000010E4C	40	172.21.205.5	172.21.7.14(12003)	3EC1
70.780	ODPK EE_NET TCID:006017A61B0000C0	40	172.21.205.5	172.21.7.14(12001)	3ECF
0.046	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A882
0.000	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A883
0.003	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ECF
0.000	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED0

- 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

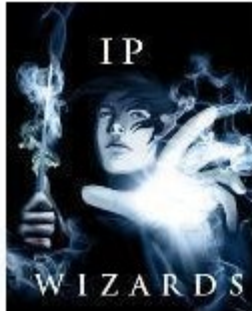
Time(Dec)	Description (short)	TTL	IP Address	IP Address (+ Port)	Iden
0.046	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A882
0.000	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A883
0.003	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED0
0.000	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED1
0.001	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED2
0.038	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED3
0.007	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED4
0.023	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED5
0.050	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED6
0.006	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED7
0.010	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED8
0.036	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3ED9
0.032	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3EDA
0.058	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A884
0.000	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A885
0.509	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A886
0.000	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A887
0.538	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A888
0.998	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	172.21.7.14	A889
1.584	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3EDB
0.001	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	172.21.7.14(12001)	3EDC

- 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

# http://tinyurl.com/ipwizards

## IP TTL: The Time To Live is a Hop Count

▼ ip wizards



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

#### Initial TTL Valuse by Operating System

OS	ICMP_TTL	UDP_TTL	TCP_TTL	ip.id	Remarks
zOS	64 PING_REQ(255)	64	64	ip.id++ / stack	
Linux 3.0			64	ip.id++ /tcp	
Linux 2.6+	255	64	64	ip.id++ /tcp	
Tandem			64	ipid++	
DataPower			195	ip.id++/tcp	sets SYN,ECN,CWR
Linux 2.5-	255		64	ip.id++ /tcp	
Solaris		255	64		
HP Printer			64		
AIX	255	30	60	ip.id++/stack	
Win	128	128	128		
i5OS		64	64	ip.id++/stack	
Routers	255	255	255		

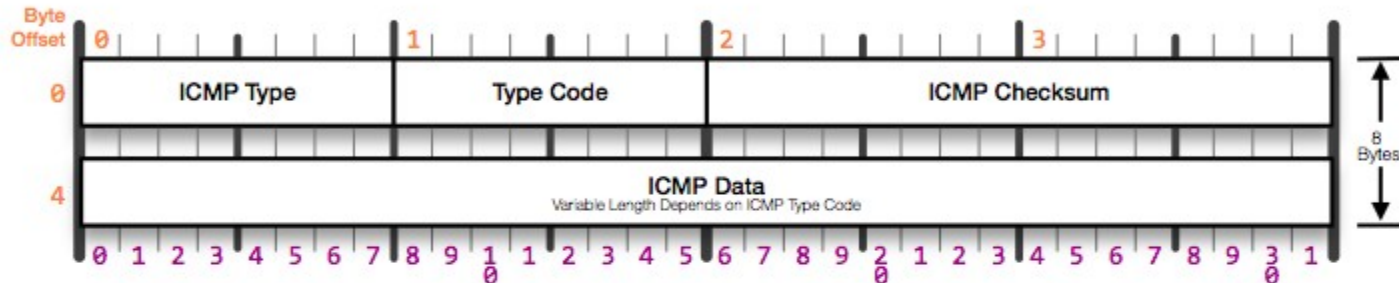
- The ip.ttl can be used to see how far a packet has travelled
  - All EE packets come in with a TTL of 40
  - All ICMP packets arrive with a TTL of 56

# Tune in to ICMP.fm

ICMP Header: <http://www.troyjessup.com/headers/>

## ICMP Header

RFC 792 Outlines the ICMP Protocol



ICMP Type	
0	Echo Reply

ICMP Type	
4	Source Quench

ICMP Type	
10	Router Solicitation

ICMP Type	
3	Destination Unreachable
Type Code	
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
4	Fragment Necessary
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown
8	Obsolete
9	Destination Network Prohibited
10	Destination Host Prohibited
11	Network Unreachable for TOS
12	Host Unreachable for TOS
13	Communication Prohibited

ICMP Type	
5	Redirect
Type Code	
0	Redirect for Network
1	Redirect for Host
2	Redirect for TOS and Network
3	Redirect for TOS and Host

ICMP Type	
11	Time to Live Exceeded
Type Code	
0	TTL Exceeded in Transit
1	TTL Exceeded in Reassembly

ICMP Type	
8	Echo Request

ICMP Type	
12	Parameter Problem
Type Code	
0	Pointer Problem
1	Required Option Missing

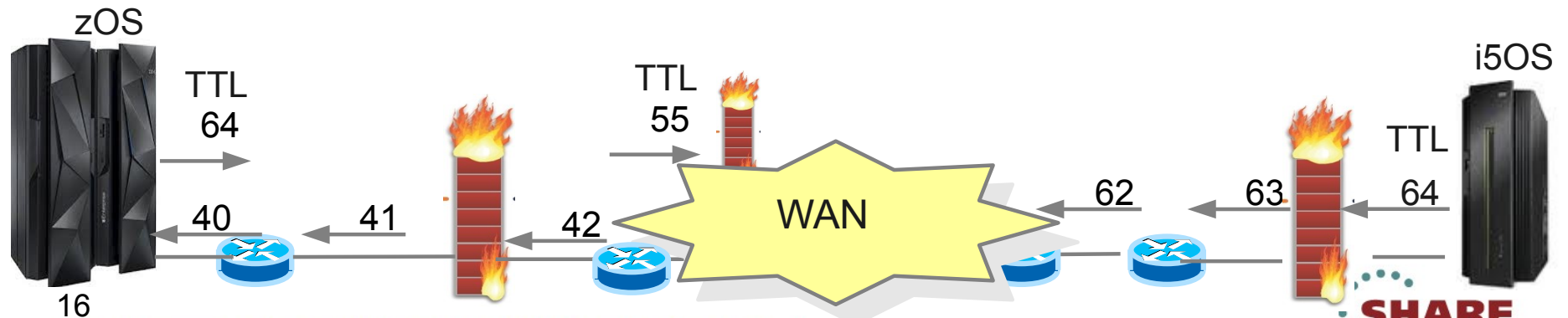
ICMP Type	
9	Router Advertisement

ICMP F  
Created by Troy

- ICMP packets, when closely inspected can tell the topology

# Wireshark - How far away is the sender of the ICMP messages?

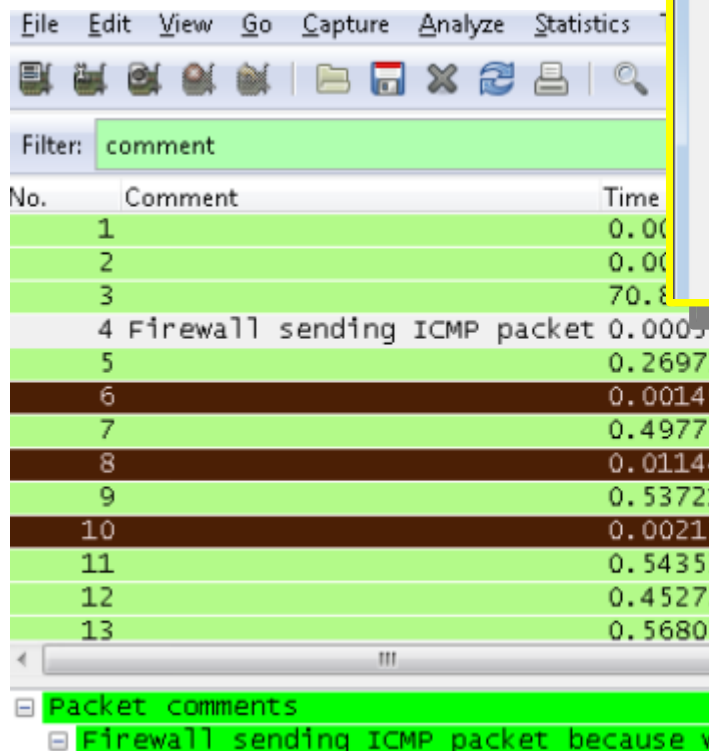
No. .	Time	len	TTL	Source	Destination	tcid	Comment	ANR
1	11:10:02.408	83	40	172.21.7.14	172.21.205.5	24ADBC3000010E4C	STATUS Request	D000000000000000FF
2	11:10:02.409	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF
3	11:11:13.228	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF
4	11:11:13.229	77	55	172.21.7.14	172.21.205.5		ICMP error	A400FF
5	11:11:13.499	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF
6	11:11:13.500	77	55	172.21.7.14	172.21.205.5		ICMP error	A400FF
7	11:11:13.998	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF
8	11:11:14.009	77	55	172.21.7.14	172.21.205.5		ICMP error	A400FF
9	11:11:14.547	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF
10	11:11:14.549	77	55	172.21.7.14	172.21.205.5		ICMP error	A400FF
11	11:11:15.092	77	64	172.21.205.5	172.21.7.14	006017A613000100	STATUS Request	A400FF





# Wireshark – pcapng (Rel. 1.8.0 and up) Allows you to leave comments

- Commenting on the file
- Commenting on packets in the file



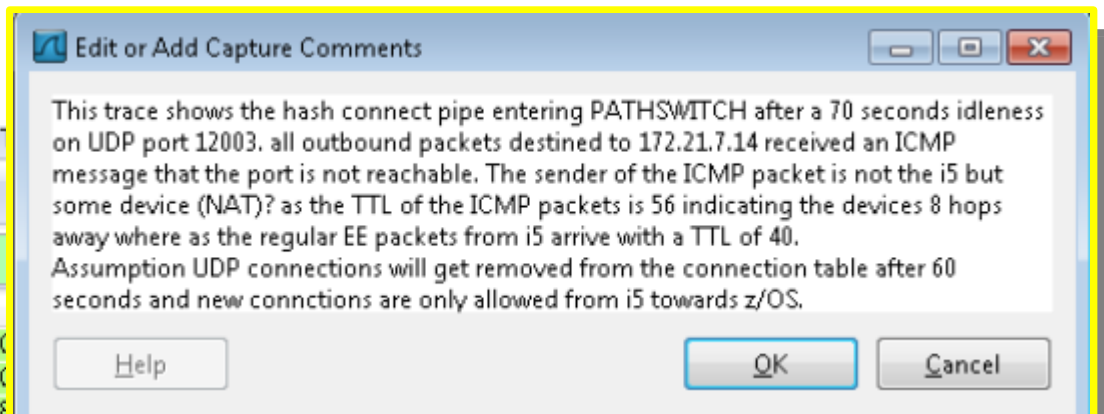
File Edit View Go Capture Analyze Statistics

Filter: comment

No.	Comment	Time
1		0.000000
2		0.000000
3		70.800000
4	Firewall sending ICMP packet	0.000000
5		0.269730
6		0.001490
7		0.497770
8		0.011440
9		0.537210
10		0.002110
11		0.543530
12		0.452720
13		0.568070

Packet comments

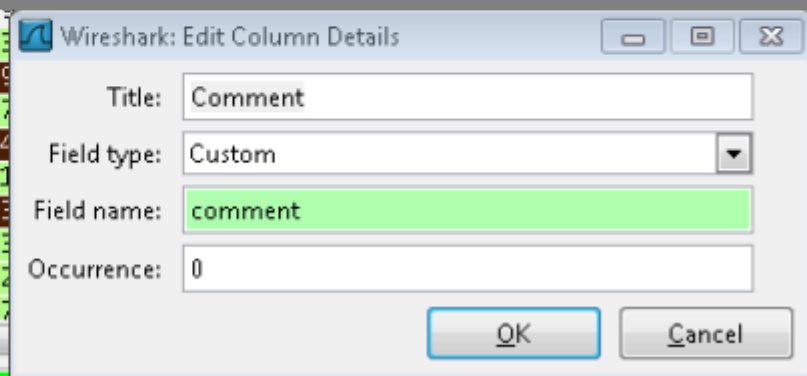
- Firewall sending ICMP packet because we are no longer in the stateful connection table



Edit or Add Capture Comments

This trace shows the hash connect pipe entering PATHSWITCH after a 70 seconds idleness on UDP port 12003. all outbound packets destined to 172.21.7.14 received an ICMP message that the port is not reachable. The sender of the ICMP packet is not the i5 but some device (NAT)? as the TTL of the ICMP packets is 56 indicating the devices 8 hops away where as the regular EE packets from i5 arrive with a TTL of 40. Assumption UDP connections will get removed from the connection table after 60 seconds and new connctions are only allowed from i5 towards z/OS.

Help OK Cancel



Wireshark: Edit Column Details

Title: Comment

Field type: Custom

Field name: comment

Occurrence: 0

OK Cancel

# 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  
Session 12856

8:00-9:00 AM  
Golden Gate 3

Twitter @mreede

Find us on Facebook at [ip.wizards@groups.facebook.com](https://www.facebook.com/ip.wizards@groups.facebook.com)  
[sna.wizards@groups.facebook.com](https://www.facebook.com/sna.wizards@groups.facebook.com)

SocialBusiness  
IBMSmartCloud

