#SHAREorg

SHARE
Technology · Connections · Results

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

SocialBusiness IBMSmartCloud

SHARE in San Francisco 2013

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.

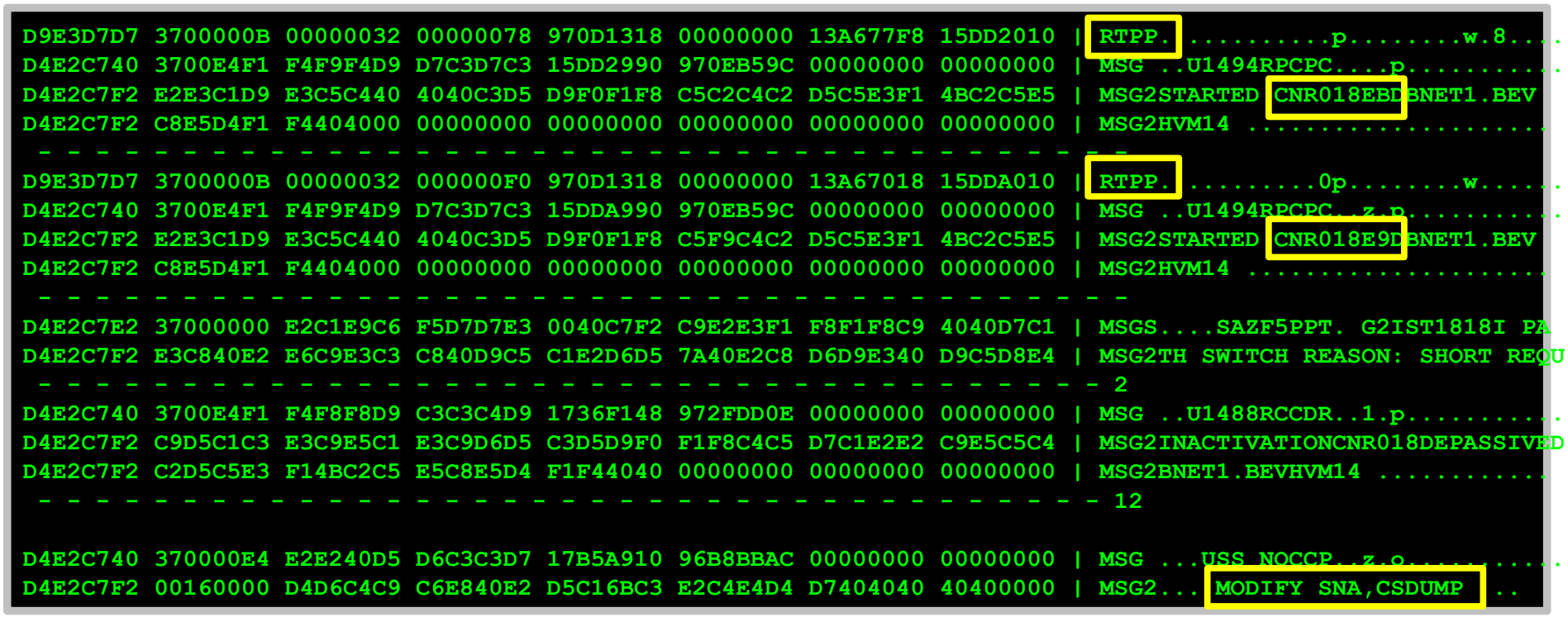
VTAM – D NET,RTPS,ID=cpname

```
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



- 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  006017A611 0000D0    24ADBC2400010E17    RSETUP     143E7018  ACTIVE  08:28.57
CNR018DE    20  006017A610 000050    24ADBC2500010E37    RSETUP     13E9D7F8
CNR018E9    25  006017A613 000100    24ADBC3000010E4C    #CONNECT   13A67018  PASSIVE 11:01:03
CNR018EB    80  006017A617 0000C8    24ADBC3200010EC9    #INTER     13A677F8  PASSIVE 11:01:03
CNR018F1   105  006017A61B 0000C0    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
    - 00**6017A610** 00**6017A613** 00**6017A617** 00**6017A61B**
  - VTAM's TCIDs have an incremental number at offset 0
    - **24ADBC25**0001 **24ADBC30**0001 **24ADBC32**0001 **24ADBC38**0001

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
F018DD ------------------------------------------------------------------------------------------------------------
 11:11:22.75  ARB 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  UDPK EE_NET TCID:006017A6110000D0 BSN:00000076 ARB REQ RS          64 172.021.204.001 172.21.205.5
 11:11:22.79  ARB RPNCB:143E7018 SR(kb/s):200 SZ:145
 11:11:22.79  NLPO RPNCB:143E7018 TCID:006017A6110000D0 BSN:000000EC RS
 11:11:22.79  UDPK 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  UDPK 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  UDPK 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 FILE From 1 to 20
ARB RPNCB:13E9D7F8 SR(kb/s):215 SZ: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 SZ: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:00003F
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:00003F
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:00003F
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:00003F
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:00003F
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:00003F
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 CFault Sense(
ODPK EE_NET TCID:006017A610000050 BSN:000045E1 CFault Sense(A0020001              64  172.021.230.002 172.21.205.5 7C40 => 172.21.7.14(12001)
```

- 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
>   CNRO18E9   #CONNECT pipe entering PATHSWITCH

Time(Del Description (short)                                                    TTL IP Address    Iden    IP Address (+ Port Iden
018E9 ------------------------------------------------------------------------------------------------------------------------Mode F1
   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
   0.000 ODPK EE_MED TCID:006017A613000100 BSN:0000084D STATUS:00000958          64 172.21.205.5 79C0   172.21.7.14(12003)
   0.009 ODPK ICMP/DESTUNR Port Unreachable                                     56 172.21.205.5        172.21.7.14        A882
   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 ICMP/DESTUNR Port Unreachable                                     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 ICMP/DESTUNR Port Unreachable                                     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 ICMP/DESTUNR Port Unreachable                                     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 RTPP RPNCB:13A67018
```

- 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

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

Time(Del Description (short)                                                                TTL IP Address   Iden  IP Address (+ Port Iden
018EB ------------------------------------------------------------------------------------------------------------------------Mode FIL
   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 ICMP/DESTUNR Port Unreachable                                                 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 ICMP/DESTUNR Port Unreachable                                                 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 ICMP/DESTUNR Port Unreachable                                                 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 ICMP/DESTUNR Port Unreachable                                                 56  172.21.205.5       172.21.7.14        A889
   0.559 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 7AF5  172.21.7.14(12002)
   0.560 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!

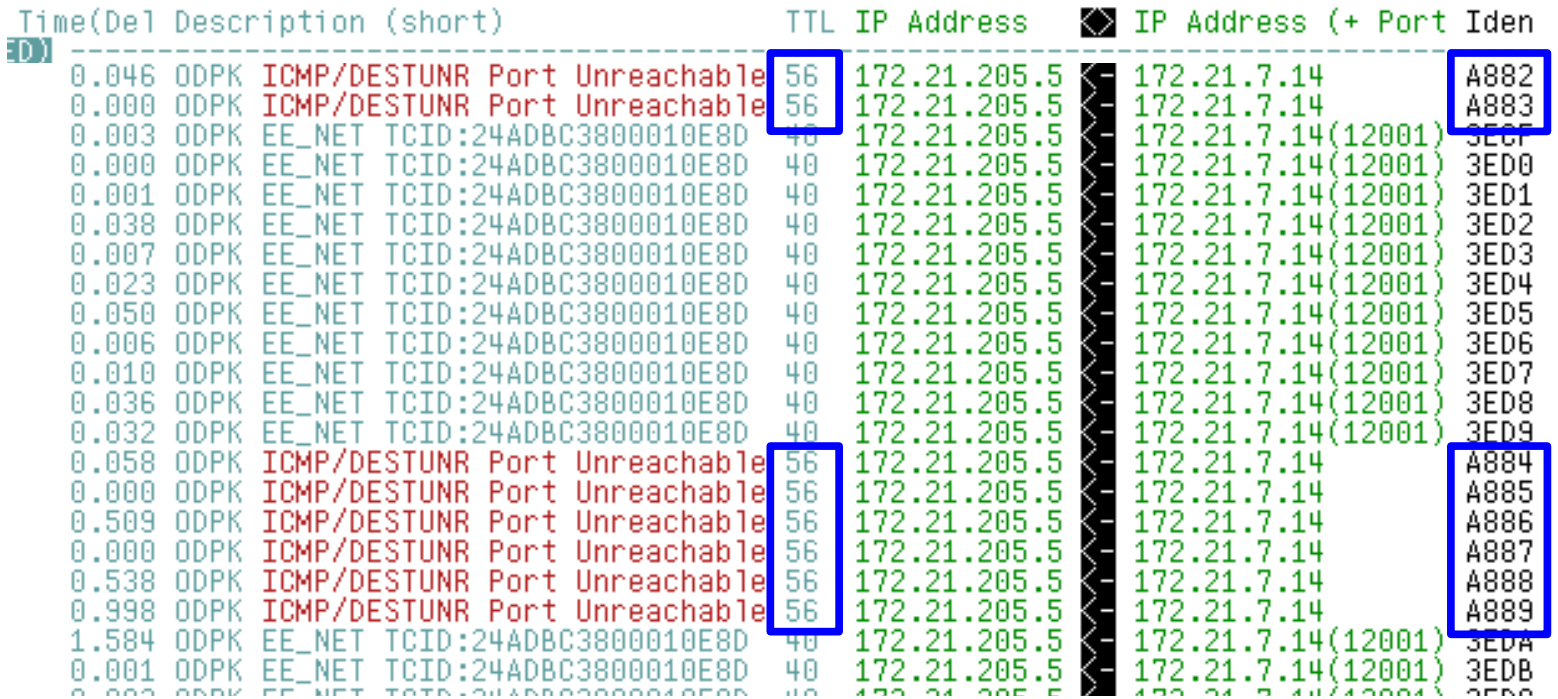
VTAM Internal Trace – inbound packets

```
------------------------------------------ 2cIP - TRACE ANALYSIS PANEL ----------------
      Inbound traffic from 'AS400'

 Time(Del Description (short)                TTL IP Address    <> IP Address (+ Port Iden
ED) ------------------------------------------------------------------------------------
    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) 3ECE
    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

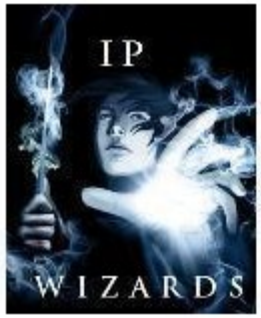


Time(Del	Description (short)	TTL	IP Address		IP Address (+ Port	Iden
0.046	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	<-	172.21.7.14	A882
0.000	ODPK ICMP/DESTUNR Port Unreachable	56	172.21.205.5	<-	172.21.7.14	A883
0.003	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ECF
0.000	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED0
0.001	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED1
0.038	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED2
0.007	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED3
0.023	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED4
0.050	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED5
0.006	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED6
0.010	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED7
0.036	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED8
0.032	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3ED9
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)	3EDA
0.001	ODPK EE_NET TCID:24ADBC3800010E8D	40	172.21.205.5	<-	172.21.7.14(12001)	3EDB

- 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

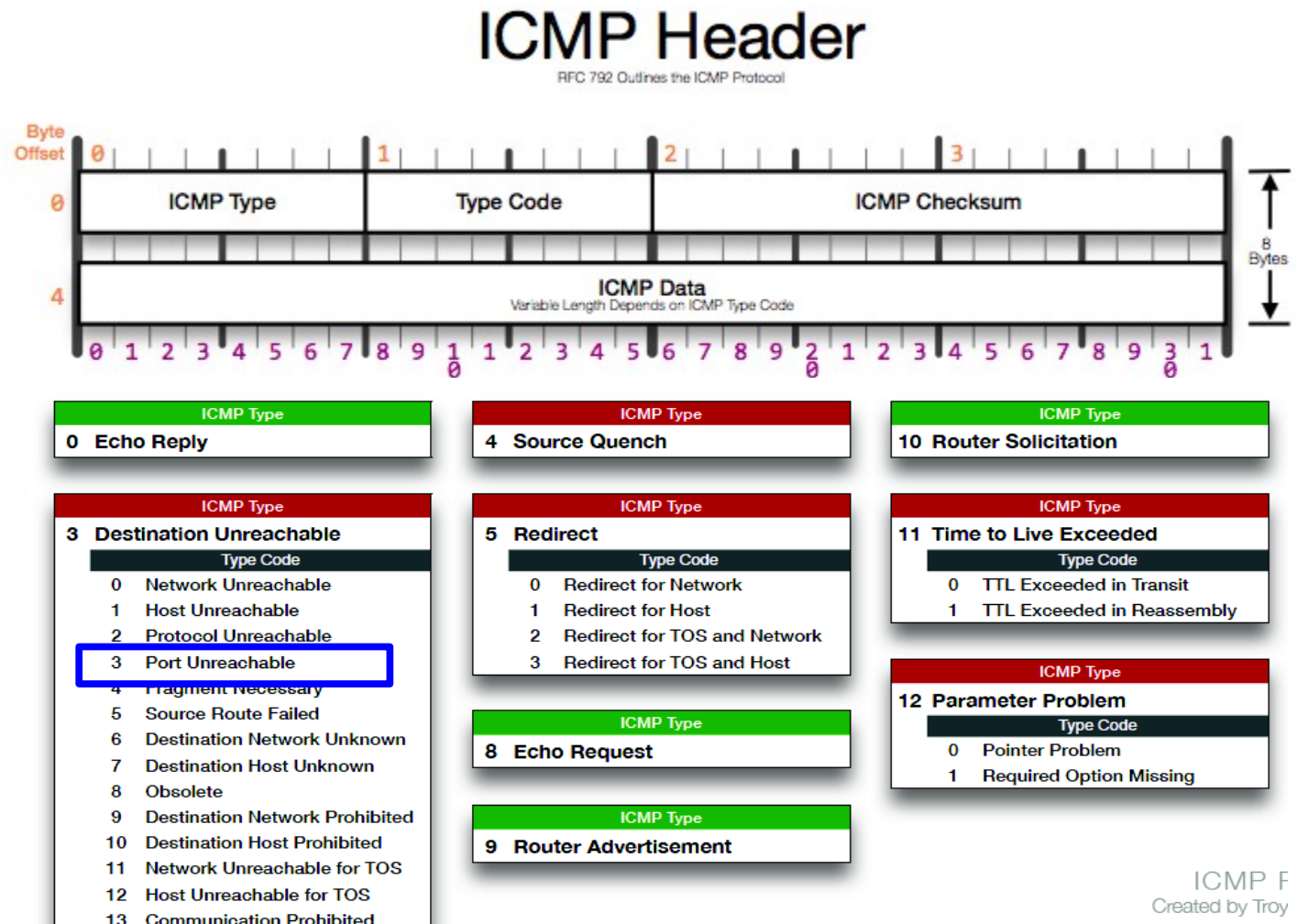


IP TTL - Who is sending this packet ?
Initial TTL Valuse by Operating System

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/



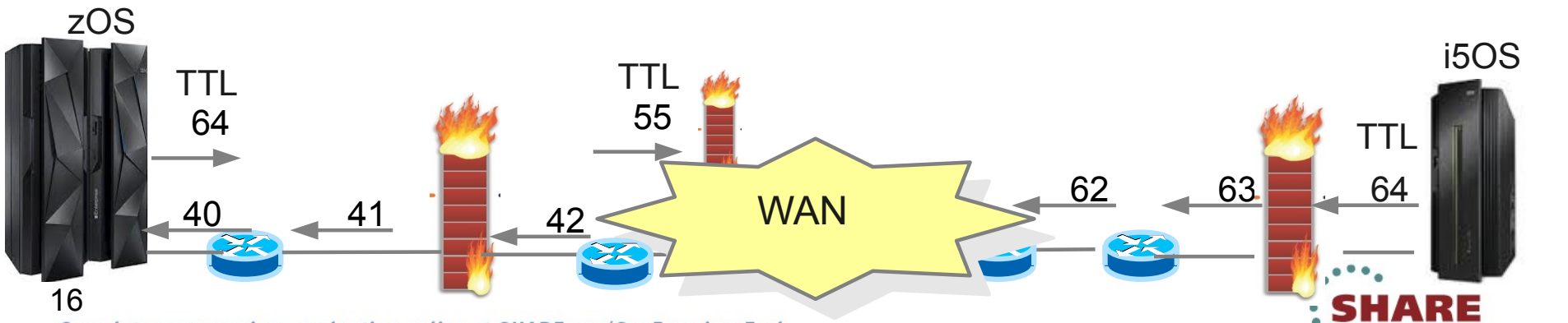
- ICMP packets, when closely inspected can tell the topology

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

File Edit View Go Capture Analyze Statistics Telephony Tools Help

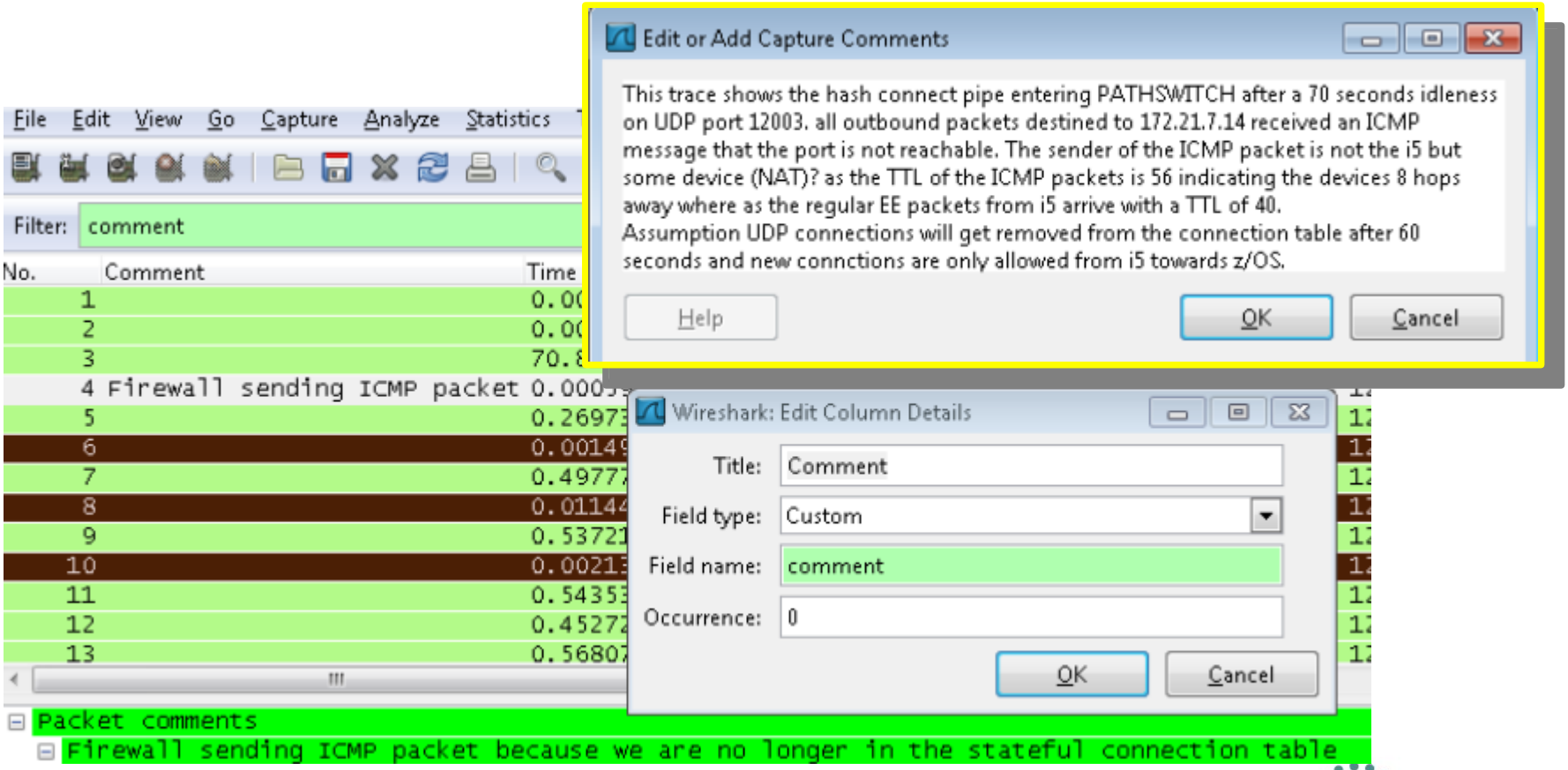
Filter: Expression... Clear Apply

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



#SHAREorg

SHARE
Technology · Connections · Results

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

SocialBusiness IBMSmartCloud

SHARE in San Francisco 2013