

Towards the OSA and beyond Using Wireshark for EE Problem Analysis

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com
Wednesday, Feb. 6 2013
Session # 12853

www.Linkedin.com/in/Matthias_Burkhard
Twitter: @mreede
Facebook: Matthias Burkhard
IBM SmartCloud: Matthias Burkhard

SocialBusiness
IBMSmartCloud



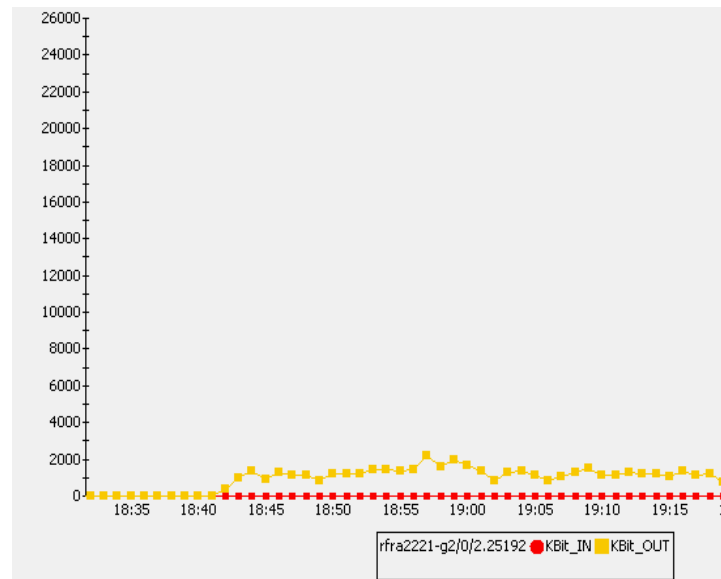
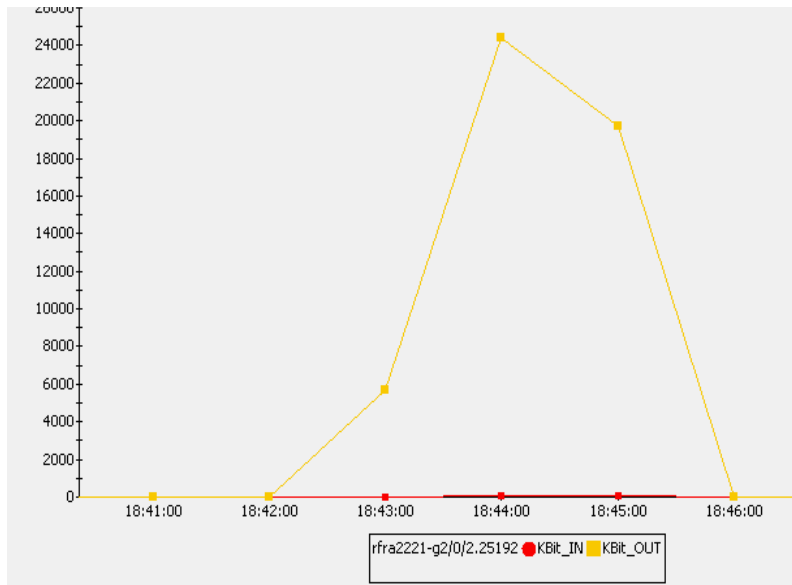
The Problem: Slow NJE File Transfer

A NJE transfer to an external business partner that used to be completed within one hour in the evening someday ran all night.

There was no obvious change in the environment.

The SNA session was using an HPR pipe over a 2-hop APPN route, the last hop being the EE link between the two Extended Border Nodes.

A few days later, the transfer went fast again, without a change!



What VTAM tells us: HPRDIAG

- D NET,ID=CNR0047A,**HPRDIAG=YES**

```
IST097I DISPLAY ACCEPTED
IST075I NAME = CNR0047A , TYPE = PU_T2.1
IST486I STATUS= ACTIV--LX-, DESIRED STATE= ACTIV
IST2244I HPRDIAG DISPLAY ISSUED ON 06/22/12 AT 10:22:53
IST1043I CP NAME = MV024 - CP NETID = NETX - DYNAMIC LU = YES
IST2178I RPNCB ADDRESS 1D509018
IST1963I APPNCOS = #INTER - PRIORITY = HIGH
IST1476I TCID X'184A07E70001011A' - REMOTE TCID X'3B9CD7730001003C'
IST1481I DESTINATION CP NETX.MV024 - NCE X'D000000000000000'
IST1587I ORIGIN NCE X'D0000000000000000'
IST1967I ACTIVATED AS PASSIVE ON 06/17/12 AT 13:47:21
IST1479I RTP CONNECTION STATE = CONNECTED/BACKPRESSURE - MNPS = NO
IST1959I DATA FLOW STATE = NORMAL
IST1855I NUMBER OF SESSIONS USING RTP = 3
```



So, is it good, bad? Should I know, should I care?

VTAM: HPRDIAG – ARB Information I.

- ARB HPR's Adaptive Rate Based Data flow Control

```
IST1968I  ARB INFORMATION:
IST1844I  ARB MODE = GREEN
IST1697I  RTP PACING ALGORITHM = ARB RESPONSIVE MODE
IST1477I  ALLOWED DATA FLOW RATE = 2207 KBITS/SEC
IST1516I  INITIAL DATA FLOW RATE = 49 KBITS/SEC
IST1841I  ACTUAL DATA FLOW RATE = 155 KBITS/SEC
IST1969I  MAXIMUM ACTUAL DATA FLOW RATE = 12 MBITS/SEC
IST1862I  ARB MAXIMUM SEND RATE = 1550 KBITS/SEC
IST1846I  CURRENT RECEIVER THRESHOLD = 47000 MICROSECONDS
IST1846I  MAXIMUM RECEIVER THRESHOLD = 47000 MICROSECONDS
IST1846I  MINIMUM RECEIVER THRESHOLD = 20800 MICROSECONDS
IST1970I  RATE REDUCTIONS DUE TO RETRANSMISSIONS = 0
IST924I  -----
```



Hmm, nothing too obvious!

Actual SendRate way below the Allowed Sendrate

VTAM: HPRDIAG – ARB Information II.

- Every pipe has 2 RTP endpoints! How about the other end?

```
IST1968I  ARB INFORMATION:
IST1844I  ARB MODE = YELLOW
IST1697I  RTP PACING ALGORITHM = ARB RESPONSIVE MODE
IST1477I  ALLOWED DATA FLOW RATE =      258 KBITS/SEC
IST1516I  INITIAL DATA FLOW RATE =      500 KBITS/SEC
IST1841I  ACTUAL DATA FLOW RATE =      266 KBITS/SEC
IST1969I  MAXIMUM ACTUAL DATA FLOW RATE =      32 MBITS/SEC
IST1862I  ARB MAXIMUM SEND RATE =      16 MBITS/SEC
IST1846I  CURRENT RECEIVER THRESHOLD =      395975 MICROSECONDS
IST1846I  MAXIMUM RECEIVER THRESHOLD =      417000 MICROSECONDS
IST1846I  MINIMUM RECEIVER THRESHOLD =      185000 MICROSECONDS
IST1970I  RATE REDUCTIONS DUE TO RETRANSMISSIONS =      11660
IST924I  -----
```



Aha, Allowed Sendrate is lower than Initial !
Lots of retransmissions!

VTAM: HPRDIAG – Transmission Information

- High percentage of retransmissions

```
IST1973I OUTBOUND TRANSMISSION INFORMATION:  
IST1974I NUMBER OF NLPS SENT =                2354126 (    2M )  
IST1975I TOTAL BYTES SENT =                   1899005183 (    1G )  
IST1849I LARGEST NLP SENT =                    1319 BYTES  
IST1980I SEQUENCE NUMBER = 1773745903 (X'69B936EF')  
IST1842I NUMBER OF NLPS RETRANSMITTED =        35283  
IST2249I NLP RETRANSMIT RATE =    1.4987%
```

Packet loss in the network!



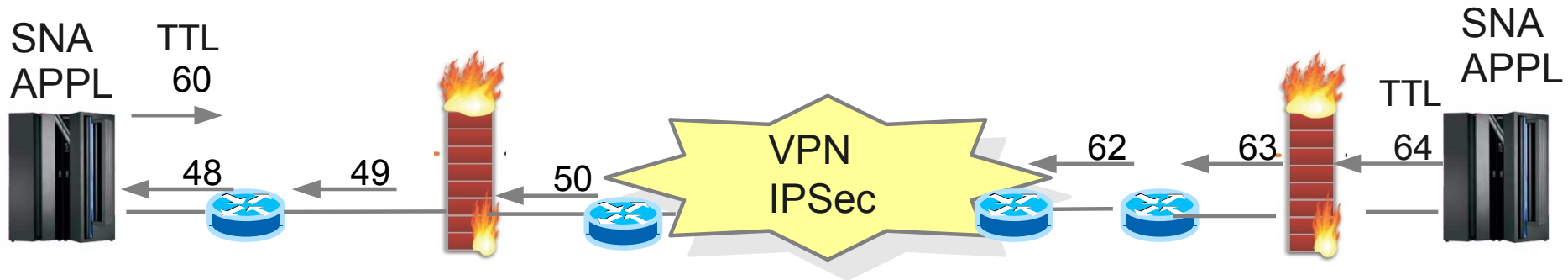
Phew! I knew it was not my problem :-)



Ticket closed?

The Environment: EE to a Business Partner

Typical former SNI now APPN EBN HPR/IP



Top 3 Root Causes of all EE Problems

- Firewall Filter Rules not in place consistently
 - Allow new UDP connections 12000 – 12004 in both directions
 - ALWAYS!
- Queue overflow due to bursty HPR traffic pattern
 - ARB Sendrate → Burstsize can grow to large # of packets
- Fragmentation
 - IPSec tunnels require reduced MTU size
 - PMTUD does not always work (efficiently)

Enterprise Extender – SNA over IP Terminology

VTAM

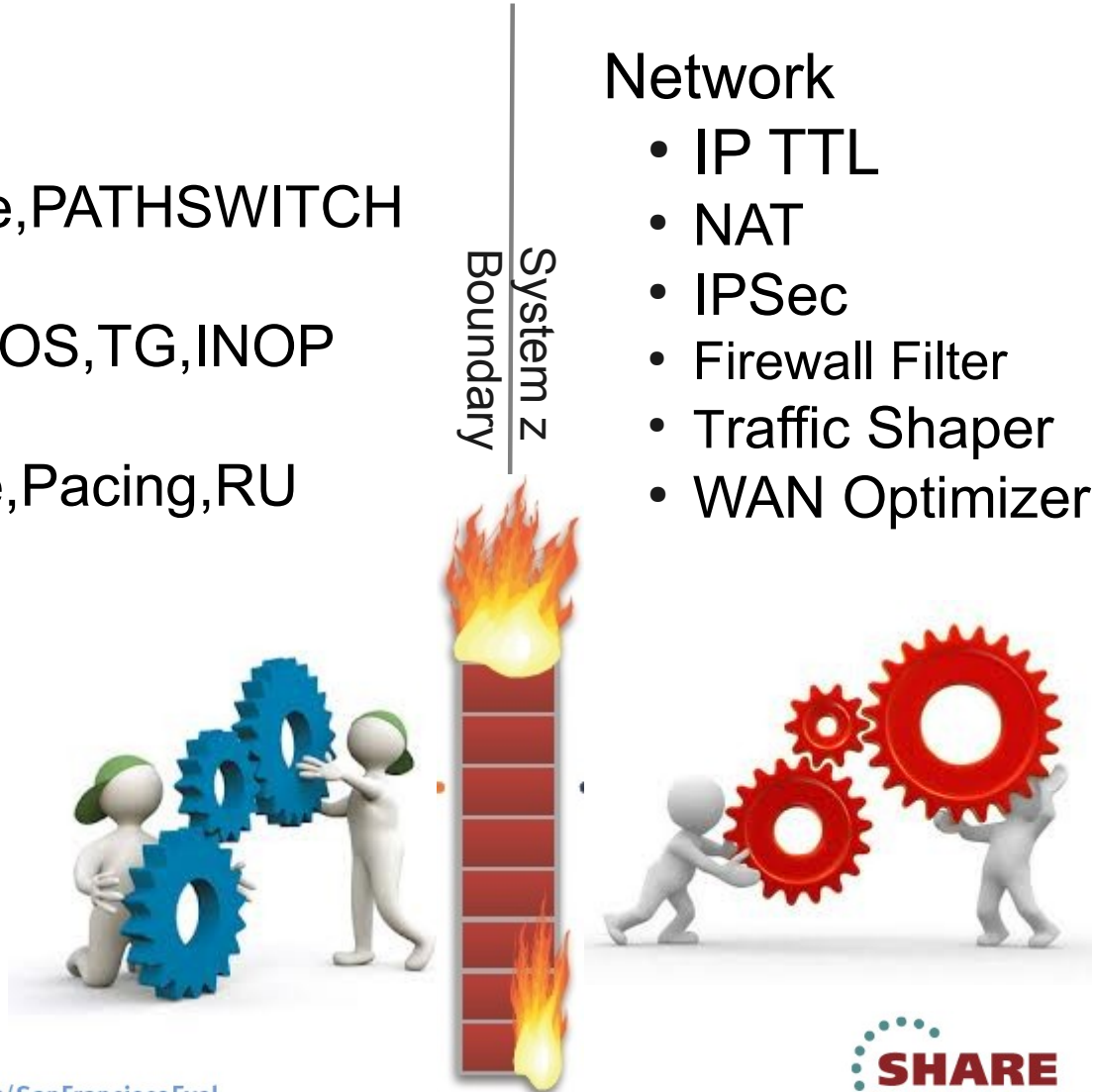
- HPR Pipes
 - TCIDs, ARB Sendrate, PATHSWITCH
- APPN
 - CP, Topology, APPNCOS, TG, INOP
- SNA
 - LU, Session, Logmode, Pacing, RU

IP

- UDP
 - Ports 12000-12004
- Static VIPA(s)
- Routing
 - Static, OSPF, RIP
- MTU
 - Jumbo Frames, IPSec

Network

- IP TTL
- NAT
- IPSec
- Firewall Filter
- Traffic Shaper
- WAN Optimizer



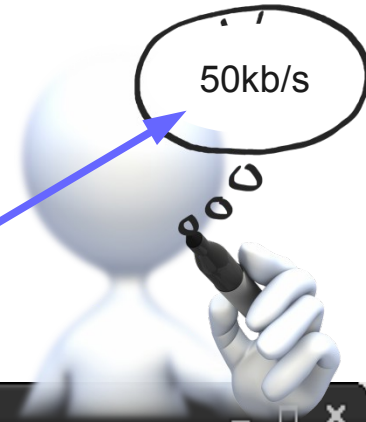
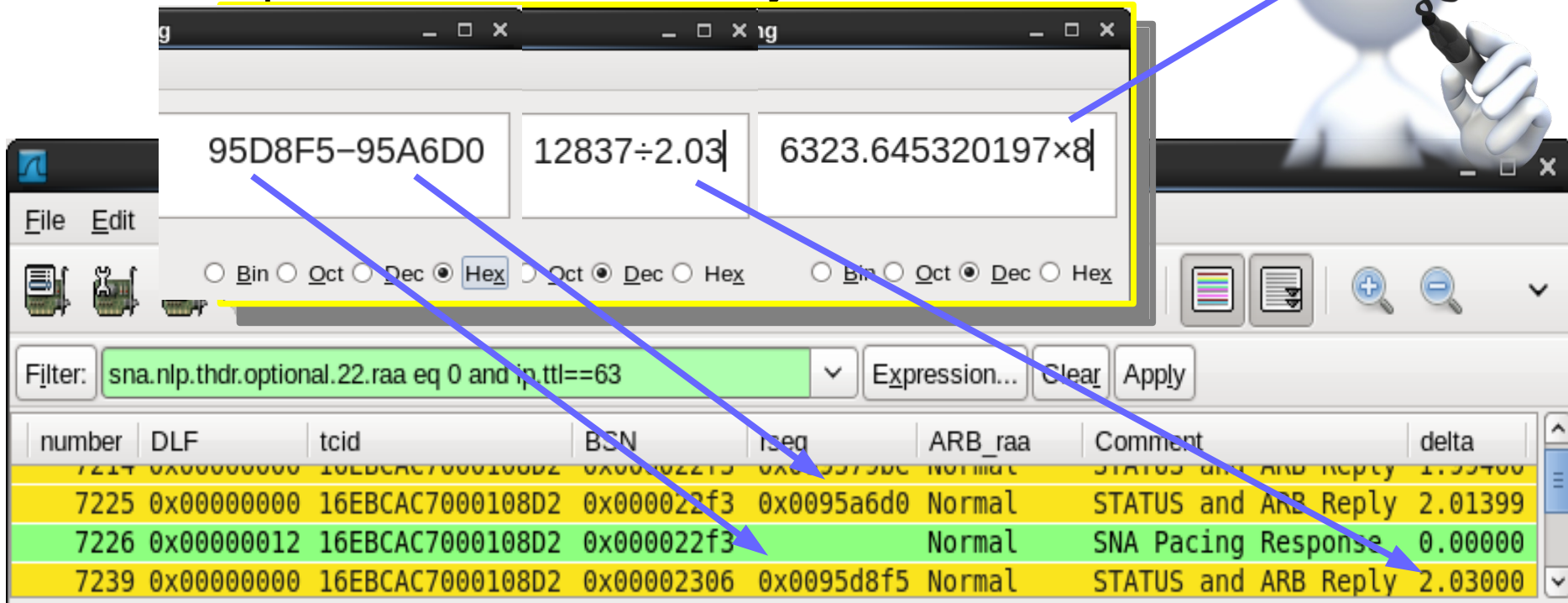
Diagnosing Enterprise Extender problems in z/OS Communications Server

- Documenting EE Problems on z/OS
 - VTAM Internal Trace
 - F NET, TRACE, TYPE=VTAM, SIZE=50M, OPTIONS=(CIA, HPR, TCP)
 - TCPIP Packet Trace
 - V TCPIP, tcpip, PKT, ON, ABBREV=250
 - Dump of VTAM and TCPIP
 - F NET, CSDUMP, TCPNAME=tcpip
- Analysing Documentation
 - IPCS
 - DUMP
 - VIT
 - SYSTCPDA
 - **Wireshark**
 - **SYSTCPDA**, sniffer, tcpdump, iptrace, snoop, nettl ...



Wireshark: Poor Performance on Pipe

- HPR's ARB operates on Data Flow Rates
 - How can we measure the actual send rate?
 - Use the delta of BSN or rseq of any two packets and divide by the delta time

95D8F5-95A6D0 12837÷2.03 6323.645320197×8

File Edit

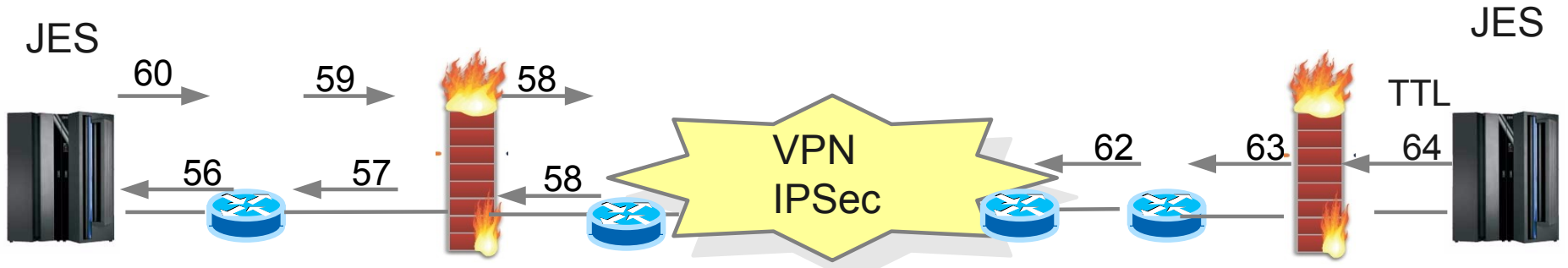
Bin Oct Dec **Hex** Oct Dec Hex Bin Oct Dec Hex

Filter: sna.nlp.thdr.optional.22.raa eq 0 and ip.ttl==63 Expression... Clear Apply

number	DLF	tcid	BSN	rseq	ARB_raa	Comment	delta
7214	0x00000000	16EBCAC7000108D2	0x000022f3	0x00095790c	Normal	STATUS and ARB Reply	1.99400
7225	0x00000000	16EBCAC7000108D2	0x000022f3	0x00095a6d0	Normal	STATUS and ARB Reply	2.01399
7226	0x00000012	16EBCAC7000108D2	0x000022f3		Normal	SNA Pacing Response	0.00000
7239	0x00000000	16EBCAC7000108D2	0x00002306	0x00095d8f5	Normal	STATUS and ARB Reply	2.03000

Wireshark: Detecting Delays in Transmission

Filter: frame.time_delta gt 0.5

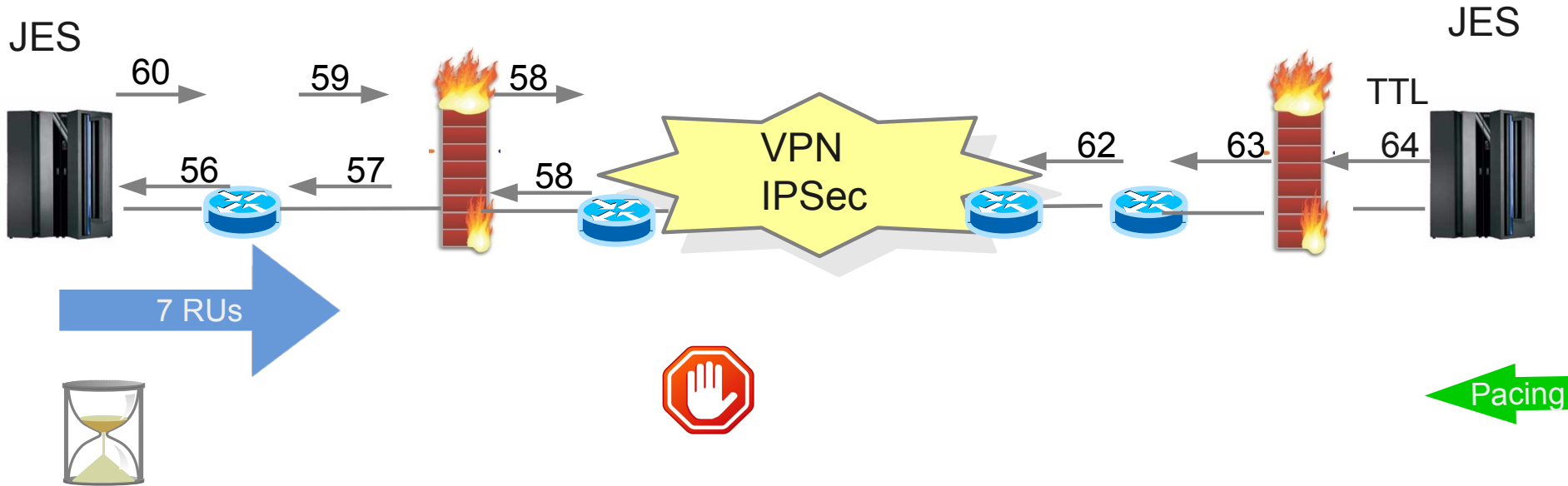


Filter: `frame.time_delta_displayed gt 0.5` Expression... Clear Apply

No.	Time	len	IPID	TTL	Source	Destination	Comment	tcid	BSN	rseq
10770	0.572	91	0x9c2d	60	192.168.101.7	92.254.251.11	RTP GAP	155CCA61000100AF	0x6d123fb3	0x00236f09
10921	0.707	91	0xd116	56	92.254.251.11	192.168.101.7	STATUS Request	16ECDA0E00010259	0x00236f7b	0x6d14496e
11361	2.604	83	0x9f31	60	192.168.101.7	92.254.251.11	STATUS Request	155CCA61000100AF	0x6d1a6927	0x00237085
11714	0.558	91	0xd1c8	56	92.254.251.11	192.168.101.7	STATUS Request	16ECDA0E00010259	0x0023717c	0x6d1f4e9d
11836	0.598	91	0xa171	60	192.168.101.7	92.254.251.11	RTP GAP	155CCA61000100AF	0x6d20f0e9	0x002371b5
12045	0.752	83	0xa25c	60	192.168.101.7	92.254.251.11	STATUS Request	155CCA61000100AF	0x6d23cc90	0x0023723a
12429	2.595	83	0xa475	60	192.168.101.7	92.254.251.11	STATUS Request	155CCA61000100AF	0x6d291b50	0x00237331
12522	0.577	91	0xa4f3	60	192.168.101.7	92.254.251.11	RTP GAP	155CCA61000100AF	0x6d2a54f4	0x0023736a
12760	0.720	91	0xd2bb	56	92.254.251.11	192.168.101.7	STATUS Request	16ECDA0E00010259	0x00237415	0x6d2d98d8
12853	0.562	91	0xa68e	60	192.168.101.7	92.254.251.11	RTP GAP	155CCA61000100AF	0x6d2ed20c	0x0023743b
13091	0.503	109	0xd310	56	92.254.251.11	192.168.101.7	SNA Pacing Res	16ECDA0E00010259	0x002374d3	0x6d31bc59
13470	2.416	83	0xa999	60	192.168.101.7	92.254.251.11	STATUS Request	155CCA61000100AF	0x6d3765b4	0x002375ca
13650	0.576	91	0xaa73	60	192.168.101.7	92.254.251.11	RTP GAP	155CCA61000100AF	0x6d39d906	0x0023763c
14408	0.519	91	0xd422	56	92.254.251.11	192.168.101.7	STATUS Request	16ECDA0E00010259	0x0023783d	0x6d44734a

File: "/home/mburkhar/2013/PMRs... Packets: 30462 Displayed: 135 Marked: 0 Profile: EE-HPR

The Root Cause: Network Layer Packets NLPs are dropped and require retransmission



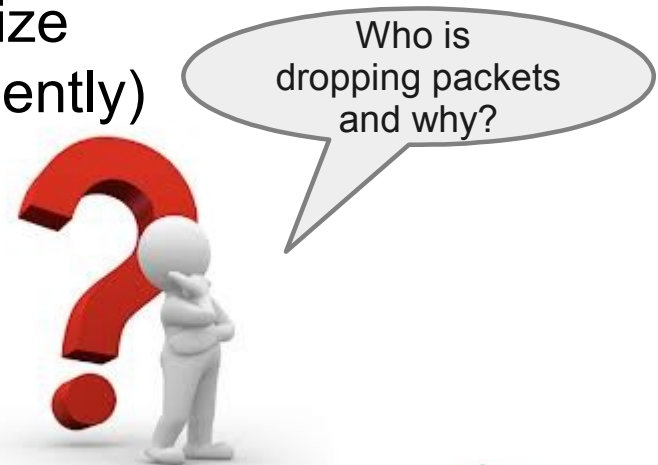
No.	Time	len	TTL	Source	Comment	snf	tcid	BSN	rser
12342	0.010	109	56	92.254.251.11	SNA Pacing Res	22451	16ECDA0E00010259	0x002372f8	0x0
12343	0.000	1432	60	192.168.101.7	SNA PACING Req	22458	155CCA61000100AF	0x6d27e1de	
12371	0.011	109	56	92.254.251.11	SNA Pacing Res	22458	16ECDA0E00010259	0x0023730b	0x0
12372	0.001	1432	60	192.168.101.7	SNA PACING Req	22465	155CCA61000100AF	0x6d284a43	
12400	0.010	109	56	92.254.251.11	SNA Pacing Res	22465	16ECDA0E00010259	0x0023731e	0x0
12401	0.001	1432	60	192.168.101.7	SNA PACING Req	22472	155CCA61000100AF	0x6d28b2cd	
12431	2.413	91	60	192.168.101.7	RTP GAP		155CCA61000100AF	0x6d291b50	0x0
12432	0.008	121	56	92.254.251.11	SNA Pacing Res	22472	16ECDA0E00010259	0x00237331	0x0

12

Summary – Poor NJE Performance: NLPs carrying PACING response are dropped

Top 3 Root Causes of all EE Problems

- Firewall Filter Rules not in place consistently
 - Allow new UDP connections 12000 – 12004 in both directions
 - ALWAYS!
- Queue overflow due to bursty HPR traffic pattern
 - ARB Sendrate → Burstsize can grow to large # of packets
- Fragmentation
 - IPSec tunnels require reduced MTU size
 - PMTUD does not always work (efficiently)



Wireshark Open Source Trace Analyzer

www.wireshark.org



- Powerful Dissector Logic for **MANY** protocols
 - Including SNA (TH,RH) - RU data knowledge is missing!
 - Including HPR (ANR,RTP) and of course IP and DLC...
 - Well known and accepted tool in the networking arena
- Always worthwhile to get the latest version
 - Stable release as of Feb 2013: 1.8.5

Wireshark Profiles – SNA information

- Visualize certain events like FMH5, pacing req/rsp etc.
 - 3 files: dfilters, colorfilters, preferences



ccr.session1.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

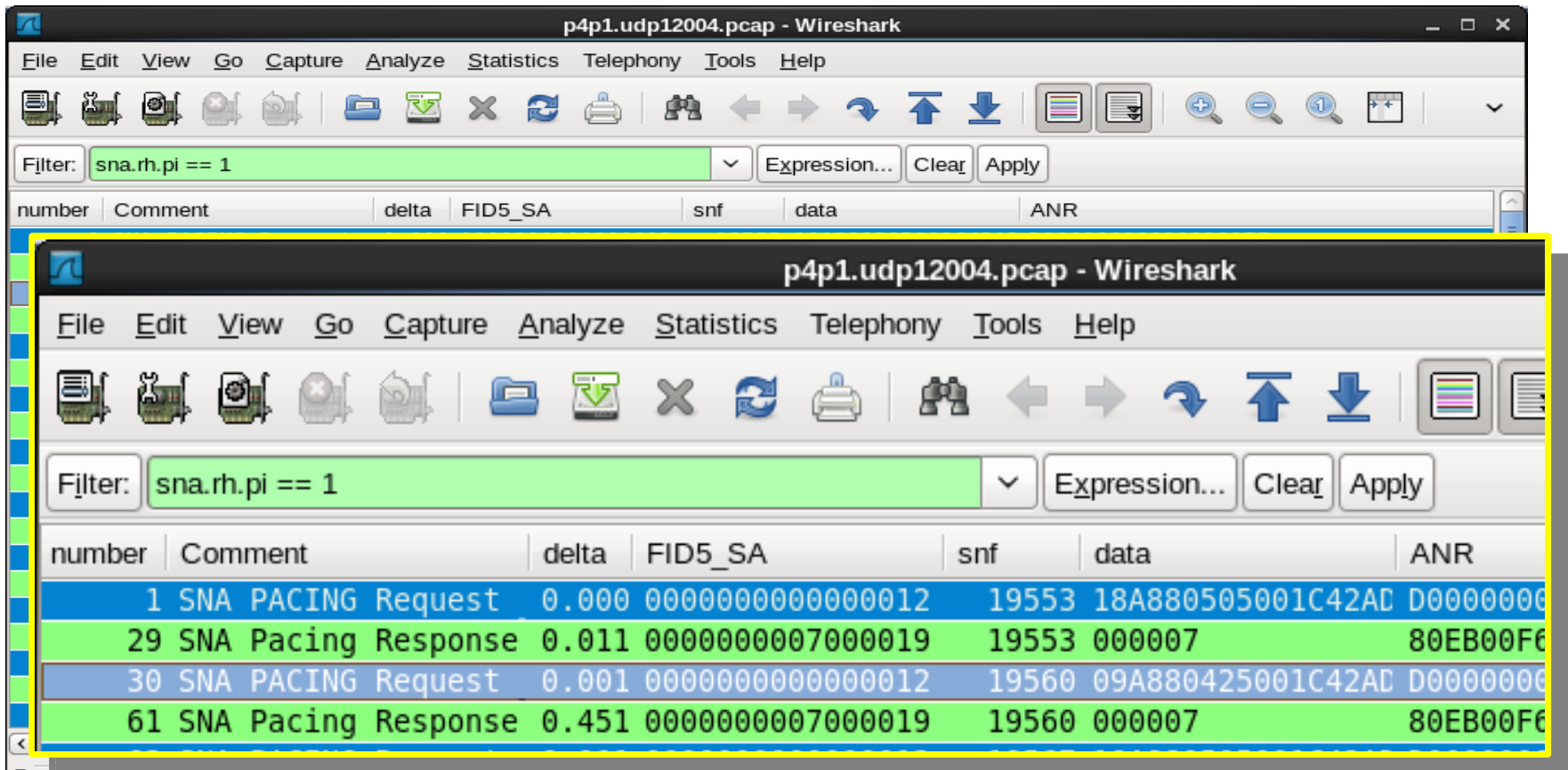
Filter: Expression... Clear Apply Save

TCID	BSN	delta	Comment	SNF	Data
2b7831a900014f35	0x8acef3a/	0.0007910	EBCDIC blanks	303	4040404040404040
2b9a51280001031e	0x4e8bfc45	0.0000560	SNA PACING rsp	301	000007
2b9a51280001031e	0x4e8c5cb8	0.0000500	EBCDIC blanks	298	4040404040404040
2b9a51280001031e	0x4e8c6cc8	0.0003510	SNA LU62 transaction end	299	4040404040404040
2b7831a900014f35	0x8adaf794	2.8058910	SNA FMH5 ALLOC	307	2f0502ff0003d10080
2b9a51280001031e	0x4e96a001	2.3509120	SNA GDS_12F2 CICS	300	001012f20c430e200
2b7831a900014f35	0x8ae9ca8e	0.0555190	SNA PACING req	308	0001060a40060001
2b9a51280001031e	0x4e96a211	0.0007040	SNA PACING rsp	308	000007
2b9a51280001031e	0x4e96a48f	0.0024400	SNA LU62 transaction end	301	0001040a0807

Name	Folder	Typical Files
"File" dialogs	\\SMBHOST\shared_mburkhar\2013\PMRs\sbsa\d0103\	capture files
Temp	C:\Users\IBM_AD~1\AppData\Local\Temp\	untitled capture files
Personal configuration	C:\Users\IBM_ADMIN\AppData\Roaming\Wireshark\	"dfilters", "preferences",
Global configuration	C:\Program Files\Wireshark	"dfilters", "preferences",

Wireshark Filter Options – SNA Pacing

- Every selectable bit can be used as a filter
 - Pacing request/response: delta time = response time



The image displays two screenshots of the Wireshark network protocol analyzer interface, showing a packet capture of SNA Pacing traffic. The top screenshot shows the filter 'sna.rh.pi == 1' applied, resulting in a list of packets. The bottom screenshot shows the same capture with alternating request and response packets highlighted in blue and green respectively.

number	Comment	delta	FID5_SA	snf	data	ANR
1	SNA PACING Request	0.000	0000000000000012	19553	18A880505001C42AD	D0000000
29	SNA Pacing Response	0.011	0000000007000019	19553	000007	80EB00F6
30	SNA PACING Request	0.001	0000000000000012	19560	09A880425001C42AD	D0000000
61	SNA Pacing Response	0.451	0000000007000019	19560	000007	80EB00F6

Wireshark Coloring Rules

- Assign different colors for certain 'events'
- Every combination of bit settings can be used



a921.dr11.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:

No.	Time	TTL	len	IPID	Source
5300	0.006	51	334	0x6f05	10.1
5301	0.008	60	109	0xd3fc	10.1
5302	0.007	51	334	0x6f06	10.1
5303	0.000	51	334	0x6f07	10.1
5304	0.003	51	334	0x6f08	10.1
5305	0.001	60	109	0xd3fd	10.1
5306	0.005	51	124	0x6f0a	10.1
5307	0.002	60	121	0xd3fe	10.1
5308	0.004	60	86	0xd3ff	10.1
5309	0.008	60	101	0xd400	10.1
5310	0.000	60	107	0xd401	10.1
5311	0.001	51	95	0x6f0b	10.1
5312	0.005	51	91	0x6f0c	10.1

Wireshark: Coloring Rules - Profile: EE-HPR

Filter

List is processed in order until match is found

Name	String
HPR Pipe Dying A0020001	sna.nlp.thdr.offset == 0x000c and sna.nlp.thdr.8 ==
HPR PATHSWITCH	sna.nlp.thdr.dlf == 0x00000000 and sna.nlp.thdr.off
RTP GAP	sna.nlp.thdr.optional.0e.gap == 1
HPR suspicious	sna.nlp.thdr.offset gt 10 and !sna.nlp.thdr.offset eq 1
XID Done	llc.control == 0x0003 and udp.dstport==12000
Pacing Response	sna.rh.pi eq 1 and sna.rh.ri == 1
SNA PACING Request	sna.rh.pi == 1 and sna.rh.ri == 0
EE_VERIFY	llc.control == 0x00f7
SNA -rsp Sense	sna.rh.sdi == 1
SNA FMH7 Sense	(data.data[0:2] eq 0707 and sna.rh.fi == 1)
FMH5	data.data[1:12] contains 0502:ff and sna.rh.fi == 1

Wireshark Coloring Rules

- Use alarming colors to see suspicious events
 - Any combined filter can be used to assign colors

p4p1.udp12004.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

number	Comment	delta	FID5_SA	snf	data	ANR
30160	SNA PACING Request	0.001	0000000000000012	26665	09A880505001C430F	D000000000000000FF
30161	zOS	0.000			FE4505880000C7C4C	D000000000000000FF
30162	zOS	0.000			F140E2E3407A40F06	D000000000000000FF
30163	zOS	0.000			95A981A4A20FA8805	D000000000000000FF
30164	zOS	0.000	0000000000000012	26666	0BA8804B5001C430F	D000000000000000FF
30165	zOS	0.000			7A40F140E2E340968	D000000000000000FF
30166	zOS	0.000			52A2810E84400185A	D000000000000000FF
30183	zOS	0.000			998B11FAE2838893A	D000000000000000FF
30184	zOS	0.000	0000000000000012	26671	09A880505001C430F	D000000000000000FF
30185	zOS	0.000			10A880505001C430F	D000000000000000FF
30186	zOS	0.000			A4A35EA413FAD981A	D000000000000000FF
30187	zOS	0.000			89967A40F140E2E34	D000000000000000FF
30188	STATUS Request	2.987				D000000000000000FF
30189	STATUS Request	0.008				80EB00F600800000D00
30190	STATUS Request	0.278				80EB00F600800000D00
30191	STATUS Request	0.000				D000000000000000FF
30192	RTP GAP	0.188			0C7D7ACB00239FA60	D000000000000000FF
30193	SNA Pacing Response	0.008	0000000007000019	26665	000007	80EB00F600800000D00

HPR: One Pipe two TCIDs

- A HPR pipe has 2 TCIDs
 - 1 TCID for NLPs from A to B ,1 TCID for NLPs from B to A
 - Combine them with a logical 'or'

tcid contains 2b9a:5128 or sna.nlp.thdr.tcid contains 2b78:31a9

Time	Source	IPID	udp.len	tcid
2011-11-14 01:09:43.053	156.1.0.21	0x6fea	63	2B9A51280001031E
2011-11-14 01:09:43.053	156.1.0.21	0x6feb	63	2B9A51280001031E
2011-11-14 01:09:43.075	156.1.0.21	0x6fed	63	2B9A51280001031E
2011-11-14 01:09:43.086	156.1.0.21	0x6fee	71	2B9A51280001031E
2011-11-14 01:09:43.087	156.1.0.21	0x6fef	71	2B9A51280001031E
2011-11-14 01:09:43.087	156.1.0.21	0x6ff0	71	2B9A51280001031E
2011-11-14 01:09:43.087	156.1.0.21	0x6ff1	71	2B9A51280001031E
2011-11-14 01:09:43.124	156.1.0.21	0x6ff2	71	2B9A51280001031E
2011-11-14 01:09:43.143	150.250.24.	0x7778	1444	2B7831A900014F35

HPR – STATUS segment with GAP

- When a packet gets lost the receiving RTP will report a GAP
- Wireshark filter: `sna.nlp.thdr.optional.0e.gap ==1`

Source	Destination
10.199.232.65	10.186.86.241
10.186.86.241	10.199.232.65
10.199.232.65	10.186.86.241
10.199.232.65	10.186.86.241
10.186.86.241	10.199.232.65
10.199.232.65	10.186.86.241
10.186.86.241	10.199.232.65
10.186.86.241	10.199.232.65
10.186.86.241	10.199.232.65
10.186.86.241	10.199.232.65
10.186.86.241	10.199.232.65
10.199.232.65	10.186.86.241
10.199.232.65	10.186.86.241
10.199.232.65	10.186.86.241
10.199.232.65	10.186.86.241
10.186.86.241	10.199.232.65
10.186.86.241	10.199.232.65
10.199.232.65	10.186.86.241

File: "/home/mburkhar/2012/p

```

    ▾ RTP Transport Header
      Transport Connection Identifier: 184A07E3000100DA
      ▸ RTP Transport Packet Header Byte 8: 0x00
      ▸ RTP Transport Packet Header Byte 9: 0x04
      Data Offset/4: 0x000e
      Data Length Field: 0x00000000
      Byte Sequence Number: 0x0db2dbac
    ▾ Status Segment
      Optional Segment Length/4: 9
      Optional Segment Type: Status Segment (0x0e)
    ▾ Status: 0x80
      1... .. = Gap Detected: True
      .0.. .. = RTP Idle Packet: False
      Number Of ABSP: 2
      Status Report Number: 0x0bd7
      Status Acknowledge Number: 0x143c
      Received Sequence Number: 0x396c3bc2
      Reserved
      ▸ Data (32 bytes)
  
```

HPR Retransmissions – GAP report: rseq

- Retransmissions can occur and RTP will cope with it, but
 - Performance is degraded
 - REFIFO timer adds a delay
 - ALLOWED DATA FLOW RATE reduces

EEPROD 111312 1800 CCR side of FW.CAP - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: sna.nlp.thdr.optional.0e.rseq == 0x984569ee or sna.nlp.thdr.bsr

Time	Source	IPID	udp.len	tcid	BSN	expctd_bsn	comment
2012-11-14 01:09:43.053	156.1.0.21	0x6fea	63	2B9A51280001031E	0x53cbc8d6	0x984569ee	
2012-11-14 01:09:43.053	156.1.0.21	0x6feb	63	2B9A51280001031E	0x53cbc8d6	0x984569ee	
2012-11-14 01:09:43.075	156.1.0.21	0x6fed	63	2B9A51280001031E	0x53cbcb72	0x984569ee	
2012-11-14 01:09:43.086	156.1.0.21	0x6fee	71	2B9A51280001031E	0x53cbcb72	0x984569ee	RTP GAP
2012-11-14 01:09:43.087	156.1.0.21	0x6fef	71	2B9A51280001031E	0x53cbcb72	0x984569ee	RTP GAP
2012-11-14 01:09:43.087	156.1.0.21	0x6ff0	71	2B9A51280001031E	0x53cbcb72	0x984569ee	RTP GAP
2012-11-14 01:09:43.087	156.1.0.21	0x6ff1	71	2B9A51280001031E	0x53cbcb72	0x984569ee	RTP GAP
2012-11-14 01:09:43.124	156.1.0.21	0x6ff2	71	2B9A51280001031E	0x53cbcb72	0x984569ee	RTP GAP
2012-11-14 01:09:43.143	150.250.24.	0x7778	1444	2B7831A900014F35	0x984569ee	0x53cbcb72	

File: "/home/mburkhar/... Packets: 404640 Displayed: 9 Marked: 0 Profile: prthpr

Wireshark – HPR STATUS GAP

- Many GAPS are indicative of many packet losses
 - Should not happen too often... (→ OA39637 HIPER)

p4p1.udp12004.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

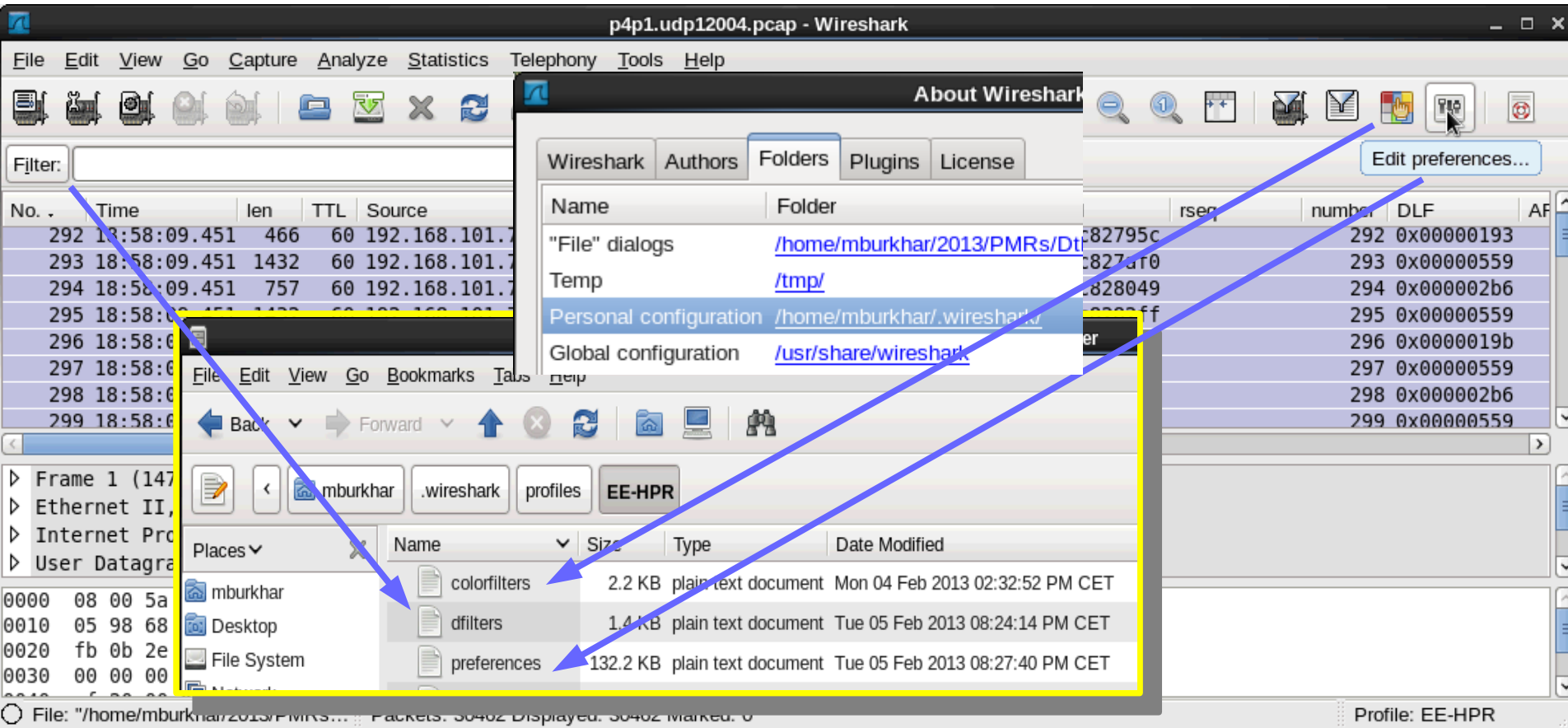
Filter: sna.nlp.thdr.optional.0e.gap ==1 or sna.rh.pi == 1

Source	Destination	number	DLF	tcid	BSN	rseq	Comment	delta
192.168.101.7	92.254.251.11	29947	0x0000055	155CCA61000100AF	0x6e1a4f25		SNA PACING Request	0.001
92.254.251.11	192.168.101.7	29975	0x0000001	16ECDA0E00010259	0x00239f21	0x6e1a6377	SNA Pacing Response	0.012
192.168.101.7	92.254.251.11	29976	0x0000055	155CCA61000100AF	0x6e1ab7b2		SNA PACING Request	0.000
92.254.251.11	192.168.101.7	30004	0x0000001	16ECDA0E00010259	0x00239f34	0x6e1ac681	SNA Pacing Response	0.011
192.168.101.7	92.254.251.11	30005	0x0000055	155CCA61000100AF	0x6e1b1faa		SNA PACING Request	0.001
92.254.251.11	192.168.101.7	30033	0x0000001	16ECDA0E00010259	0x00239f47	0x6e1b2e83	SNA Pacing Response	0.012
192.168.101.7	92.254.251.11	30034	0x0000055	155CCA61000100AF	0x6e1b886f		SNA PACING Request	0.001
92.254.251.11	192.168.101.7	30062	0x0000001	16ECDA0E00010259	0x00239f5a	0x6e1b9f8a	SNA Pacing Response	0.011
192.168.101.7	92.254.251.11	30063	0x0000055	155CCA61000100AF	0x6e1bf143		SNA PACING Request	0.001
192.168.101.7	92.254.251.11	30095	0x0000000	155CCA61000100AF	0x6e1c59b6	0x00239f6d	RTP GAP	0.767
192.168.101.7	92.254.251.11	30097	0x0000000	155CCA61000100AF	0x6e1c59b6	0x00239f6d	RTP GAP	0.002
92.254.251.11	192.168.101.7	30098	0x0000001	16ECDA0E00010259	0x00239f6d	0x6e1c59b6	SNA Pacing Response	0.005
192.168.101.7	92.254.251.11	30099	0x0000055	155CCA61000100AF	0x6e1c59b6	0x00239f80	SNA PACING Request	0.001
92.254.251.11	192.168.101.7	30130	0x0000001	16ECDA0E00010259	0x00239f80		SNA Pacing Response	0.010
192.168.101.7	92.254.251.11	30131	0x0000055	155CCA61000100AF	0x6e1cc290	0x00239f93	SNA PACING Request	0.000
92.254.251.11	192.168.101.7	30159	0x0000001	16ECDA0E00010259	0x00239f93	0x6e1cd6b7	SNA Pacing Response	0.011
192.168.101.7	92.254.251.11	30160	0x0000055	155CCA61000100AF	0x6e1d2b05		SNA PACING Request	0.001
192.168.101.7	92.254.251.11	30192	0x0000000	155CCA61000100AF	0x6e1d9329	0x00239fa6	RTP GAP	3.463
92.254.251.11	192.168.101.7	30193	0x0000001	16ECDA0E00010259	0x00239fa6	0x6e1d9329	SNA Pacing Response	0.008

Wireshark Profiles dfilters, colorfilters, preferences

Three files located in Personal Configuration folder

- Help → About Wireshark → Folders



The screenshot shows the Wireshark interface with the 'About Wireshark' dialog box open. The 'Folders' tab is selected, showing the following configuration folders:

Name	Folder
"File" dialogs	/home/mburkhar/2013/PMRs/Dt...
Temp	/tmp/
Personal configuration	/home/mburkhar/.wireshark/
Global configuration	/usr/share/wireshark/

A yellow box highlights the 'Personal configuration' folder. Below the dialog, a file explorer window shows the contents of the personal configuration folder:

Name	Size	Type	Date Modified
colorfilters	2.2 KB	plain text document	Mon 04 Feb 2013 02:32:52 PM CET
dfilters	1.4 KB	plain text document	Tue 05 Feb 2013 08:24:14 PM CET
preferences	132.2 KB	plain text document	Tue 05 Feb 2013 08:27:40 PM CET

Blue arrows indicate the path from the 'Personal configuration' folder in the 'About Wireshark' dialog to the file explorer window, and from the 'Edit preferences...' button in the main interface to the file explorer window.

Need more Wireshark



Facebook groups

sna.wizards@groups.facebook.com

ip.wizards@groups.facebook.com

IBM SmartCloud Community

„**ip wizards in the Cloud**“



<https://www.ibm.com/cloud-computing/social/us/en/>

Wireshark Bootcamp 2013

4 days Hands-on Training

Mainz, Germany – March 12, June 25

<http://tinyurl.com/zowie0de>

Towards the OSA and beyond Using Wireshark for EE Problem Analysis

Matthias Burkhard
IBM Germany

Wednesday, Feb. 6 2013
Session # 12853

Twitter: @mreede

Facebook: <https://www.facebook.com/matthias.burkhard.9>

IBM SmartCloud: Matthias Burkhard

SocialBusiness
IBMSmartCloud



Appendix

Wireshark Display Filters EE-HPR

dfilters

```
"SNA PACING Req/Rsp" sna.rh.pi == 1
"SNA Sense Code " (data.data[0:2] eq 0707 and sna.rh.fi == 1) or sna.rh.sdi == 1
"SNA BIND" sna.rh.ru_category == 0x03 and sna.rh and data.data[0]==31
"SNA UNBIND Cleanup" sna.rh.ru_category == 0x03 and sna.rh and data.data[0:2]==320f
"LU62 GDS12F2 or GDS12FF or CEBI (end of transacton)" data.data[2:2] == 12f2 or data.data[2:2] == 12ff or sna.rh.cebi==1
"LU62 FMH5 ALLOC" data.data[1:3] eq 0502:ff and sna.rh.fi == 1 or data.data[1:3] eq 0502:ff and sna.rh.fi == 1 or sna.rh.cebi==1
"HPR GAP " sna.nlp.thdr.optional.0e.gap ==1 and sna.nlp.thdr.bsn >= 0x00000000
"HPR_suspicious" sna.nlp.thdr.offset gt 10 and !sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.tcid lt 8000:0000:0000:0000
"HPR New Pipe " sna.nlp.thdr.tcid ge 8000:0000:00:00:00:00 or sna.nlp.thdr.bsn == 0x00000000
"HPR Pipe CFAULT" sna.nlp.thdr.offset == 0x000c and sna.nlp.thdr.8 == 0x30
"HPR PATHSWITCH" sna.nlp.thdr.dlf eq 0 and sna.nlp.thdr.offset gt 24
"APPN LOCATE" data.data[1:13] contains 22f0:f0f3
"APPN DLUR" data.data[1:13] contains 22f0:f0f6
"EEDIAG Requests Port 12000" udp.length eq 56 and udp.port==12000 and ip.ttl gt 222
```

Appendix

Wireshark Coloring Rules EE-HPR

coloringrules

```
# DO NOT EDIT THIS FILE! It was created by Wireshark http://tinyurl.com/zowie0de
@HPR Pipe Dying A0020001@sna.nlp.thdr.offset == 0x000c and sna.nlp.thdr.8 == 0x30@[45246,3377,3377][65065,62762,3452]
@HPR New Pipe @sna.nlp.thdr.tcid ge 8000:0000:00:00:00:00 or sna.nlp.thdr.bsn == 0x00000000@[53390,56329,4993][0,0,0]
@HPR PATHSWITCH@sna.nlp.thdr.dlf == 0x00000000 and sna.nlp.thdr.offset gt 24@[61806,9014,9014][61013,57372,57372]
@ARB Slowdon __@sna.nlp.thdr.optional.22.raa gt 0@[64100,40309,9845][6682,6682,6682]
@RTP GAP __@sna.nlp.thdr.optional.0e.gap == 1@[54250,18969,3886][57939,63129,62332]
@HPR suspicious@sna.nlp.thdr.offset gt 10 and !sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.tcid lt 8000:0000:0000:0000@[63686,10683,3829][65535,63222,0]
@GDS12Fx x-action reply@data.data[2:2] == 12f2 or data.data[2:2] == 12ff @[6891,39551,24911][63014,62969,61744]
@XID Done@llc.control == 0x0003 and udp.dstport==12000@[0,0,0][65535,63222,0]
@CEBI end_x-acion@sna.rh.cebi==1@[28834,57427,65533][0,0,0]
@SNA Pacing Response __@sna.rh.pi eq 1 and sna.rh.ri == 1@[36107,65535,32590][0,0,0]
@EE_VERIFY@llc.control == 0x00f7@[13576,63959,2451][0,0,0]
@SNA -rsp Sense@sna.rh.sdi == 1@[34452,55316,60779][43091,4099,7349]
@SNA FMH7 Sense @(data.data[0:2] eq 0707 and sna.rh.fi == 1)@[42633,51957,58948][40938,4330,2708]
@APPN LOCATE@data.data[1:13] contains 22F0:F0F3@[51199,38706,65533][0,0,0]
@DLUR@data.data[1:13] contains 22f0:f0f6@[65534,62325,54808][3276,736,62996]
@SNA PACING Request __@sna.rh.pi == 1 and sna.rh.ri == 0@[661,33529,53256][59411,61712,59538]
@FMH5@data.data[1:3] eq 0502:ff and sna.rh.fi == 1@[65534,64008,39339][0,0,0]
@SNA BIND@sna.rh.ru_category == 0x03 and sna.rh and data.data[0]==31@[16579,16707,52185][62667,62061,62061]
@UNBIND Cleanup@sna.rh.ru_category == 0x03 and sna.rh and data.data[0:2]==320f@[37008,0,0][65535,65535,65535]
@ECDIC blanks@data.data[0:8] eq 4040:4040:4040:4040@[46083,28000,53733][65535,61287,61287]
@STATUS Request@sna.nlp.thdr.offset eq 10 and sna.nlp.thdr.dlf eq 0@[63635,61951,13274][10971,656,656]
@STATUS and ARB Reply@sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.dlf eq 0@[64135,58485,7892][6682,6682,6682]
@zOS@ip.ttl==60 or ip.ttl==64 or ip.ttl==63@[51146,50751,57850][0,0,0]
@EEVERIFY REQ@udp.length eq 56 and udp.port==12000 and ip.ttl gt 222@[41026,41026,41026][0,0,0]
```

Appendix

Wireshark Coloring Rules EE-HPR

coloringrules

```
# DO NOT EDIT THIS FILE! It was created by Wireshark http://tinyurl.com/zowie0de
@HPR Pipe Dying A0020001@sna.nlp.thdr.offset == 0x000c and sna.nlp.thdr.8 == 0x30@[45246,3377,3377][65065,62762,3452]
@HPR New Pipe @sna.nlp.thdr.tcid ge 8000:0000:00:00:00:00 or sna.nlp.thdr.bsn == 0x00000000@[53390,56329,4993][0,0,0]
@HPR PATHSWITCH@sna.nlp.thdr.dlf == 0x00000000 and sna.nlp.thdr.offset gt 24@[61806,9014,9014][61013,57372,57372]
@ARB Slowdon __@sna.nlp.thdr.optional.22.raa gt 0@[64100,40309,9845][6682,6682,6682]
@RTP GAP __@sna.nlp.thdr.optional.0e.gap == 1@[54250,18969,3886][57939,63129,62332]
@HPR suspicious@sna.nlp.thdr.offset gt 10 and !sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.tcid lt 8000:0000:0000:0000@[63686,10683,3829][65535,63222,0]
@GDS12Fx x-action reply@data.data[2:2] == 12f2 or data.data[2:2] == 12ff @[6891,39551,24911][63014,62969,61744]
@XID Done@llc.control == 0x0003 and udp.dstport==12000@[0,0,0][65535,63222,0]
@CEBI end_x-acion@sna.rh.cebi==1@[28834,57427,65533][0,0,0]
@SNA Pacing Response __@sna.rh.pi eq 1 and sna.rh.ri == 1@[36107,65535,32590][0,0,0]
@EE_VERIFY@llc.control == 0x00f7@[13576,63959,2451][0,0,0]
@SNA -rsp Sense@sna.rh.sdi == 1@[34452,55316,60779][43091,4099,7349]
@SNA FMH7 Sense @(data.data[0:2] eq 0707 and sna.rh.fi == 1)@[42633,51957,58948][40938,4330,2708]
@APPN LOCATE@data.data[1:13] contains 22F0:F0F3@[51199,38706,65533][0,0,0]
@DLUR@data.data[1:13] contains 22f0:f0f6@[65534,62325,54808][3276,736,62996]
@SNA PACING Request __@sna.rh.pi == 1 and sna.rh.ri == 0@[661,33529,53256][59411,61712,59538]
@FMH5@data.data[1:3] eq 0502:ff and sna.rh.fi == 1@[65534,64008,39339][0,0,0]
@SNA BIND@sna.rh.ru_category == 0x03 and sna.rh and data.data[0]==31@[16579,16707,52185][62667,62061,62061]
@UNBIND Cleanup@sna.rh.ru_category == 0x03 and sna.rh and data.data[0:2]==320f@[37008,0,0][65535,65535,65535]
@ECDIC blanks@data.data[0:8] eq 4040:4040:4040:4040@[46083,28000,53733][65535,61287,61287]
@STATUS Request@sna.nlp.thdr.offset eq 10 and sna.nlp.thdr.dlf eq 0@[63635,61951,13274][10971,656,656]
@STATUS and ARB Reply@sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.dlf eq 0@[64135,58485,7892][6682,6682,6682]
@zOS@ip.ttl==60 or ip.ttl==64 or ip.ttl==63@[51146,50751,57850][0,0,0]
@EEVERIFY REQ@udp.length eq 56 and udp.port==12000 and ip.ttl gt 222@[41026,41026,41026][0,0,0]
```