#SHAREorg

SHARE
Technology · Connections · Results

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

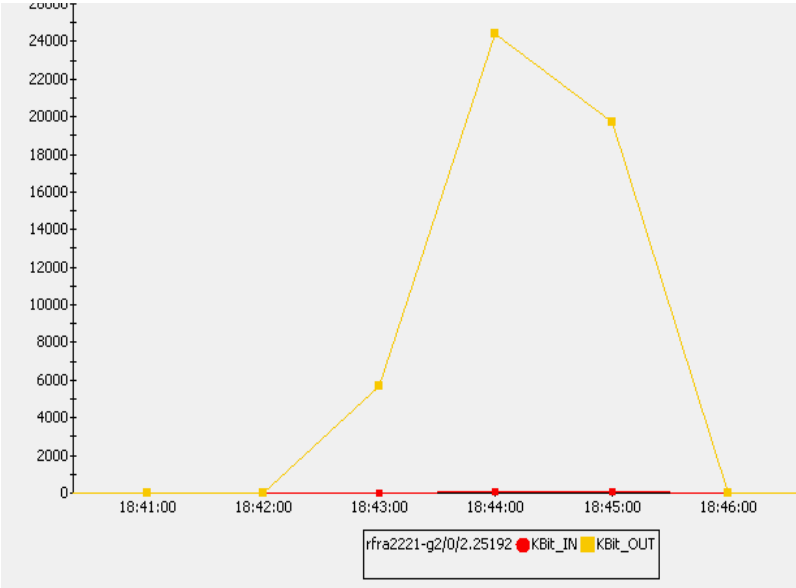


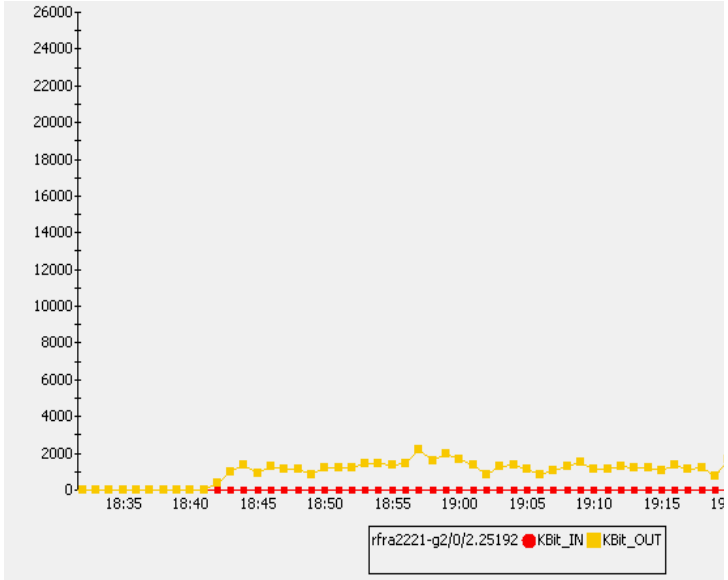
SHARE in San Francisco 2013

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'D0000000000000000'
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 =    470000 MICROSECONDS
IST1846I  MAXIMUM RECEIVER THRESHOLD =    470000 MICROSECONDS
IST1846I  MINIMUM RECEIVER THRESHOLD =    208000 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

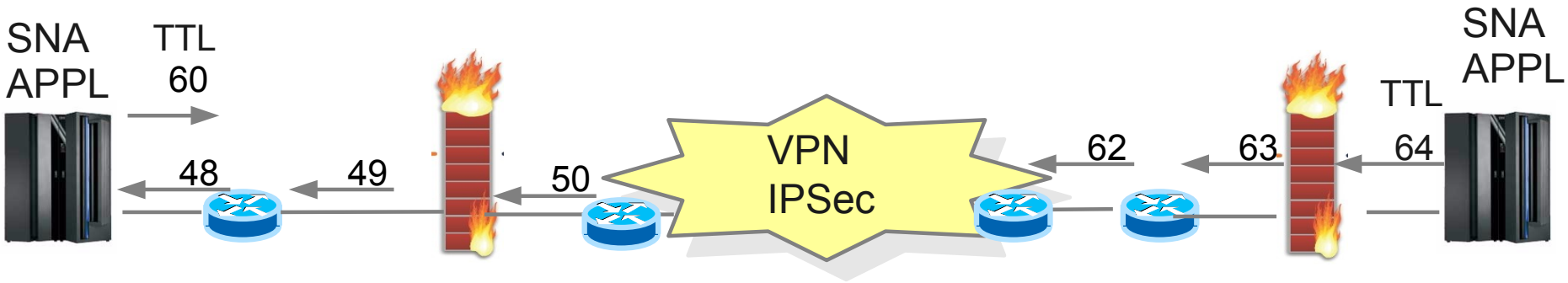
```
IST1973I OUTBOUND TRANSMISSION INFORMATION:
IST1974I NUMBER OF NLPS SENT =              2354126 (   2M )
IST1975I TOTAL BYTES SENT =           1899005183 (   1G )
IST1849I LARGEST NLP SENT =       1319 BYTES
IST1980I SEQUENCE NUMBER = 1773745903 (X'69B936EF')
IST1842I NUMBER OF NLPS RETRANSMITTED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

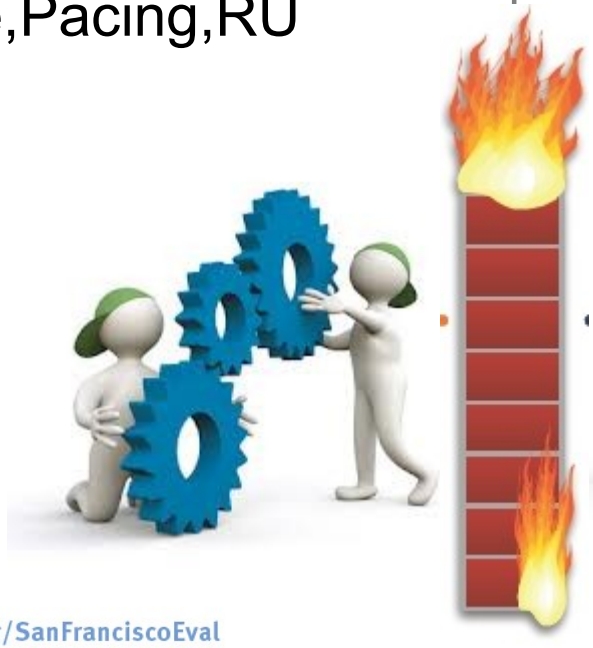
Enterprise Extender – SNA over IP Terminology

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

System z Boundary

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

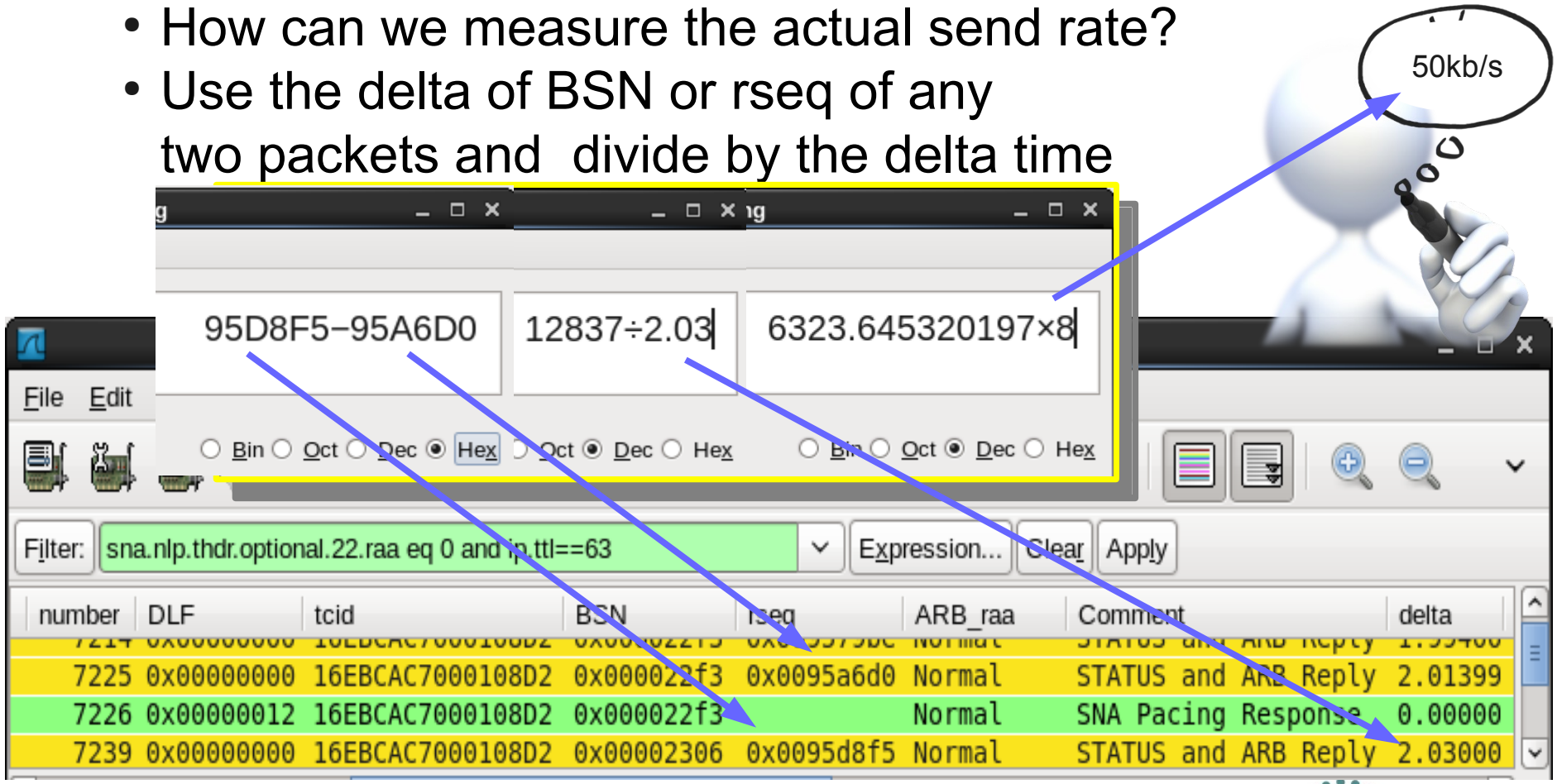


Diagnosing Enterprise Extender problems in z/OS Communications Server

- 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



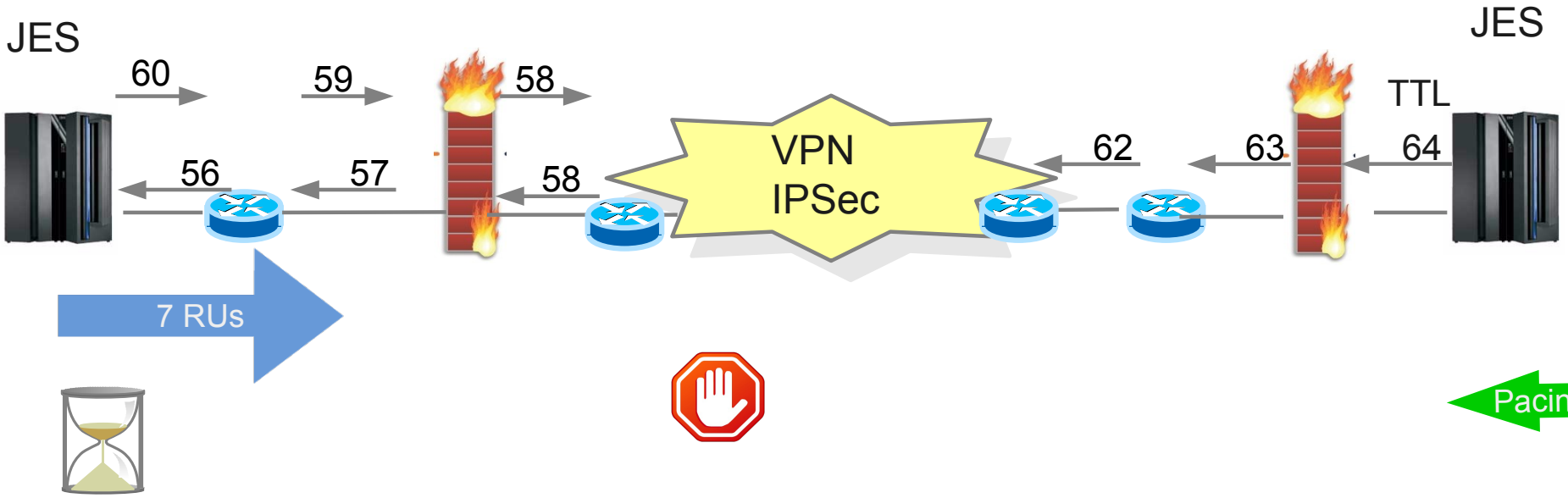
Wireshark: Detecting Delays in Transmission
Filter: frame.time_delta gt 0.5

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



Filter: frame.coloring_rule.name contains __ | Expression... | Clear | Apply

No.	Time	len	TTL	Source	Comment	snf	tcid	BSN	rse
12342	0.010	109	56	92.254.251.11	SNA Pacing Res	22451	16ECDA0E00010259	0x002372f8	0x6
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	0x6
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	0x6
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	0x6
12432	0.008	121	56	92.254.251.11	SNA Pacing Res	22472	16ECDA0E00010259	0x00237331	0x6

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

Top 3 Root Causes of all EE Problems

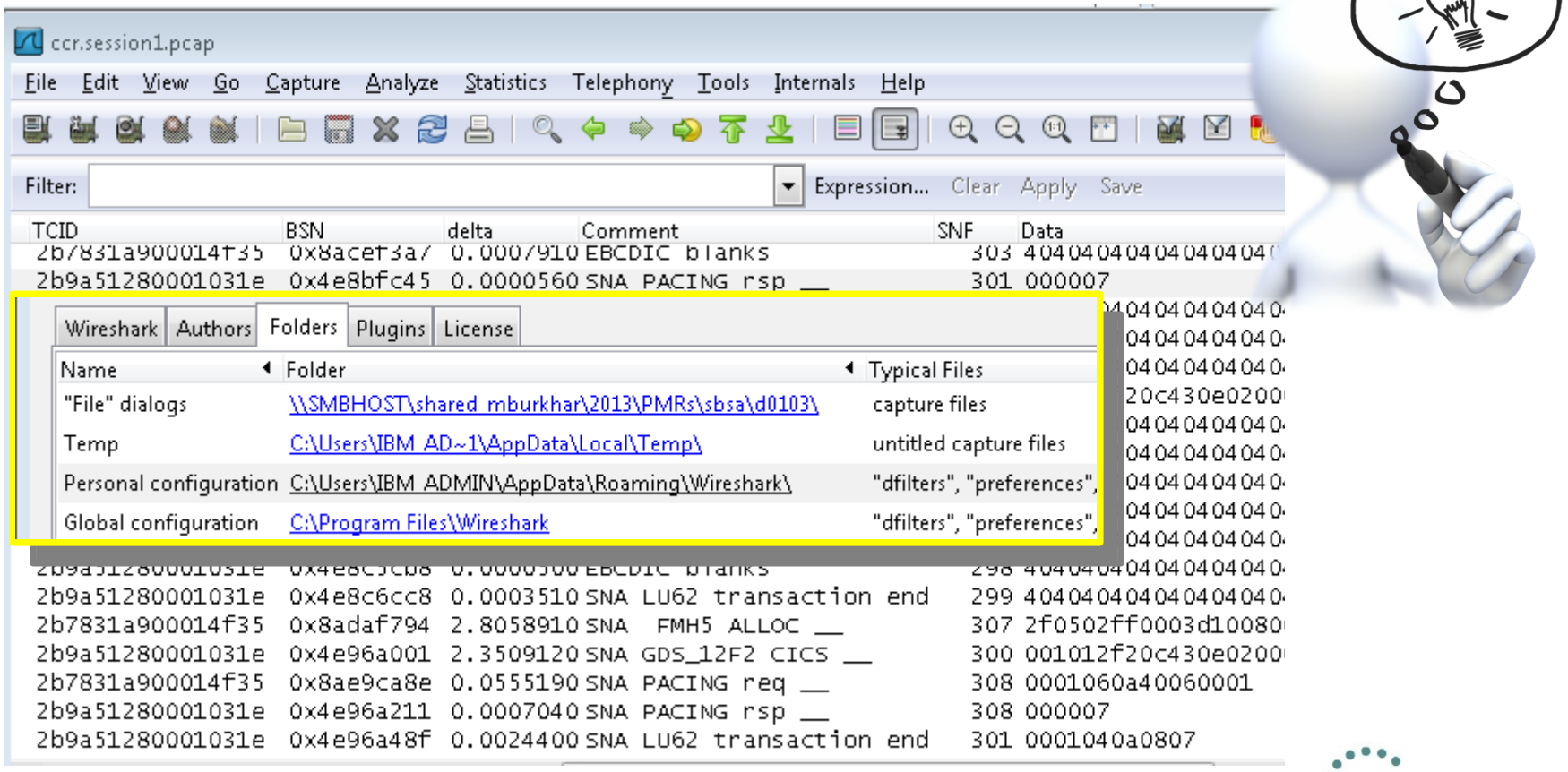
- Firewall Filter Rules not in place consistently
  - Allow new UDP connections 12000 – 12004 in both directions
    - ALWAYS!
- Queue overflow due to bursty HPR traffic pattern
  - ARB Sendrate → Burstsize can grow to large # of packets
- Fragmentation
  - IPSec tunnels require reduced MTU size
   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

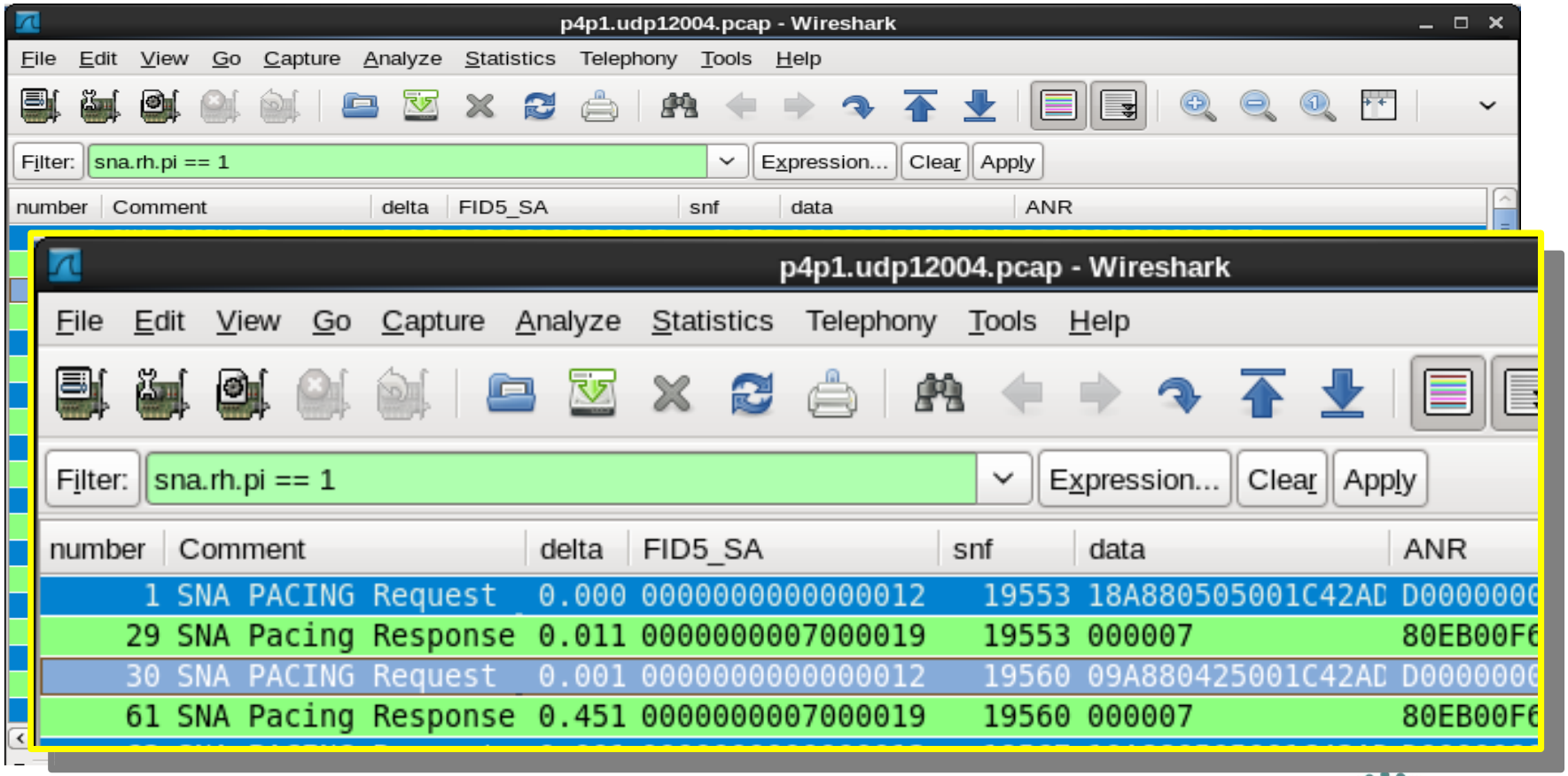
Wireshark Profiles – SNA information

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



Wireshark Filter Options – SNA Pacing

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



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	Sourc
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

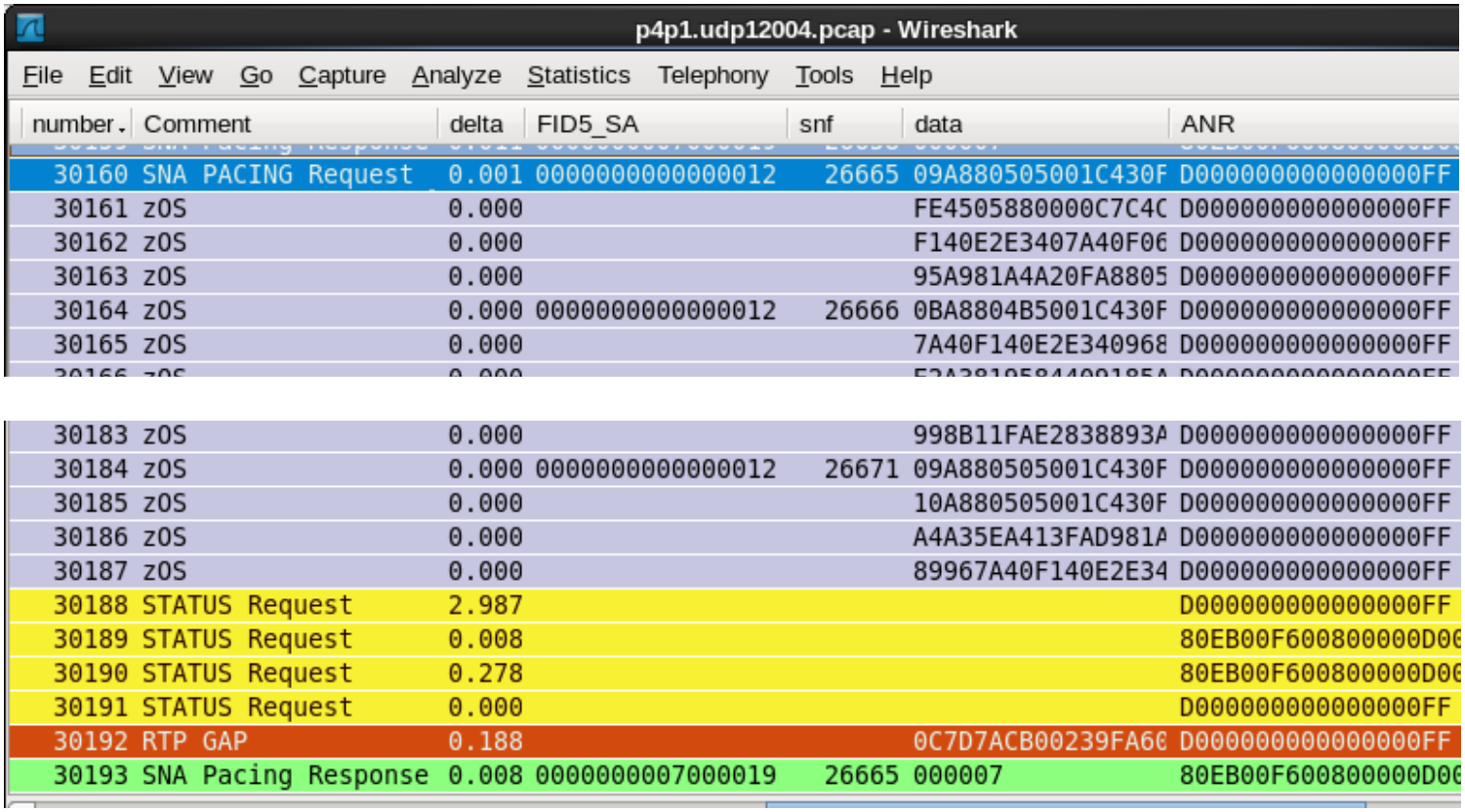
Filter

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.offs
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.rri == 1
SNA PACING Request	sna.rh.pi == 1 and sna.rh.rri == 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

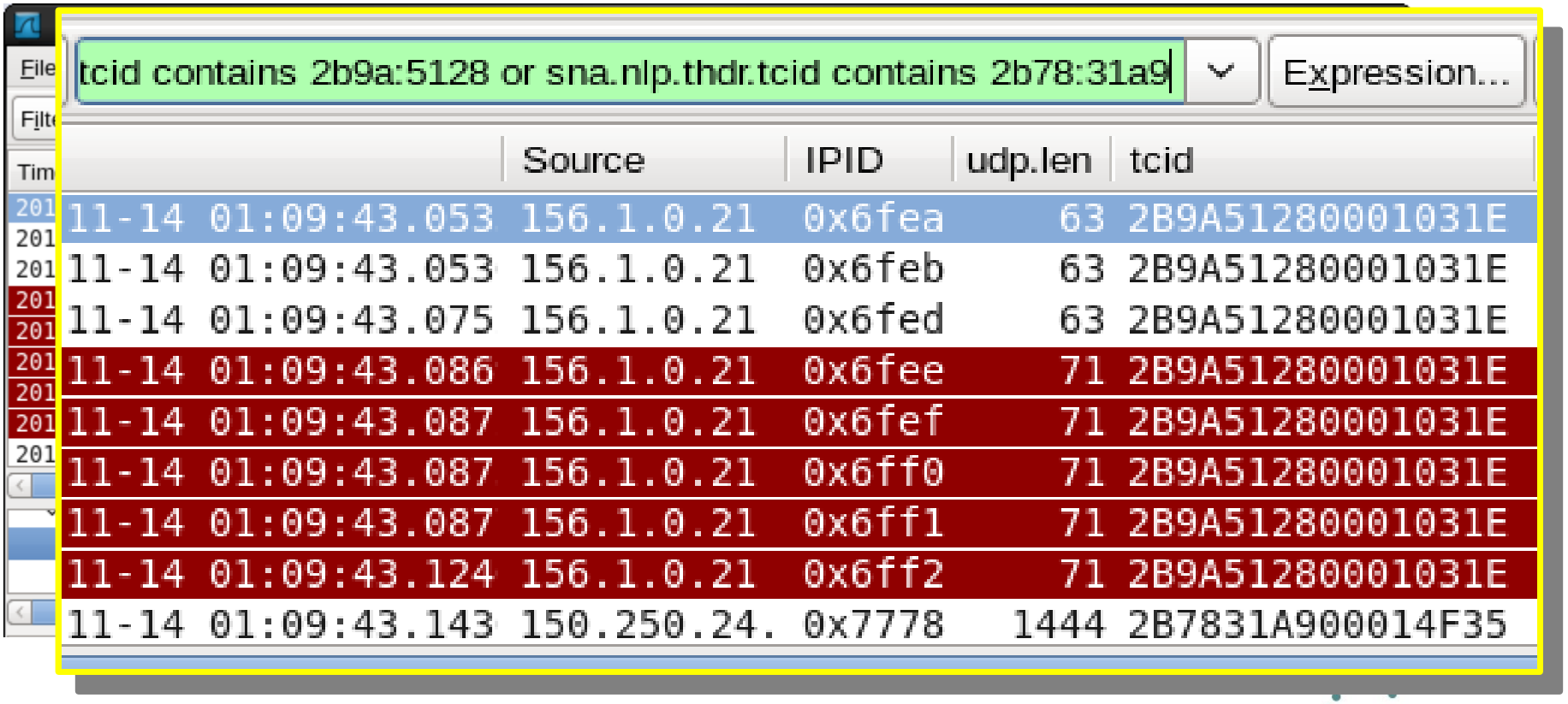
Wireshark Coloring Rules

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



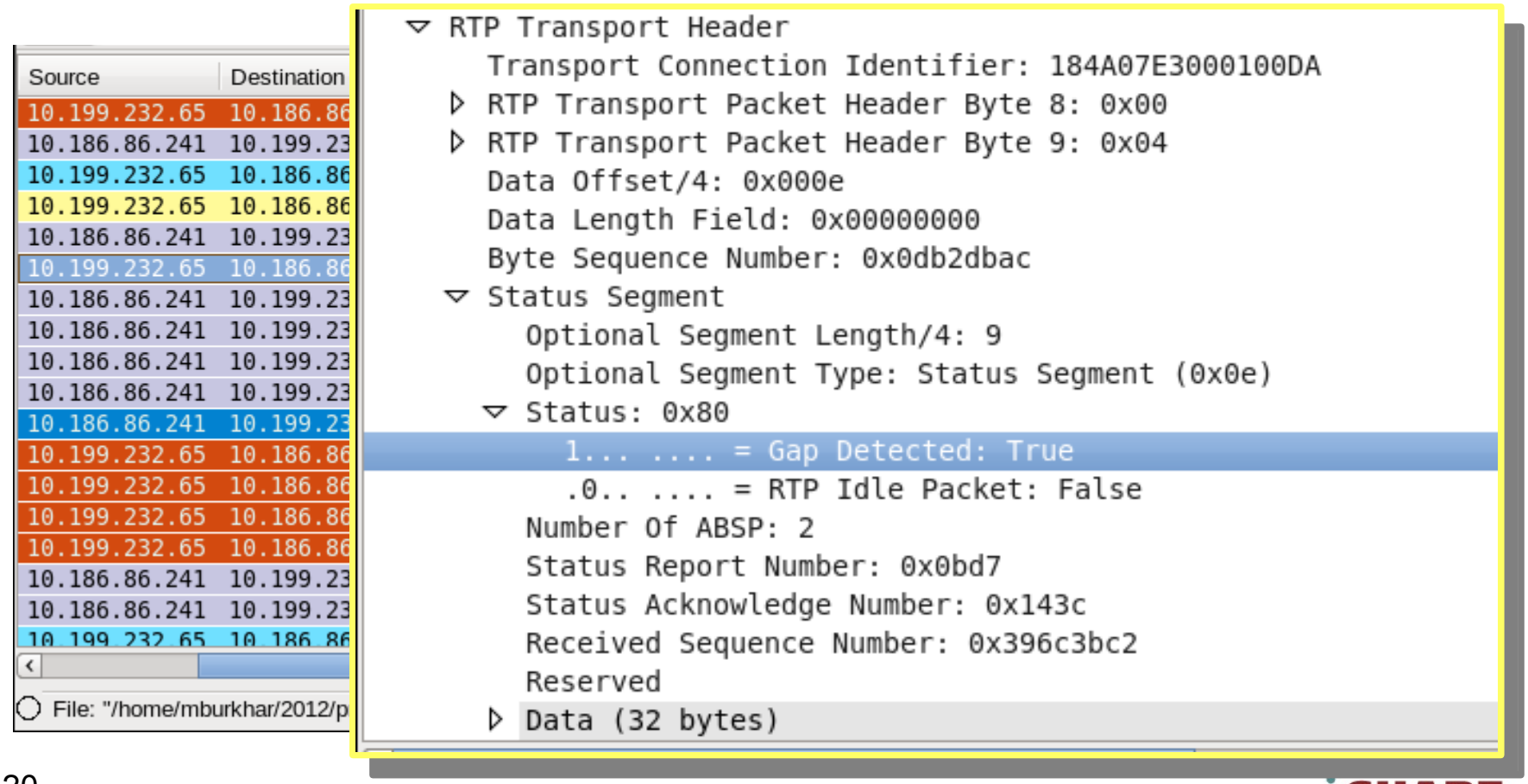
HPR: One Pipe two TCIDs

- 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'



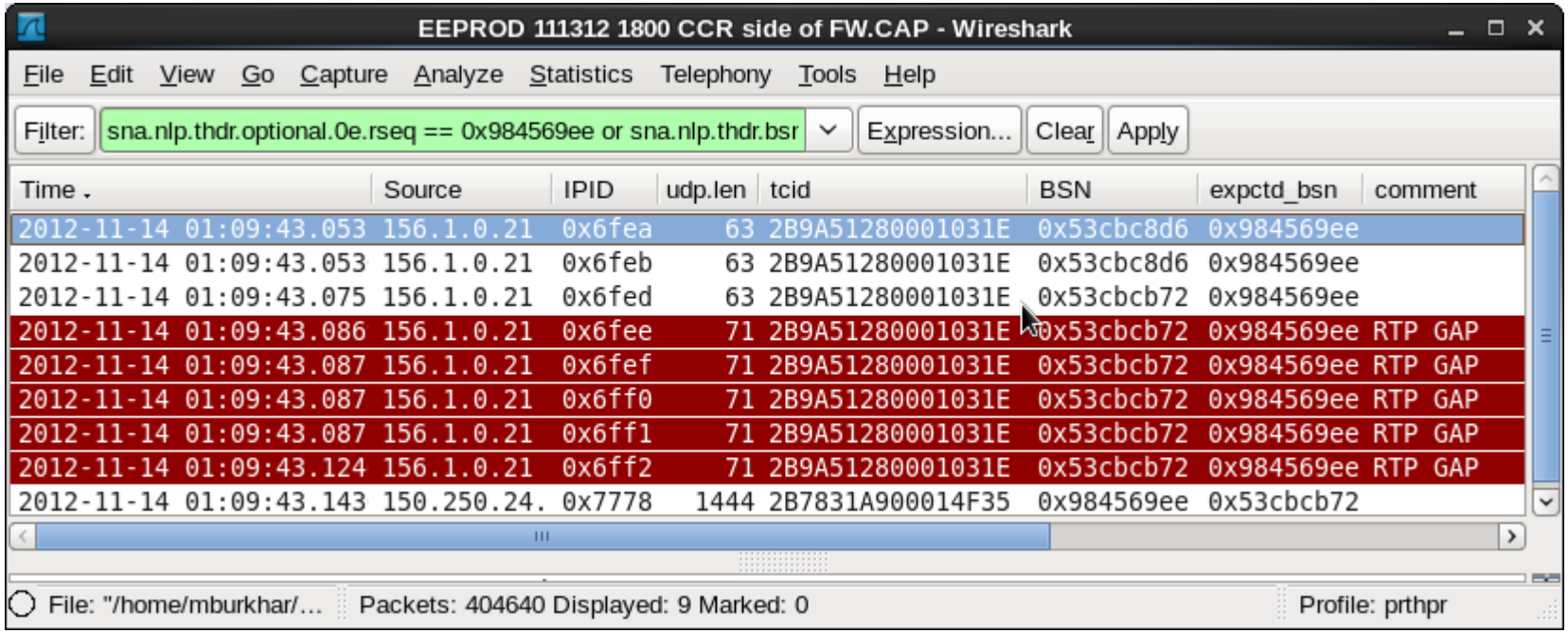
HPR – STATUS segment with GAP

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



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



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

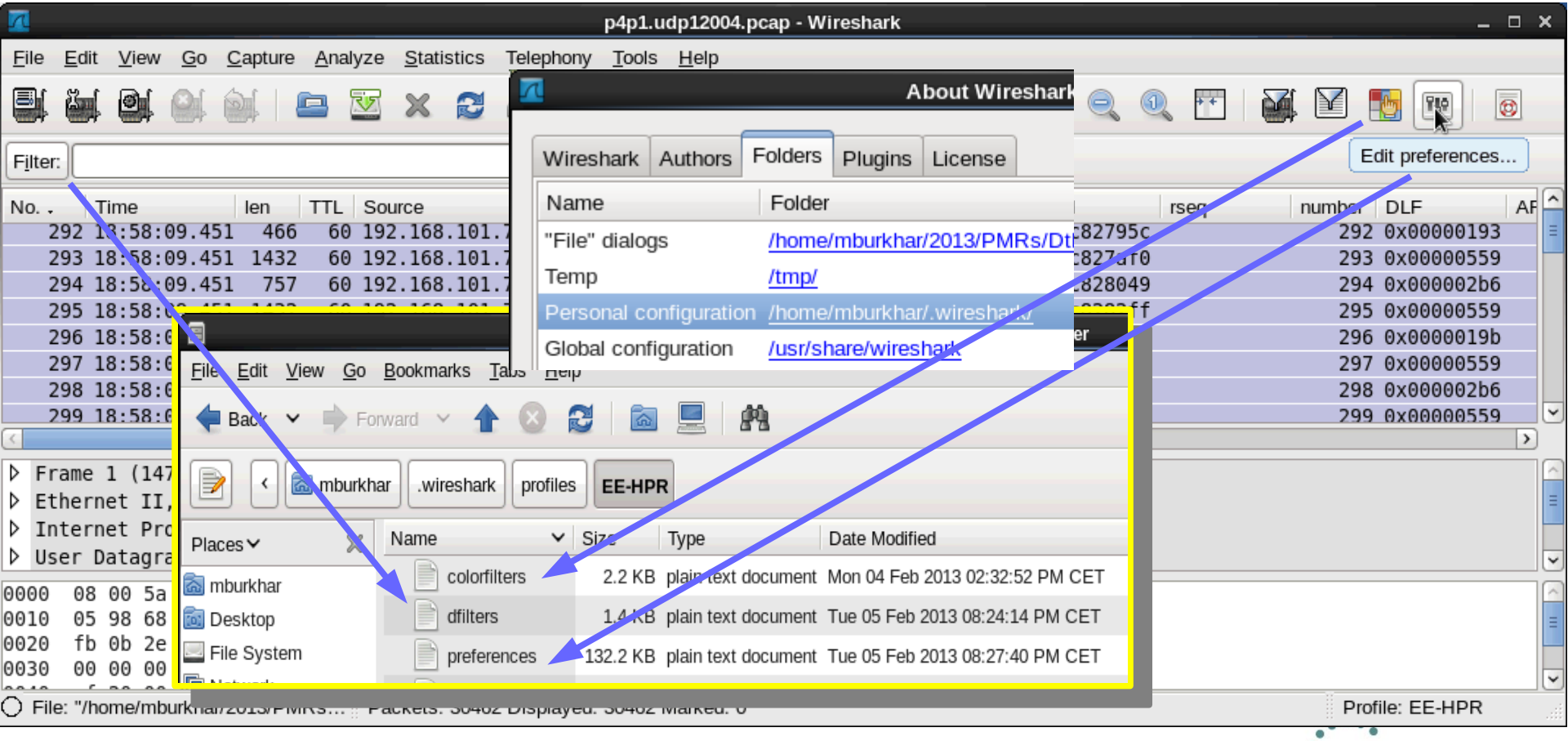
Filter: sna.nlp.thdr.optional.0e.gap ==1 or sna.rh.pi == 1 | Expression... | Clear | Apply

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

Wireshark Profiles
dfilters, colorfilters, preferences

Three files located in Personal Configuration folder

- Help → About Wireshark → Folders



Need more Wireshark

Facebook groups

sna.wizards@groups.facebook.com

ip.wizards@groups.facebook.om

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

#SHAREorg

SHARE
Technology · Connections · Results

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

SHARE in San Francisco 2013

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.rri == 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.rri == 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.rri == 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.rri == 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]
```