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
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 RPNBC 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 1.

- 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?

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

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?
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,tcip,PKT,ON,ABBREV=250
  - Dump of VTAM and TCPIP
    - F NET,CSDUMP,TCPNAME=tcip

- 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 Screen Shot](image.png)

Filter: sna.nlp.thdr.optional.22.raa eq 0 and ip_ttl==63

<table>
<thead>
<tr>
<th>number</th>
<th>DLF</th>
<th>tcid</th>
<th>BSN</th>
<th>lseq</th>
<th>ARB_raa</th>
<th>Comment</th>
<th>delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>7214</td>
<td>0x00000000</td>
<td>16EBCAC7000108D2</td>
<td>0X000022F3</td>
<td>0x0095a6d0</td>
<td>Normal</td>
<td>STATUS and ARB Reply 1.954000</td>
<td>7225 0x00000000</td>
</tr>
</tbody>
</table>
Wireshark: Detecting Delays in Transmission
Filter: frame.time_delta gt 0.5

Table:

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Len</th>
<th>IPID</th>
<th>TTL</th>
<th>Source</th>
<th>Destination</th>
<th>Comment</th>
<th>tcid</th>
<th>BSN</th>
<th>rseq</th>
</tr>
</thead>
<tbody>
<tr>
<td>10770</td>
<td>0.572</td>
<td>91</td>
<td>0x9c2d</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>RTP GAP</td>
<td>155CA61000100AF</td>
<td>0x6d123fb3</td>
<td>0x00236f09</td>
</tr>
<tr>
<td>10921</td>
<td>0.707</td>
<td>91</td>
<td>0xd116</td>
<td>56</td>
<td>192.254.251.11</td>
<td>192.168.101.7</td>
<td>STATUS Request</td>
<td>16ECDA0E00010259</td>
<td>0x00236f7b</td>
<td>0x6d14496e</td>
</tr>
<tr>
<td>11361</td>
<td>2.604</td>
<td>83</td>
<td>0x9f31</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>STATUS Request</td>
<td>155CA61000100AF</td>
<td>0x6d1a6927</td>
<td>0x00237085</td>
</tr>
<tr>
<td>11714</td>
<td>0.558</td>
<td>91</td>
<td>0xd1c8</td>
<td>56</td>
<td>192.254.251.11</td>
<td>192.168.101.7</td>
<td>STATUS Request</td>
<td>16ECDA0E00010259</td>
<td>0x0023717c</td>
<td>0x6d1f4e9d</td>
</tr>
<tr>
<td>11836</td>
<td>0.598</td>
<td>91</td>
<td>0xa171</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>RTP GAP</td>
<td>155CA61000100AF</td>
<td>0x6d20f0e9</td>
<td>0x002371b5</td>
</tr>
<tr>
<td>12045</td>
<td>0.752</td>
<td>83</td>
<td>0xa25c</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>STATUS Request</td>
<td>155CA61000100AF</td>
<td>0x6d23cc90</td>
<td>0x0023723a</td>
</tr>
<tr>
<td>12429</td>
<td>2.595</td>
<td>83</td>
<td>0xa475</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>STATUS Request</td>
<td>155CA61000100AF</td>
<td>0x6d291b50</td>
<td>0x00237331</td>
</tr>
<tr>
<td>12522</td>
<td>0.577</td>
<td>91</td>
<td>0xa4f3</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>RTP GAP</td>
<td>155CA61000100AF</td>
<td>0x6d2a54f4</td>
<td>0x0023736a</td>
</tr>
<tr>
<td>12760</td>
<td>0.720</td>
<td>91</td>
<td>0xd2bb</td>
<td>56</td>
<td>192.254.251.11</td>
<td>192.168.101.7</td>
<td>STATUS Request</td>
<td>16ECDA0E00010259</td>
<td>0x00237415</td>
<td>0x6d2d98d8</td>
</tr>
<tr>
<td>12853</td>
<td>0.562</td>
<td>91</td>
<td>0xa68e</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>RTP GAP</td>
<td>155CA61000100AF</td>
<td>0x6d2ed20c</td>
<td>0x0023743b</td>
</tr>
<tr>
<td>13091</td>
<td>0.503</td>
<td>109</td>
<td>0xd310</td>
<td>56</td>
<td>192.254.251.11</td>
<td>192.168.101.7</td>
<td>SNA Pacing Res</td>
<td>16ECDA0E00010259</td>
<td>0x002374d3</td>
<td>0x6d31bc59</td>
</tr>
<tr>
<td>13470</td>
<td>2.416</td>
<td>83</td>
<td>0xa999</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>STATUS Request</td>
<td>155CA61000100AF</td>
<td>0x6d3765b4</td>
<td>0x002375ca</td>
</tr>
<tr>
<td>13650</td>
<td>0.576</td>
<td>91</td>
<td>0xaa73</td>
<td>60</td>
<td>192.168.101.7</td>
<td>92.254.251.11</td>
<td>RTP GAP</td>
<td>155CA61000100AF</td>
<td>0x6d39d906</td>
<td>0x0023763c</td>
</tr>
<tr>
<td>14408</td>
<td>0.519</td>
<td>91</td>
<td>0xd422</td>
<td>56</td>
<td>192.254.251.11</td>
<td>192.168.101.7</td>
<td>STATUS Request</td>
<td>16ECDA0E00010259</td>
<td>0x0023783d</td>
<td>0x6d44734a</td>
</tr>
</tbody>
</table>

Complete your sessions evaluation online at SHARE.org/SanFranciscoEval
The Root Cause: Network Layer Packets NLPs are dropped and require retransmission.
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)

Who is dropping packets and why?
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
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`

![Wireshark screenshot showing RTP Transport Header and Status Segment]
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)
Wireshark Profiles
dfilters, colorfilters, preferences

Three files located in Personal Configuration folder
• Help → About Wireshark → Folders

Complete your sessions evaluation online at SHARE.org/SanFranciscoEval
Need more Wireshark

Facebook groups
  sna.wizards@groups.facebook.com
  ip.wizards@groups.facebook.com

IBM SmartCloud Community
  „ip wizards in the Cloud“

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
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 transaction)" 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.nl.thdr.optional.0e.gap ==1 and sna.nl.thdr.bsn >= 0x00000000
"HPR_suspicious" sna.nl.thdr.offset gt 10 and !sna.nl.thdr.offset eq 13 and sna.nl.thdr.tcid lt 8000:0000:0000:0000
"HPR New Pipe " sna.nl.thdr.tcid ge 8000:0000:00:00:00:00 or sna.nl.thdr.bsn == 0x00000000
"HPR Pipe CFAULT" sna.nl.thdr.offset == 0x000c and sna.nl.thdr.offset gt 10 and !sna.nl.thdr.offset eq 13
"HPR PATHSWITCH" sna.nl.thdr.dlf eq 0 and sna.nl.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 == 0x00c and sna.nlp.thdr.dr.== 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 Slowdown @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-action@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.fii == 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.fii == 1[@65534,64008,39339][0,0,0]
@SNA BIND@sna.rh.category == 0x03 and sna.rh and data.data[0]==31[@16579,16707,52185][62667,62061,62061]
@UNBIND Cleanup@sna.rh.category == 0x03 and sna.rh and data.data[0]==31[@16579,16707,52185][62667,62061,62061]
@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 A002001@sna.nlp.thdr.offset == 0x000c and sna.nlp.thdr.tci 8 == 0x30@[45246,3377,3377][65065,62762,3452]
@HPR New Pipe @sna.nlp.thdr.tci 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@[65535,62969,61744]
@HPR suspicious@sna.nlp.thdr.offset gt 10 and !sna.nlp.thdr.offset eq 13 and sna.nlp.thdr.tci lt 8000:0000:0000:0000@[63686,10683,3829]
@GDS12Fx x-action reply@data.data[2:2] == 12f2 or data.data[2:2] == 12ff@[6891,39551,24911]
@XID Done@llc.control == 0x0003 and udp.dstport==12000@0,0,0][65535,63222,0]
@CEBI end_x-action@sna.rh.cebi==1@0,0,0]
@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.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@[65535,63225,54808][3276,736,62996]
@sna.RPACING 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]==31@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]