Winter 2011 – Session 8319
End the journey through the dark
Turn on the light with wireshark

Matthias Burkhard
IBM Germany
mburkhar@de.ibm.com

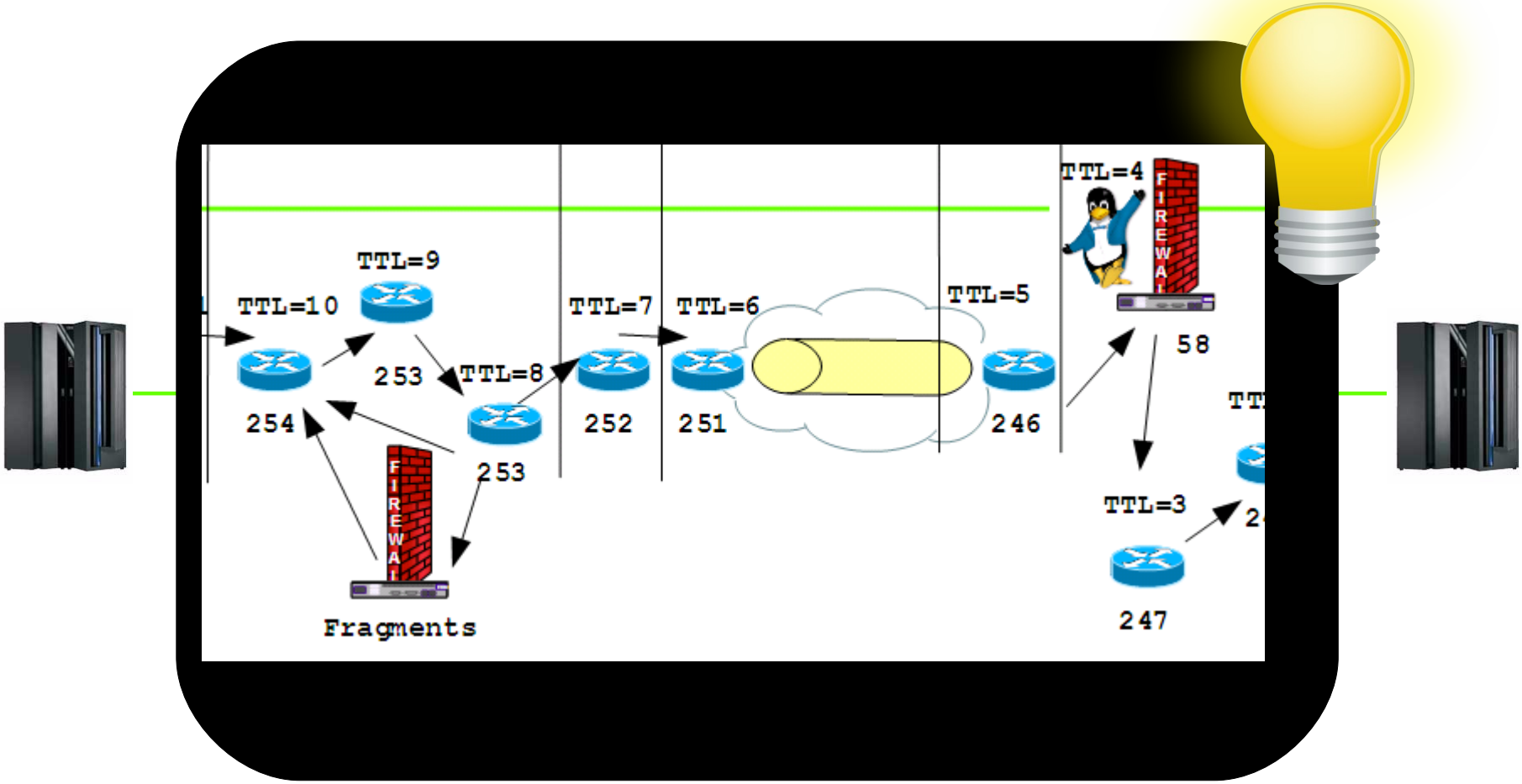
: mreede
Twitter

: Matthias Burkhard
ip.wizards@groups.facebook.com
IP Wizards

Tuesday, March 1, 2011: 4:30PM-5:30PM
Anaheim Convention Center, Room 212A

End the journey through the dark

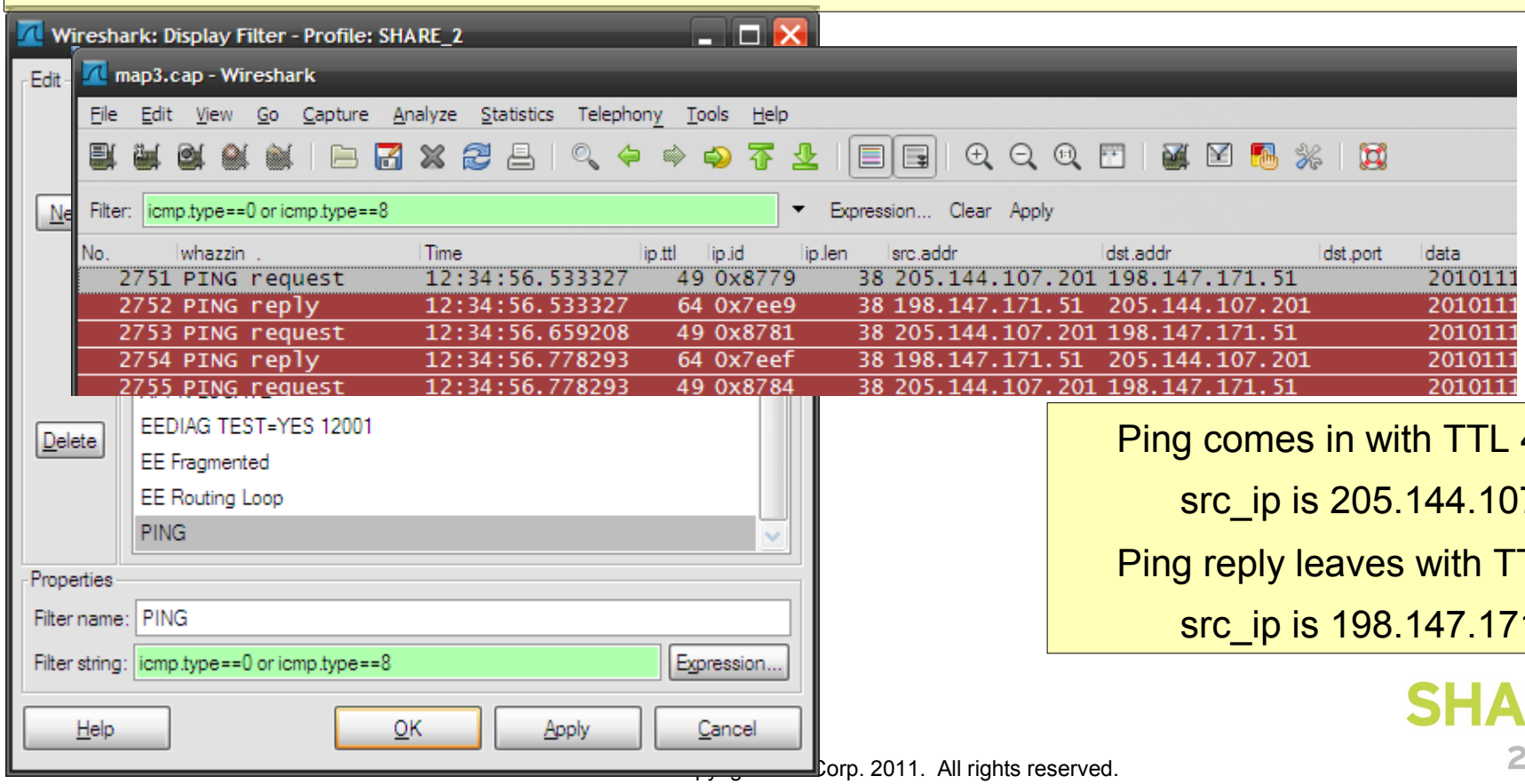
Turn on the light with wireshark



The mother of all IP diagnostics: PING

http://en.wikipedia.org/wiki/Sonar

„active sonar is emitting pulses of sounds and listening for echoes. Sonar may be used as a means of acoustic location and of measurement of the echo characteristics of "targets" in the water.“



Ping comes in with TTL 49

src_ip is 205.144.107.201

Ping reply leaves with TTL 64

src_ip is 198.147.171.51

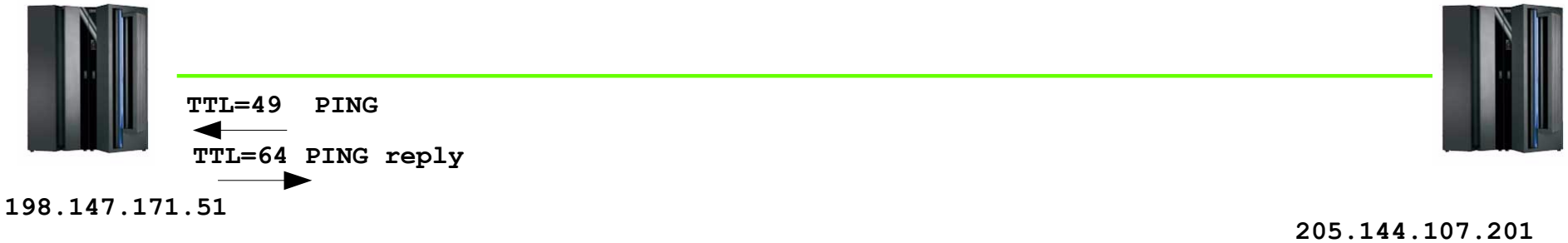
TTL and Topology I.

Ping comes in with TTL 49

src_ip is 205.144.107.201

Ping reply leaves with TTL 64

src_ip is 198.147.171.51



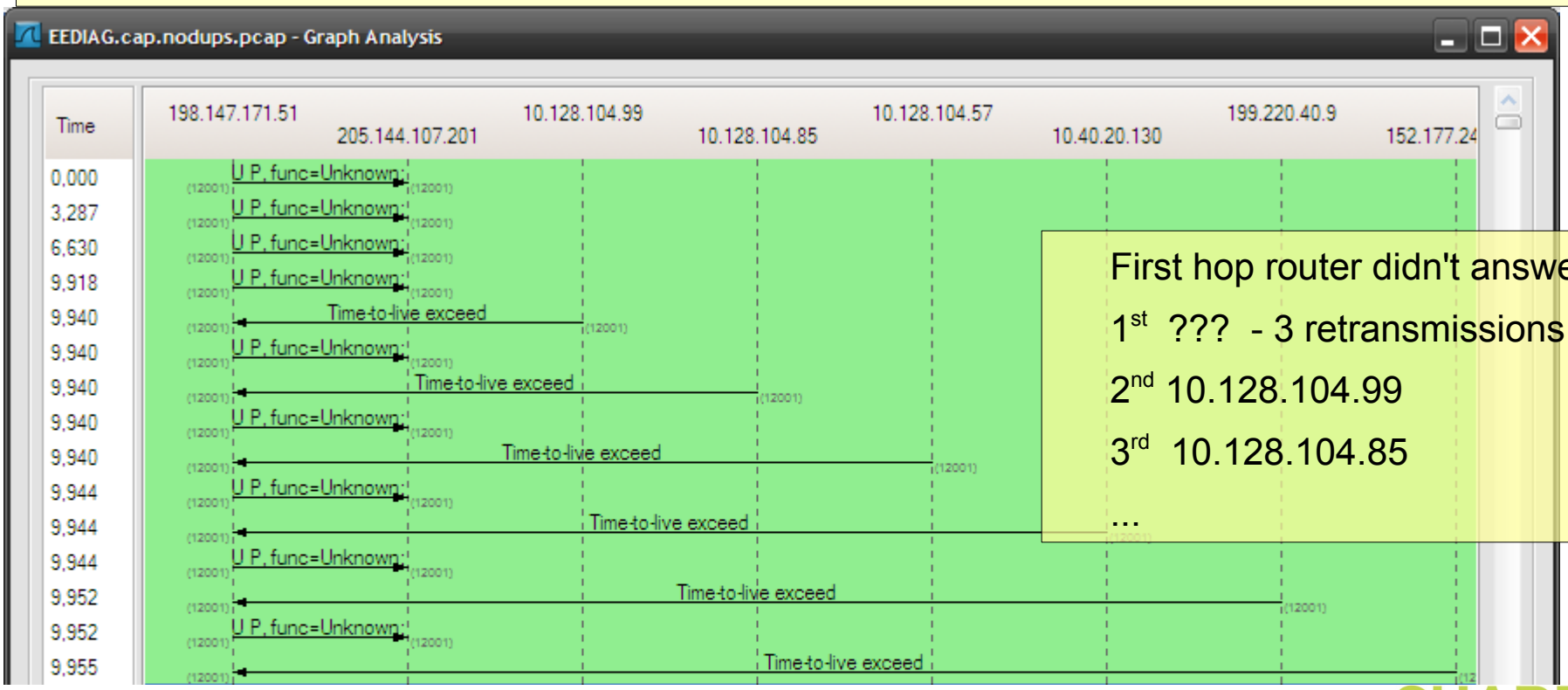
D NET,EEDIAG,TEST=YES can be used to determine the ip route towards a destination host

Works similar to the IP traceroute, sending IP packets with too short TTL soliciting ICMP TTL exceeded messages.

Flow Graph
EEDIAG TEST=YES

IP Packets are sent to all EE ports with TTL of 1, if no ICMP TTL exceeded response is received the packet is resent with 3.3 seconds interval)

If a TTL exceeded message is received, the sender's src_ip and the RTT will be remembered



First hop router didn't answer

1st ??? - 3 retransmissions

2nd 10.128.104.99

3rd 10.128.104.85

...

The traceroute for HPR/IP: EEDIAG TEST=YES

EEDIAG.cap.nodups.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: udp.port==12001 Expression... Clear Apply

No.	whazzin	Time	ip.ttl	ip.id	ip.len	src.addr	dst.addr	dst.port	llc.ctrl
102	EEDIAG TEST req	0.000000	10	0x7497	76	198.147.171.51	205.144.107.201	12001	0x00f7
107	EEDIAG RTT reply	0.046825	1	0x7497	76	205.144.107.201	198.147.171.51	12001	
109	EEDIAG TEST req	0.000000	11	0x749c	76	198.147.171.51	205.144.107.201	12001	0x00f7
117	EEDIAG RTT reply	0.079326	1	0x749c	76	205.144.107.201	198.147.171.51	12001	
122	EEDIAG TEST req	0.019701	12	0x74a2	76	198.147.171.51	205.144.107.201	12001	0x00f7
127	EEDIAG RTT reply	0.014944	1	0x74a2	76	205.144.107.201	198.147.171.51	12001	
132	EEDIAG TEST req	0.000000	13	0x74a7	76	198.147.171.51	205.144.107.201	12001	0x00f7
137	EEDIAG TEST OK	0.077552	49	0x4984	76	205.144.107.201	198.147.171.51	12001	0x00f7
142	EEDIAG TEST req	19.710413	1	0x76e2	76	198.147.171.51	205.144.107.201	12001	0x00f7

Edit

New

Delete

Properties

Filter name: EEDIAG TEST=YES 12001

Filter string: llc.control == 0x00f7 and udp.dstport==12001 Expression...

Help OK Apply Cancel

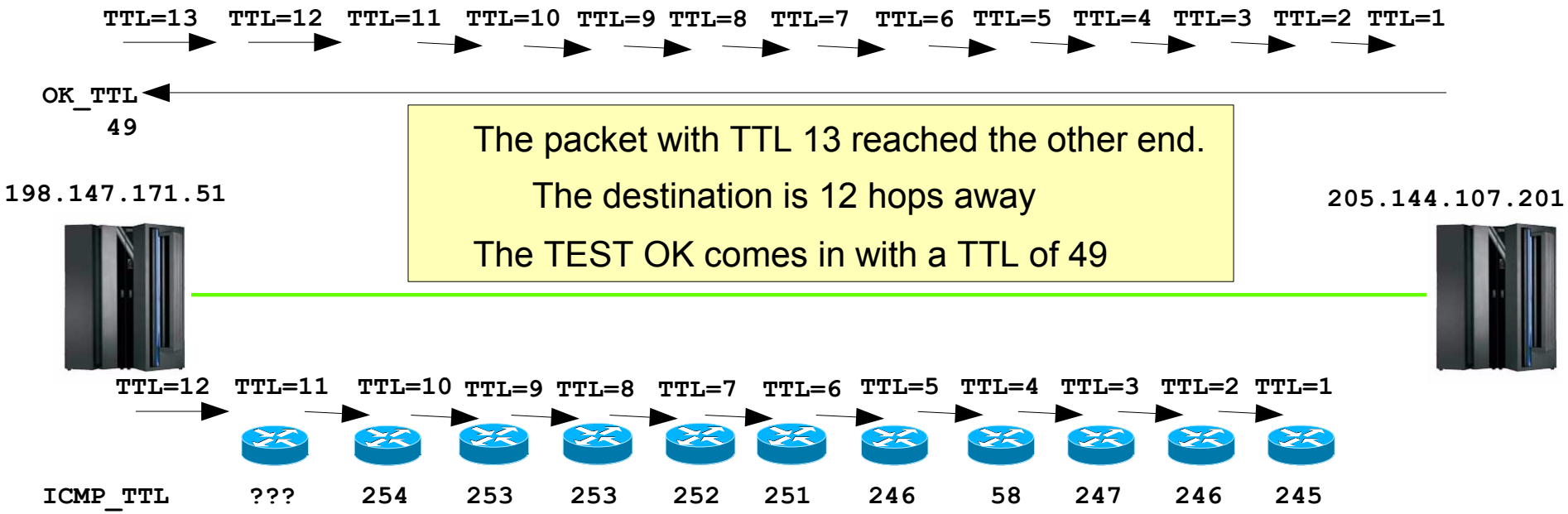
TTL 12 was the last packet getting an ICMP

TTL 13 reached the other end.

The destination is 12 hops away

The TEST OK comes in with a TTL of 49

TTL and Topology II.



The packet with TTL 13 reached the other end.

The destination is 12 hops away

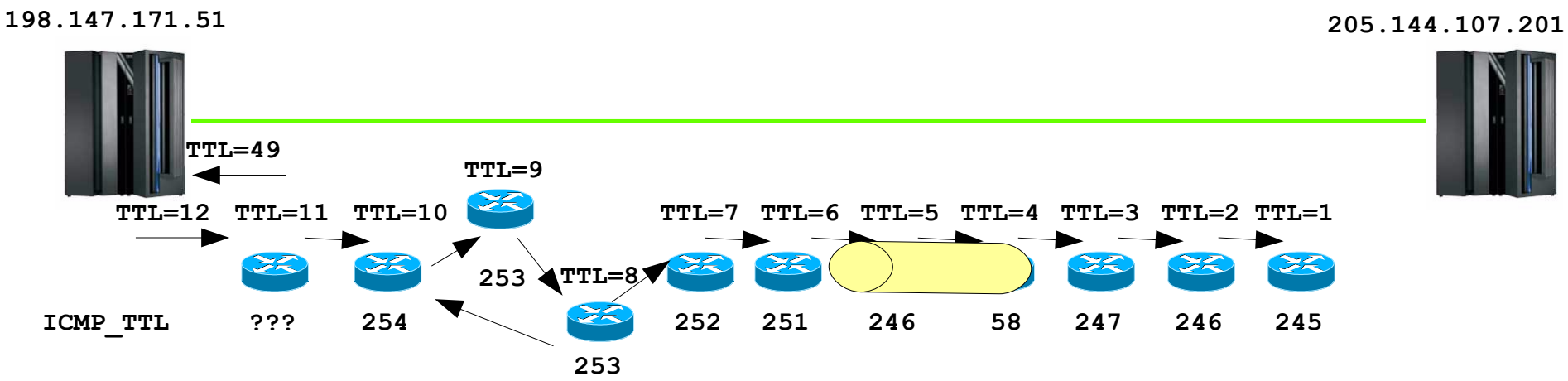
The TEST OK comes in with a TTL of 49

If the TTL is too low, it will solicit an ICMP packet from the router that saw a TTL=1

Inspecting the source ip address and its own TTL enables us to complete the picture

TTL and Topology III.

Looking at the returned TTLs, we can make assumptions as to how the routers are connected.

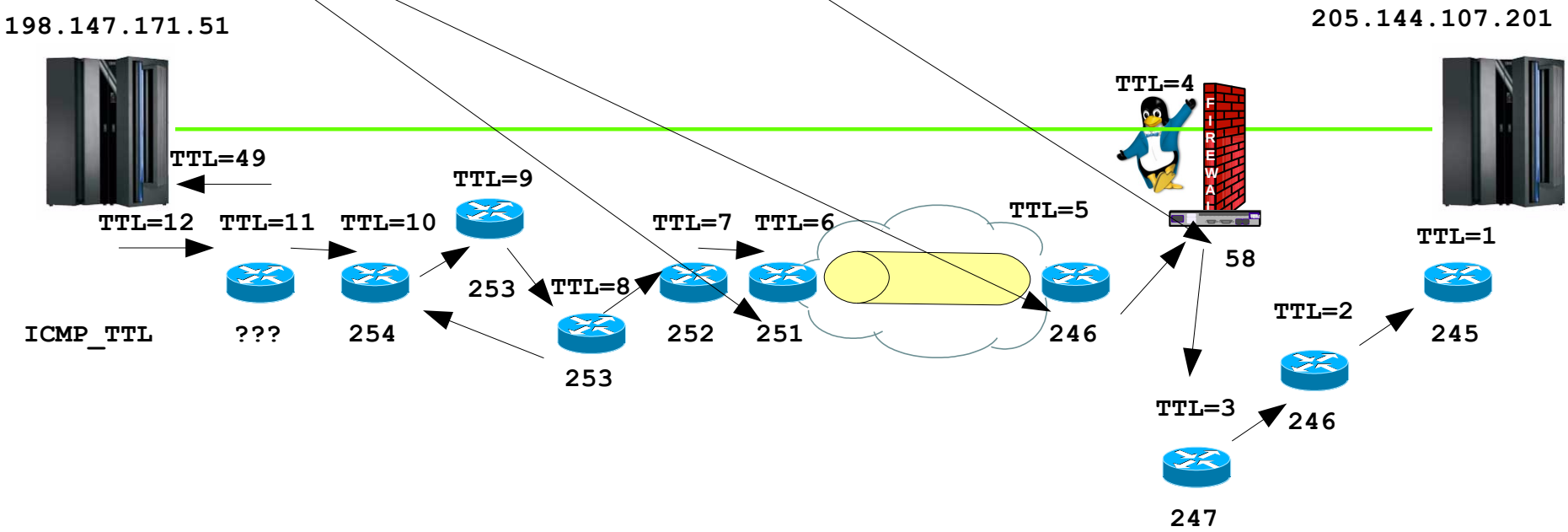


TTL and Topology IV.

Routers send with a TTL of 255

Linux sends with a TTL of 64

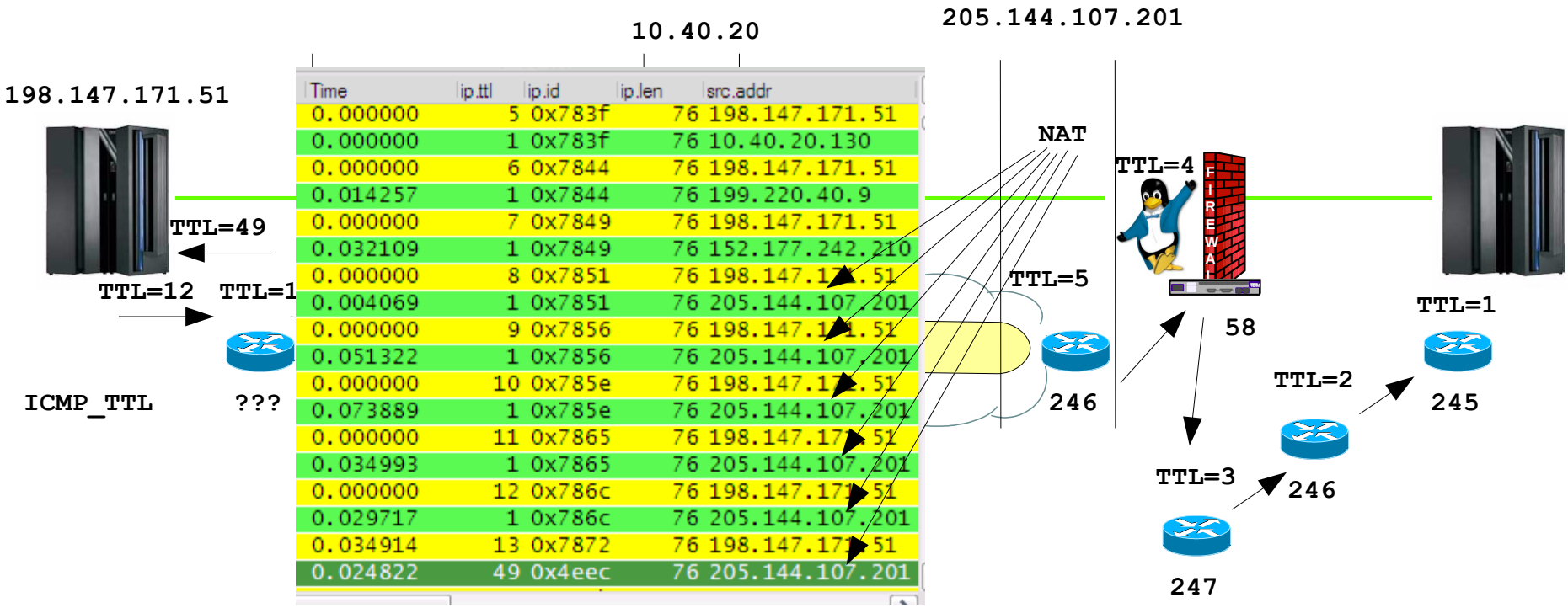
A gap in the TTLs indicates a VPN IPSec tunnel is in the path



TTL and Topology V. - NAT

The ICMP messages from the last 6 hops are all 'from the same ip-address“

The TTLs are different though and so are the IPID ranges



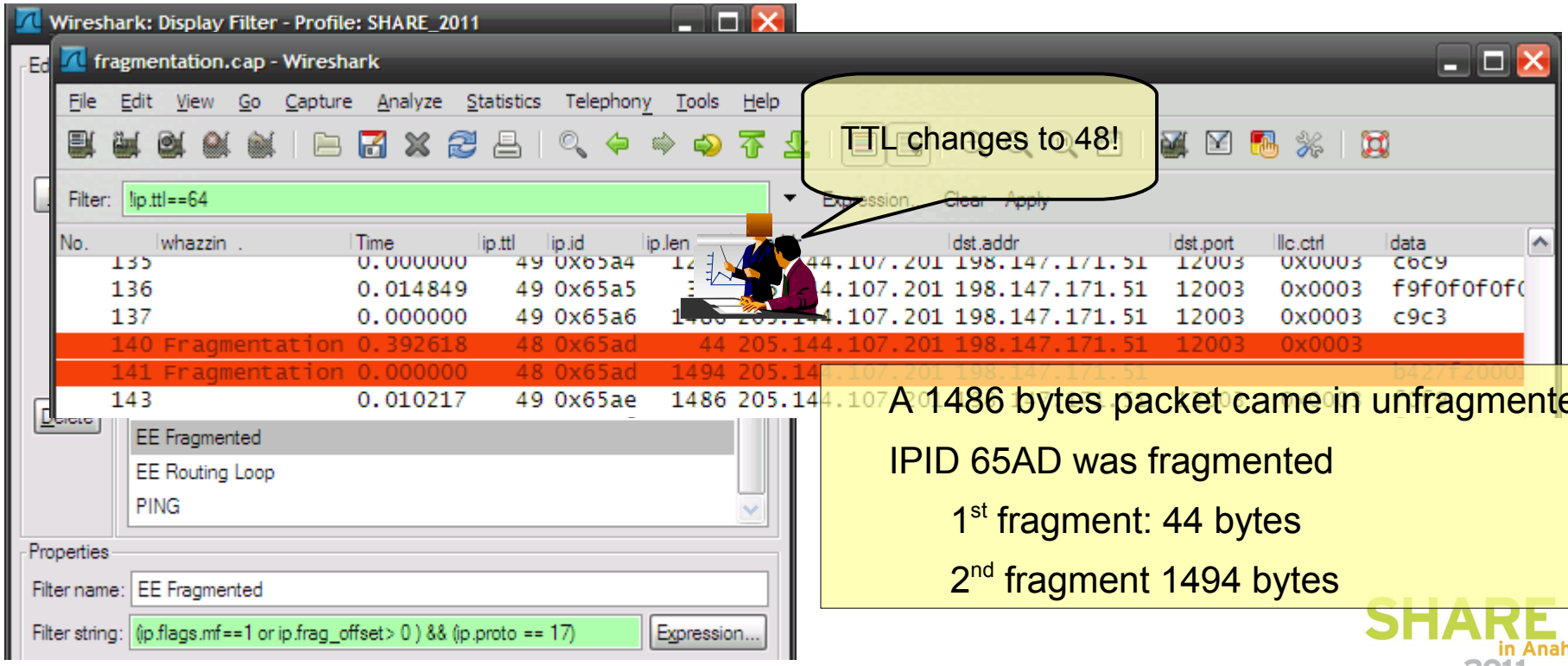
Time	ip.ttl	ip.id	ip.len	src.addr
0.000000	5	0x783f	76	198.147.171.51
0.000000	1	0x783f	76	10.40.20.130
0.000000	6	0x7844	76	198.147.171.51
0.014257	1	0x7844	76	199.220.40.9
0.000000	7	0x7849	76	198.147.171.51
0.032109	1	0x7849	76	152.177.242.210
0.000000	8	0x7851	76	198.147.171.51
0.004069	1	0x7851	76	205.144.107.201
0.000000	9	0x7856	76	198.147.171.51
0.051322	1	0x7856	76	205.144.107.201
0.000000	10	0x785e	76	198.147.171.51
0.073889	1	0x785e	76	205.144.107.201
0.000000	11	0x7865	76	198.147.171.51
0.034993	1	0x7865	76	205.144.107.201
0.000000	12	0x786c	76	198.147.171.51
0.029717	1	0x786c	76	205.144.107.201
0.034914	13	0x7872	76	198.147.171.51
0.024822	49	0x4eec	76	205.144.107.201

Fragmentation is bad – BAD – BAD

While the IP protocol provides for fragmentation and reassembly in today's networks we cannot assume that fragmented ip packets will allways be allowed through the firewall infrastructure.

FW filter rules typically check on ip address pair, protocol and port numbers

With fragmentation, this information is not present in 2nd and following fragments.



A 1486 bytes packet came in unfragmented

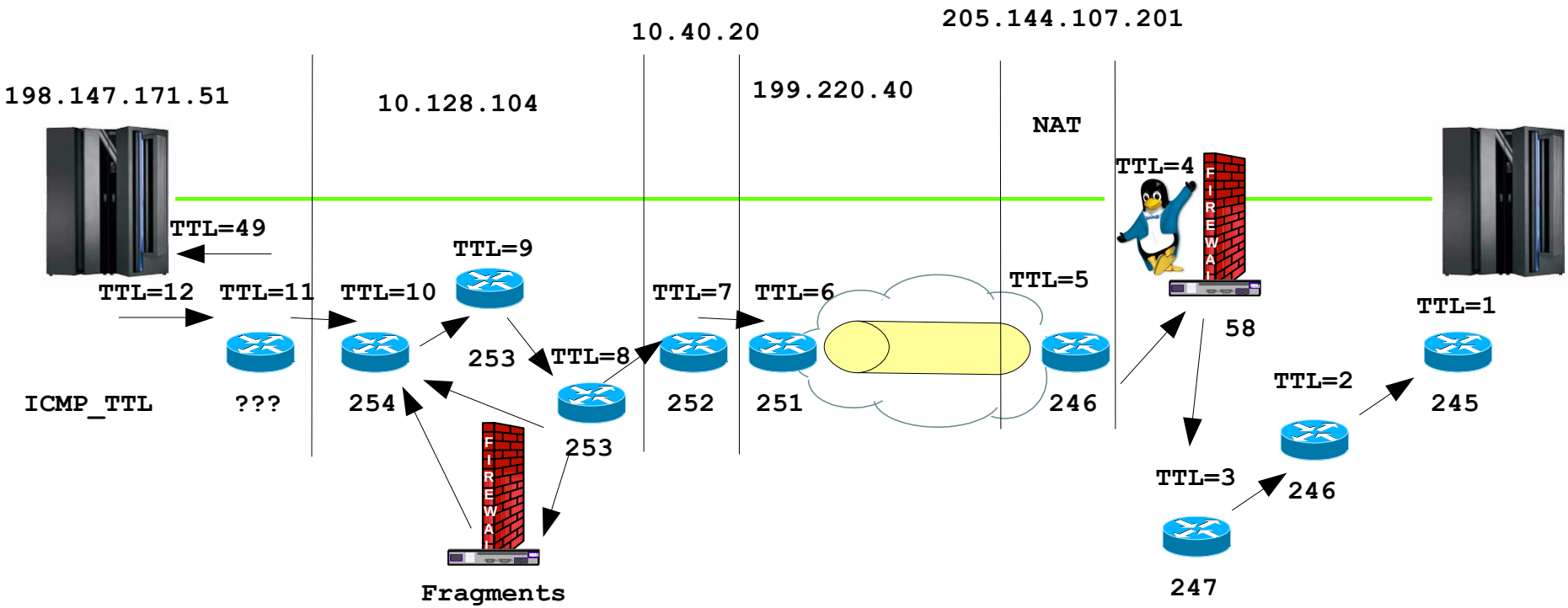
IPID 65AD was fragmented

1st fragment: 44 bytes

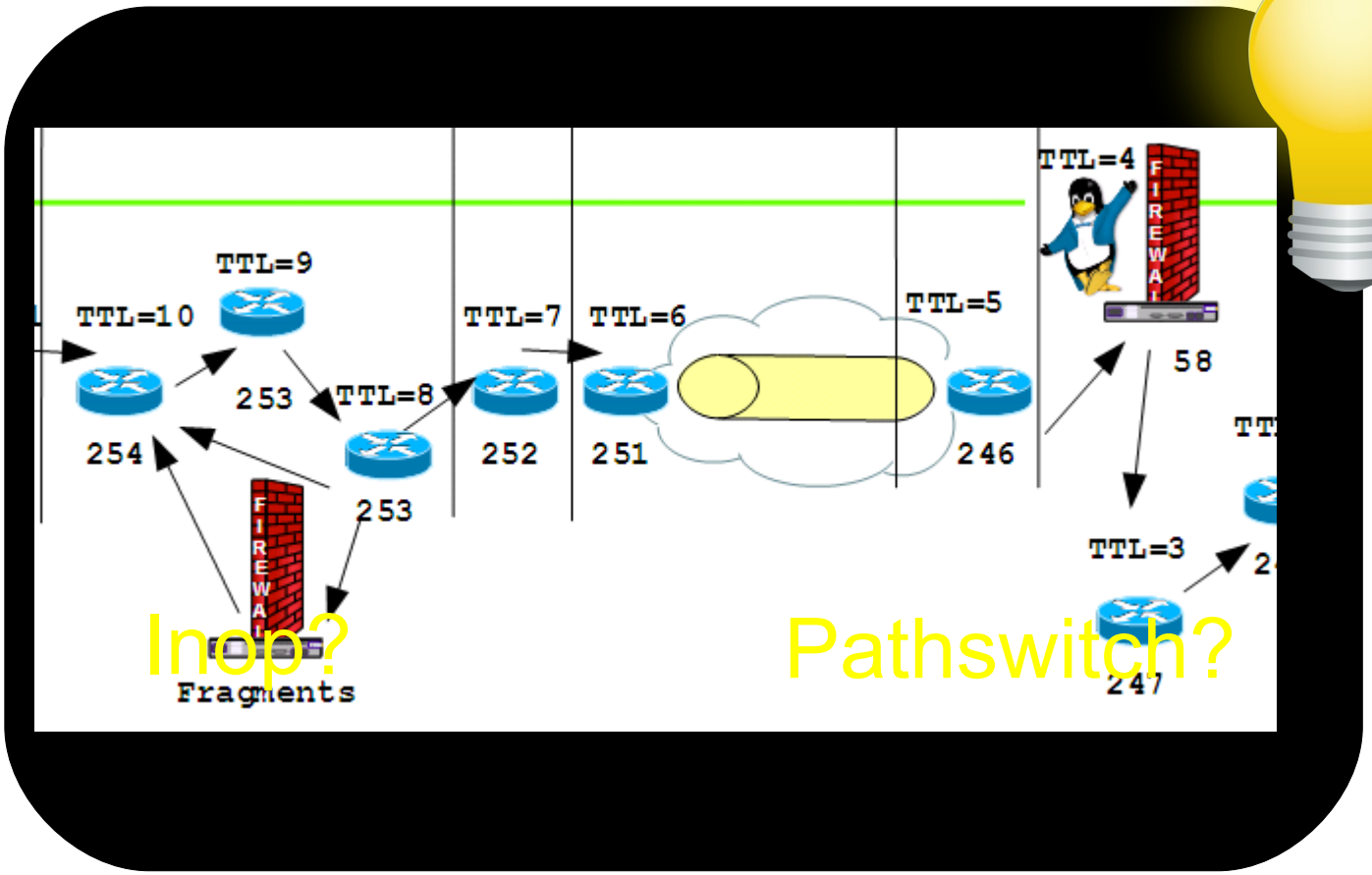
2nd fragment 1494 bytes

TTL and Topology VI. - Fragmentation

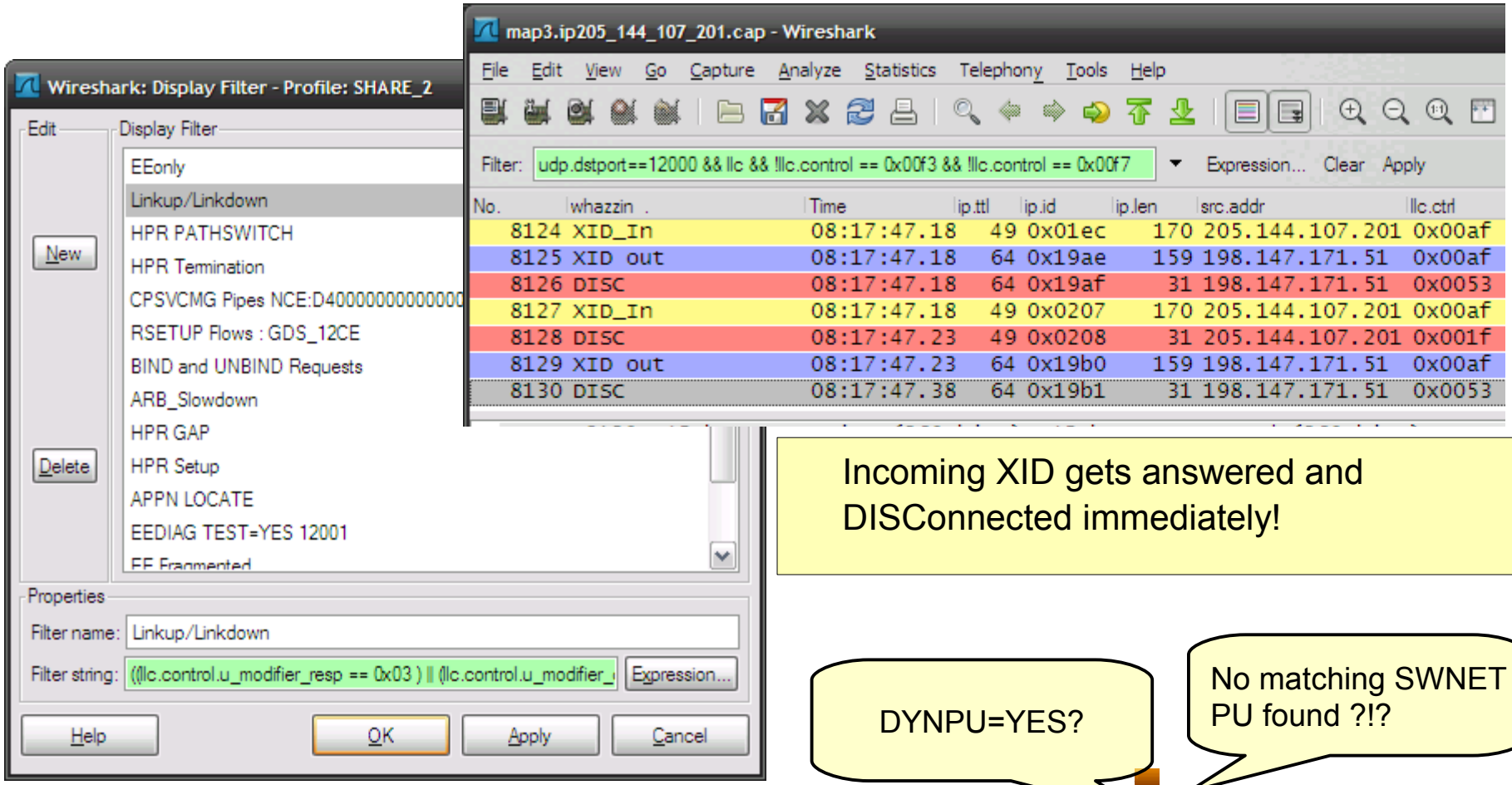
Fragmented IP packets get inspected adding an additional hop to the ip path.



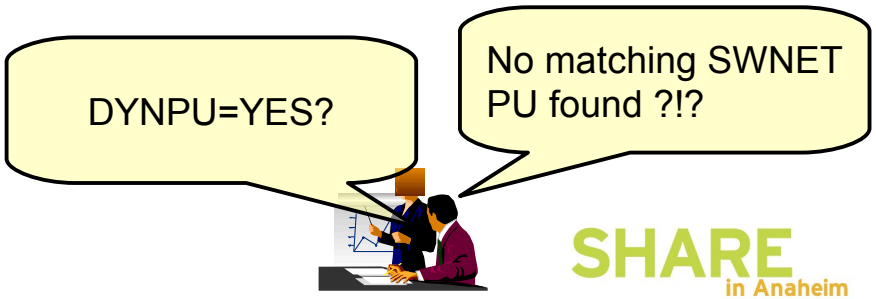
Now we have picture of the environment
Time to get started working on the 'problem'



Detecting INOPs with wireshark



Incoming XID gets answered and DISConnected immediately!



Active link – sSAP and dSAP

map3.ip205_144_107_201.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	whazzin .	Time	ip.ttl	ip.id	ip.len	src.addr	dst.addr	llc.ctrl
8121	HPR STATUS	08:17:39.41	64	0x1915	103	198.147.171.51	205.144.107.201	0x0003
8122		08:17:39.46	64	0x1916	99	198.147.171.51	205.144.107.201	0x0003
8123	HPR STATUS	08:17:39.46	49	0xfd80	104	205.144.107.201	198.147.171.51	0x0003
8124	XID_In	08:17:47.18	49	0x01ec	170	205.144.107.201	198.147.171.51	0x00af
8125	XID out	08:17:47.18	64	0x19ae	159	198.147.171.51	205.144.107.201	0x00af
8126	DISC	08:17:47.18	64	0x19af	31	198.147.171.51	205.144.107.201	0x0053
8127	XID_In	08:17:47.18	49	0x0207	170	205.144.107.201	198.147.171.51	0x00af
8128	DISC	08:17:47.23	49	0x0208	31	205.144.107.201	198.147.171.51	0x001f
8129	XID out	08:17:47.23	64	0x19b0	159	198.147.171.51	205.144.107.201	0x00af
8130	DISC	08:17:47.38	64	0x19b1	31	198.147.171.51	205.144.107.201	0x0053
8131	Idle link out	08:17:52.77	64	0x1a6f	31	198.147.171.51	205.144.107.201	0x0053

```
⊞ Frame 8123: 118 bytes on wire (944 bits), 94 bytes captured (752 bits)
⊞ Ethernet II, Src: Switchco_00:00:01 (00:50:9b:00:00:01), Dst: Gigabit_00:00:01 (00:0f:a1:00:
⊞ Internet Protocol, Src: 205.144.107.201 (205.144.107.201), Dst: 198.147.171.51 (198.147.171.51)
⊞ User Datagram Protocol, Src Port: 12001 (12001), Dst Port: 12001 (12001)
⊟ Logical-Link Control
    DSAP: SNA Path Control (0x04)
    IG Bit: Individual
    SSAP: SNA (0x08)
    CR Bit: Command
  ⊟ Control field: U, func=UI (0x03)
```

There is an active HPR pipe between the two ip addresses when the XIDcomes in

Local SAP is 4, remote SAP is 8.

Yes SAPADDR=8 in SWNET is default

So this link was activated by our VTAM

New link – sSAP and dSAP

map3.ip205_144_107_201.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	whazzin	Time	ip.ttl	ip.id	ip.len	src.addr	dst.addr	llc.ctrl
8121	HPR STATUS	08:17:39.41	64	0x1915	103	198.147.171.51	205.144.107.201	0x0003
8122		08:17:39.46	64	0x1916	99	198.147.171.51	205.144.107.201	0x0003
8123	HPR STATUS	08:17:39.46	49	0xfd80	104	205.144.107.201	198.147.171.51	0x0003
8124	XID_In	08:17:47.18	49	0x01ec	170	205.144.107.201	198.147.171.51	0x00af
8125	XID out	08:17:47.18	64	0x19ae	159	198.147.171.51	205.144.107.201	0x00af
8126	DISC	08:17:47.18	64	0x19af	31	198.147.171.51	205.144.107.201	0x0053
8127	XID_In	08:17:47.18	49	0x0207	170	205.144.107.201	198.147.171.51	0x00af
8128	DISC	08:17:47.23	49	0x0208	31	205.144.107.201	198.147.171.51	0x001f
8129	XID out	08:17:47.23	64	0x19b0	159	198.147.171.51	205.144.107.201	0x00af
8130	DISC	08:17:47.38	64	0x19b1	31	198.147.171.51	205.144.107.201	0x0053
8131	Idle link out	08:17:52.77	64	0x1a6f	31	198.147.171.51	205.144.107.201	0x00f3

```
⊞ Frame 8124: 184 bytes on wire (1472 bits), 94 bytes captured (752 bits)
⊞ Ethernet II, Src: Switchco_00:00:01 (00:50:9b:00:00:01), Dst: Gigabit_00:00:01 (00:0f:a1:00:
⊞ Internet Protocol, Src: 205.144.107.201 (205.144.107.201), Dst: 198.147.171.51 (198.147.171.
⊞ User Datagram Protocol, Src Port: 12000 (12000), Dst Port: 12000 (12000)
⊟ Logical-Link Control
    DSAP: SNA (0x08)
    IG Bit: Individual
    SSAP: SNA Path Control (0x04)
    CR Bit: Command
  ⊟ Control field: U, func=XID (0xAF)
```

The XIDcomes in with a

Local SAP of 8, remote SAP is 4.

No longer supported between same IP-pair

So this link is a parrallel TG between the two!

Now we have picture of the environment
Time to get started working on the 'problem'

So, what is your problem?

Pathswitch?

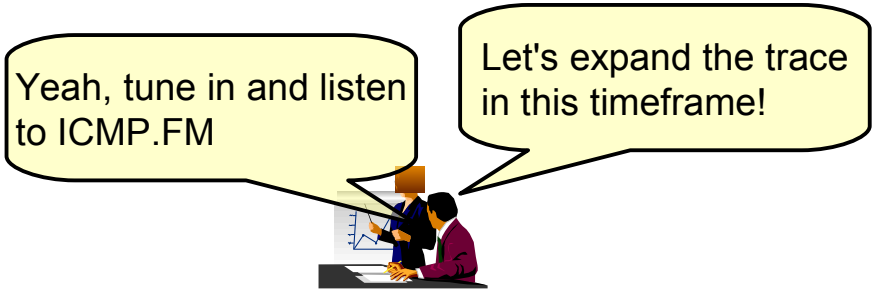
How to find switching pipes

Wireshark: Display Filter - Profile: SHARE_2011

Edit | Display Filter

New

- EEonly
- Linkup/Linkdown
- HPR PATHSWITCH
- HPR Termination
- CPSVCMG Pipes NCE:D400000000000000
- RSETUP Flows : GDS_12CE
- BIND and UNBIND Requests
- ARB_Slowdown
- HPR GAP



routingloop_1.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: sna.nlp.thdr.offset > 13 && sna.nlp.thdr.bsn > 0 or (expert.group == "Malformed

Expression... Clear Apply

No.	whazzin .	Time	ip.ttl	ip.id	ip.len	src.addr	TCID	BSN	sna.dlf
806	PATHSWITCH	12:21:01.726086	64	0x1ad2	175	198.147.171.51	18163f95000	0x00733452	0x00000000
811	PATHSWITCH	12:21:02.752501	64	0x1b14	175	198.147.171.51	18163f95000	0x00733452	0x00000000
813	PATHSWITCH	12:21:02.845070	49	0xd950	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
816	PATHSWITCH	12:21:03.780714	64	0x1b38	175	198.147.171.51	18163f95000	0x00733452	0x00000000
820	PATHSWITCH	12:21:04.002299	49	0xd971	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
823	PATHSWITCH	12:21:04.816496	64	0x1b88	175	198.147.171.51	18163f95000	0x00733452	0x00000000
827	PATHSWITCH	12:21:04.984725	49	0xd988	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
830	PATHSWITCH	12:21:05.846220	64	0x1bc2	175	198.147.171.51	18163f95000	0x00733452	0x00000000

PATHSWITCH due to routing loop

Yes, if they don't make it to the remote RTP a PATHSWITCH is the logical consequence

Our outbound NLPs die in a routing loop!

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	whazzin	Time	ip.ttl	ip.id	ip.len	src.addr	TCID		sna.dlf
806	PATHSWITCH	12:21:01.726086	64	0x1ad2	175	198.147.171.51	18163f950	33452	0x00000000
807	CPSVCMG	12:21:01.759857	49	0xd937	83	205.144.107.201	3db3edf20	64dd	0x00000000
808	CPSVCMG	12:21:01.759857	64	0x1ae0	83	198.147.171.51	18163f94	1e4	0x00000000
809	Routing Loop	12:21:01.777066	1	0x1ad2	175	205.144.107.201			
810	Routing Loop	12:21:01.811979	1	0x1ae0	83	205.144.107.201			
811	PATHSWITCH	12:21:02.752501	64	0x1b14	175	198.147.171.51	18163f95000	0x00733452	0x00000000
812	Routing Loop	12:21:02.752501	1	0x1b14	175	205.144.107.201			
813	PATHSWITCH	12:21:02.845070	49	0xd950	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
814	CPSVCMG	12:21:02.846496	64	0x1b1c	83	198.147.171.51	18163f94000	0x000111e4	0x00000000
815	Routing Loop	12:21:02.887722	1	0x1b1c	83	205.144.107.201			
816	PATHSWITCH	12:21:03.780714	64	0x1b38	175	198.147.171.51	18163f95000	0x00733452	0x00000000
817	Routing Loop	12:21:03.838649	1	0x1b38	175	205.144.107.201			
818	CPSVCMG	12:21:03.838649	64	0x1b43	83	198.147.171.51	18163f94000	0x000111e4	0x00000000
819	Routing Loop	12:21:03.838649	1	0x1b43	83	205.144.107.201			
820	PATHSWITCH	12:21:04.002299	49	0xd971	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
821	CPSVCMG	12:21:04.002299	64	0x1b4b	83	198.147.171.51	18163f94000	0x000111e4	0x00000000
822	Routing Loop	12:21:04.054003	1	0x1b4b	83	205.144.107.201			
823	PATHSWITCH	12:21:04.816496	64	0x1b88	175	198.147.171.51	18163f95000	0x00733452	0x00000000
824	Routing Loop	12:21:04.857312	1	0x1b88	175	205.144.107.201			
825	CPSVCMG	12:21:04.914814	64	0x1b8d	83	198.147.171.51	18163f94000	0x000111e4	0x00000000
826	Routing Loop	12:21:04.914814	1	0x1b8d	83	205.144.107.201			
827	PATHSWITCH	12:21:04.984725	49	0xd988	175	205.144.107.201	3db3edf2000	0x007964dd	0x00000000
828		12:21:04.984725	64	0x1b8e	83	198.147.171.51	18163f94000	0x000111e4	0x00000000
829		12:21:05.083692	1	0x1b8e	83	205.144.107.201			

Routing Loop: TTL exceeded

Filter: ip.ttl<10 and !udp.length==56

No.	whazzin	Time	ip.ttl	ip.id	ip.len
788	Routing Loop	12:20:58.315699	1	0x1a09	95
790	Routing Loop	12:20:58.349276	1	0x1a0d	464
792	Routing Loop	12:20:59.230057	1	0x1a46	83
795	Routing Loop	12:20:59.394710	1	0x1a69	83
798	Routing Loop	12:20:59.526947	1	0x1a6b	31

```
Internet Protocol, Src: 205.144.107.201 (205.144.107.201
    Version: 4
    Header length: 20 bytes
  ⊞ Type of service: 0x00 (None)
    Total Length: 56
    Identification: 0x6c5e (27742)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 245
    Protocol: ICMP (1)
  ⊞ Header checksum: 0xae45 [validation disabled]
    Source: 205.144.107.201 (205.144.107.201)
    Destination: 198.147.171.51 (198.147.171.51)
Internet Control Message Protocol
    Type: 11 (Time-to-live exceeded)
    Code: 0 (Time to live exceeded in transit)
    Checksum: 0x61bd [correct]
  Internet Protocol, Src: 198.147.171.51 (198.147.171.51), Dst: 205.

0020  ab 33 0b 00 61 bd 00 00  00 00 45 00 00 5f 1a 09   .3..a... ..E.
0030  00 00 01 11 f4 64 c6 93  ab 33 cd 90 6b c9 2e e1   .....d.. .3..
0040  2e e1 00 4b 35 35                                  ...K55
```

Wireshark: Display Filter - Profile: SHARE_2011

The ICMP message comes in with a TTL of 245

Who's that?
Let's check our picture!

New
Delete

RSETUP Flows : GDS_12CE
BIND and UNBIND Requests
ARB_Slowdown
HPR GAP
HPR Setup
APPN LOCATE
EEDIAG TEST=YES 12001
EE Fragmented
EE Routing Loop
PING

Properties
Filter name: EE Routing Loop
Filter string: ip.ttl<10 and !udp.length==56
Expression...

Help | OK | Apply | Cancel

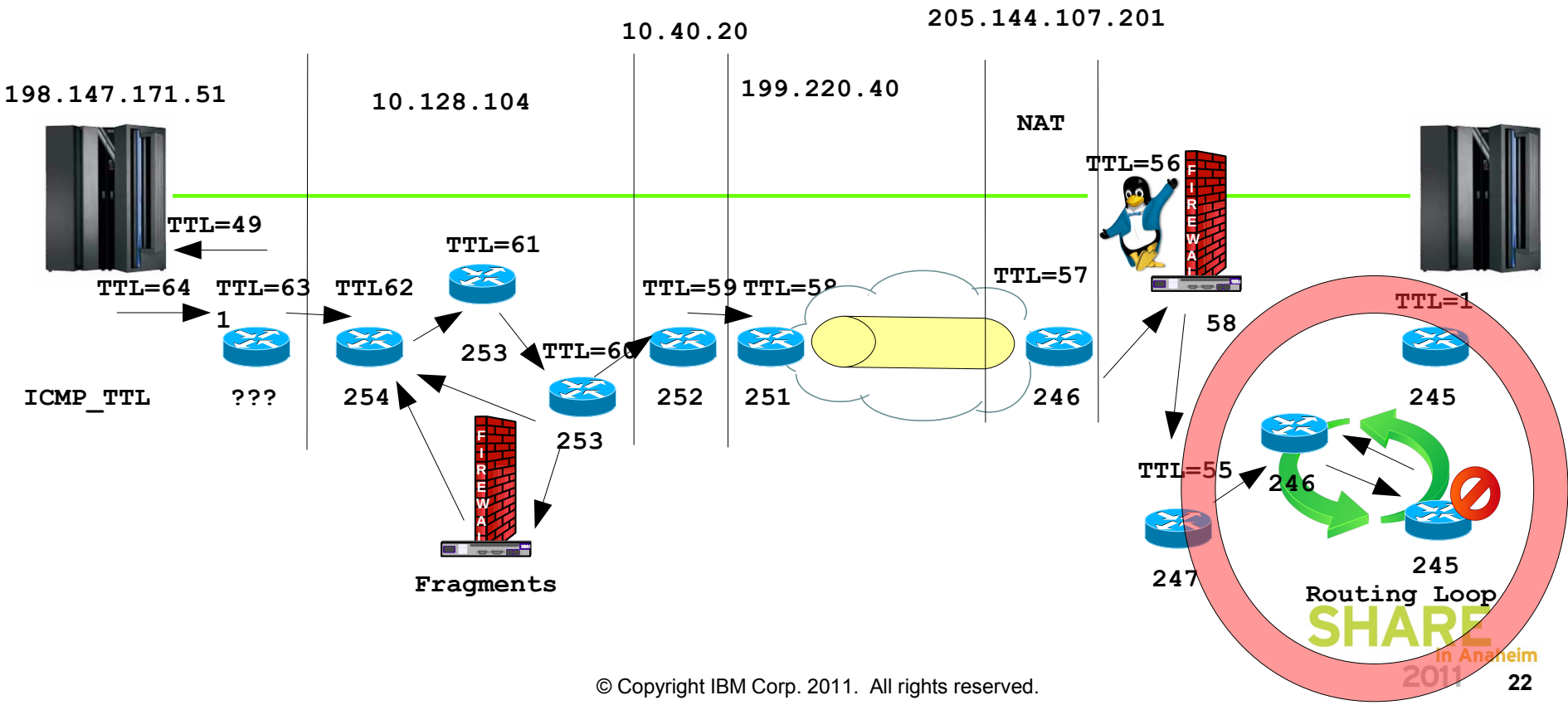
Now we have picture of the environment
Time to get started working on the 'problem'

So, what is your problem?

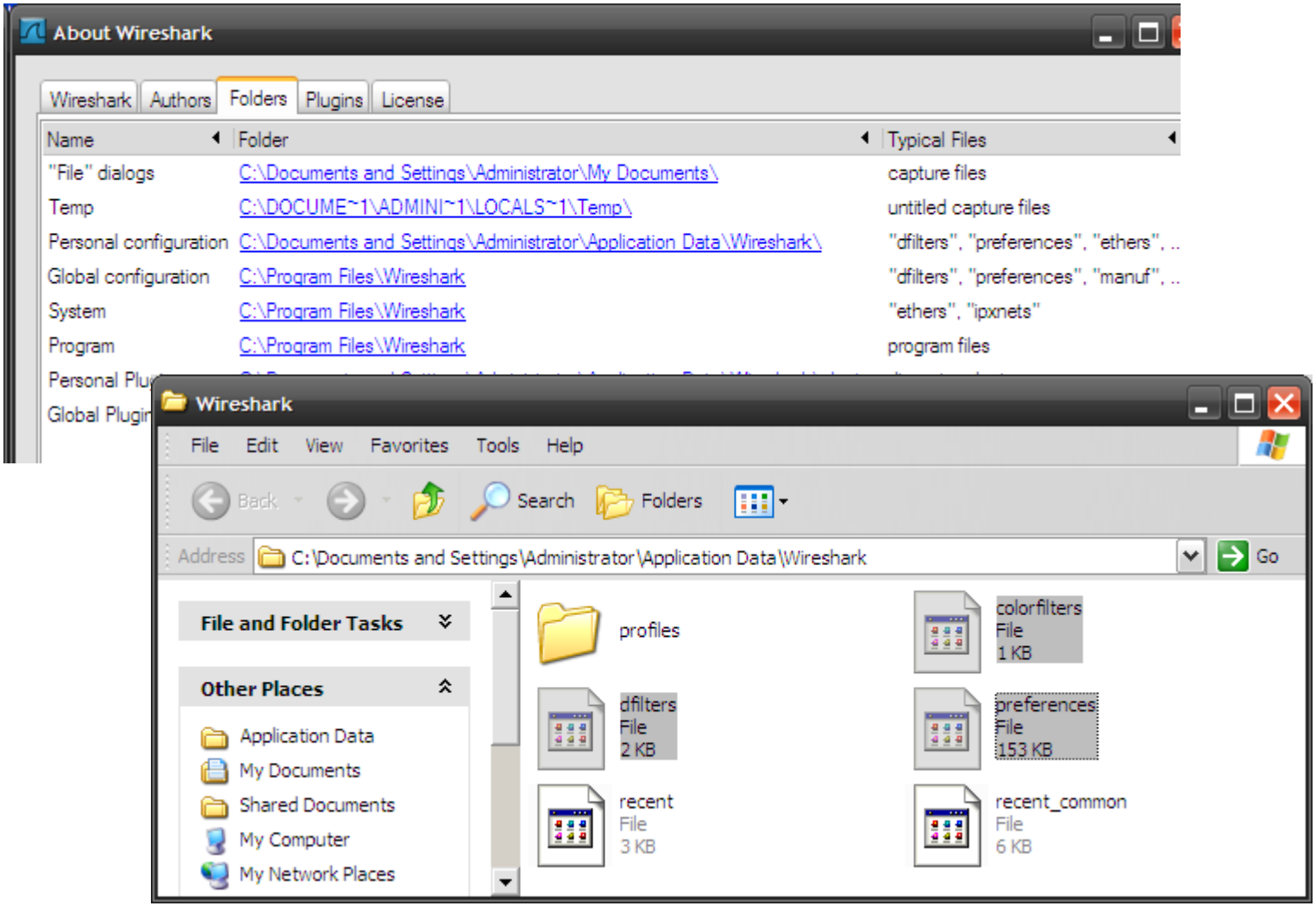
Pathswitch?

TTL and Topology VII. - Here's the problem

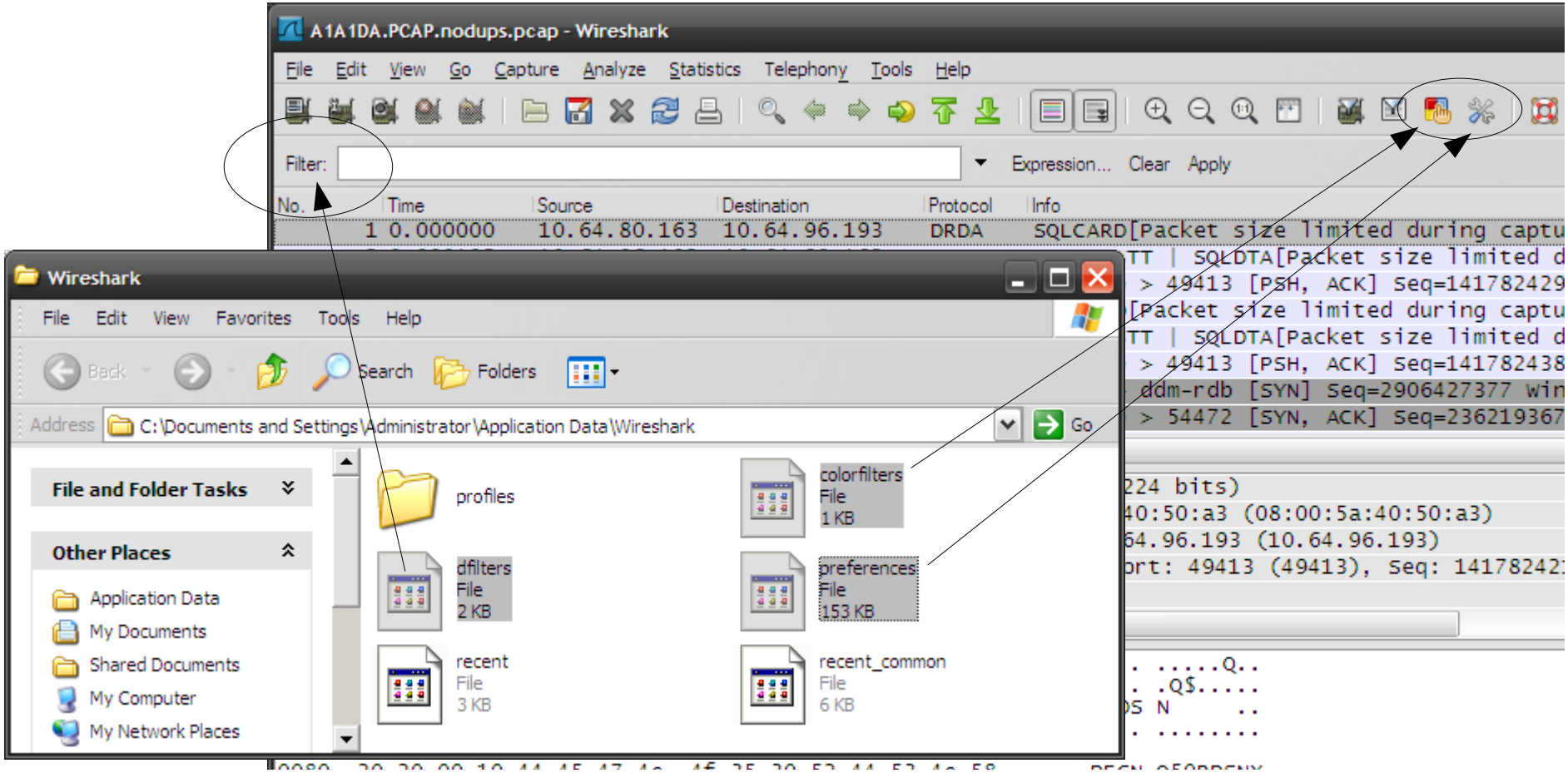
Fragmented IP packets get inspected adding an additional hop to the ip path.



Wireshark
Personal Configuration Files - Profiles



Wireshark
Personal Configuration Files - Profiles



Questions

- IP Wizards on Facebook

- Wireshark Bootcamp 2011
  - Germany: http://tinyurl.com/ZOWIE0DE
  - Canada : http://tinyurl.com/ZOWIE0CE

Appendix

- IP Fragmentation

Fragmentation: Why ? – Part I.
An unfragmented packet arrives

fragmentation.cap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	whazzin .	Time	ip.ttl	ip.id	ip.len	src.addr	dst.addr	dst.port
137		0.000000	49	0x65a6	1486	205.144.1	07.201	19
138		0.000000	64	0x6b3f	83	198.147.1	71.51	205.144.107.201 12003
139		0.351288	64	0x6bc1	93	198.147.1	71.51	205

```
⊟ Internet Protocol, Src: 205.144.107.201 (205.144.107.201), Dst: 198.147.171.51 (198.147.1
    Version: 4
    Header length: 20 bytes
  ⊞ Type of service: 0x00 (None)
    Total Length: 1486
    Identification: 0x65a6 (26022)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 49
    Protocol: UDP (17)
  ⊞ Header checksum: 0x7358 [validation disabled]
    Source: 205.144.107.201 (205.144.107.201)
    Destination: 198.147.171.51 (198.147.171.51)
⊟ User Datagram Protocol, Src Port: 12003 (12003), Dst Port: 12003 (12003)
    Source port: 12003 (12003)
    Destination port: 12003 (12003)
    Length: 1466
  ⊞ Checksum: 0x605b [unchecked, not all data available]
⊞ Logical-Link Control
```

```
⊟ RTP Transport Header
    Transport Connection Identifier: 3db427f20001097c
  ⊞ RTP Transport Packet Header Byte 8: 0x3c
  ⊞ RTP Transport Packet Header Byte 9: 0x00
    Data Offset/4: 0x0005
    Data Length Field: 0x0000058f
    Byte Sequence Number: 0x0010a6ca
  ⊞ Transmission Header
  ⊞ Request/Response Header
⊞ Data (2 bytes)
```

IPID 65AB arrived unfragmented

ip.len==1486

udp.length == 1466

sna.nlp.thdr.dlf == 0x0000058f

The NLP payload was 0x058f = 1423 bytes

ip.len is 20 bytes more than udp.length

Fragmentation: Why ? – Part II.
What was the original size of the packet?

No.	whazzin .	Time	ip.ttl	ip.id	ip.len	src.addr	dst.addr	dst.port
140		0.000000	48	0x65ad	44	205.144.107.201	198.147.171.51	12003

```
⊞ Type of service: 0x00 (None)
  Total Length: 44
  Identification: 0x65ad (26029)
⊞ Flags: 0x01 (More Fragments)
  Fragment offset: 0
  Time to live: 48
  Protocol: UDP (17)
⊞ Header checksum: 0x59f3 [validation disabled]
  Source: 205.144.107.201 (205.144.107.201)
  Destination: 198.147.171.51 (198.147.171.51)
⊟ User Datagram Protocol, Src Port: 12003 (12003), Dst Port: 12003 (12003)
  Source port: 12003 (12003)
  Destination port: 12003 (12003)
  Length: 1498
⊞ Checksum: 0x128d [unchecked, not all data available]
⊞ Logical-Link Control
⊟ Systems Network Architecture
  ⊟ Network Layer Packet Header
    ⊞ Network Layer Packet Header Byte 0: 0xc2
    ⊞ Network Layer Packet Header Byte 1: 0x08
      Automatic Network Routing Entry: d0000000000000ff
      Reserved
```

```
0000  00 0f a1 00 00 04 00 50  9b 00 00 04 08 00 45 00   ..~....& ........
0010  00 2c 65 ad 20 00 30 11  59 f3 cd 90 6b c9 c6 93   .,.[ ... .3..,IF]
0020  ab 33 2e e3 2e e3 05 da  12 8d 04 08 03 c2 08 d0   .3.T.T.. .....B.}
0030  00 00 00 00 00 00 00 ff  00 3d                     ........ .=
```

Automatic Network Routing Entry (sna.nlp.nhdr.anr), 9 bytes | Packets: 200 Displayed: 2 Marked: 0 Load tim... | Profile: SHARE_2

IP Header 1st fragment

- ip.len==44
- ip.id == 0x65ad
- ip.flags.mf == 1

UDP Header

- udp.length == 1498

ANR Header

- sna.nlp.nhdr.anr == d0:00:00:00:00:00:00:00:ff

RTP THDR:

- sna.nlp.thdr.tcid == 3d:??:??:??:??:??:??:??

ip,len at the sender must have been 1498+20 bytes!

Fragmentation: Why ? – Part III. What was the original DLF of the NLP?

```
⊞ Internet Protocol, Src: 205.144.107.201 (205.144.107.201), Dst: 198.147.
⊟ User Datagram Protocol, Src Port: 12003 (12003), Dst Port: 12003 (12003)
    Source port: 12003 (12003)
    Destination port: 12003 (12003)
    Length: 1498
  ⊞ Checksum: 0x128d [unchecked, not all data availabl]
⊞ Logical-Link Control
⊟ Systems Network Architecture
  ⊞ Network Layer Packet Header
⊞ [Unreassembled Packet: SNA]

0000  00 0f a1 00 00 04 00 50  9b 00 00 04 08 00 45 00
0010  00 2c 65 ad 20 00 30 11  59 f3 cd 90 6b c9 c6 93
0020  ab 33 2e e3 2e e3 05 da  12 8d 04 08 03 c2 08 d0
0030  00 00 00 00 00 00 00 ff  00 3d
```

```
  ⊞ Type of service: 0x00 (None)
    Total Length: 1494
    Identification: 0x65ad (26029)
  ⊞ Flags: 0x00
    Fragment offset: 24
    Time to live: 48
    Protocol: UDP (17)
  ⊞ Header checksum: 0x7446 [validation disabled]
    Source: 205.144.107.201 (205.144.107.201)
    Destination: 198.147.171.51 (198.147.171.51)
⊞ Data (60 bytes)

0000  00 0f a1 00 00 04 00 50  9b 00 00 04 08 00 45 00
0010  05 d6 65 ad 00 03 30 11  74 46 cd 90 6b c9 c6 93
0020  ab 33 b4 27 f2 00 01 09  7c 3c 04 00 0d 00 00 05
0030  8f 00 10 ac 5a 03 22 c5  58 00 06 db 80 00 00 00
0040  00 05 0e 00 00 00 01 00  02 00 00 01 a7 00 00 00
0050  00 00 00 00 00 5c 00 03  02 00 00 00 00 34
```

IP Header: 2nd fragment

- ip.len==1494
- ip.id == 0x65ad

RTP THDR:

- sna.nlp.thdr.tcid == 3d:b4:27:f2:00:01:09:7c
- sna.nlp.thdr.offset == 0x000d
- sna.nlp.thdr.dlf == 0x0000058f
- sna.nlp.thdr.bsn == 0x0010ac5a

Optional Segments

- sna.nlp.thdr.optional.type == 0x22
- sna.nlp.thdr.optional.type == 0x0e

FID5 TH

NLP payload was 0x058f
Same as before!