Internet Engineering Task Force

RFC for IPv6 IPID Sequence number field

IETF 86 Wednesday March 13, 2013

Nalini Elkins (Inside Products) and

Michael Ackermann (BCBS Michigan)

TODAY'S AGENDA

- IPID FIELD IN IPv4 – BACKGROUND
- IPID FIELD IN IPv6 – CURRENT STATE
- ENTERPRISE DATA CENTER OPERATORS (EDCO) PERSPECTIVE
- USE CASES / EXAMPLES
- CONCLUSIONS – RECOMMENDATIONS – NEXT STEPS

FOCUS ISSUES IN RED TEXT

IPID FIELD IN IPv4 - BACKGROUND

- **IPID: Internet Protocol Identification. Provides a unique identifying number for a given IP Packet within a flow.**
- Sometimes called Datagram number.
- **USAGE/VALUE**
- Enable Fragmentation.
- Packet sequencing at end points (Edge Networks).
- **Diagnostics! Logically associate packets across complex network situations.**
- IPID is frequently used in IPv4 troubleshooting for the purposes of “watermarking” the packets to correlate them in different troubleshooting scenarios. The implementations are such that the IPID is infrequently changed by middle boxes even if the content is.

IPID FIELD IN IPv6 – CURRENT STATE

- **IMPLEMENTED IN FRAGMENT HEADER EXTENSION (TYPE 44).**
- **LOCATION:**
  - 32 bit field at offset 4 in FHE.
- **ISSUES:**
  - Only used if fragmentation required!

- **IPID not always available to facilitate network diagnostics!**

Why We Need It

- Provides recognition of sequencing and duplication of packets
  - TCP SEQ / ACK (retransmissions, duplication: true and false)
  - UDP – no sequence number
  - ICMP – need to see sequence number in embedded packet
  - Across multiple trace points
  - **It's not going to get any easier.**

EDCO PERSPECTIVE

1. EDCO includes: corporations, universities, and government agencies.
2. De facto use of the IPID has enhanced problem diagnosis. It has significantly reduced problem resolution time.
3. Several use case examples are shown on subsequent slides.
4. **If a problem/performance issue can be fixed in minutes, as opposed to hours, this can mean significant savings to large enterprises.**
5. The IPID is critical when debugging involves traces or packet captures.
6. Its absence in IPv6 could lead to protracted problem diagnosis, and extended problem resolution time.
7. **One related concern is that this could slow the deployment and acceptance of IPv6.**
8. Vendors and network service providers may not share this perspective, as packets could continue to flow. But ***availability / performance*** may not be acceptable during the extended problem resolution time.

EDCO BUSINESS VALUE

Of Network Performance /Availability

NETWORK/APP EXAMPLE - OCT 2008

- 19,900 online users during peak hours
- $5.6 billion total medical claim value
- Thousands of file transfers per day
- Value per hour $21 million

So as my boss tells me, if you take 2 hours instead of 1, to diagnose the issue, you cost the company $21 million.

EDCO BUSINESS VALUE - 2

Of Network Performance / Availability

- These are **real numbers** used in presentations to executives.
- They illustrate the **dollar value** of network availability and the need to keep problem resolution time to an absolute minimum.
- As network **size and complexity** increases, the IPID becomes more critical.
- Previous figures do not include the cost of extended problem resolution, such as storage, CPU, staff, travel, etc.
- IPID should be reinstated.

From Gerald Combs: Original Developer of WireShark

- I think this is a great idea! An explicit (and separate) diagnostic field for IPv6 would definitely be helpful for WireShark, Pilot (particularly for its MSA feature), and many other tools.

  Two quick notes:

  You might want to add a SHOULD NOT or MUST NOT, explicitly stating that gateways must not modify or remove the IPID from packets that they forward.

  Many OSs support random IP IDs (e.g. my laptop has a "net.inet.ip.random_id" sysctl, which is currently enabled), primarily to improve security. Is that needed here?

Use Case Examples

SOME PREVIOUS SITUATIONS WHERE IPID REDUCED PROBLEM RESOLUTION TIME SIGNFICANTLY.

For several different large organizations.

USE CASE #1 --- Large Computer Corp

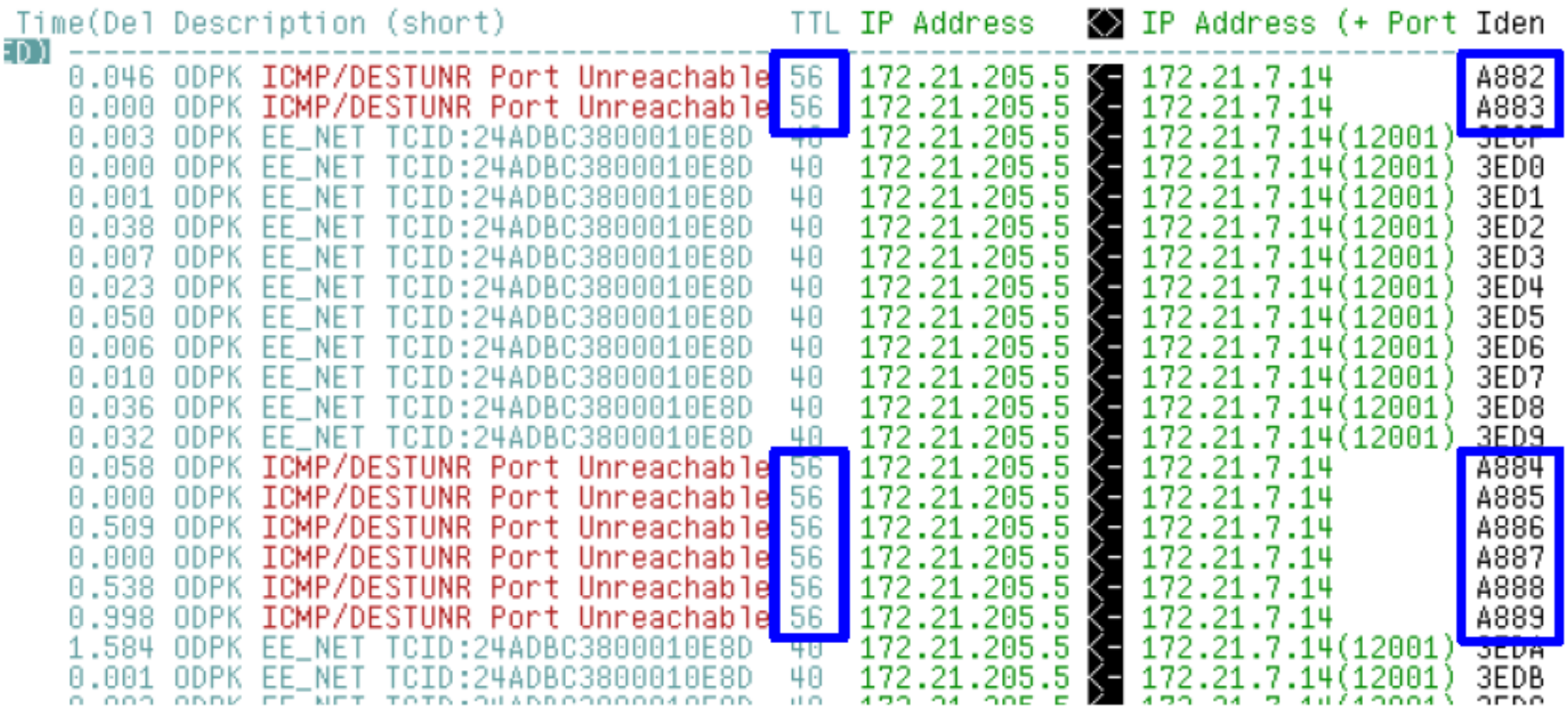
CRUCIAL FIELD

- An example of how this IPID is used is be found in the public SHARE presentation:

https://share.confex.com/share/120/webprogram/Session12856.html

- By: Matthias Burkhard (IBM Corporation) and Mike Riches (IBM Corporation)

VTAM Internal Trace – inbound packets



```
 Time(Del Description (short)                    TTL IP Address    IP Address (+ Port Iden
ED)
    0.046 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A882
    0.000 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A883
    0.003 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ECF
    0.000 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED0
    0.001 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED1
    0.038 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED2
    0.007 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED3
    0.023 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED4
    0.050 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED5
    0.006 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED6
    0.010 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED7
    0.036 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED8
    0.032 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3ED9
    0.058 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A884
    0.000 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A885
    0.509 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A886
    0.000 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A887
    0.538 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A888
    0.998 ODPK ICMP/DESTUNR Port Unreachable     56 172.21.205.5   172.21.7.14          A889
    1.584 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3EDA
    0.001 ODPK EE_NET TCID:24ADBC3800010E8D      40 172.21.205.5   172.21.7.14(12001)   3EDB
```

- All packets come from the same IP address
  - All EE packets come in with a TTL of 40
    - `ip.id increments: 3ECF … 3EDB`
  - All ICMP packets arrive with a TTL of 56

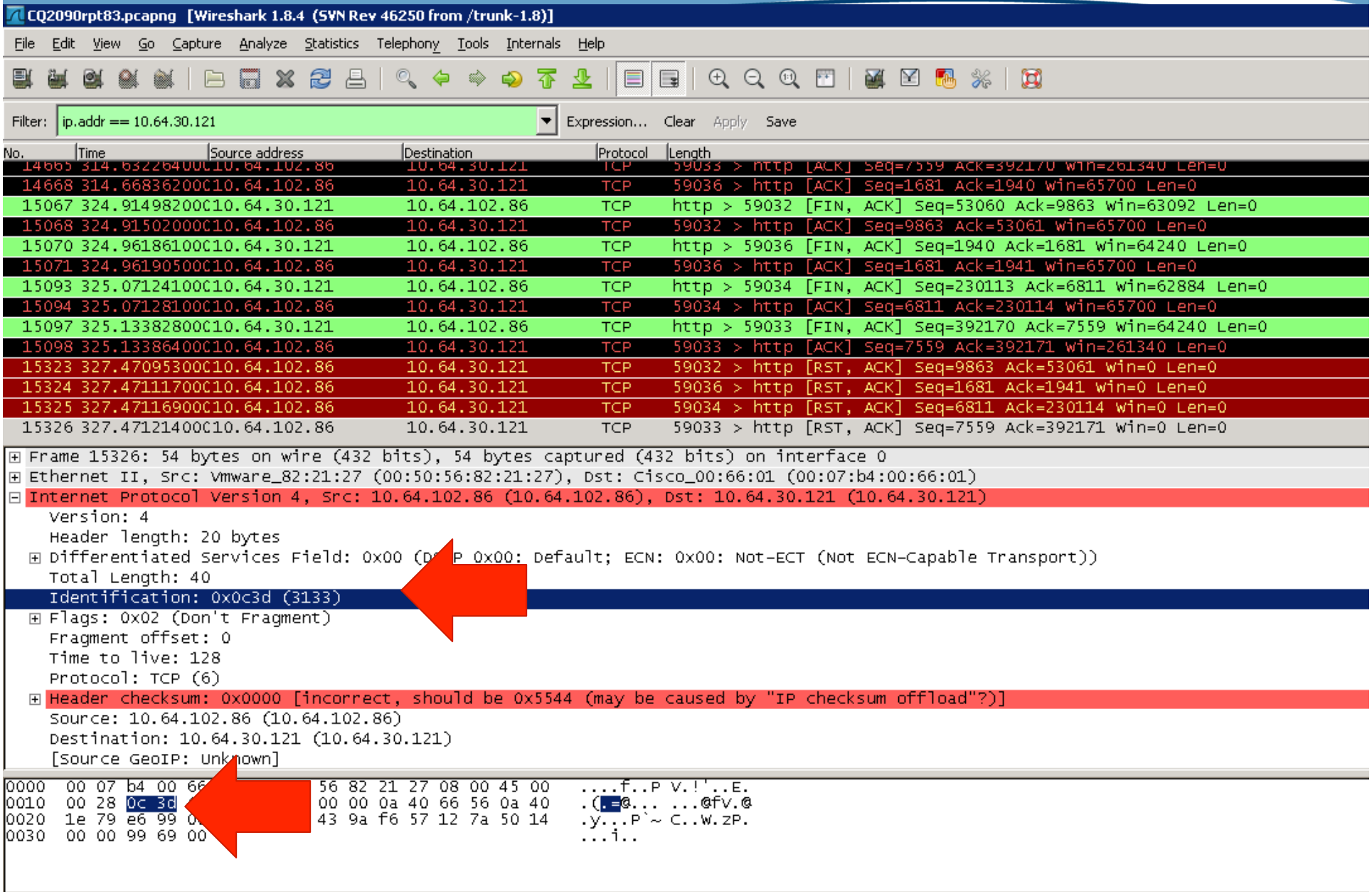
USE CASE #2 --- Large Insurance

Estimated time saved by use of IPID – 7 hours

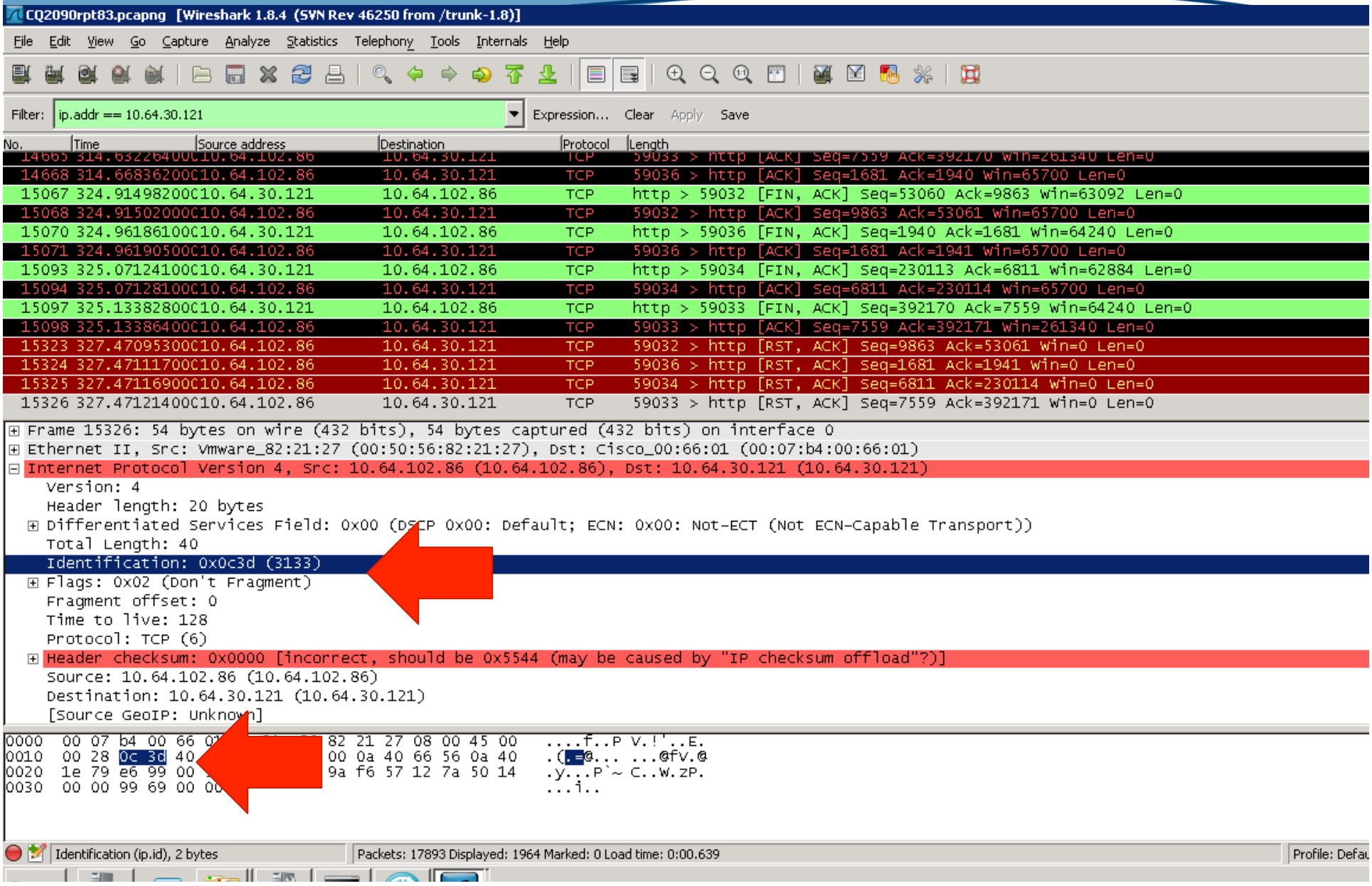
PERFORMANCE TOOL PRODUCES EXTRANEOUS PACKETS?

- Issue was if performance tool was accurately replicating session flow during performance testing?
- Compared a packet trace of the tool generated session, to a packet trace of the same session generated by a person using a browser.
- Trace IPIDs showed more HTTP packet sequences within same flow from performance tool, as compared to the browser.
- Having the clear sequence numbers also showed where and why.
- Solution: Problem rectified in subsequent version of performance tool.
- IPID allowed us to be clear and convincing with the vendor, so they would believe they have an issue.

USE CASE #2 - WireShark 1 - IE



USE CASE #2 - WireShark 2 - Tool



USE CASE #3 --- Large Bank

Estimated time saved by use of IPID – 6 hours

VERY SLOW INTERACTIVE PERFORMANCE.

- All network links looked good.
- Traces showed duplicated small packets (which can be OK).
- Saw that IPID was equal but TTL was always + 1.
- Network device was “splitting” small packets only (2 interfaces).
- The small packets were control info, telling other side to slow down.
- Erroneously looked like network congestion.
- Solution: Network device replaced and good interactive performance restored.
- Without IPID, flows would have appeared OK.

USE CASE #4 --- Law Enforcement Agency

Estimated time saved by use of IPID – 11 hours

BAD PACKETS INJECTED

- Session across VPN getting reset. End points upset.
- Devices/orgs in middle claimed no problem.
- All parties (both sides of VPN connection, application, devices/orgs in the middle, etc.) say they see no issues.
- **Problem goes on for weeks.**
- Finally, we took a trace which showed packets with IPID and TTL that did not match others in the flow AT ALL.
- Solution: Router in network required a software upgrade.
- Until trace with IPID illuminated issue, no one would “own” the problem, much less address and resolve it.

USE CASE #5 --- Diagnostic Tool

Estimated time saved by use of IPID – 8 hours

IP TRACE FACILITY PRODUCES DUPLICATE PACKETS

- Degraded performance experienced at end points.
- Did not own network. Had to diagnose at end.
- Everyone in middle said “we see no problems”.
- Duplicate packets were observed, but this can be OK.
- Where these “true” duplicates or “false extraneous” dups?
- How could you tell? Without IPID, it was impossible.
- These were “false” duplicate packets, intermittently produced by platform trace facility on an IDS like device.
- Solution: Trace facility was turned off.
- Without IPID, would one may assume “true” dups and focus on finding slow network paths. And never find the problem.

Show TCP Packets - Diagnostics
Sort Order : Packet Number
Showing Entries : 1 -20

-	-	Packet Number	Packet Date	Source Interface	Destination Interface	Source Address	Source Port	Destination Address	Destination Port	IP ID	Data Length	Sequence	ACK	Expected ACK	Delta (ss.milli.micro)	E
1		1	2140-02-20 14:18:47.000000	00.A0.8E.A6.65.62	00.00.0C.07.AC.01		1453		4625	3396	0	2142443321	4080085184	0	0.000.000	
2		2	2140-02-23 21:01:07.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52A	0	4080085184	2142443322	0	283340.000.000	
3		3	2140-02-23 21:01:42.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52A	0	4080085184	2142443322	0	35.000.000	DL
4		4	2232-06-16 09:38:47.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52E	272	4080085724	2142443322	4080085996	2913107825.000.000	
5		5	2232-06-16 09:41:12.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52E	272	4080085724	2142443322	4080085996	145.000.000	DL
6		6	2232-06-16 11:32:06.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52C	540	4080085184	2142443322	4080085724	6654.000.000	
7		7	2232-06-16 11:36:18.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	52C	540	4080085184	2142443322	4080085724	252.000.000	DL
8		8	2232-06-16 14:22:06.000000	00.A0.8E.A6.65.62	00.00.0C.07.AC.01		1453		4625	7008	0	2142443322	4080085184	0	9948.000.000	
9		9	2232-06-16 16:08:24.000000	00.A0.8E.A6.65.62	00.00.0C.07.AC.01		1453		4625	7009	0	2142443322	4080085996	0	6378.000.000	DL
10		10	2232-06-21 18:58:04.000000	00.A0.8E.A6.65.62	00.00.0C.07.AC.01		1453		4625	700F	540	2142443322	4080085996	2142443862	442180.000.000	
11		11	2232-06-25 11:22:03.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	530	0	4080085996	2142443862	0	318239.000.000	
12		12	2232-06-25 11:22:40.000000	00.13.5F.C6.B4.00	00.00.5E.00.01.18		4625		1453	530	0	4080085996	2142443862	0	37.000.000	DL

USE CASE #6 --- Large Bank

Estimated time saved by use of IPID – 4 hours

UDP TRANSFER DURATION INCREASES 12X

- 30 minute transfer started taking 6-8 hours.
- Proprietary protocol: vendor not forthcoming.
- Two data centers. Did not have access to all routers.
- Possible packet loss? All vendors said no.
- Other apps were working OK. Including FTP (TCP).
- 4 trace points used and IPIDs compared.
- Sessions using UDP; made IPID even more essential.
- Using IPID found 7% packet loss at application level.
- App over-reacts. App bug.
- Solution: WAN hardware was replaced and problem fixed.
- Without IPID, no one would admit they had a problem.

CONCLUSION REGARDING IPID FIELD IN IPv6

- **IPID is very valuable to large enterprises (EDCO) in trace analysis, specifically in reducing problem diagnosis and resolution time.**
- **Shorter diagnostic time means real money.**
- **IPID should be part of IPv6 for all situations where it can provide value. (As it is IPv4.) Not just where fragmentation is required.**

RECOMMENDATION FOR IPID FIELD IN IPv6

- Specific implementation/solution should be considered by IETF.
- One approach is the interactive “list” developed by Andrew Yourtchenko (Cisco)
- Several possible solutions have been discussed already. Some on subsequent slides in Appendix A, with relevant pros/cons/questions.
- Need to consider if it is viable, and/or desirable, to have a solution that can be turned on whenever required, but does not necessarily need to be there all the time?
- Those crafting solutions should be aware of how important timely problem diagnosis and resolution are to end users and large enterprise support teams!
- **REMEMBER SECURITY!**
  - **Security Implications of Predictable Fragment Identification Values (draft-gont-6man-predictable-fragment-id-03)**

Statement of Support

- We feel that a group (v6edco) should be formed at the IETF to look at performance, diagnostics and security end-to-end expressly as it affects enterprises (corporations, government agencies, and universities).
- We, of course, will be a part of this. Can co-chair.
- One of the first items on this groups charter should be to address, design and recommend a viable/optimal solution to the IPID in IPv6 issue.
- In general, more active involvement from EDCO networks in IETF should beneficial to all!

Organizations supporting formation of v6edco: Blue Cross Blue Shield of Michigan, US Bank, Depository Trust and Clearing Corporation, Inside Products.

QUESTIONS AND COMMENTS

- ???

Appendix A: POSSIBLE SOLUTIONS

- **IMPLEMENT IN DESTINATION OPTIONS HEADER EXTENSION (TYPE 60):**
- **LOCATION:**
  - 32 or 64 bit field at offset 8 in DOH. (Options Field).
- **DETAILS:**
  - Header sent by implementations upon request.
  - If sent in Diagnostic Mode, header MUST be ignored by receiver (intended for packet trace systems only).
  - New DOH Option 143 is proposed.
  - Future: Additional Options could be added for other diagnostic or security purposes as deemed appropriate.

OTHER POSSIBLE SOLUTIONS - 1

- **USE A HASHING ALOGRITHM:**
  - Create a hash of the packets in IPv6, using the invariant fields + payload.
  - This will not work because all it shows is if the packet is a duplicate. It is impossible to tell if the packet is an actual duplicate or a 'false' duplicate. For example, created by where the packet is traced. Traces at some points in the capture process create false duplicates easily seen today because of IPID.
- **USE TCP SEQUENCE NUMBER:**
  - TCP has a SEQ / ACK number. Use that sequence packets.
  - This will not work for same reason as above.
- **USE IP FLOW LABEL:**
  - Is not unique.
  - Not always used.

OTHER POSSIBLE SOLUTIONS - 2

- **IPV6 ATOMIC FRAGMENTS:**
  - Processing of IPv6 "atomic" fragments
  - draft-ietf-6man-ipv6-atomic-fragments-03
  - In response to ICMPv6 Packet Too Big error message.

- Related questions.
  - How to turn on/off?
  - Is IPID consistent with current use?
  - Is IPID per specific flow or all between particular end points?
  - Is a 32 bit field large enough?
  - Per connection or all?
  - Security Implications of Predictable Fragment Identification Values draft-gont-6man-predictable-fragment-id-03

Situations to Accommodate

- IPID is very useful in tracking packets that span NAT boundaries.
- Although NAT per se may not be prevalent in IPv6, IPID will help when connections span ANY type of boundary.
- Connections that use tunnels or translations will benefit from the use of IPID.
- IPID will be even more useful when using transport layer protocols other than TCP (UDP, ICMP, etc.).
- How will the sequence number field in the Encapsulation Security Payload Header (IPSec), be populated in IPv6?