
IPv6
REPLY_PD
RENEW_PD
REPLY_NA
RENEW_NA
REPLY
REQUEST
ADVERTISE
SOLICIT
RFC 8415
RFC 7550
RFC 7283
RFC 7083
RFC 4242
RFC 3736
RFC 3633
RFC 3315
Access Layer Challenges for DHCPv6
Raju Chalise © WORLDLINK COMMUNICATIONS LTD.

IPv6 in WorldLink

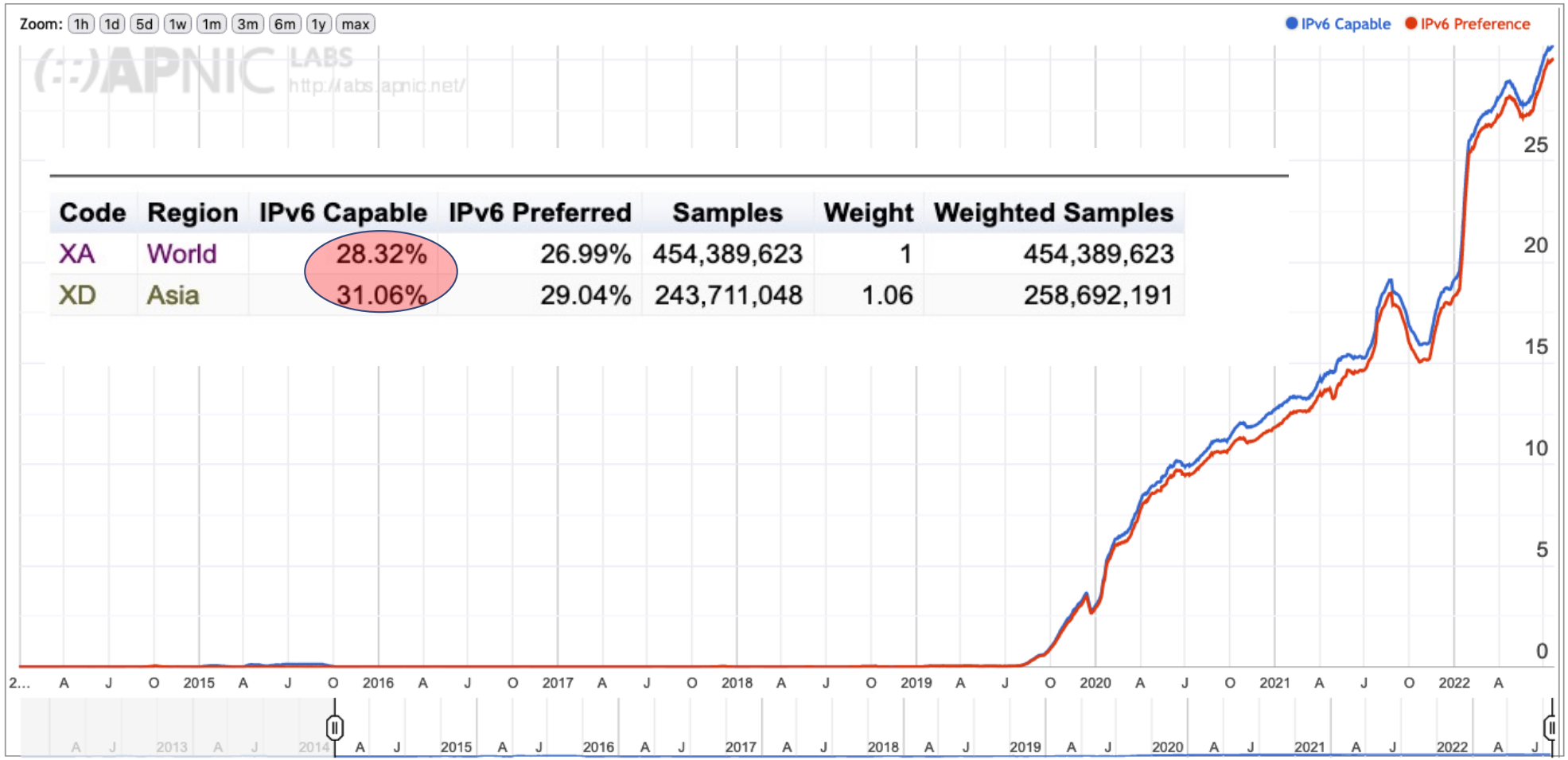
Testing Started: May 2016

Went Live : July 2019

Implementation Type: Dual Stack with Stateful DHCPv6 [CPE-BNG], Stateless [CPE-Devices]

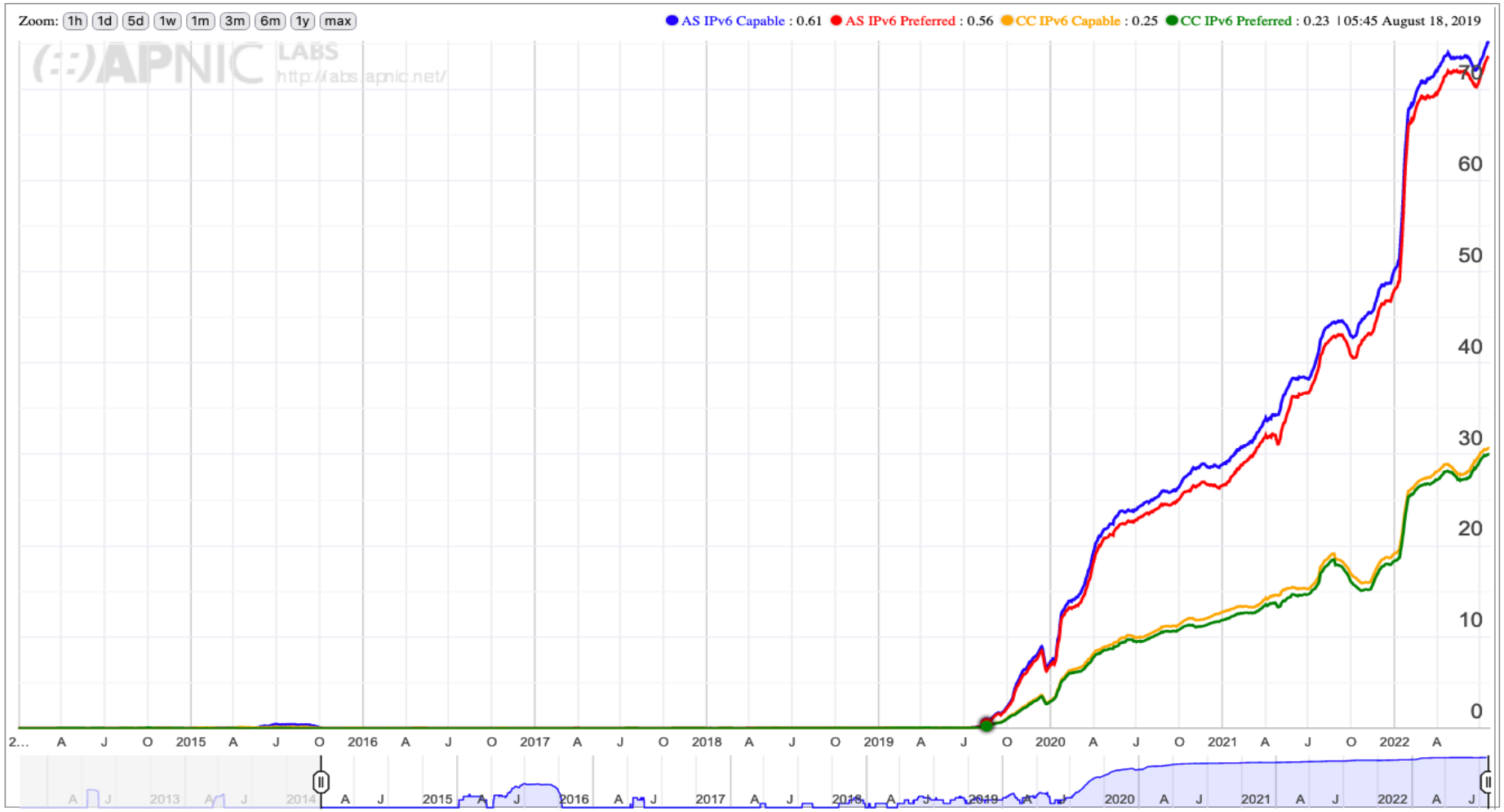
Result: Major Contributor for the IPv6 uptake in Nepal

Use of IPv6 for Nepal (NP)



Code	Region	IPv6 Capable	IPv6 Preferred	Samples	Weight	Weighted Samples
XA	World	28.32%	26.99%	454,389,623	1	454,389,623
XD	Asia	31.06%	29.04%	243,711,048	1.06	258,692,191

Deployment for AS17501: WLINK-NEPAL-AS-AP WorldLink Communications



KEYPOINTS:

1. **Understanding the FLOW [SARR | RENEW-REPLY | REBIND-FAILURE]**
2. **RFC implementations across CPE and BNG**
3. **Enabling Multicast Control**
4. **Turning off DHCPv6 Snooping Options.**

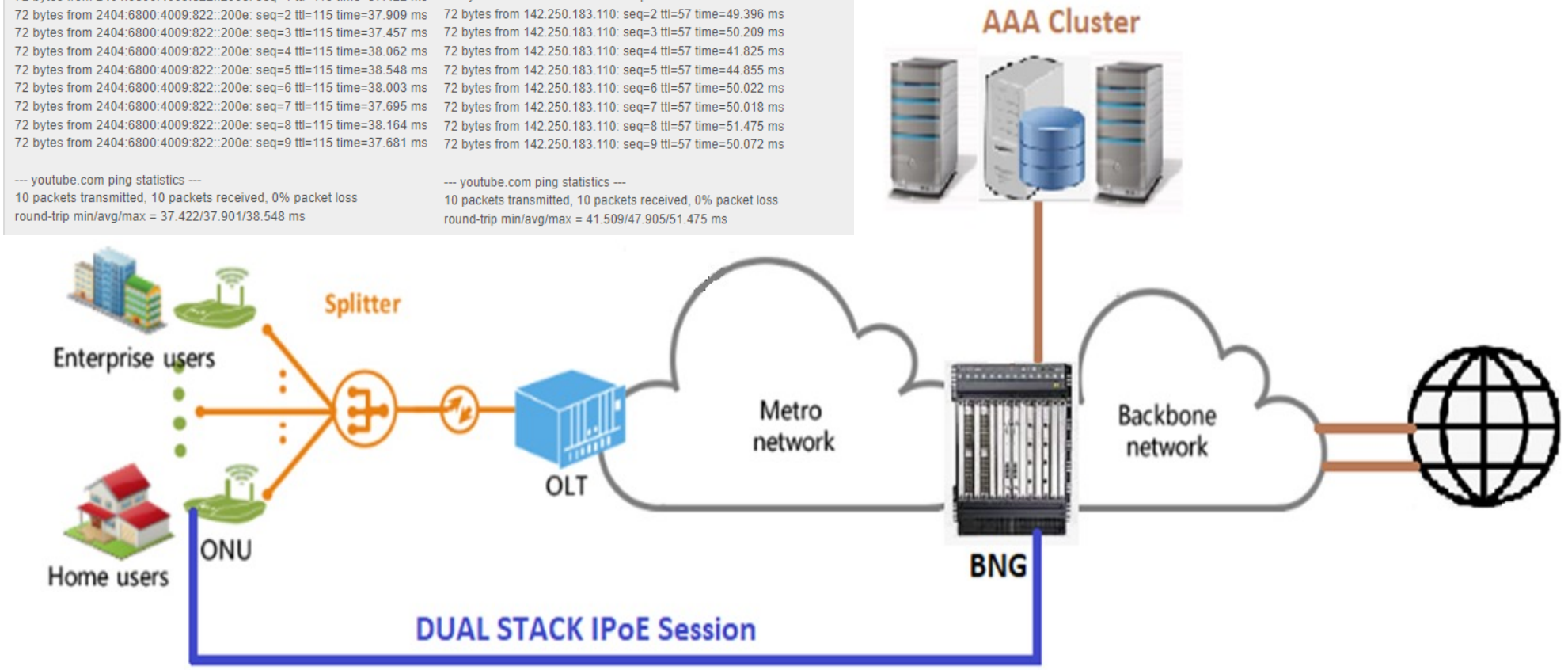
1. Understanding the flow

```
PING youtube.com (2404:6800:4009:822::200e): 64 data bytes
72 bytes from 2404:6800:4009:822::200e: seq=0 ttl=115 time=38.075 ms
72 bytes from 2404:6800:4009:822::200e: seq=1 ttl=115 time=37.422 ms
72 bytes from 2404:6800:4009:822::200e: seq=2 ttl=115 time=37.909 ms
72 bytes from 2404:6800:4009:822::200e: seq=3 ttl=115 time=37.457 ms
72 bytes from 2404:6800:4009:822::200e: seq=4 ttl=115 time=38.062 ms
72 bytes from 2404:6800:4009:822::200e: seq=5 ttl=115 time=38.548 ms
72 bytes from 2404:6800:4009:822::200e: seq=6 ttl=115 time=38.003 ms
72 bytes from 2404:6800:4009:822::200e: seq=7 ttl=115 time=37.695 ms
72 bytes from 2404:6800:4009:822::200e: seq=8 ttl=115 time=38.164 ms
72 bytes from 2404:6800:4009:822::200e: seq=9 ttl=115 time=37.681 ms

--- youtube.com ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 37.422/37.901/38.548 ms
```

```
PING youtube.com (142.250.183.110) from 100.90.28.223: 64 data bytes
72 bytes from 142.250.183.110: seq=0 ttl=57 time=41.509 ms
72 bytes from 142.250.183.110: seq=1 ttl=57 time=49.674 ms
72 bytes from 142.250.183.110: seq=2 ttl=57 time=49.396 ms
72 bytes from 142.250.183.110: seq=3 ttl=57 time=50.209 ms
72 bytes from 142.250.183.110: seq=4 ttl=57 time=41.825 ms
72 bytes from 142.250.183.110: seq=5 ttl=57 time=44.855 ms
72 bytes from 142.250.183.110: seq=6 ttl=57 time=50.022 ms
72 bytes from 142.250.183.110: seq=7 ttl=57 time=50.018 ms
72 bytes from 142.250.183.110: seq=8 ttl=57 time=51.475 ms
72 bytes from 142.250.183.110: seq=9 ttl=57 time=50.072 ms

--- youtube.com ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 41.509/47.905/51.475 ms
```

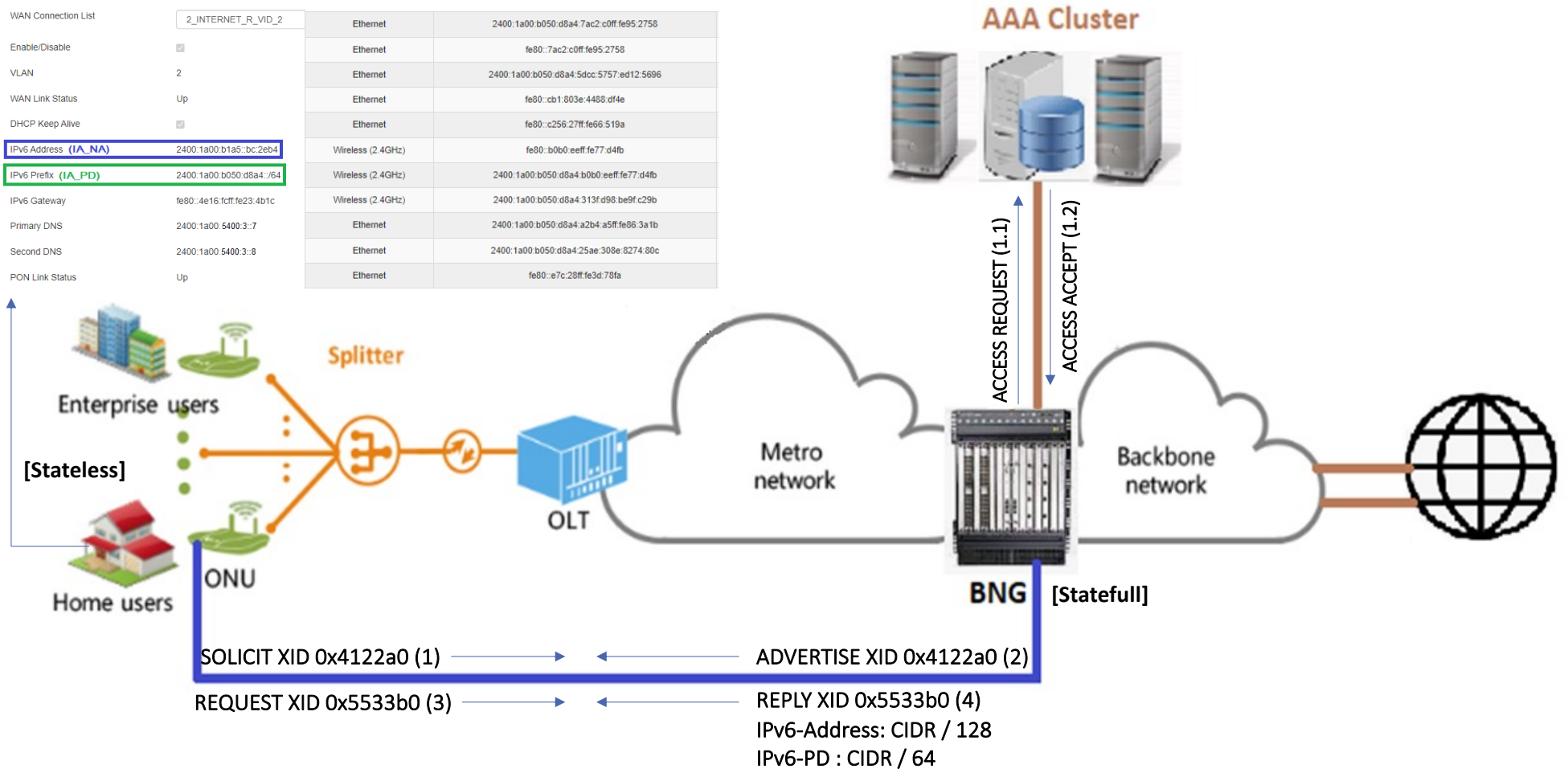


CPE-BNG SYMBOLIC TOPOLOGY

1. Understanding the flow

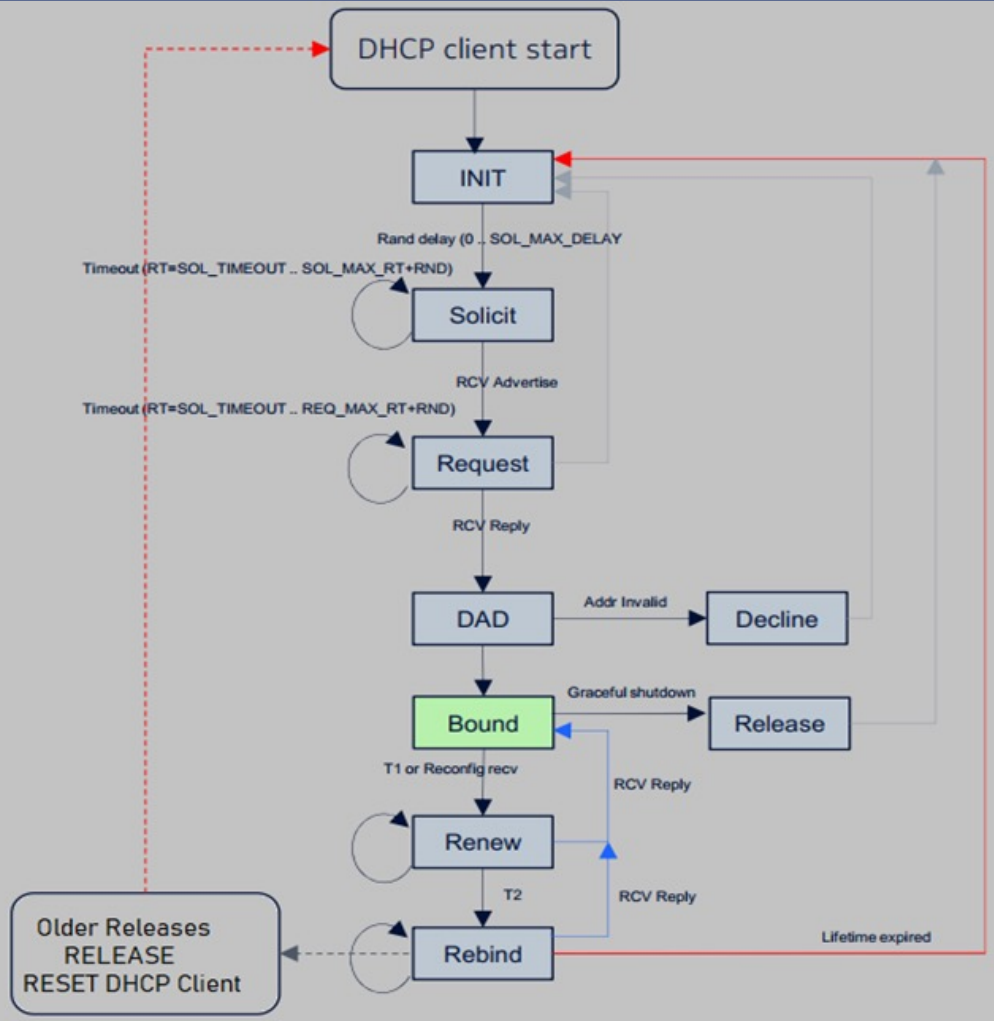
WAN Connection List	2_INTERNET_R_VID_2
Enable/Disable	☑
VLAN	2
WAN Link Status	Up
DHCP Keep Alive	☑
IPv6 Address (IA_NA)	2400:1a00:b1a5::bc:2eb4
IPv6 Prefix (IA_PD)	2400:1a00:b050:d8a4::/64
IPv6 Gateway	fe80::4e16:fcff:fe23:4b1c
Primary DNS	2400:1a00:5400:3::7
Second DNS	2400:1a00:5400:3::8
PON Link Status	Up

Ethernet	2400:1a00:b050:d8a4:7ac2:c0ff:fe95:2758
Ethernet	fe80::7ac2:c0ff:fe95:2758
Ethernet	2400:1a00:b050:d8a4:5dcc:5757:ed12:5696
Ethernet	fe80::cb1:803e:4488:df4e
Ethernet	fe80::c256:27ff:fe66:519a
Wireless (2.4GHz)	fe80::b0b0:eeff:fe77:d4fb
Wireless (2.4GHz)	2400:1a00:b050:d8a4:b0b0:eeff:fe77:d4fb
Wireless (2.4GHz)	2400:1a00:b050:d8a4:313f:d98:be9f:c29b
Ethernet	2400:1a00:b050:d8a4:a2b4:a5ff:fe86:3a1b
Ethernet	2400:1a00:b050:d8a4:25ae:308e:8274:80c
Ethernet	fe80::e7c:28ff:fe3d:78fa



CPE-BNG STATEFUL DHCPv6 FLOW

1. Understanding The Flow [UTF]



Message Types:
SOLICIT
ADVERTISE
REQUEST
REPLY

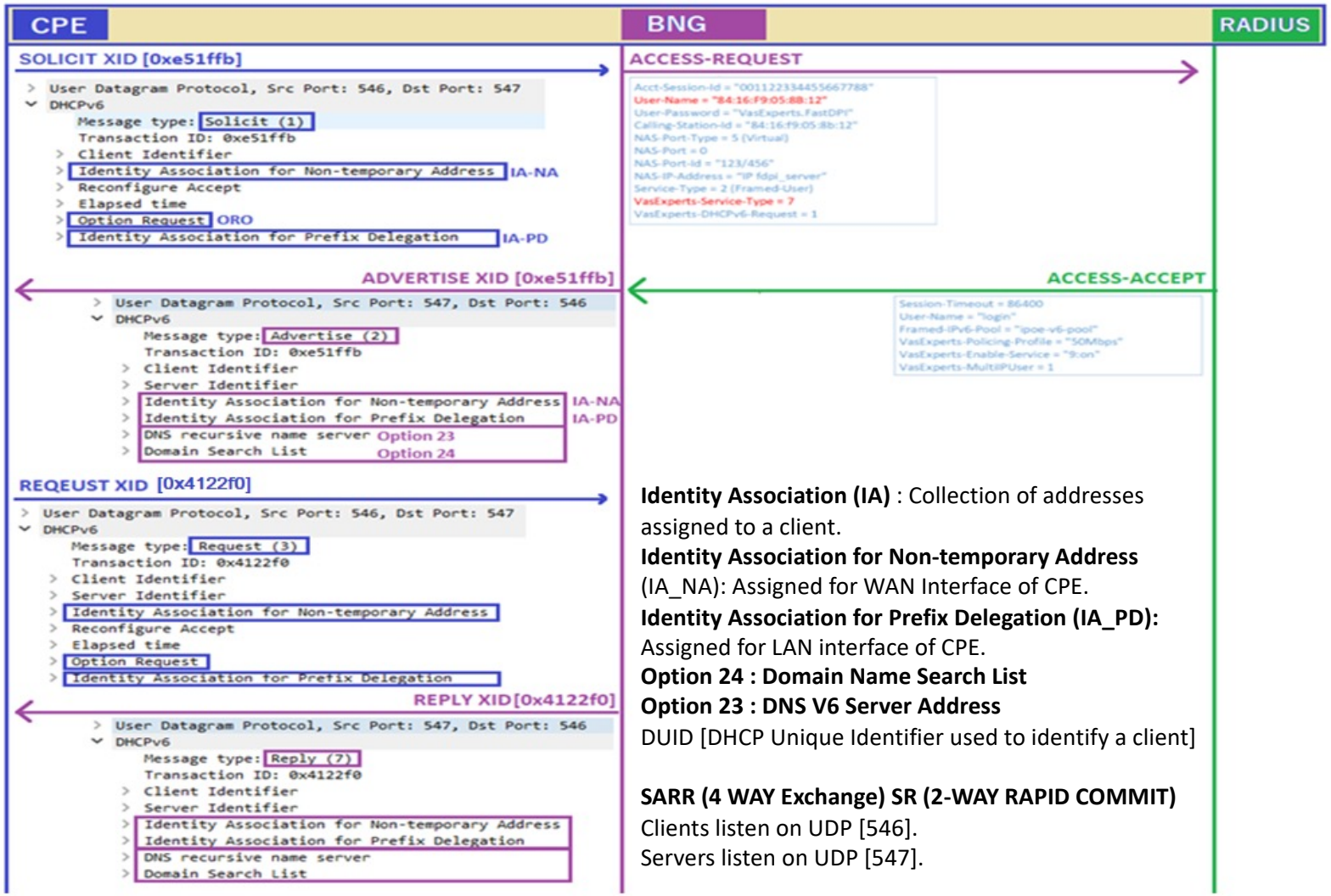
REQUEST WITH ORO ONLY
SOLICIT WITH ORO ONLY

RENEW WITH IA_NA +ORO
RENEW WITH IA_PD + ORO

REBIND WITH IA_NA + ORO
REBIND WITH IA_PD + ORO

RELEASE
ORO [Option Request Options]
Option 24 (DNS Search List)
Option 23 (DNS Servers)

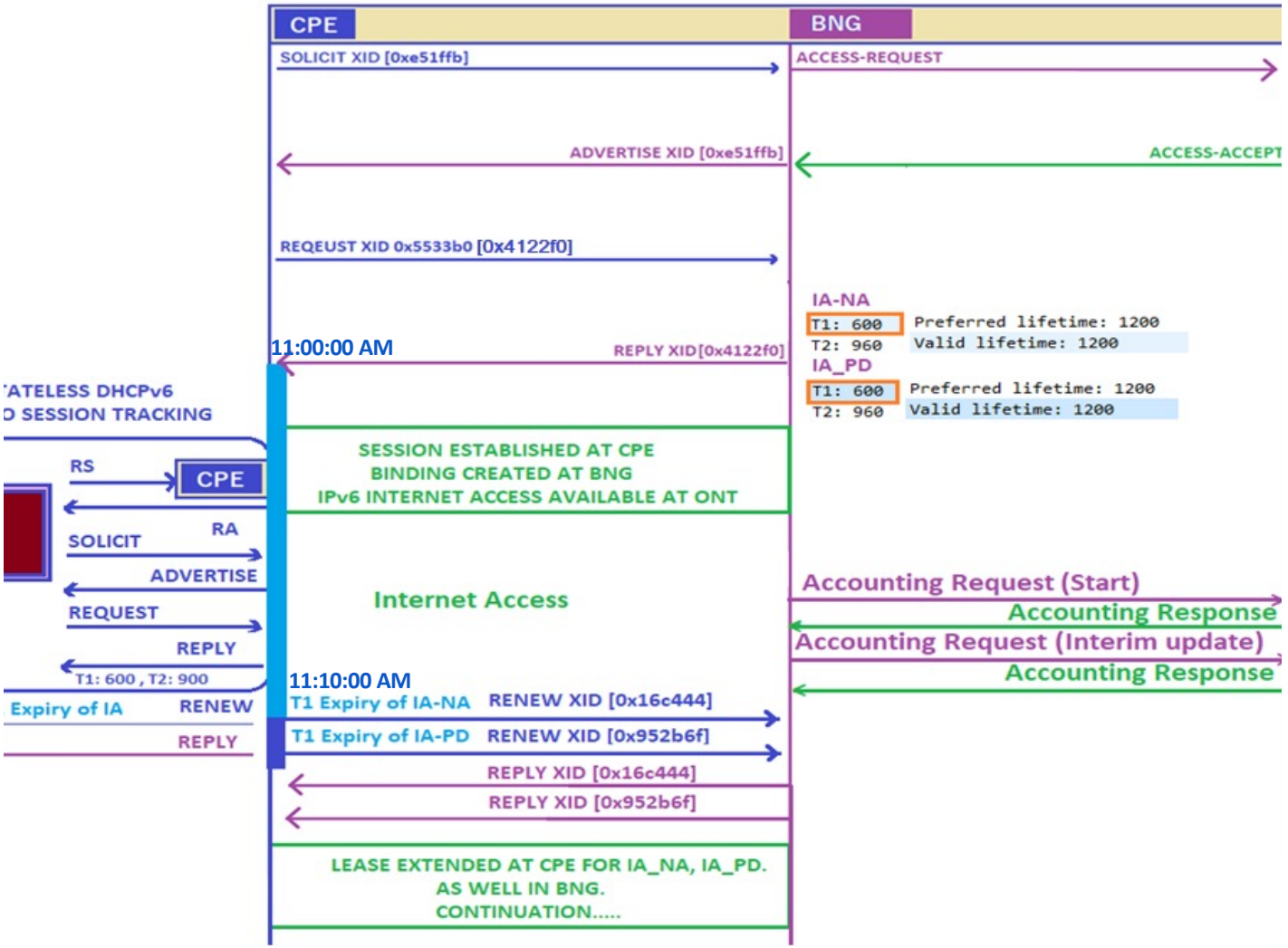
1. UTF - SARR



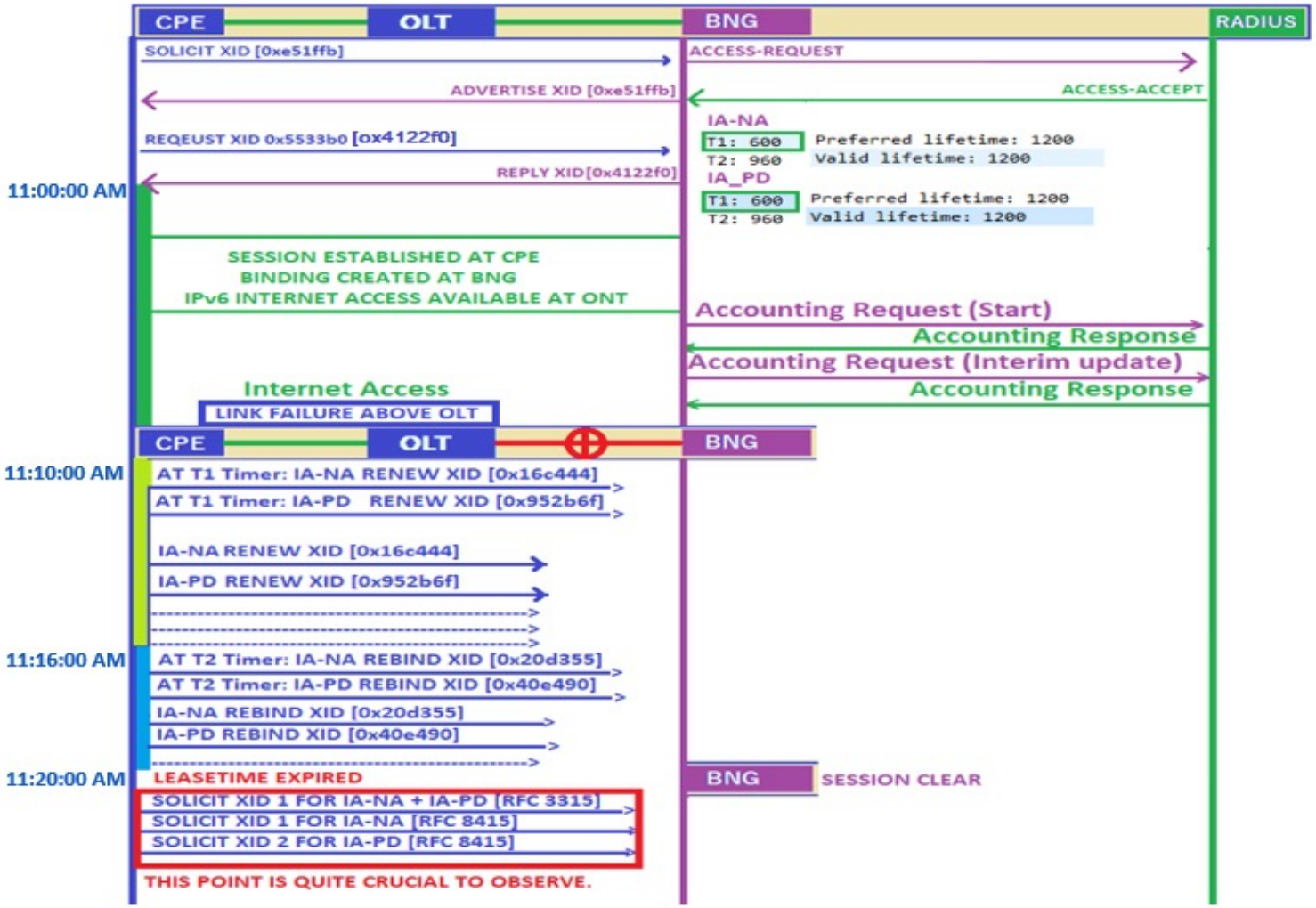
Identity Association (IA) : Collection of addresses assigned to a client.
Identity Association for Non-temporary Address (IA_NA): Assigned for WAN Interface of CPE.
Identity Association for Prefix Delegation (IA_PD): Assigned for LAN interface of CPE.
Option 24 : Domain Name Search List
Option 23 : DNS V6 Server Address
DUID [DHCP Unique Identifier used to identify a client]

SARR (4 WAY Exchange) SR (2-WAY RAPID COMMIT)
Clients listen on UDP [546].
Servers listen on UDP [547].

1. UTF - [RENEW-REPLY]



1. UTF - [RENEW-REBIND-FAILURE]



1. UTF - [WHY Multiple XIDs in SOLICIT Messages?]

1. Why multiple XIDs in SOLICIT Messages?
2. Can't DHCPv6 go with single XID retransmistted in SOLICIT messages to avoid any further complications?

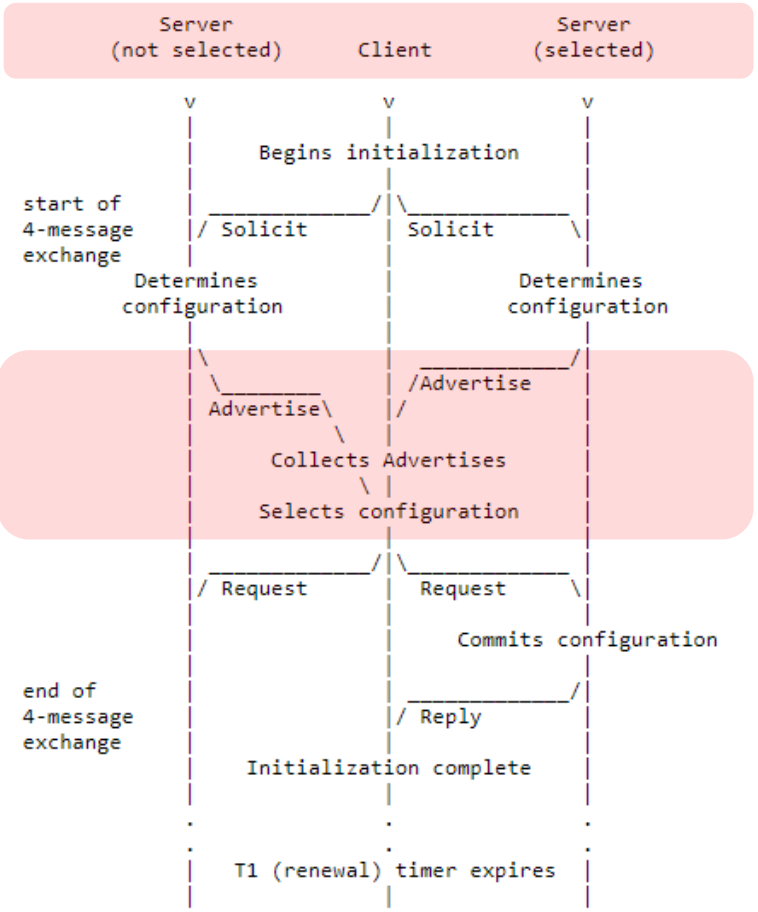
To track the transaction of each different IA Options [IA_NA | IA_PD, ORO-23 , ORO-24 and etc] separately.
Multiple XIDs give granular control over different IA Options but when DHCPv6 servers are not configured accordingly or don't have such capabilities to configure in running environment, multiple XIDs can pileup and if there is no mechanism to reinitiate them, this can hit very badly at the control plane of DHCPv6 server.

REAL CASE: 116 solicits in 1 Minute from a single CPE, imagine for just 10% of 80K subscribers in a BNG. [8000 * (116 /60) = 15,467 SOLICIT Per Second. With such numbers, **your BNG's DHCPv6 SOLICIT violation is never going to clear.**

```
1  <47>Feb 24 20:35:00 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10219: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
2  <47>Feb 24 20:35:00 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10220: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
3  <47>Feb 24 20:35:00 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10221: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
4  <47>Feb 24 20:35:01 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10222: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
5  <47>Feb 24 20:35:04 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10223: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
6  <47>Feb 24 20:35:04 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10224: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
7  <47>Feb 24 20:35:05 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10225: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
8  <47>Feb 24 20:35:05 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10226: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
9  <47>Feb 24 20:35:06 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10227: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
10 <47>Feb 24 20:35:06 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10228: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
11 <47>Feb 24 20:35:06 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10229: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
12 <47>Feb 24 20:35:06 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10230: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2

100 <47>Feb 24 20:35:53 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10318: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
101 <47>Feb 24 20:35:54 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10319: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
102 <47>Feb 24 20:35:54 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10320: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
103 <47>Feb 24 20:35:54 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10321: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
104 <47>Feb 24 20:35:54 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10322: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
105 <47>Feb 24 20:35:55 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10323: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
106 <47>Feb 24 20:35:55 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10324: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
107 <47>Feb 24 20:35:56 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10325: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
108 <47>Feb 24 20:35:56 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10326: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
109 <47>Feb 24 20:35:56 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10327: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
110 <47>Feb 24 20:35:57 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10328: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
111 <47>Feb 24 20:35:57 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10329: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
112 <47>Feb 24 20:35:57 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10330: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
113 <47>Feb 24 20:35:58 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10331: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
114 <47>Feb 24 20:35:59 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10332: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
115 <47>Feb 24 20:35:59 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10333: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
116 <47>Feb 24 20:35:59 OLT-THML-01 DHCPv6: Packet-Summary: Logical_uni: 1/1/5/16/43/14/1: Seq:10334: SesID:0: receive  DHCPv6-SOLICIT with src fe80::c648:faff:fe93:286 dst ff02::1:2
117 116 SOLICITs in one Minute from a single CPE.
```

1. UTF - [RFC 8415 – talks about multiple DHCPv6 servers]



21.8. Preference Option

The Preference option is sent by a server to a client to control the selection of a server by the client.

The format of the Preference option is:

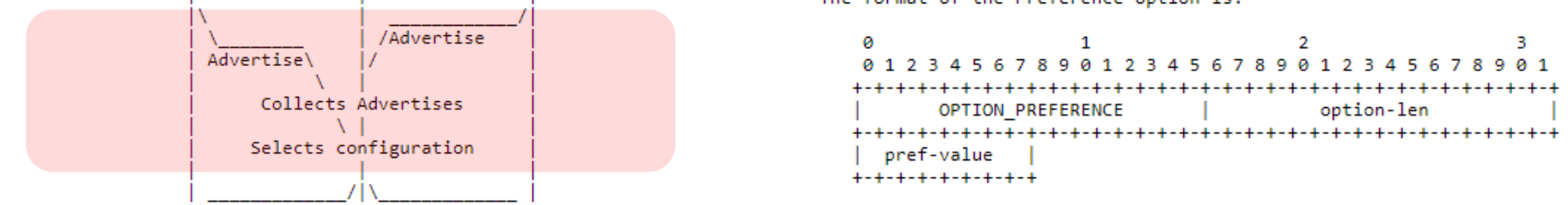


Figure 19: Preference Option Format

option-code: OPTION_PREFERENCE (7).

option-len: 1.

pref-value: The preference value for the server in this message. A 1-octet unsigned integer.

A server MAY include a Preference option in an Advertise message to control the selection of a server by the client. See Section 18.2.9 for information regarding the use of the Preference option by the client and the interpretation of the Preference option data value.

1. UTF - [RFC 8415 – talks about SOLICIT with ORO]

18.2.1. Creation and Transmission of Solicit Messages

The client sets the "msg-type" field to SOLICIT. The client generates a transaction ID and inserts this value in the "transaction-id" field.

The client MUST include a Client Identifier option (see Section 21.2) to identify itself to the server. The client includes IA options for any IAs to which it wants the server to assign leases.

The client MUST include an Elapsed Time option (see Section 21.9) to indicate how long the client has been trying to complete the current DHCP message exchange.

The client uses IA_NA options (see Section 21.4) to request the assignment of non-temporary addresses, IA_TA options (see Section 21.5) to request the assignment of temporary addresses, and IA_PD options (see Section 21.21) to request prefix delegation. IA_NA, IA_TA, or IA_PD options, or a combination of all, can be included in DHCP messages. In addition, multiple instances of any IA option type can be included.

The client MAY include addresses in IA Address options (see Section 21.6) encapsulated within IA_NA and IA_TA options as hints to the server about the addresses for which the client has a preference.

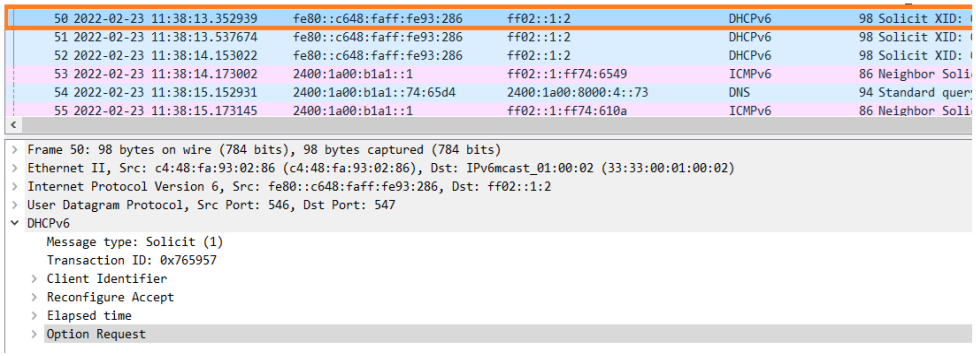
The client MAY include values in IA Prefix options (see Section 21.22) encapsulated within IA_PD options as hints for the delegated prefix and/or prefix length for which the client has a preference. See Section 18.2.4 for more on prefix-length hints.

The client MUST include an Option Request option (ORO) (see Section 21.7) to request the SOL_MAX_RT option (see Section 21.24) and any other options the client is interested in receiving. The client MAY additionally include instances of those options that are identified in the Option Request option, with data values as hints to the server about parameter values the client would like to have returned.

singleton option	An option that is allowed to appear only once as a top-level option or at any encapsulation level. Most options are singletons.

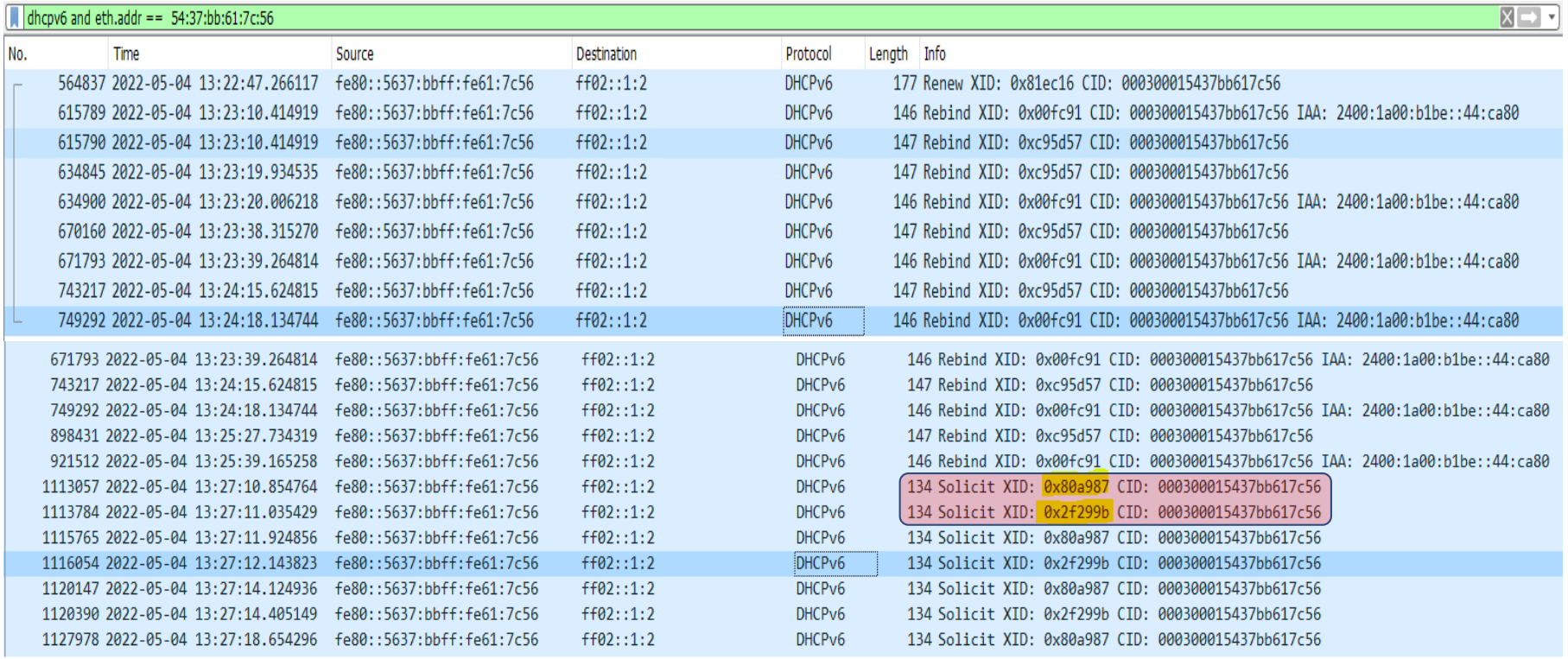
(only allowed to appear once as a top-level or encapsulated option; see Section 16 of [RFC7227]). Table 4 provides the data for the options assigned by IANA at the time of writing this document.

Option	Option Name ("OPTION" prefix removed)	Client ORO (1)	Singleton Option
1	CLIENTID	No	Yes
2	SERVERID	No	Yes
3	IA_NA	No	No
4	IA_TA	No	No
5	IAADDR	No	No
6	ORO	No	Yes
7	PREFERENCE	No	Yes
8	ELAPSED_TIME	No	Yes



1. UTF - [Triggers for Multiple XIDs in SOLICIT Messages?]

SOLICIT with different XIDs are generated after the REBIND Failure. [When ONT's lease fails to get renewed.]



dhcpv6 and eth.addr == 54:37:bb:61:7c:56

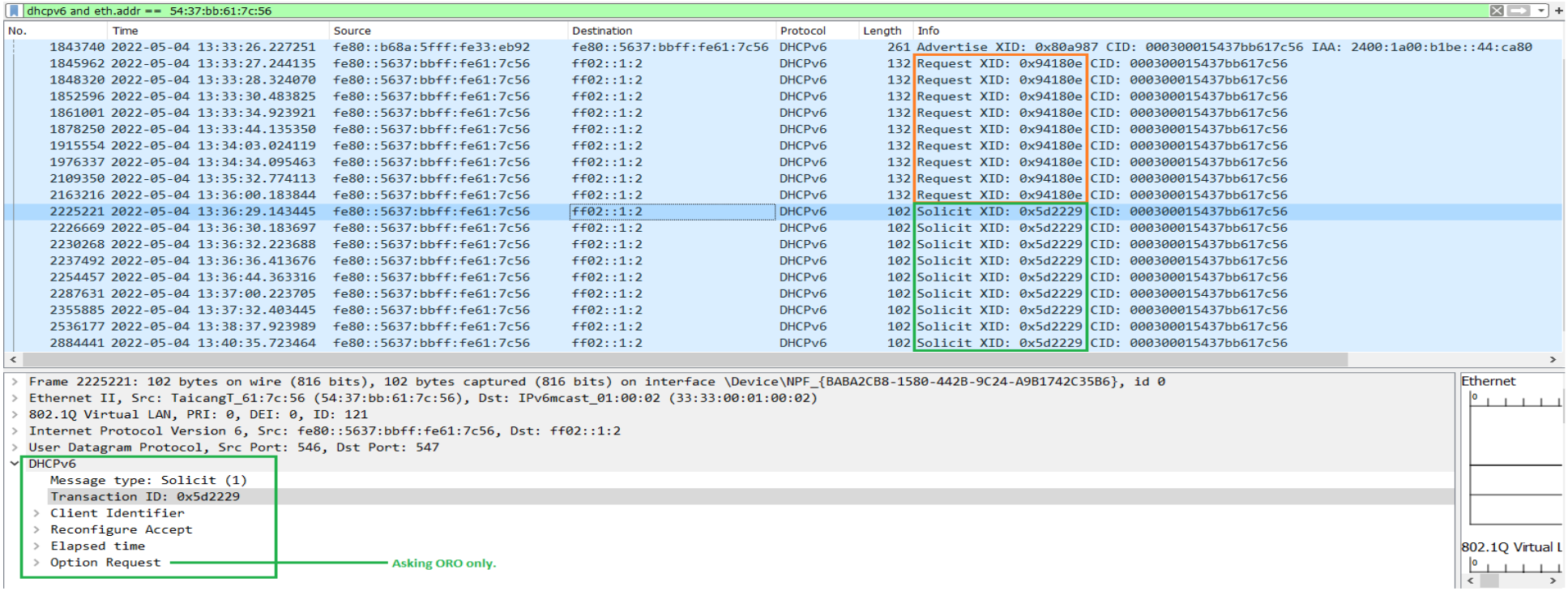
No.	Time	Source	Destination	Protocol	Length	Info
564837	2022-05-04 13:22:47.266117	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	177	Renew XID: 0x81ec16 CID: 000300015437bb617c56
615789	2022-05-04 13:23:10.414919	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
615790	2022-05-04 13:23:10.414919	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
634845	2022-05-04 13:23:19.934535	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
634900	2022-05-04 13:23:20.006218	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
670160	2022-05-04 13:23:38.315270	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
671793	2022-05-04 13:23:39.264814	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
743217	2022-05-04 13:24:15.624815	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
749292	2022-05-04 13:24:18.134744	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
671793	2022-05-04 13:23:39.264814	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
743217	2022-05-04 13:24:15.624815	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
749292	2022-05-04 13:24:18.134744	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
898431	2022-05-04 13:25:27.734319	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	147	Rebind XID: 0xc95d57 CID: 000300015437bb617c56
921512	2022-05-04 13:25:39.165258	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	146	Rebind XID: 0x00fc91 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
1113057	2022-05-04 13:27:10.854764	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1113784	2022-05-04 13:27:11.035429	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x2f299b CID: 000300015437bb617c56
1115765	2022-05-04 13:27:11.924856	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1116054	2022-05-04 13:27:12.143823	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x2f299b CID: 000300015437bb617c56
1120147	2022-05-04 13:27:14.124936	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1120390	2022-05-04 13:27:14.405149	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x2f299b CID: 000300015437bb617c56
1127978	2022-05-04 13:27:18.654296	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56

Illustration: XID1 is for existing IA_NA REBIND Failure and XID2 for IA_PD REBIND FAILURE.

Note: Unless BNG is capable of handling multiple SOLICIT XIDs, this behavior from CPE can be taxing to BNG. CPE must stop older processes after REBIND failure and generate and retransmit the same XID for SOLICIT until SARR gets completed.

1. UTF - [Triggers for Multiple XIDs in SOLICIT Messages?]

After 10 **REQUEST with ORO**, now SOLICIT with ORO only with new XID will populate.



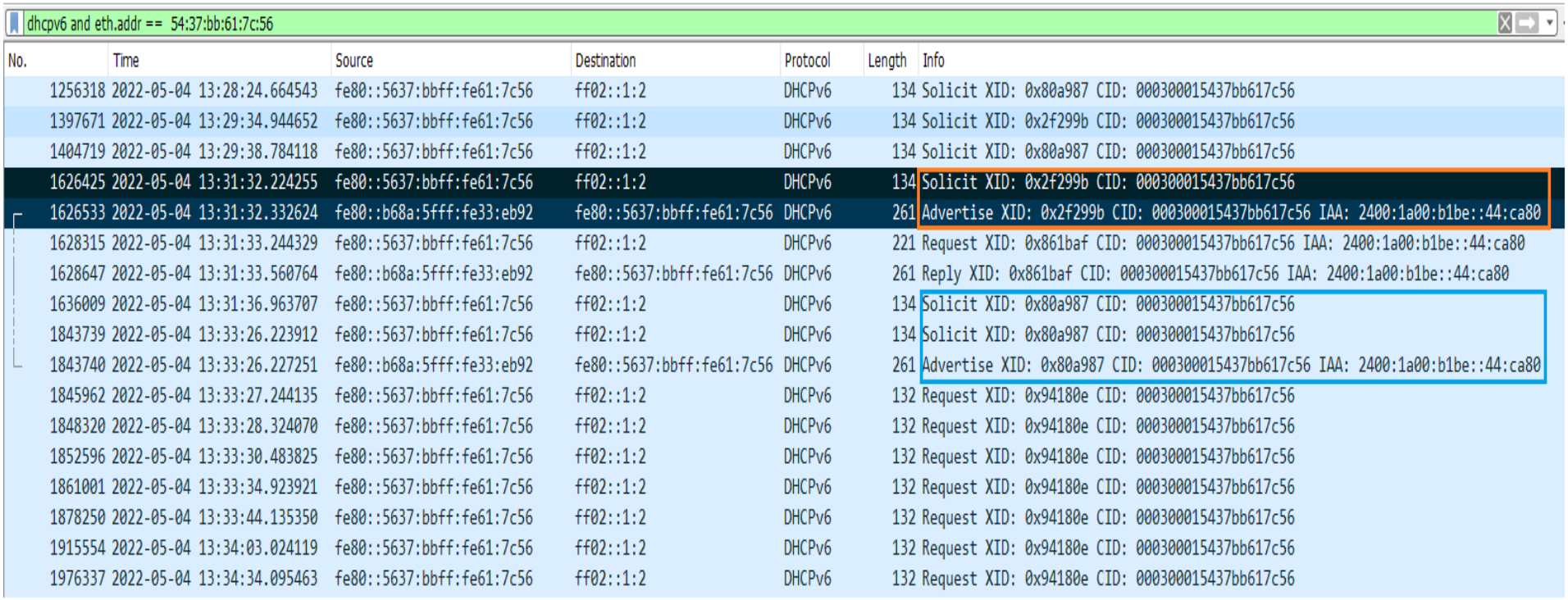
CPE Vendor clarification: SOLICIT with ORO are genuine messages in RFC 8415.

BNG Vendor question: What is the real significance of SOLICIT with ORO only packets?

CPE Vendor clarification: To comply with the RFC. ORO-23 and ORO-24 are mandatory to pass IPv6 BBF compliance. ORO-23 is DNSv6 server address list. ORO-24 is Domain Name SearchList (eg: abc.com.np)

1. UTF - [Triggers for Multiple XIDs in SOLICIT Messages?]

Further consequennces [Multiple SOLICIT XIDs, one got SARR, another SA, and ONT started sending REQEUST with ORO.



dhcpv6 and eth.addr == 54:37:bb:61:7c:56

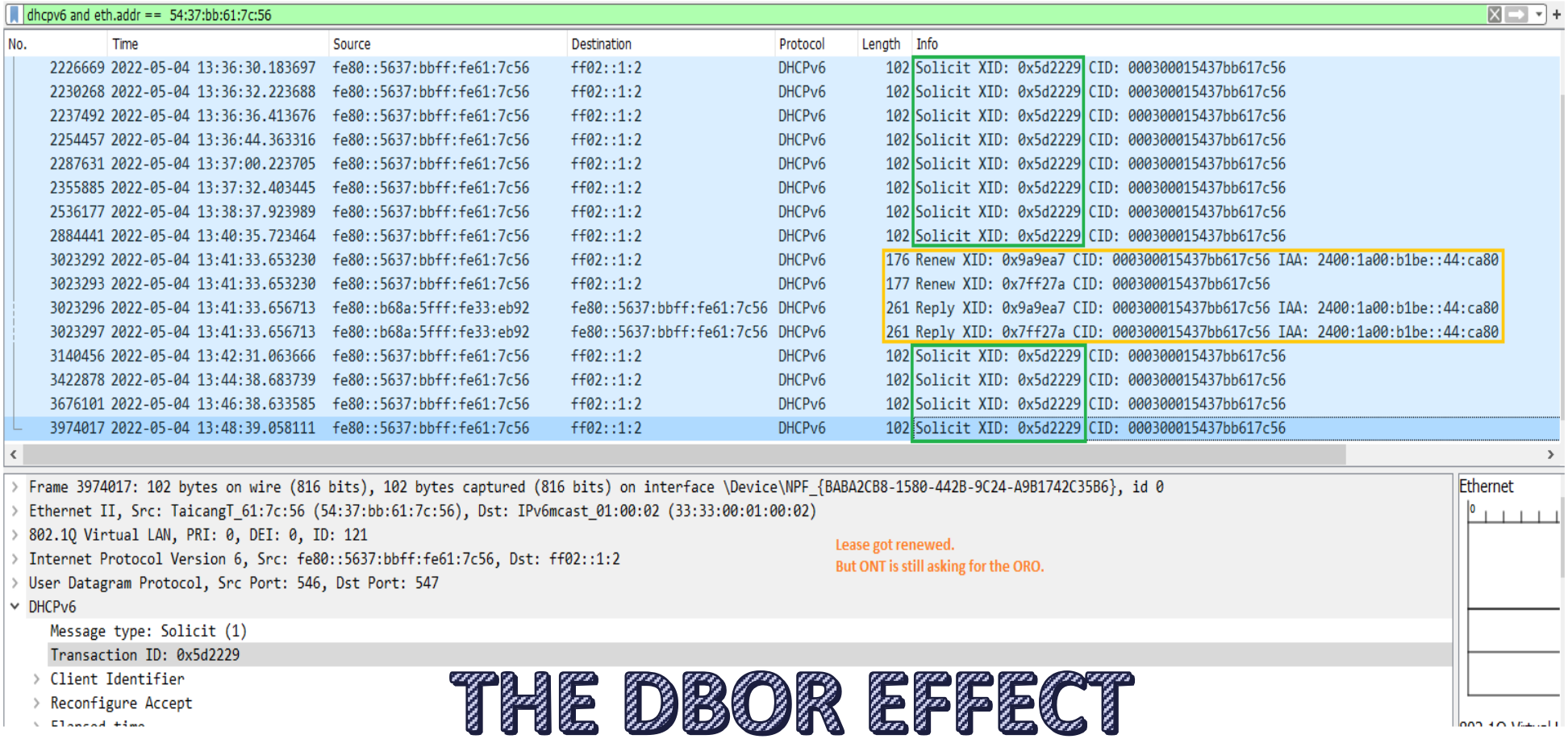
No.	Time	Source	Destination	Protocol	Length	Info
1256318	2022-05-04 13:28:24.664543	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1397671	2022-05-04 13:29:34.944652	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x2f299b CID: 000300015437bb617c56
1404719	2022-05-04 13:29:38.784118	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1626425	2022-05-04 13:31:32.224255	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x2f299b CID: 000300015437bb617c56
1626533	2022-05-04 13:31:32.332624	fe80::b68a:5fff:fe33:eb92	fe80::5637:bbff:fe61:7c56	DHCPv6	261	Advertise XID: 0x2f299b CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
1628315	2022-05-04 13:31:33.244329	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	221	Request XID: 0x861baf CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
1628647	2022-05-04 13:31:33.560764	fe80::b68a:5fff:fe33:eb92	fe80::5637:bbff:fe61:7c56	DHCPv6	261	Reply XID: 0x861baf CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
1636009	2022-05-04 13:31:36.963707	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1843739	2022-05-04 13:33:26.223912	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	134	Solicit XID: 0x80a987 CID: 000300015437bb617c56
1843740	2022-05-04 13:33:26.227251	fe80::b68a:5fff:fe33:eb92	fe80::5637:bbff:fe61:7c56	DHCPv6	261	Advertise XID: 0x80a987 CID: 000300015437bb617c56 IAA: 2400:1a00:b1be::44:ca80
1845962	2022-05-04 13:33:27.244135	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1848320	2022-05-04 13:33:28.324070	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1852596	2022-05-04 13:33:30.483825	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1861001	2022-05-04 13:33:34.923921	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1878250	2022-05-04 13:33:44.135350	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1915554	2022-05-04 13:34:03.024119	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56
1976337	2022-05-04 13:34:34.095463	fe80::5637:bbff:fe61:7c56	ff02::1:2	DHCPv6	132	Request XID: 0x94180e CID: 000300015437bb617c56

BNG Vendor clarification |Question : BNG is deliberately sending ORO-23 and ORO-24 in explicit REPLY messages. Verification at cat /etc/resolv.conf shows it. REPLY message has ORO-24 Packet, still why CPE is asking it again and again ?

CPE Vendor question: The EXPLICIT ORO-ONLY REQUEST and SOLICITs are not replied ? That's why. It's due to multiple states maintained at CPE for Multiple IA-Options. [Finding: Multiple States of IA Options and Explicit ORO aren't required].

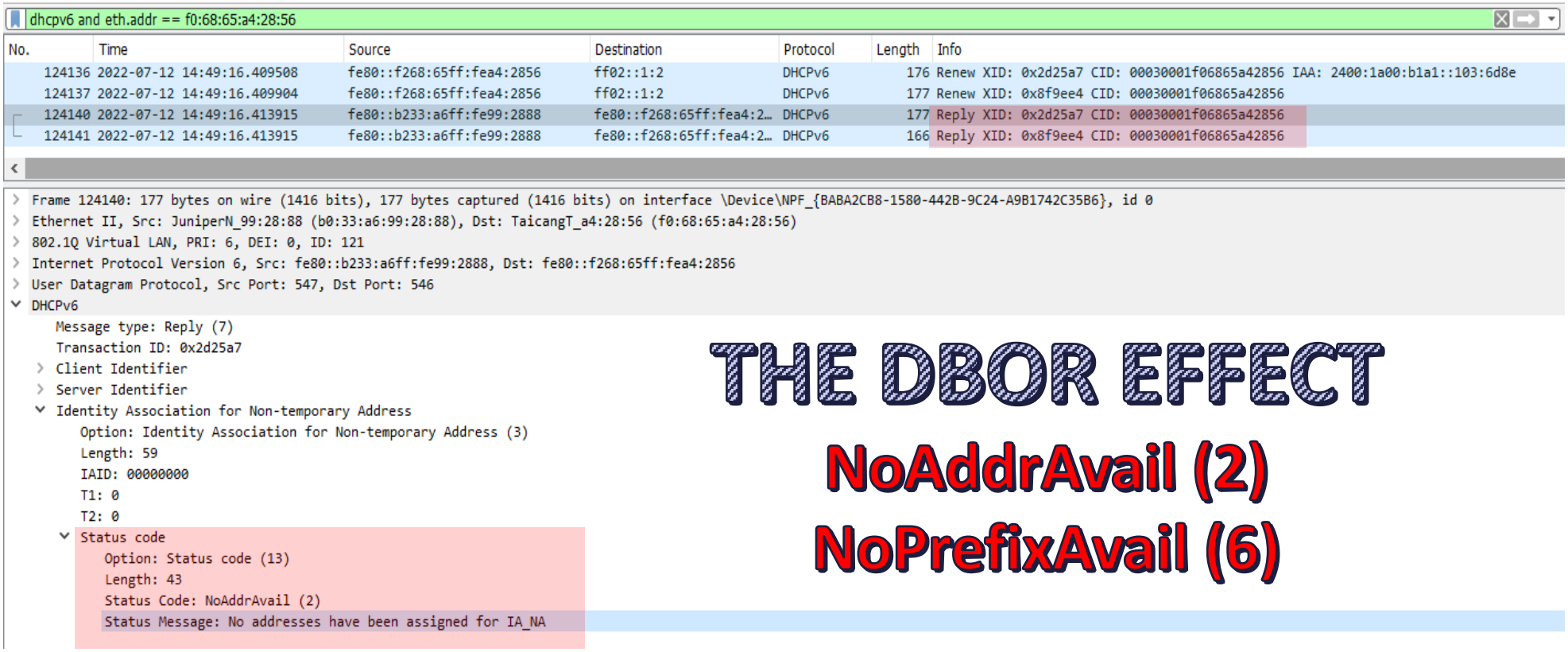
1. UTF - [Impact of Multiple SOLICIT XIDs with DBOR in both IPv4 and IPv6]

If you haven't configured **Delete Binding On Renegotiation [DBOR] for DHCPv6**, your client will still have IPv6 session amidst these. But at BNG's control plane, DDOS Protection stats against SOLICIT will start spiking.



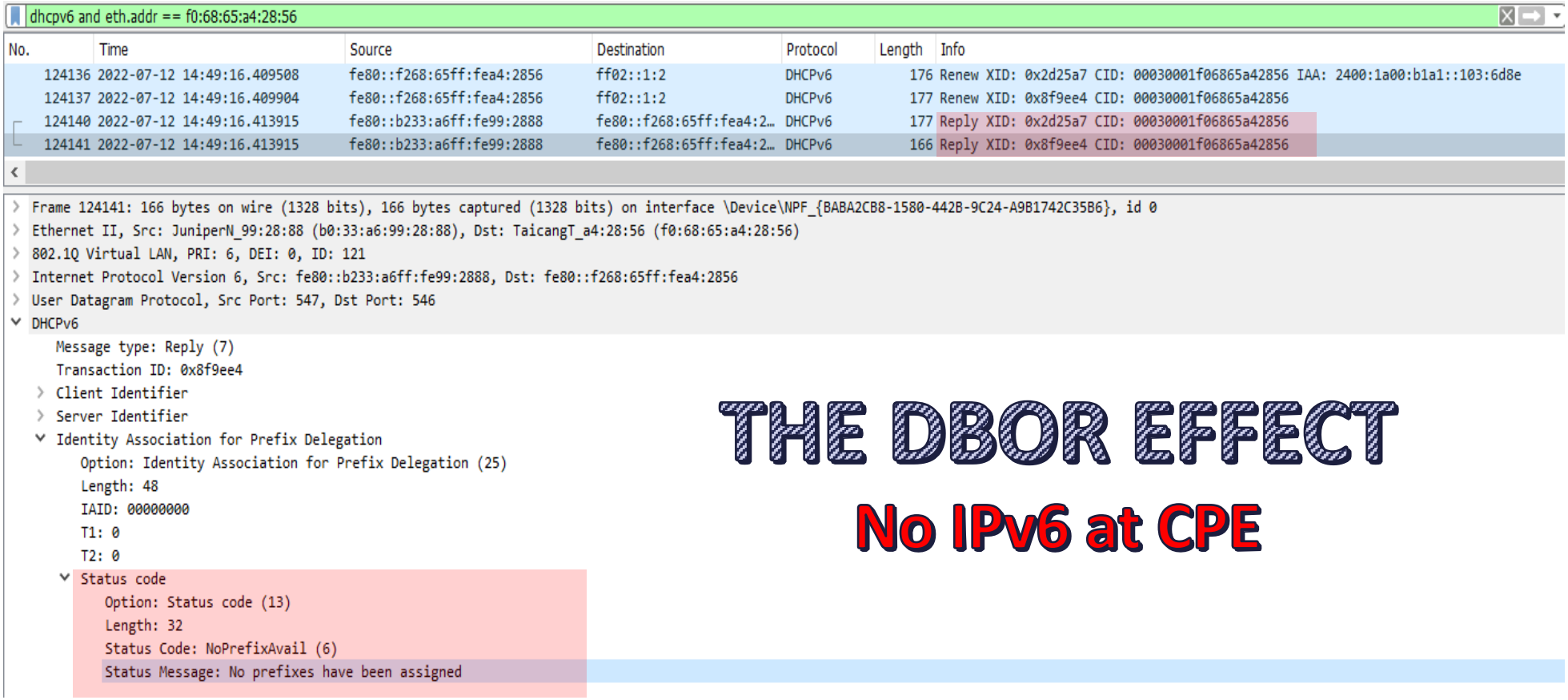
1. UTF - [Impact of Multiple SOLICIT XIDs with DBOR in both IPv4 and IPv6]

If DBOR is there for DHCPv6 – with repeated SOLICIT, BNG will tear down the existing whole session [IPv4 + IPv6], create a new one. Amidst these, the CPE will be reported with DHCPv6 REPLY packets with Status Code: NoAddressAvail (2) & NoPrefixAvail (6) from BNG whereas no information will be passed in DHCPv4. And after this, customer will start having the issues as BNG has newer session and CPE has older session.



1. UTF - [Impact of Multiple SOLICIT XIDs with DBOR in both IPv4 and IPv6]

Status Code: 13 – NoAddrAvail(2)
Status Code: 13 – NoPrefixAvail(6)



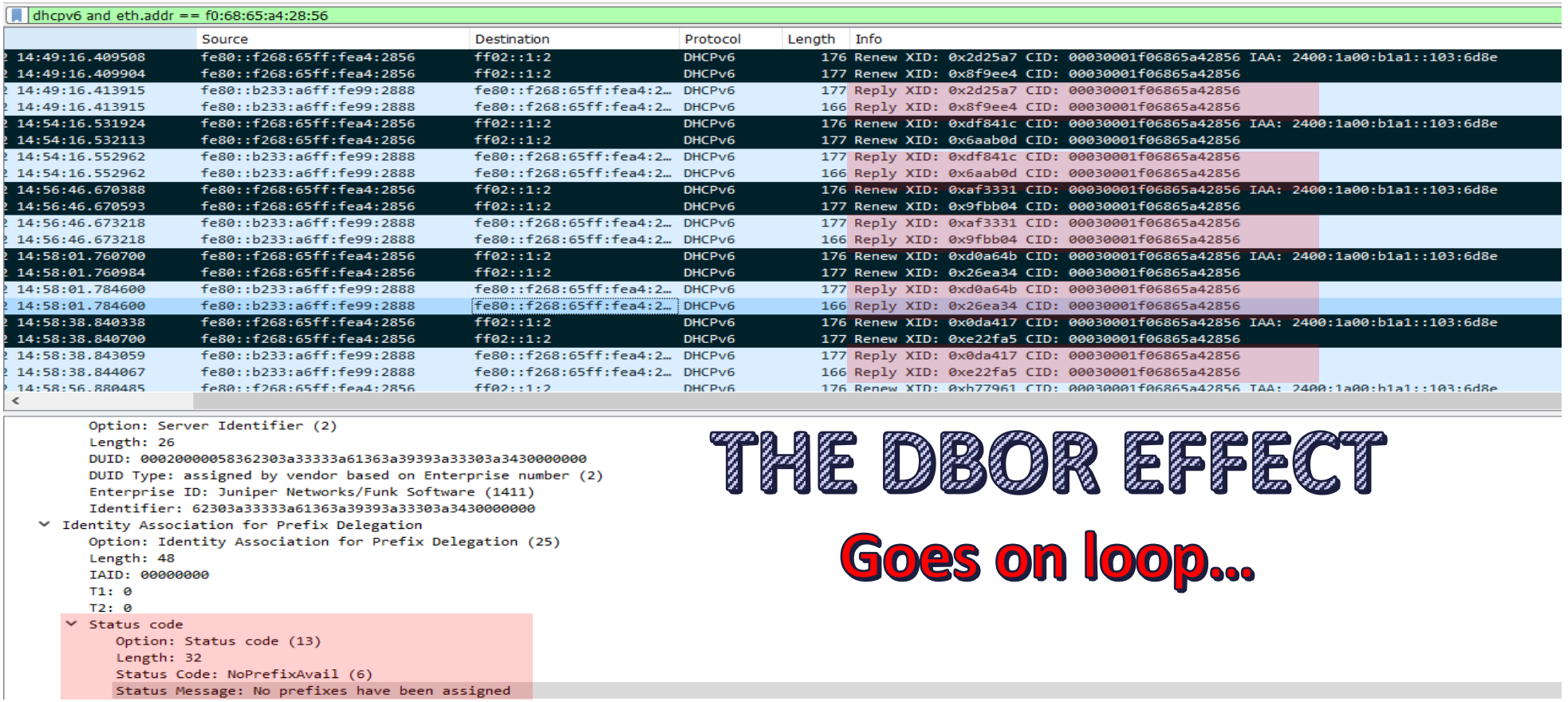
THE DBOR EFFECT

No IPv6 at CPE

1. UTF - [Impact of Multiple SOLICIT XIDs with DBOR in both IPv4 and IPv6]

Status Code: 13 – NoAddrAvail(2)
Status Code: 13 – NoPrefixAvail(6)

And it keeps on looping until CPE faces power cut or fiber cut.



THE DBOR EFFECT

Goes on loop…

1. UTF - [Impact of Multiple SOLICIT XIDs with DBOR in both IPv4 and IPv6]

Q. While this was going on, what was the impact at the control plane of BNG ?

Protocol group	Packet type	Received (packets)	Dropped (packets)	Rate (pps)	Violation counts	State
dhcpv6	solicit	545494512411134	45454287195655	8553	54560	viol

Q. How was IPv6 connectivity at users who went into the state of Multiple SOLICIT XIDs ?

No IPv6 at all.

Spike in MAMS card for IPv4 NAT Traffic.

Call center flooded with slower facebook, youtube, google services complaints.

Q. Observations against different location resolving the issues?

NEW Router replacement with older router as immediate fix. [It fixed those customers as is in older RFC 3315].

Q. Quick fixes or workarounds.

Rebooted problematic CPEs sending higher number of SOLICIT XIDs.

KEYPOINTS:

1. **Understanding the FLOW [SARR | RENEW-REPLY | REBIND-FAILURE]**
2. **RFC implementations across CPE and BNG**
3. **Enabling Multicast Control**
4. **Turning off DHCPv6 Snooping Options.**

2. RFC Implementations across CPE and BNG

18.2. Client Behavior

A client uses the Solicit message to discover DHCP servers configured to assign leases or return other configuration parameters on the link to which the client is attached.

A client uses Request, Renew, Rebind, Release, and Decline messages during the normal lifecycle of addresses and delegated prefixes.

When a client requests multiple IA option types or multiple instances of the same IA types in a Solicit, Request, Renew, or Rebind, it is possible that the available server(s) may only be configured to offer a subset of them. When possible, the client SHOULD use the best configuration available and continue to request the additional IAs in subsequent messages. This allows the client to maintain a single session and state machine. In practice, especially in the case of handling IA_NA and IA_PD requests [RFC7084], this situation should be rare or a result of a temporary operational error. Thus, it is more likely that the client will get all configuration if it continues, in each subsequent configuration exchange, to request all the configuration information it is programmed to try to obtain, including any stateful configuration options for which no results were returned in previous message exchanges.

CPE can continue to request additional IAs , ORO parameters with explicit SOLICIT in RFC 8415.

2. RFC Implementations across CPE and BNG

CPE can continue to request additional IAs , ORO parameters with explicit SOLICIT in RFC 8415.

But what if BNG is configured with DBOR [delete-binding-on-renegotiation] settings?
https://www.juniper.net/documentation/us/en/software/junos/subscriber-mgmt-sessions/topics/ref/statement/delete-binding-on-renegotiation-edit-dhcp.html

Description

Configure DHCP to override the default behavior when the local server or relay agent receives a DHCPv4 Discover or DHCPv6 Solicit message while in a bound state. In this case, DHCP drops the message and it is not processed. On a DHCP relay agent, the agent sends a Release message to the local server. DHCP cleans up the existing session and deletes the existing client entry, removing the binding. When a second Discover or Solicit message is received from the client, the message is processed and DHCP negotiation proceeds.

A consequence of the override behavior is that the time to complete a DHCP negotiation is prolonged if the client begins negotiation before the existing client entry is expired. The delay can be up to several seconds.

The default behavior (this statement is not configured) is that DHCP maintains the client entry if it receives a Discover or Solicit message that has a client ID that matches the existing client. DHCP then processes the new message using the existing client entry and responds to the client with an Offer or Advertise message.

If DBOR is explicitly enabled in DHCPv6, most likely with SOLICIT ORO only packets, existing DHCPv6 binding will get cleared up and new session will get established without informing the CPE. Now imagine, what will happen to the client for next T1 interval & This continues with every new SOLICIT XIDs.

2. RFC Implementations across CPE and BNG

CPE complying to new RFC 8415 can maintain separate state machine for IA_NA and IA_PD Options. In addition, they can request the Option Request Options [ORO] in separate SOLICIT XIDs.

If we opt for Multiple Exchanges of IA Options in CPE, it is very much need in BNG side as well.

Adverse situations like Session Teardown [with delete-binding-on-renegotiation enabled] , V4|V6 Address Mismatch in CPE & BNG, Repeated longer DDOS violations for DHCPv6 are most likely to happen with differing RFC implementations.

So what are the recommendations?
Both CPE as well BNG should have same implementation on RFC 8415 or the Single Exchange for Multiple IA Options.

18.1. A Single Exchange for Multiple IA Options

This document assumes that a client SHOULD use a single transaction for all of the IA options required on an interface; this simplifies the client implementation and reduces the potential number of transactions required (for the background on this design choice, refer to Section 4 of [RFC7550]). To facilitate a client's use of a single transaction for all IA options, servers MUST return the same T1/T2 values for all IA options in a Reply (see Sections 18.3.2, 18.3.4, and 18.3.5) so that the client will generate a single transaction when renewing or rebinding its leases. However, because some servers may not yet conform to this requirement, a client MUST be prepared to select appropriate T1/T2 times as described in Section 18.2.4.

2. RFC Implementations across CPE and BNG

18.1. A Single Exchange for Multiple IA Options — Section 4 of [RFC7550]

4. Handling of Multiple IA Option Types

The DHCPv6 specification [RFC3315] was written with the assumption that the only stateful options were for assigning addresses. DHCPv6 Prefix Delegation [RFC3633] describes how to extend the DHCPv6 protocol to handle prefix delegation, but does not clearly specify how the DHCP address assignment and prefix delegation coexist.

If a client requests multiple IA option types, but the server is configured to only offer a subset of them, the client could react in several ways:

1. Reset the state machine and continue to send Solicit messages,

Resetting the state machine and continuing to send Solicit messages may result in the client never completing DHCP and is generally not considered a good solution. It can also result in a packet storm if the client does not appropriately rate limit its sending of Solicit messages or if there are many clients on the network. Client implementors that follow this approach SHOULD implement the updates to RFC 3315 specified in [RFC7083].

2. Create separate DHCP sessions for each IA option type and continue to Solicit for the unfulfilled IA options, or

Creating a separate DHCP session (separate instances of the client state machine) per IA option type, while conceptually simple, causes a number of issues: additional host resources required to create and maintain multiple instances of the state machine in clients, additional DHCP protocol traffic, unnecessary duplication of other configuration options and the potential for conflict, and divergence in that each IA option type specification specifies its 'own' version of the DHCP protocol.

3. The client could continue with the single session and include the unfulfilled IA options in subsequent messages to the server.

The single session and state machine allows the client to use the best configuration it is able to obtain from a single DHCP server during the configuration exchange. Note, however, that the server may not be configured to deliver the entire configuration requested by the client. In that case, the client could continue to operate only using the configuration received, even if other servers can provide the missing configuration. In practice, especially in the case of handling IA_NA and IA_PD, this situation should be rare or a temporary operational error. So, it is more likely for the client to get all configuration if it continues, in each subsequent configuration exchange, to request all the configuration information it is programmed to try to obtain, including any stateful configuration options for which no results were returned in previous exchanges.

2. RFC Implementations across CPE and BNG

18.1. A Single Exchange for Multiple IA Options

RFC 7550 Multiple Stateful Options May 2015

If a client requests multiple IA option types, but the server is configured to only offer a subset of them, the client could react in several ways:

1. Reset the state machine and continue to send Solicit messages,
2. Create separate DHCP sessions for each IA option type and continue to Solicit for the unfulfilled IA options, or
3. The client could continue with the single session and include the unfulfilled IA options in subsequent messages to the server.

Q: Which option is best suited for implementation?
You may opt for Clause : 3 but it is still not failproof.

In this context, compliance between CPE and BNG is a very crucial point. You may need to customize CPE's behavior as per your BNG's capabilities or vice-versa whichever is quicker to implement.

One major issue of this last approach is that it is difficult to allow it with the current DHCPv6 specifications; in some cases they are not clear enough, and in other cases existing restrictions can make it impossible. This document introduces some clarifications and small modifications to the current specifications to address these concerns.

While all approaches have their own pros and cons, approach number 3 above SHOULD be used and is the focus of this document because it is deemed to work best for common cases of the mixed use of IA_NA and IA_PD. But this document does not exclude other approaches. Also, in some corner cases it may not be feasible to maintain a single DHCPv6 session for both IA_NA and IA_PD. These corner cases are beyond the scope of this document and may depend on the network in which the client (CE router) is designed to operate and on the functions the client is required to perform.

2. RFC Implementations across CPE and BNG

Q. Why you need DBOR for both DHCPv4 and DHCPv6 together at BNG?

Delete-Binding-On-Renegotiation [DBOR] is a vendor proprietary implementation and before going for it you really need to brainstorm for what purposes you need it in specific protocols.

Because with lack of proper keepalive mechanism in entire dual stack IPoE, persistent DHCP at least for the leasetime duration is the key-essence for maintaining subscribers' sessions.

Q. What impact DBOR can have in DHCPv4 ?

Mostly in DHCPv4, CPE may not send another DISCOVER if it has a bounded session with BNG. Even in discovery stage, a standard CPE's DISCOVER XID gets changed after each three attempts in subsequent attempts[2 + 4 + 7 or 2 + 4 + 13 seconds]. That is why only for DHCPv4, DBOR won't create much issues threoritically.

672	2022-07-12 12:27:27.987268	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x5eccea7e
3009	2022-07-12 12:27:35.047289	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8ef69b1c
3585	2022-07-12 12:27:37.077911	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8ef69b1c
4425	2022-07-12 12:27:41.107302	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8ef69b1c
5844	2022-07-12 12:27:48.157481	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x958da978
6479	2022-07-12 12:27:50.157755	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x958da978
7681	2022-07-12 12:27:54.177859	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x958da978
9456	2022-07-12 12:28:01.227739	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8dd1bd6e
9766	2022-07-12 12:28:03.260814	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8dd1bd6e
10437	2022-07-12 12:28:07.277735	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0x8dd1bd6e
12070	2022-07-12 12:28:14.327474	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0xdd6e1253
12840	2022-07-12 12:28:16.347939	0.0.0.0	255.255.255.255	DHCP	319 DHCP Discover - Transaction ID 0xdd6e1253

But with different CPEs, different implementations are likely to be found so proper analysis is always required.

Recommendations:

CPE END

 # Suppression of ORO Only SOLICIT and REQUEST Messages.
 # Single State Machine for IA_NA + IA_PD + ORO.

 # Single Exchange of Messages for Multiple IA Options in SOLICIT.
 # Single Exchange of Messages for Multiple IA Options in RENEW.
 # Single Exchange of Messages for Multiple IA Options in REBIND.

 # AFTER RENEW-REBIND Failure, V6Stack should terminate existing SOLICIT XID processes.
 # SOLICIT with new XID must be retransmitted further after REBIND Failure.
 # Proper Status Code for Immediate Stack Reset of CPE. [NoBinding instead of NoAddressAvail | NoPrefixAvail]

BNG End

 # Enabling Option24 ORO Parameters in BNG if supported.
 # Keeping same leasetimer in IA_NA and IA_PD explicitly.

KEYPOINTS:

1. **Understanding the FLOW [SARR | RENEW-REPLY | REBIND-FAILURE]**
2. **RFC implementations across CPE and BNG**
3. **Enabling Multicast Control**
4. **Turning off DHCPv6 Snooping Options.**

3. Enabling Multicast Controls

Different vendors have different knob for multicast enabling.
As DHCPv6 runs on Multicast, it is mandatory to enable Multicast control.

Any multicast MAC [33:33:00:01:XX:XX to 33:33:FF:FF:FF:FF**] filter applied into respective ports of switches where DHCPv6 will run must be turned off.**

Vendor specific VLAN level multicast control must be enabled in OLTs.

Multicast Listener Discovery must be enabled at switches.

Specific Multicast storm-control limit should be turned off in trunk ports in switches.
Some vendors have specific way of limiting multicast at certain pps, need to take care of that as well.

KEYPOINTS:

1. **Understanding the FLOW [SARR | RENEW-REPLY | REBIND-FAILURE]**
2. **RFC implementations across CPE and BNG**
3. **Enabling Multicast Control**
4. **Turning off DHCPv6 Snooping Options.**

4. Turning off DHCPv6 snooping options

For easier troubleshooting of CPEs, you may enable snooping for DHCPv4 as well DHCPv6 at vlan level of OLTs. Though this is good for troubleshooting aspects but in production networks, where 5K, 8K subscribers are running at OLTs, repetitive fiber flappings , mass-power cuts restoration will overwrite V4 and V6 snooped address table entries so rigorously at significant rates. Limitations imposed in storing DHCP entries for a CPE and the functional aspect of this function will eventually becomes a real bottleneck in transmission of network control traffic for V4 and V6 resulting to odd situations like -

Eg: If an implementation to retain maximum 4 snooped entries per CPE is there, OLT will end up discarding the v6-REPLY or v4-ACK to the CPE resulting idle connectivity at CPE end.

Until this implementation is optimized, then it's always better to not to play with such options at least in production network and leave the OLTs to do pure forwarding and ranging.

Similar snooping related options should be disabled in subsequent trunk ports of switches.

To mitigate security concerns of Rouge DHCPv6 servers from Customer End, Bridge Mode to CPE and U2U communication must be prohibited towards downstream side.

Thank you for the listening.
Your queries regarding the topics are highly appreciated.

End of Session