Device ID in EDNS0 Records for DNS over UDP and TCP

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product (s) or Functional Area	P-GW
Applicable Platforms	• ASR 5500 • UAS • VPC-SI • VPC-DI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	• *P-GW Administration Guide* • *Command Line Interface Reference*

Revision History

Table 2: Revision History

Revision Details	Release
The EDNS feature is enhanced to support both UDP and TCP protocols.	21.18.23
First Introduced	21.18.21

Feature Description

The Device ID in EDNS0 offers each enterprise with a customized domain blocking through Umbrella. To enable this functionality:

- The P-GW must reformat a subscriber DNS request into an EDNS0 request, and
- The P-GW must include an Umbrella “Device ID” in the EDNS0 packet so that the Umbrella DNS resolver can use the Device ID to apply the domain filter associated/configured with the Device ID in the EDNS0 packet.

Presently, the PCRF/PCF passes the content filtering policy ID to the P-GW in the Gx events (CCA-I/CCA-U/RAR). The gateway uses the content filtering policy ID to apply content filtering functionality to the subscriber:

As part of this feature, a new configurable EDNS0 content filtering range parameter to trigger the EDNS0 functionality is supported in P-GW to accept and use the full 64-bit Device ID from the PCRF/PCF. The new configurable parameter determines if the subscribers can have a content filtering service or an EDNS0 service.

Note The Device ID in EDNS0 records for DNS over UDP or TCP feature is based on the existing content-filtering license.

Also, P-GW allow subscribers to utilize both the content filter service and EDNS0 services. P-GW follows the following mechanism:

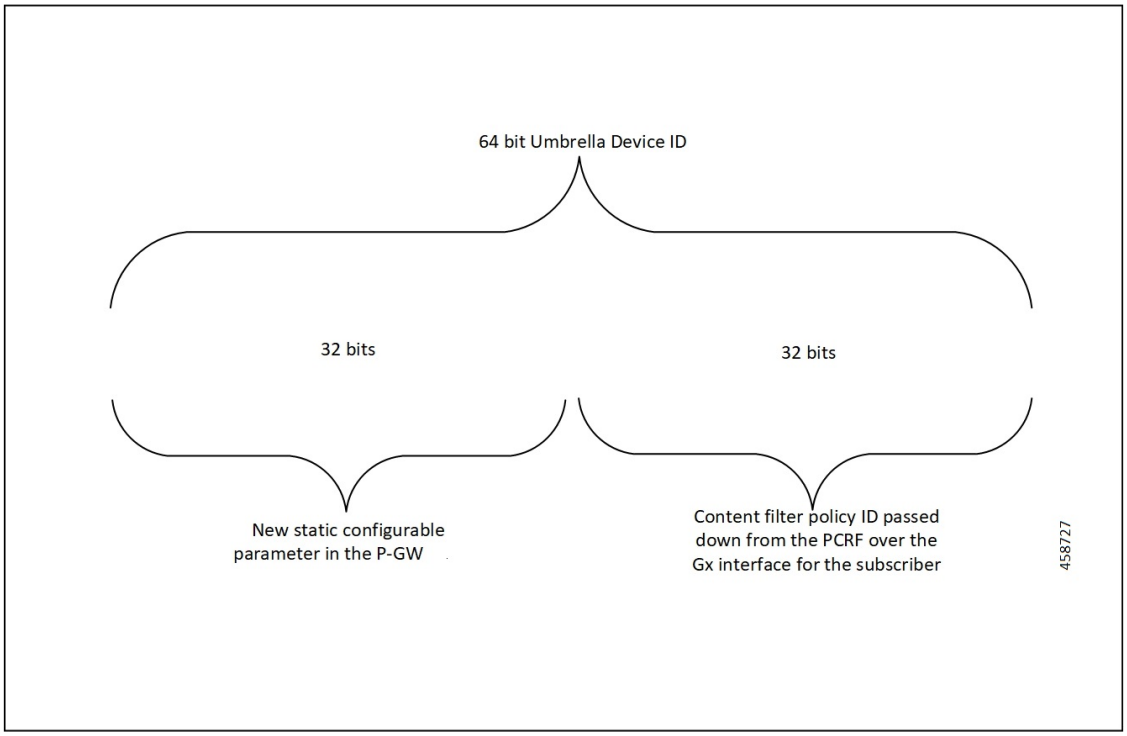
- In the EDNS0 packet, 64-bit Device ID is sent as OPT RR data.
- In the P-GW, the first (MSB) 32-bits of all Device IDs is configured as a fixed value.
- The content filter ID, which is the last (LSB) 32-bits of a subscriber’s device ID is received from the PCRF over the Gx interface.
- The P-GW concatenates the two 32-bit values to build a subscriber’s full 64-bit Device ID and displays in the subscriber’s EDNS0 queries.

As part of this feature, using CLI command you can configure the first 32 bit of **static device-id** value addition.

How it Works

New CLIs are introduced to configure and trigger the EDNS0 functionality.

Figure 1:



- To create a Device ID and send in EDNS0 query, the Content Filtering ID, which P-GW receives in Gx messages from PCRF is used. The EDNS0 packet includes the 64-bit device ID as OPT RR data.

Note The first 32 bits of all device IDs is a fixed value configured in the P-GW. The last 32 bits of a subscriber device ID is the content filter policy ID value received from the PCRF over Gx Interface.

- The CF-Policy-ID from the PCRF is received in any Gx event (CCA-I/CCA-U/RAR), when there is any change in the CF-Policy-ID, subscriber call line gets updated with the same ID. Later, based on this CF-Policy-ID, configured range gets evaluated at the time of the creation of the new flow.

Note To trigger EDNS0 encoding, it is mandatory that subscriber should get any Gx event, either of CCAI/CCAU/RAR from the PCRF and that event must contain CF policy ID AVP.

- Once CF-Policy-ID is received in Gx event for a subscriber, further on every Gx event range evaluation takes place, irrespective of the CF-Policy-ID presence in any Gx event. This allows to apply the range updates to the new flow.
- The trigger to create new flow is associated with the service-scheme configuration. Service-scheme configuration is associated with the subscriber, which is associated with the subscriber class.

Note Range evaluation is done only during the flow creation. If flow1 is ongoing and if any change in the range configuration happens, it takes effect only during the new flow creation for that subscriber.

- To create the flow associated with service scheme, association of the trigger condition and the trigger action is used. Then external-content-filtering trigger condition gets evaluated for the same flow, and associated trigger actions (edns-encoding/ip-readdressing) is taken on that flow. If no CF-Policy-ID is received in Gx event, then previous value is used.

Note When Security-profile has device-id configured instead of cf-policy-id-static-prefix, eDNS encoding is done with prefix all 00 for MSB 32 bits and PCRF received value as LSB 32 bits.

- The P-GW concatenates the two 32-bit values to build a subscriber full 64-bit Device ID for populating in the subscriber EDNS0 queries. New CLI helps to configure the first 32 bit of static device-id value.

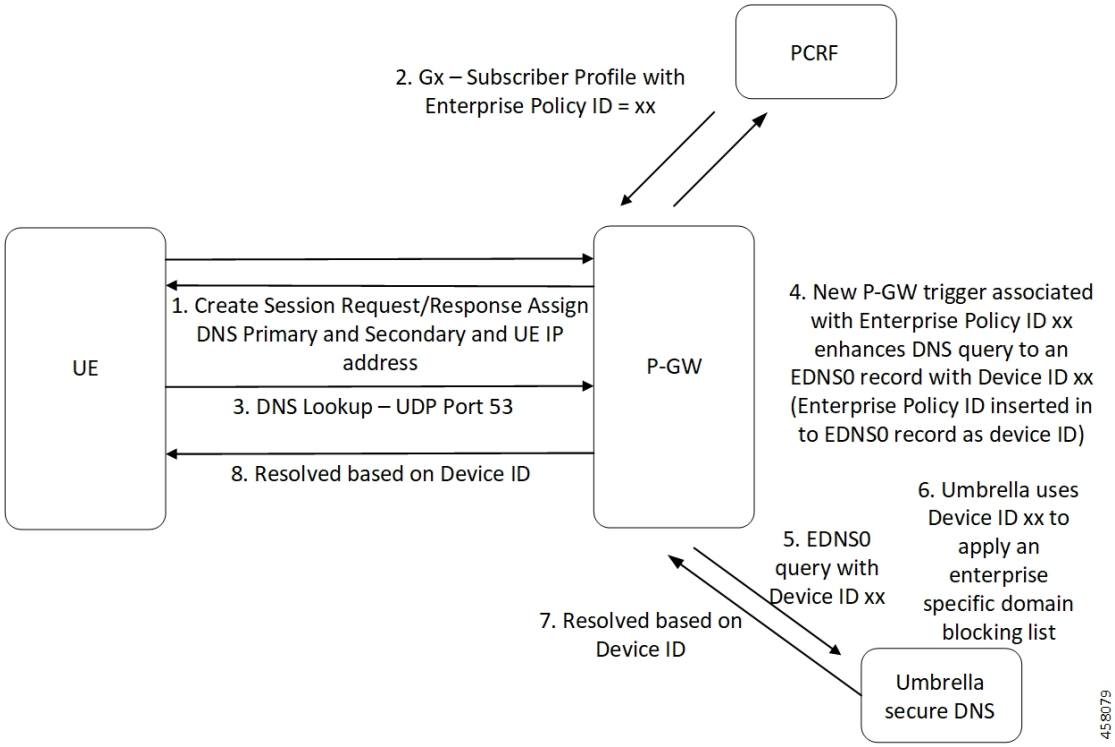
The Device ID number in the EDNS0 record allows the Umbrella DNS system to apply a custom set of domain filters for the EDNS0 queries.

Note DNS analyzer configuration is mandatory for this feature.

Process Flow

The following process flow describes about the Content Filtering enhancement to insert Device ID in EDNS0 records:

Figure 2:



EDNS over TCP

The EDNS over TCP feature supports an enterprise/group offer that allows each enterprise to have customized domain blocking through Umbrella. As part of this feature, unlike UDP, the need for extra messages and extra processing of the TCP sequence (seq) and acknowledgment (ack) numbers is required.

The TCP massager acts between the UE and EDNS Server and UE will massage the seq/ack number changes. Through this process, the UE and EDNS server is unaware of the TCP packets that are manipulated at the P-GW.

Delay Charging and Post Processing

For TCP DNS flows, if delay charging is enabled, you need to enable post processing feature in ACS.

This enables post processing of packets even if rule matching for packets is disabled. When delay charging is enabled, initial TCP handshake packets, such as the SYN and SYN/ACK, does not get processed and IP readdressing is not applied. To apply IP readdressing correctly, apply post processing rule feature, which enables the processing of initial handshake packets, and thus packets are readdressed correctly.

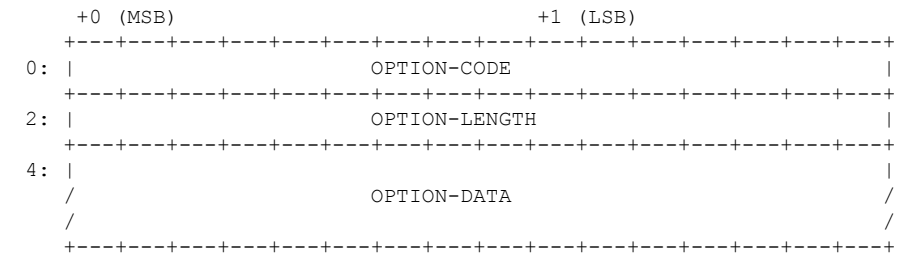
EDNS0 Packet Format

The enterprise policy ID (CF_POLICY_ID) from PCRF helps to create the Device ID. The PCRF sends the device ID to the P-GW. Adding the Device ID to the DNS packet helps in creating the EDNS0 packet. The format of EDNS0 packets is specified by RFC2671. The following are few specifics:

- Following is the structure for the fixed part of an OPT RR:

```
Field Name   Field Type     Description
-----------------------------------------------------
NAME         domain name    empty (root domain)
TYPE           u_int16_t          OPT
CLASS          u_int16_t          sender's UDP payload size
TTL            u_int32_t          extended RCODE and flags
RDLEN          u_int16_t          describes RDATA
RDATA          octet stream       {attribute, value} pairs
```

- Following is the variable part of an OPT RR encoded in its RDATA:



  - OPTION-CODE: Assigned by IANA
  - OPTION-LENGTH: Size (in octets) of OPTION-DATA
  - OPTION-DATA- Varies per OPTION-CODE

Example: If received policy-id from PCF/PCRF is “1234” and static prefix configured on P-GW is “5678”.

64-bits Device-ID will be “0000162e000004d2”.

- 0000162e -- 5678 (Decimal)
- 000004d2 -- 1234 (Decimal)

RDATA 69 42 00 0f 4f 70 65 6e 44 4e 53 00 00 16 2e 00 00 04 d2

- 6942 -- option-code
- 000f -- option-length
- 4f70656e444e53 -- OpenDNS (String)
- 0000162e -- 5678 (MSB)
- 000004d2 -- 1234 (LSB)

EDNS with IP Readdressing

The new CLI is configured within trigger action to readdress the DNS traffic to the Umbrella DNS. This CLI uses the existing readdress server list configuration from the ACS service. Readdressing of packets based on the destination IP address of the packets enables redirecting gateway traffic to configured server/port in the readdressed server list.

Behavior and Restrictions

Following are the behavior and restrictions applicable for this feature:

- Trigger Condition is evaluated at flow creation time. Any change in trigger condition in between the flow doesn't affect the existing flow but affects the new flows.
- Any change to trigger action is applicable on the same flow.
- Cases where the 'security-profile' CLI is not associated with the 'EDNS format' CLI in Trigger Action, the device-id in the outgoing EDNS packet is sent with only 32-bit CF Policy ID.
- DNS queries with type other than A, AAAA, CNAME, NS, PTR, SRV, TXT, NULL are not to be EDNS converted.
- CF Policy ID change over Gx in between inflow are not applicable for the current flows. The current flows continue to insert the CF Policy ID present at the time of flow creation.

Limitations

Following are the limitations for this feature:

- When malformed DNS packet is received by analyzer and marked invalid, packets gets EDNS encoded and readdressed as a normal DNS packet.
- When PCRF sends cf-policy-id 0 and external-content-filtering config as true in trigger condition, trigger condition does not match and encoding/readdressing does not apply.
- When there is configuration change in content-filtering range for any subscriber, it disables EDNS feature and enables the content filtering feature. EDNS disables for the next flow. To enable content filtering feature, it is mandatory to trigger the Gx event with cf policy ID from PCRF.
- If packet received with additional RR value as FFFF, the EDNS encoding is not done and marked as EDNS failure. In this case even if EDNS encoding fails readdressing happens.
- The feature does not support the interoperability with next hop and vlan ID.
- The CLI available in trigger action supports only server list configuration, It does not support single server IP or port configuration like charging action.
- Due to several limitations in the DNS Analyzer it does not support TCP Segmentation and it does not recognize multiple queries in the same data packet. These limitations affects the processing of statistics in both DNS Queries and Responses.
- EDNS encoding is implemented at the layer 4 TCP level with the following limitations:
  - If this CLI setting is not set, each segment is processed as an EDNS failed encoded packet.
  - The mechanism relies on the DNS Payload length not being corrupted/incorrect.
  - The mechanism rejects segments lower than 14 bytes in size.

Configuring EDNS0

Use the following configuration to configure Content Filtering Range, Trigger Action, Trigger Condition, edns static prefix, edns fields and edns tags under the active changing service.

```
configure
   active-charging-service service_name
   [default] content-filtering range range
      trigger-condition trigger_condition_name
         app-proto = dns
         external-content-filtering
               end
```

NOTES:

- **app-proto** = **dns** : Avoids the IP readdressing of the non-DNS traffic. If this CLI is enabled with multiline-or cli, then all DNS traffic will be EDNS encoded.
- **external-content-filtering** : Enables EDNS0 feature.When this flag is true along with the range criteria, EDNS0 feature is enabled. By default, this flag is disabled.
- **content-filtering range**: Enter start number and end number for the **cf-policy-id**. *range_values* can be integers. For example, 1-4294967295.
- If range parameter is set to 1-1000, any subscriber with a content filtering policy ID greater than or equal to 1 and lower than or equal to 1000 should use the standard content filtering functionality. And any subscriber profile with a content filter policy ID outside the range of 1-1000 can trigger the new EDNS0 functionality.
- **default** : By default, the content-filtering range is 1 to 4294967295. Any value in CF-Policy-ID AVP is considered for CF. It will not be shown by default and will be shown in verbose config. To restore default functionality, use the cli **default content-filtering range**

If the content filter policy ID for any Subscriber profile is outside the range of 1 to 1000, use the following CF policy id range CLI commands to enable the new EDNS0 functionality.

```
configure
   active-charging-service service_name
   content-filtering
        category
        range
          content-filitering range range_start_number to range_end_number
          content-filtering range 1 to 1000
          [ default ] content-filtering
          [ no ] content-filtering
       end
```

NOTES:

- **range**: Specifies policy-id range for content filtering feature.
- **content-filitering range** : Enter the starting number and ending number for the cf-policy-id range. *range_start_number* to *range_end_number* can be integers. For example, 1-4294967295.
- **no content-filitering range**: When chassi comes up, the **no content-filitering range** CLI is displayed in verbose.
- **default content-filitering range**If you configure a default content filtering range, then range configured should be between 1 to 4294967295. In this scenario CF-Policy-ID value that comes up in Gx event is considered for Content Filtering. You can view this range in both verbose and non- verbose mode.

- If you change either the minimum or maximum value, any value outside this range is for EDNS. To restore default functionality, the **default content-filtering range** CLI.

The following configuration leads the trigger action to define the EDNS format to be inserted in the EDNS packet. The following CLI also associates the security profile with the EDNS format as part of the trigger action:

```
configure
   active-charging-service service_name
      trigger-action trigger_action_name
         edns-format format_name [ security-profile ] profile_name
         flow action readdress server-list  server_list_name  [ hierarchy ] [
round-robin ][ discard-on-failure ]
            end
```

NOTES:

- **trigger-action** *trigger_action_name*: To use EDNS with IP readdressing configure the flow action CLIs in the trigger action.
- **edns-format** *format_name*: Use the EDNS format when EDNS is applied.
- **security-profile** *profile_name*: Defines the security profile configuration in the EDNS to add mapping with the Device-id.
- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin][discard-on-failure]**: Use IP readdressing to readdress the packets to the configured server Ips. This CLI in trigger action supports only server list configuration. It does not support single server IP or port configuration like charging action.

In the ACS You can configure the trigger condition and trigger action under service-scheme:

```
configure
   active-charging-service service_name
      service-scheme service-scheme_name
         trigger flow-create
          priority  number trigger-condition value trigger-action value
          end
```

NOTES: For readdressing, port configuration in server list is not mandatory. In case only readdressed server IP is configured under server-list, destination port from incoming packet is used for readdressing.

Use the following configuration to insert the CF policy ID in the EDNS:

```
configure
   active-charging-service service_name
      edns
         security-profile  security_profile cf-policy-id-static-prefix
static_prefix_value
         fields fields_name
            [ default ] tag  number cf-policy-id  payload-length ( tcp | udp
 )
            end
```

NOTES:

- **security-profile**: Security profile is used to configure the 32 MS bit static value.

- **cf-policy-id-static-prefix** *static_prefix_value*: Enter the integer value.

  The 32 bit static ID is used as MSB bytes in 64 bit device ID. If security-profile static prefix does not have any **cf-policy-id-prefix** defined, then device-id is encoded with only 32 bit **cf-policy-id**.

- **payload-length (tcp | udp)**: Specifies the RR UDP or TCP Payload-length value. You can enter the value ranging from 512 to 4096.

- **tcp** : Specifies the RR UDP-Payload-Length value for TCP.

- **udp** : Specifies RR UDP-Payload-Length value for UDP.

Note If the optional **udp** or **tcp** CLI **payload-length** field is not configured, a default value of 1280 is added into the EDNS **Additional RR CLASS/UDP Payload size** field.

- **default tag** *number* **cf-policy-id** : Resets the UDP or TCP payload-length field to an unconfigured default value of 1280.

Note If you enter a **default tag** *number* on a tag number that is not configured, the following error message is displayed:

```
Failure: Cannot reset the payload-length value as no such tag value
configured with cf-policy-id in edns field.
```

Sample Configuration

Following is the sample configuration for configuring the EDNS packets:

```
config
  active-charging service ACS
    content-filtering range 1 to 1000
    edns
      security-profile SP1 cf-policy-id-static-prefix 999999
      fields CFPiD
        tag 1 cf-policy-id
        #exit
      format FP1
        fields CFPiD encode
        #exit
      #exit
   readdress-server-list SL
     server 40.40.40.3
     server 4001::3
   #exit
   ruledef dns_route
     udp either-port = 53
     rule-application routing
   #exit
   rulebase RB1
      route priority 100 ruledef dns_route analyzer dns
   #exit
```

```
   trigger-action TA1
      edns format FP1 security-profile SP1
      flow action readdress server-list SL
   #exit
   trigger-condition TC1
      app-proto = dns
      external-content-filtering
   #exit
   service-scheme SS1
      trigger flow-create
      priority 1 trigger-condition TC1 trigger-action TA1
    #exit
   subs-class SC1
      rulebase = RB1
   #exit
   subscriber-base SB1
      priority 1 subs-class SC1 bind service-scheme SS1
   #exit
#exit
```

Viewing Configured and Unconfigured Payload-length Values

show config | grep tag

Use the following sample configuration to view configured tag number cf-policy-id payload-length values:

```
[local]qvpc-si# show config | grep tag
        tag 1 cf-policy-id payload-length udp 1300
```

show config verbose | grep tag

Use the following sample configuration to view the configured and unconfigure tag number cf-policy-id payload-length values.

```
[local]qvpc-si# show config verbose | grep tag
         tag 1 cf-policy-id payload-length udp 1300 tcp 1280
```

show configuration active-charging service name acs v | grep range

Use the sample configuration to view the EDNS statistics:

```
[local]qvpc-si(config-acs)#  no content-filtering range
        [local]qvpc-si# show configuration active-charging service name
         acs v | grep range no content-filtering range
        [local]qvpc-si#
```

Monitoring and Troubleshooting

Following are the show commands and outputs that enhance content filtering support to Insert device ID in EDNS0 records.

Show Commands and Outputs

Following are the show commands and outputs modified to show EDNS statistics and counters.

- **show active-charging trigger-condition name <tc>**: output is modified to include "app-proto = dns" and "external-content-filtering".
- **show active-charging trigger-action name <ta>**: output is modified to include "IP-addressing" and "edns encode".
- **show active-charging analyzer statistics name dns**: output is modified to include the "EDNS Encode Success Bytes" in the "EDNS Over UDP" section.
- **show active-charging session full all**: output is modified to include "GX CF Policy ID".
- **show active-charging service all**: output is modified to include "Range", "Start Value", and "End Value".
- **show active-charging subscribers full imsi <IMSI>**: output is modified to include the following parameters in the EDNS statistics per subscriber.
  - DNS-to-EDNS Uplink Pkts
  - DNS-to-EDNS Uplink Bytes
  - GX CF Policy ID

Note

- EDNS Encode success Bytes have extra added bytes added to convert the packet.
- DNS-to-EDNS Uplink Bytes have complete packet length along with extra bytes added.