Device ID in EDNS0 Records

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- How it Works, on page 2
- Configuring EDNS Format and Trigger Action, on page 5
- Monitoring and Troubleshooting, on page 7

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product (s) or Functional Area	5G-UPF
Applicable Platforms	VPC-SI SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	*UCC 5G UPF Configuration and Administration Guide*

Revision History

Table 2: Revision History

Revision Details	Release
TCP support is added.	2021.02.1
First introduced.	2021.01.2

Feature Description

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

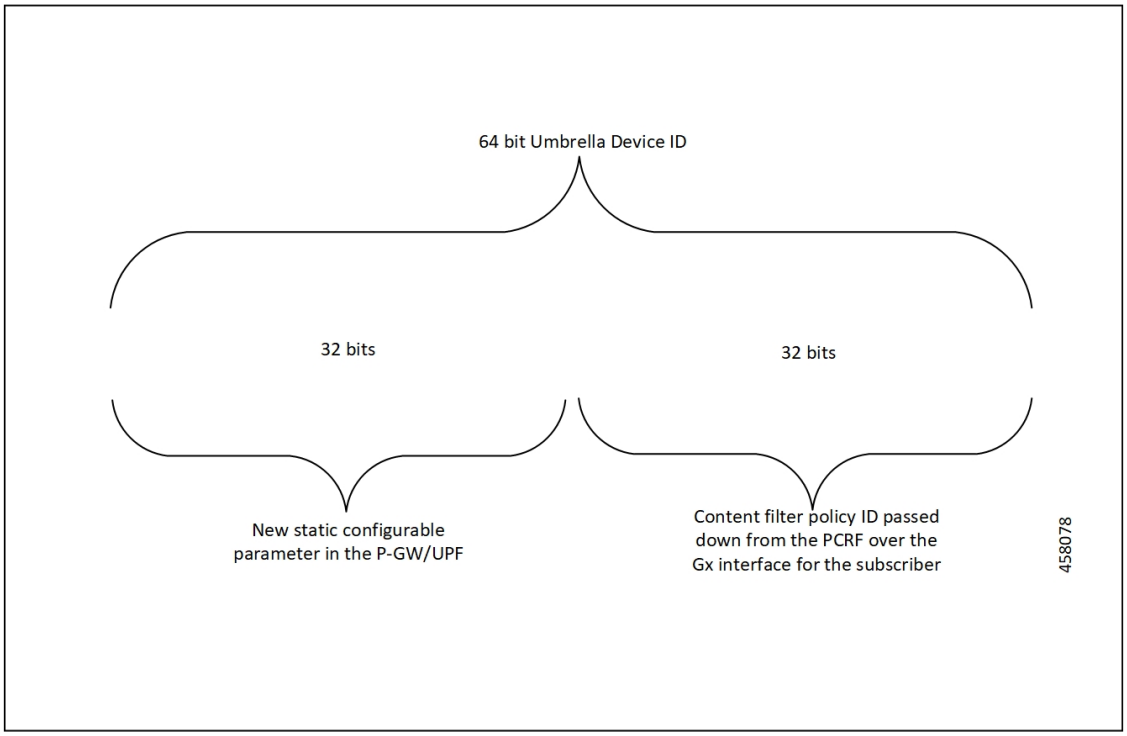
- The UPF must reformat a subscriber DNS request into an EDNS0 request, and.
- The UPF must include an Umbrella “Device ID” in the EDNS0 packet so that the Umbrella DNS resolver can use the Device ID to apply the domain filter associated or configured with the Device ID in the EDNS0 packet.

Presently, the Session Management Function (SMF) receives the domain filtering policy ID from PCRF/PCF. The SMF passes the domain filtering policy ID to the User Plane Function (UPF) in the Subscriber Parameters. The UPF uses the domain filtering policy ID to apply domain filtering functionality to the subscriber.

How it Works

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

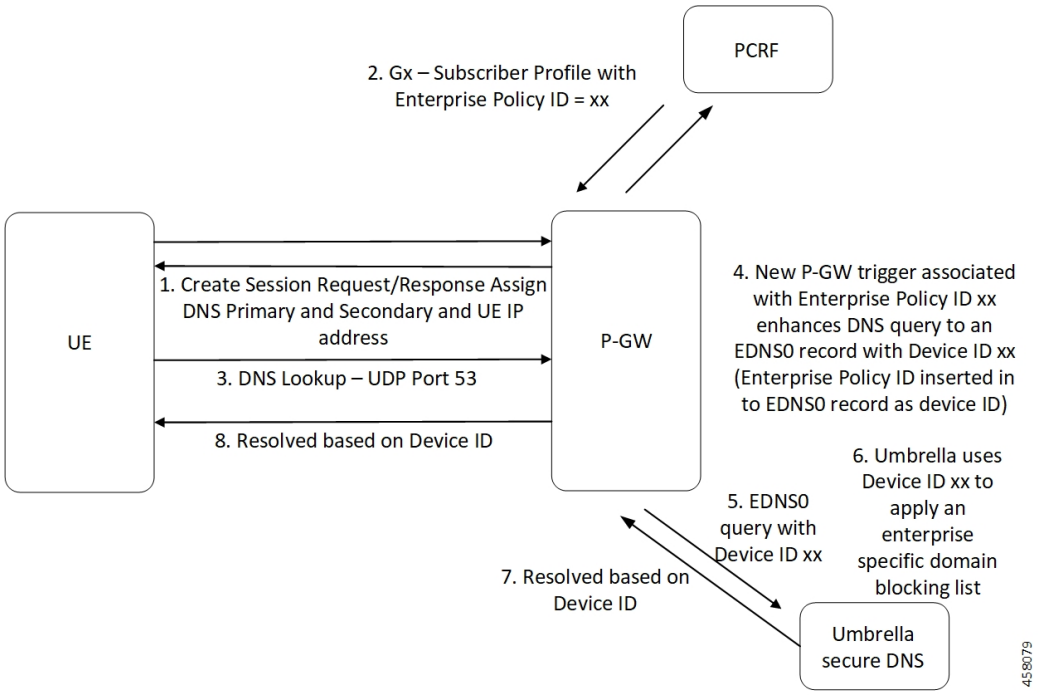
The EDNS0 packet receives the 64-bit device ID as OPT RR data. The first 32 bits of all device IDs is a fixed value that is configured in the UPF. The last 32 bits of a subscriber device ID is the content filter ID value received from the PCRF/PCF. The UPF concatenates the two 32-bit values to build 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. If you don’t configure the 32-bit static prefix CLI, the outgoing packet shows the device-id = 32-bit CF PolicyID.



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.

Process Flow

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



EDNS0 Packet Format

The enterprise policy ID (CF_POLICY_ID) from PCRF helps to create the Device ID. The SMF sends the device ID to the UPF. 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:

```
     +0 (MSB)                            +1 (LSB)
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 0: |                         OPTION-CODE                           |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
 2: |                         OPTION-LENGTH                         |
```

```
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
4: |                                                               |
   /                       OPTION-DATA                             /
   /                                                               /
   +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

- 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 UPF 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)

EDNS0 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.
- Neither CF nor EDNS is enforced when the CF Policy ID range is defined but Service-schema is not defined, or the Trigger condition pertaining to EDNS is not configured.
- If no CF Policy ID is received from Gx, range check is not performed, and content filtering works as defined in rule base.
- 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.

Limitation

Following are the limitations for this feature:

- The feature doesn't support the EDNS response packet reformat.
- The UPF must be able to include the IMSI MSISDN tag value in the EDNS0 queries. This feature doesn't support the encrypted IMSI in EDNS0 packet. This feature also doesn't support the following configuration on the EDNS fields currently.

```
configure
   active-charging-service  service_name
      edns
         fields  fields_name
            tag default device-id
            tag 101 imsi encrypt
            tag 102 pgw-address
            end
```

Configuring EDNS Format and Trigger Action

Use the following configuration to enable DNS filtering:

```
configure
   active-charging-service service_name
      content-filtering range start_min_val to end_max_val
```

If the range parameter is set from 10 through 1000, any subscriber profile with a content filter policy ID from 10 through 1000 uses the standard content filtering functionality. Any subscriber profile with a content filter policy ID higher than 1000 or lower than 10 triggers the new EDNS0 functionality.

Use the following configuration to disable DNS filtering:

```
configure
   active-charging-service service_name
      no content-filtering range
```

When DNS filtering is disabled, the standard content filtering policies resume as configured or as received from the PCF.

Use the following configuration to configure the EDNS packet action and format under the active-charging service:

```
configure
   active-charging-service service_name
      trigger-condition trigger_condition_name
         external-content-filtering
```

```
        app-proto = dns
      end
```

NOTES:

- **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.
- **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 is EDNS encoded.

The following configuration leads the trigger action to define the EDNS format to be inserted in the EDNS packet:

```
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*: Enables you to 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.

Note Device ID in EDNS0 Records feature supports multiple security profiles.

- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin] [discard-on-failure]**: Associates the EDNS with IP readdressing. Use IP readdressing to readdress the packets to the configured server IPs. This CLI in trigger action supports only server list configuration. It doesn't support single-server IP or port configuration like charging action.

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

```
configure
  active-charging-service service_name
    edns
      fields fields_name
        tag { val { imsi | msisdn | cf-policy-id }}
        end
```

To configure the 32 MS bit, static value is provided at the EDNS level with the security profile.

```
security-profile security_profile cf-policy-id-static-prefix value
```

Use the following configuration to insert a new tag specifying the payload length:

```
tag default payload-length [ tcp | udp ] value
```

Value range: 576–4096

Sample Configuration

Following is the sample configuration for configuring the EDNS packets:

```
configure
active-charging service ACS
content-filtering range 10 to 100
ruledef dns-port
udp either-port = 53
tcp either-port = 53
multi-line-or all-lines
rule-application routing
#exit
 readdress-server-list re_adr_list_ta
  server 209.165.202.141
  server 2001::14
  server 209.165.202.142
  server 2001::15
#exit
rulebase starent
route priority 20 ruledef dns-port analyzer dns
#exit
edns
security-profile sec_profile cf-policy-id-static-prefix 123456
fields test_fields
tag 26946 cf-policy-id
#exit
format test_format
fields test_fields encode
#exit
#exit
trigger-action TA1
edns format test_format security-profile sec_profile
flow action readdress server-list re_adr_list_ta hierarchy
#exit
trigger-condition TC1
external-content-filtering
app-proto = dns
#exit
service-scheme SS1
trigger flow-create
priority 1 trigger-condition TC1 trigger-action TA1
#exit
subs-class SC1
rulebase = starent
multi-line-or all-lines
#exit
subscriber-base SB1
priority 1 subs-class SC1 bind service-scheme SS1
exit
end
```

Monitoring and Troubleshooting

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

Show Commands and Outputs

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

- **show user-plane-service inline-services info**

```
CF Range: Enabled <<<<
  Start Value:  1 <<<<
  End Value:    1000 <<<
```

- **show user-plane-service statistics analyzer name dns**: output is modified to include the "EDNS Response Received" in both "EDNS Over UDP" and "EDNS Over TCP" sections.
- **show subscribers user-plane-only full callid**: output is modified to include the following parameters in the EDNS statistics per subscriber.
  - DNS-to-EDNS Uplink Pkts
  - DNS-to-EDNS Uplink Bytes
  - EDNS Response Received
- **show user-plane-service edns all**

```
Fields:
    Fields Name: fields_1
    tag 26946 cf-policy-id

    Fields Name: fields_2
    tag 2001 imsi
    tag 2002 msisdn
    tag 26946 cf-policy-id

    Format:
    Format Name: format_1
    fields fields_1 encode

    Format Name: format_2
    fields fields_2 encode

    Security-profile Name: high
    CF Prefix Policy ID: 1234
```

Use the following show commands to view the Trigger Action statistics:

- **show user-plane-service statistics trigger-action all**
- **show user-plane-service statistics trigger-action name** *trigger_action_name*
- **show user-plane-service trigger-condition all**

```
Trigger-Condition: TC1
       External-content-filtering : Enabled
       App-proto : dns
       Multi-line-OR All lines : Disabled
```

- **show user-plane-service trigger-action all**

```
Trigger-Action: TA1
       HTTP Response Based TRM      : none
       HTTP Response Based Charging : none
       Throttle Suppress            : Disabled
```

```
Flow Recovery                : Disabled
Traffic Optimization         : Disabled
Step Up GBR                  : Disabled
Step Down GBR                : Disabled
TCP Acceleration             : Disabled
TCP Acceleration Threshold   : Disabled
Service-Chain                : none
UP-Service-Chain             : none
EDNS-Encode                  : Enabled
Flow-IP-Readdressing         : Enabled
```

Bulk Statistics

The following bulk statistics are available in support of the Device ID in EDNS0 Records feature:

SCHEMA: ECS	
Statistics	**Description**
ecs-dns-udp-edns-encode-succeed	The count of DNS to EDNS converted packets over UDP
ecs-dns-udp-edns-encode-failed	The count of failed DNS to EDNS conversions over UDP
ecs-dns-udp-edns-encode-response	The count of responses received for EDNS query over UDP
ecs-dns-tcp-edns-encode-succeed	The count of DNS to EDNS converted packets over TCP
ecs-dns-tcp-edns-encode-failed	The count of failed DNS to EDNS conversions over TCP
ecs-dns-tcp-edns-encode-response	The count of responses received for EDNS query over TCP