

Behavior of IDFT Feature in StarOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure IDFT](#)

[Problem](#)

[Analysis](#)

[Solution](#)

Introduction

This document describes the behavior of the Indirect Forwarding Tunnel (IDFT) Feature in Control and User Plan Separation (CUPS) and legacy/baremetal setup.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- StarOS
- Serving Gateway(SGW) function related to IDFT

Components Used

The information in this document is based on the SGW - 21.25.9 (in legacy and CUPS) software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

SGW supports IDFT procedures for creation and deletion, which are applicable for Pure-S and Collapsed calls with multi-Packet Data Network (PDN) and multi-bearers. This feature is applicable for IDFT support with or without SGW relocation and collision scenarios.

The IDFT feature supports these functionalities:

- Create IDFT request for Collapsed, Pure-S, a combination of Collapsed and Pure-S multi-PDN calls with multiple bearers.
- Data transfer on downlink and uplink IDFT bearers.
- Deletion of IDFT request from Mobility Management Engine (MME). Also, timer-based deletion of IDFT bearer after expiration of a default value of 100 seconds, if the MME does not send an IDFT request for deletion.
- Deletion of IDFT PDN, which includes Clear/Delete subscribers from MME/P-GW, when normal PDN goes down.
- Sx-Path Failure Handling in case of Pure-S and collapsed calls at the time of IDFT Active/IDFT Create Sx-Pending state.
- Message interaction and collision at the time of IDFT PDN establishment or deletion with any other procedure.
- S11/S5 and Sx-Path Failure Handling on non-IDFT PDN is now supported when IDFT PDN is Active.

Configure IDFT

This section describes the CLI commands available in support of the IDFT feature.

On Control Plane, use these CLI commands to enable or disable the IDFT feature.

```
configure
  context context_name
    sgw-service service_name
      [ default | no ] egtp idft-support
    end
```

Problem

SGW Processes the Create IDFT Request even when the feature is off. This behavior is seen in legacy/baremetal nodes.

Here is the IDFT configuration present in the node:

```
sgw-service SGW-SVC
  accounting context EPC gtp group default
  accounting mode gtp
  associate ingress egtp-service S11-SGW
  associate egress-proto gtp egress-context EPC egtp-service S5-S8-SGW
```

no egtp idft-support

----> IDFT

feature is off in the node.

Analysis

The traces and debug logs are taken through simulation of this scenario in the lab and the behavior of Create IDFT Request and Create IDFT Response is seen.

1) MME sends the Create IDFT Request to SGW.

The screenshot shows a Wireshark packet capture of a GTPv2 message. The selected packet (13) is a 'Create Indirect Data Forwarding Tunnel Request' sent from MME (192.168.1.100) to SGW (192.168.1.100). The packet details show the following structure:

- Message Type: Create Indirect Data Forwarding Tunnel Request (166)
- Message Length: 30
- Tunnel Endpoint Identifier: 0x80000005 (2147516421)
- Sequence Number: 0x000002 (2)
- Spare: 0
- Bearer Context: [Grouped IE]
 - IE Type: Bearer Context (93)
 - IE Length: 18
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - EPS Bearer ID (EBI) : 5
 - Fully Qualified Tunnel Endpoint Identifier (F-TEID) : eNodeB GTP-U interface for DL data forwarding, TEID/GRE Key: 0x200111a0, IPv4 192.168.1.106

2) SGW processes the request and sends the response Create IDFT Response back to MME with the cause 'Request accepted'.

The screenshot shows a Wireshark packet capture of a GTPv2 message. The selected packet (15) is a 'Create Indirect Data Forwarding Tunnel Response' sent from SGW (192.168.1.100) to MME (192.168.1.100). The packet details show the following structure:

- Message Length: 81
- Tunnel Endpoint Identifier: 0x10010001 (268500993)
- Sequence Number: 0x000002 (2)
- Spare: 0
- Cause : Request accepted (16)
 - IE Type: Cause (2)
 - IE Length: 2
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - Cause: Request accepted (16)
 - 0000 0... = Spare bit(s): 0
 - 0... = PCE (PDN Connection IE Error): False
 -0 = BCE (Bearer Context IE Error): False
 -0 = CS (Cause Source): Originated by node sending the message
- Bearer Context : [Grouped IE]
 - IE Type: Bearer Context (93)
 - IE Length: 63
 - 0000 = CR Flag: 0
 - 0000 = Instance: 0
 - EPS Bearer ID (EBI) : 5
 - Cause : Request accepted (16)
 - IE Type: Cause (2)
 - IE Length: 2
 - 0000 = CR flag: 0
 - 0000 = Instance: 0
 - Cause: Request accepted (16)
 - 0000 0... = Spare bit(s): 0
 - 0... = PCE (PDN Connection IE Error): False
 -0 = BCE (Bearer Context IE Error): False
 -0 = CS (Cause Source): Originated by node sending the message
 - Fully Qualified Tunnel Endpoint Identifier (F-TEID) : SGW GTP-U interface for data forwarding, TEID/GRE Key: 0x80010005, IPv4 10.1.4.1
 - Fully Qualified Tunnel Endpoint Identifier (F-TEID) : SGW GTP-U interface for data forwarding, TEID/GRE Key: 0x80010005, IPv4 10.1.4.1
 - Fully Qualified Tunnel Endpoint Identifier (F-TEID) : SGW GTP-U interface for data forwarding, TEID/GRE Key: 0x80010005, IPv4 10.1.4.1
 - Fully Qualified Tunnel Endpoint Identifier (F-TEID) : SGW GTP-U interface for data forwarding, TEID/GRE Key: 0x80010005, IPv4 10.1.4.1

In this Create IDFT Response it is expected that SGW must send Create IDFT Response with the cause 'Data Forwarding not supported' as this feature is disabled in the configuration.

The same configuration is used in the CUPS setup:

1) MME sends the Create IDFT Request to SGW.

```

# 0.113_2022-07-15 08:05:09.159000 192.168.1.100 10.1.10.1 GTPv2 Request accepted,Request accepted Modify Bearer Response
5 0.020_2022-07-15 08:05:09.174000 10.1.10.1 192.168.1.100 GTPv2 Echo request Echo response
6 0.345_2022-07-15 08:05:09.519000 192.168.1.108 10.1.20.3 GTP Create Indirect Data Forwarding Tunnel...
7 0.000_2022-07-15 08:05:09.519000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
8 26.20_2022-07-15 08:05:35.726000 192.168.1.100 10.1.10.1 GTPv2 Data forwarding not supported Create Indirect Data Forwarding Tunnel...
9 0.000_2022-07-15 08:05:35.726000 10.1.10.1 192.168.1.100 GTPv2 Echo request Echo response
10 3.792_2022-07-15 08:05:39.518000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
11 0.000_2022-07-15 08:05:39.518000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
12 0.074_2022-07-15 08:05:39.592000 10.1.20.3 192.168.1.108 GTP Modify Bearer Request Modify Bearer Response
13 0.001_2022-07-15 08:05:39.593000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
14 29.92_2022-07-15 08:06:09.517000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
15 0.000_2022-07-15 08:06:09.517000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
16 2.002_2022-07-15 08:06:11.519000 10.1.10.1 192.168.1.100 GTPv2 Request accepted,Request accepted Modify Bearer Response
17 0.610_2022-07-15 08:06:12.129000 192.168.1.100 10.1.10.1 GTPv2 Request accepted,Request accepted Modify Bearer Response
18 0.002_2022-07-15 08:06:12.131000 10.1.10.1 192.168.1.100 GTPv2 Request accepted,Request accepted Modify Bearer Response

```

> Frame 8: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 10.1.10.1
> User Datagram Protocol, Src Port: 10000, Dst Port: 2123
GPRS Tunneling Protocol V2
 > Flags: 0x48
 > Message Type: Create Indirect Data Forwarding Tunnel Request (166)
 > Message Length: 30
 > Tunnel Endpoint Identifier: 0x80000006 (2147483654)
 > Sequence Number: 0x000002 (2)
 > Spare: 0
 > Bearer Context : [Grouped IE]
 > IE Type: Bearer Context (93)
 > IE Length: 18
 > 0000 = CR flag: 0
 > 0000 = Instance: 0
 > EPS Bearer ID (EBI) : 5
 > Fully Qualified Tunnel Endpoint Identifier (F-TEID) : eNodeB GTP-U interface for DL data forwarding, TEID/GRE Key: 0x20010089, IPv4 192.168.1.106

2) SGW processes the request and sends the response Create IDFT Response back to MME with the cause 'Data Forwarding not supported'.

```

7 0.000_2022-07-15 08:05:09.519000 10.1.20.3 192.168.1.108 GTP Echo response
8 26.20_2022-07-15 08:05:35.726000 192.168.1.100 10.1.10.1 GTPv2 Create Indirect Data Forwarding Tunnel...
9 0.000_2022-07-15 08:05:35.726000 10.1.10.1 192.168.1.100 GTPv2 Data forwarding not supported Create Indirect Data Forwarding Tunnel...
10 3.792_2022-07-15 08:05:39.518000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
11 0.000_2022-07-15 08:05:39.518000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
12 0.074_2022-07-15 08:05:39.592000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
13 0.001_2022-07-15 08:05:39.593000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
14 29.92_2022-07-15 08:06:09.517000 192.168.1.108 10.1.20.3 GTP Echo request Echo response
15 0.000_2022-07-15 08:06:09.517000 10.1.20.3 192.168.1.108 GTP Echo request Echo response
16 2.002_2022-07-15 08:06:11.519000 10.1.10.1 192.168.1.100 GTPv2 Modify Bearer Request Modify Bearer Response
17 0.610_2022-07-15 08:06:12.129000 192.168.1.100 10.1.10.1 GTPv2 Modify Bearer Request Modify Bearer Response
18 0.002_2022-07-15 08:06:12.131000 10.1.10.1 192.168.1.100 GTPv2 Request accepted,Request accepted Modify Bearer Response

```

> Frame 9: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 10.1.10.1, Dst: 192.168.1.100
> User Datagram Protocol, Src Port: 2123, Dst Port: 10000
GPRS Tunneling Protocol V2
 > Flags: 0x48
 > Message Type: Create Indirect Data Forwarding Tunnel Response (167)
 > Message Length: 14
 > Tunnel Endpoint Identifier: 0x10010001 (268500993)
 > Sequence Number: 0x000002 (2)
 > Spare: 0
 > Cause : Data forwarding not supported (106)
 > IE Type: Cause (2)
 > IE Length: 2
 > 0000 = CR flag: 0
 > 0000 = Instance: 0
 > Cause: Data forwarding not supported (106)
 > 0000 0... = Spare bit(s): 0
 >0. = PCE (PDN Connection IE Error): False
 >0 = BCE (Bearer Context IE Error): False
 >0 = CS (Cause Source): Originated by node sending the message

From the admin guide, to enable this feature you need to perform these steps:
On Control Plane, use these CLI commands to enable or disable the IDFT feature.

configure

```

context context_name

sgw-service service_name

[ default | no ] egtp idft-support

end

```

If you follow these steps in legacy to enable/disable the service, you cannot see any options to toggle it.

```
[sgw]TITAN-ULTRA-001(config-sgw-service)# egtp
```

cause-code - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
modify-bearer-req - Configuration related to handling Modify Bearer Request

```
[sgw]TITAN-ULTRA-001(config-sgw-service)# no egtp
```

cause-code - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
modify-bearer-req - Configuration related to handling Modify Bearer Request

When you try to enable/disable it in the CUPS setup, it shows the option to toggle it.

```
[SAEGW]saegw-cpl(config-sgw-service)# egtp
```

cause-code - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
idft-support - Enable/Disable the IDFT Feature for CUPS. By default, it is disabled
modify-bearer-req - Configuration related to handling Modify Bearer Request

```
[SAEGW]saegw-cpl(config-sgw-service)# egtp
```

cause-code - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
idft-support - Enable/Disable the IDFT Feature for CUPS. By default, it is disabled
modify-bearer-req - Configuration related to handling Modify Bearer Request

Solution

The reason for this behavior is described here:

Legacy behavior:

- There was no CLI in legacy to control IDFT behavior.
- IDFT is always supported in legacy code.

```
[local]ESC-CP# show license information
Tuesday July 12 02:30:39 UTC 2022
Session Limits:
      Sessions  Session Type
      -
      120000    HA
      100000    GGSN
      120000    ECS
      100000    Integrated Content Filtering Service
      100000    Application Detection and Control
      100000    PGW
      100000    SGW
      100000    SAE GW Bundle
[saegw]ESC-CP(config-sgw-service)# egtp
cause-code      - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
modify-bearer-req - Configuration related to handling Modify Bearer Request
```

CUPS behavior:

- The CLI is license controlled, that is, it is available only with a CUPS license.
- It can be enabled/disabled in CUPS.

```
[local]ESC-CP# show license information
Tuesday July 12 02:36:59 UTC 2022
Session Limits:
      Sessions  Session Type
      -
      10000     HA
      100000    GGSN
      2000      ECS
      1000      Integrated Content Filtering Service
      1000      Application Detection and Control
      1000      PGW
      1000      SGW
      1000      SAE GW Bundle
      1000      CUPS SAEGW CP Bundle 1K/10k Sessions for ASR5k/QVPC
[saegw]ESC-CP(config-sgw-service)# egtp
cause-code      - Configuration to related to handling failure response from peer
change-notification-req - Configuration related to handling change notification request
idft-support    - Enable/Disable the IDFT Feature for CUPS. By default it is disabled
modify-bearer-req - Configuration related to handling Modify Bearer Request
```