

# Comportement de la fonctionnalité IDFT dans StarOS

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer IDFT](#)

[Problème](#)

[Analyse](#)

[Solution](#)

---

## Introduction

Ce document décrit le comportement de la fonctionnalité de tunnel de transfert indirect (IDFT) dans le contrôle et la séparation du plan utilisateur (CUPS) et la configuration héritée/sans système d'exploitation.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- StarOS
- Fonction SGW (Serving Gateway) associée à IDFT

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles et matérielles SGW - 21.25.9 (dans les versions héritées et CUPS).

The information in this document was created from the devices in a specific lab environment. Tous les dispositifs utilisés dans ce document ont démarré par une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

SGW prend en charge les procédures IDFT pour la création et la suppression, qui sont

applicables aux appels Pure-S et aux appels condensés avec un réseau de données à paquets multiples (PDN) et des supports multiples. Cette fonctionnalité est applicable à la prise en charge IDFT avec ou sans scénarios de déplacement et de collision SGW.

La fonction IDFT prend en charge les fonctionnalités suivantes :

- Créez une requête IDFT pour les appels Pure-S, réduits, une combinaison d'appels Pure-S et d'appels Pure-S multiPDN avec plusieurs supports.
- Transfert de données sur les supports IDFT de liaison descendante et de liaison montante.
- Suppression de la requête IDFT du moteur de gestion de la mobilité (MME). En outre, la suppression temporisée du support IDFT après l'expiration d'une valeur par défaut de 100 secondes, si le MME n'envoie pas de requête IDFT pour suppression.
- Suppression du PDN IDFT, qui inclut les abonnés Clear/Delete de MME/P-GW, lorsque le PDN normal tombe en panne.
- Traitement des échecs de Sx-Path en cas d'appels Pure-S et réduits au moment de l'état IDFT Active/IDFT Create Sx-Pending.
- Interaction et collision du message au moment de l'établissement ou de la suppression du PDN IDFT avec toute autre procédure.
- La gestion des défaillances de S11/S5 et de Sx-Path sur un PDN non IDFT est désormais prise en charge lorsque le PDN IDFT est actif.

## Configurer IDFT

Cette section décrit les commandes CLI disponibles pour la prise en charge de la fonction IDFT.

Dans le plan de contrôle, utilisez ces commandes CLI pour activer ou désactiver la fonction IDFT.

```
configure
```

```
context context_name
```

```
sgw-service service_name
```

```
[ default | no ] egtp idft-support
```

```
end
```

## Problème

SGW traite la requête Create IDFT même lorsque la fonction est désactivée. Ce comportement est observé dans les noeuds hérités/sans système d'exploitation.

Voici la configuration IDFT présente dans le noeud :

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

## Analyse

Les traces et les journaux de débogage sont obtenus par simulation de ce scénario dans les travaux pratiques et le comportement des commandes Create IDFT Request et Create IDFT Response est observé.

1) MME envoie la requête Create IDFT à SGW.

The image shows a Wireshark capture of a GTPv2 message. The packet list pane shows a 'Create Indirect Data Forwarding Tunnel Request' (IDFT) from 192.168.1.100 to 10.1.17.1. The packet details pane shows the following structure:

- Frame 13: 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: 10.1.17.1
- 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: 0x00000005 (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

The packet bytes pane shows the raw data in hexadecimal and ASCII format.

2) SGW traite la demande et renvoie la réponse Create IDFT Response à MME avec la cause « Request accept » (Demande acceptée).

11	0.065	2022-07-11 10:49:09.238000	192.168.1.100	10.1.17.1	GTPv2		Modify Bearer Request
12	0.000	2022-07-11 10:49:09.238000	10.1.17.1	192.168.1.100	GTPv2	Request accepted,Request accepted	Modify Bearer Response
13	0.49	2022-07-11 10:49:19.736000	192.168.1.100	10.1.17.1	GTPv2		Create Indirect Data Forwarding Tunnel Request
14	0.001	2022-07-11 10:49:19.737000	10.1.17.1	192.168.1.100	GTPv2	Request accepted,Request accepted	Create Indirect Data Forwarding Tunnel Response
15	11.18	2022-07-11 10:49:30.924000	192.168.1.100	10.1.17.1	GTPv2		Modify Bearer Request
16	0.001	2022-07-11 10:49:30.925000	10.1.4.1	192.168.1.100	GTP		End Marker
17	0.000	2022-07-11 10:49:30.925000	10.1.17.1	192.168.1.100	GTPv2	Request accepted,Request accepted	Modify Bearer Response
18	0.064	2022-07-11 10:49:30.989000	192.168.1.100	10.1.4.1	GTP		End Marker
19	0.000	2022-07-11 10:49:30.989000	10.1.4.1	192.168.1.106	GTP		End Marker
20	30.14	2022-07-11 10:50:01.131000	10.1.10.1	10.1.9.1	GTPv2		Echo Request

```

Message Length: 81
Tunnel Endpoint Identifier: 0x10010001 (268508993)
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
  
```

Dans cette réponse Create IDFT, SGW doit envoyer une réponse Create IDFT avec la cause « Data Forwarding not supported », car cette fonctionnalité est désactivée dans la configuration.

La même configuration est utilisée dans la configuration CUPS :

1) MME envoie la requête Create IDFT à SGW.

4	0.113	2022-07-15 08:05:09.134000	192.168.1.100	10.1.10.1	GTPv2		Modify Bearer Request
5	0.020	2022-07-15 08:05:09.174000	10.1.10.1	192.168.1.100	GTPv2	Request accepted,Request accepted	Modify Bearer Response
6	0.345	2022-07-15 08:05:09.519000	192.168.1.108	10.1.20.3	GTP		Echo request
7	0.000	2022-07-15 08:05:09.519000	10.1.20.3	192.168.1.108	GTP		Echo response
8	26.26	2022-07-15 08:05:35.726000	192.168.1.100	10.1.10.1	GTPv2		Create Indirect Data Forwarding Tunnel Request
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 Response
10	3.792	2022-07-15 08:05:39.518000	192.168.1.108	10.1.20.3	GTP		Echo request
11	0.000	2022-07-15 08:05:39.518000	10.1.20.3	192.168.1.108	GTP		Echo response
12	0.074	2022-07-15 08:05:39.592000	10.1.20.3	192.168.1.108	GTP		Echo request
13	0.001	2022-07-15 08:05:39.593000	192.168.1.108	10.1.20.3	GTP		Echo response
14	29.92	2022-07-15 08:06:09.517000	192.168.1.108	10.1.20.3	GTP		Echo request
15	0.000	2022-07-15 08:06:09.517000	10.1.20.3	192.168.1.108	GTP		Echo response
16	2.002	2022-07-15 08:06:11.519000	10.1.10.1	192.168.1.100	GTPv2		Echo Request
17	0.610	2022-07-15 08:06:12.129000	192.168.1.100	10.1.10.1	GTPv2		Modify Bearer Request
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) on interface 0
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 traite la demande et renvoie la réponse Create IDFT Response à MME avec la cause « Data Forwarding not supported ».



change-notification-req - Configuration related to handling change notification request

modify-bearer-req - Configuration related to handling Modify Bearer Request

Lorsque vous essayez de l'activer/désactiver dans la configuration CUPS, il affiche l'option permettant de le basculer.

```
[SAEGW]saegw-cp1(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-cp1(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

La raison de ce comportement est décrite ici :

Comportement hérité :

- Il n'y avait pas d'interface de ligne de commande pour contrôler le comportement IDFT.
- IDFT est toujours pris en charge dans le code hérité.

```
[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
```

## Comportement de CUPS :

- L'interface de ligne de commande est contrôlée par licence, c'est-à-dire qu'elle est disponible uniquement avec une licence CUPS.
- Il peut être activé/désactivé dans 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
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.