

Comportamento do recurso IDFT no StarOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar IDFT](#)

[Problema](#)

[Análise](#)

[Solução](#)

Introduction

Este documento descreve o comportamento do recurso Indirect Forwarding Tunnel (IDFT) em Control and User Plan Separation (CUPS) e configuração de legado/baremetal.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- StarOS
- Função de Gateway de Serviço (SGW) relacionada ao IDFT

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware SGW - 21.25.9 (em versões legadas e CUPS).

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento foram iniciados com uma configuração limpa (padrão). Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O SGW suporta procedimentos de IDFT para criação e exclusão, que são aplicáveis para chamadas Pure-S e Recolhidas com rede de dados de vários pacotes (PDN) e vários transmissores. Este recurso é aplicável para suporte de IDFT com ou sem cenários de realocação e colisão de SGW.

O recurso IDFT suporta estas funcionalidades:

- Crie uma solicitação IDFT para Collapsed, Pure-S, uma combinação de chamadas multiPDN Collapsed e Pure-S com vários transmissores.
- Transferência de dados em portadores de IDFT de downlink e uplink.
- Exclusão da solicitação de IDFT do MME (Mobility Management Engine). Além disso, a exclusão do portador de IDFT com base no temporizador após a expiração de um valor padrão de 100 segundos, se o MME não enviar uma solicitação de IDFT para exclusão.
- Exclusão de PDN de IDFT, que inclui Limpar/Excluir assinantes de MME/P-GW, quando o PDN normal fica inativo.
- Tratamento de falhas do Sx-Path em caso de Pure-S e chamadas recolhidas no momento de IDFT Ativo/IDFT Criar estado Sx-Pendente.
- Interação e colisão de mensagens no momento do estabelecimento ou exclusão da PDN do IDFT com qualquer outro procedimento.
- O tratamento de falhas S11/S5 e Sx-Path em PDN não-IDFT agora é suportado quando o PDN IDFT está ativo.

Configurar IDFT

Esta seção descreve os comandos CLI disponíveis para suportar o recurso IDFT.

No plano de controle, use esses comandos CLI para ativar ou desativar o recurso IDFT.

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

Problema

O SGW processa a solicitação Criar IDFT mesmo quando o recurso está desativado. Esse comportamento é visto em nós herdados/baremetal.

Esta é a configuração de IDFT presente no nó:

```
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.

Análise

Os rastreamentos e logs de depuração são obtidos por meio da simulação deste cenário no laboratório e o comportamento de Criar solicitação IDFT e Criar resposta IDFT é visto.

1) O MME envia a solicitação de criação de IDFT ao SGW.

Wireshark capture showing a GTPv2 message from MME to SGW. The message is a 'Create Indirect Data Forwarding Tunnel Request' with a length of 30 bytes. The cause is 'Request accepted'.

```

11 0.000... 2022-07-11 10:49:09.230000 192.168.1.100 10.1.17.1 GTPv2 modify bearer request
12 0.000... 2022-07-11 10:49:09.230000 10.1.17.1 192.168.1.100 GTPv2 Request accepted,Request accepted Modify Bearer Response
13 10.49... 2022-07-11 10:49:19.730000 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
  
```

Frame 13: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on 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

GRE Tunneling Protocol V2

Flags: 0x48

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) O SGW processa a solicitação e envia a resposta Create IDFT Response de volta ao MME com a causa 'Solicitação aceita'.

Wireshark capture showing a GTPv2 message from SGW to MME. The message is a 'Create Indirect Data Forwarding Tunnel Response' with a length of 81 bytes. The cause is 'Request accepted'.

```

11 0.065... 2022-07-11 10:49:09.230000 192.168.1.100 10.1.17.1 GTPv2 modify bearer request
12 0.000... 2022-07-11 10:49:09.230000 10.1.17.1 192.168.1.100 GTPv2 Request accepted,Request accepted Modify Bearer Response
13 10.49... 2022-07-11 10:49:19.730000 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 (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

Nessa resposta Criar IDFT, espera-se que o SGW envie Criar resposta IDFT com a causa 'Encaminhamento de dados sem suporte', pois esse recurso está desabilitado na configuração.

A mesma configuração é usada na configuração do CUPS:

1) O MME envia a solicitação de criação de IDFT ao SGW.

2) O SGW processa a solicitação e envia a resposta Create IDFT Response de volta ao MME com a causa 'Data Forwarding not supported'.

No guia do administrador, para habilitar esse recurso, você precisa executar estas etapas:
No plano de controle, use esses comandos CLI para ativar ou desativar o recurso IDFT.

configure

```
context context_name

sgw-service service_name

[ default | no ] egtp idft-support

end
```

Se você seguir essas etapas em legado para ativar/desativar o serviço, não poderá ver nenhuma opção para alterná-lo.

```
[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

Quando você tenta habilitá-lo/desabilitá-lo na configuração do CUPS, ele mostra a opção para alterná-lo.

[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

Solução

A razão para esse comportamento está descrita aqui:

Comportamento herdado:

- Não havia CLI no legado para controlar o comportamento de IDFT.
- IDFT é sempre suportado em código legado.

```
[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
```

Comportamento do CUPS:

- O CLI é controlado por licença, ou seja, está disponível somente com uma licença CUPS.
- Ele pode ser ativado/desativado no 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
```