

UCC 5G UPF 構成およびアドミニストレーション ガイド、リリース 2026.02

最終更新：2026 年 10 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



目 次

Full Cisco Trademarks with Software License ?

はじめに：

このガイドについて xxxvii

使用する表記法 xxxviii

第 1 章

5G アーキテクチャ 1

機能の概要と変更履歴 1

要約データ 1

更新履歴 1

アーキテクチャの概要 2

コントロール プレーン ネットワーク機能 2

ユーザー プレーン ネットワーク機能 3

サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ 4

コントロール プレーン ネットワーク機能アーキテクチャ 5

第 2 章

5G-UPF の概要 9

機能の概要と変更履歴 9

要約データ 9

更新履歴 10

製品の説明 10

ユースケースと機能 11

UPF の構成と導入要件 11

RAT 内および RAT 間モビリティのアンカーポイント 11

データネットワークにインターコネクトする外部 PDU セッションポイント 12

パケットインスペクション 12
ポリシールールの適用のユーザープレーン部分 12
合法的傍受 13
通信使用状況レポート（課金） 13
ユーザープレーンの QoS 処理 13
ダウンリンク パケット バッファリングおよびデータ通知トリガー処理 14
エンドマーカーをソース NG-RAN ノードに転送する 14
MVNO サポート 14
スマートライセンシング 15
展開アーキテクチャおよびインターフェイス 15
UPF アーキテクチャ 15
UPF デプロイメント アーキテクチャ 15
VM の展開 16
サポートするインターフェイス 19
標準準拠 19

第 I 部 : 特長と機能 21

第 3 章 1:1 冗長性 23
機能の概要と変更履歴 23
要約データ 23
マニュアルの変更履歴 23
機能説明 24
機能の仕組み 24
1:1 UPF 冗長性を構成する 31
アクティブ UPF とスタンバイ UPF 間の BFD モニタリングを構成する 31
各 UPF とネクストホップ ルータ間の BGP 状態モニタリングを構成する 32
アクティブ UPF およびスタンバイ UPF で Sx/N4 モニタリングを構成する 34
アクティブ UPF およびスタンバイ UPF で VPP モニターを構成する 35
ユーザープレーンのスイッチバックを防止する 35
デュアル アクティブ エラー シナリオの防止 36

Sx/N4 モニター障害をリセットする 36
UPF 状態を保留アクティブからアクティブに変更する 37
モニタリングおよびトラブルシューティング 37
show コマンドや出力 37
show srp monitor bfd 37
show srp monitor bgp 38
show srp monitor sx 38
show srp monitor vpp 39
show srp statistics 40
L2 ICSR のサポート 40
機能説明 40
SRP ループバック インターフェイス 40
機能の仕組み 41
ステートマシン 42
SRP コンテキストで L2 ICSR を構成する 43
プライマリシャーシとバックアップシャーシからの C-C および C-R BFD を構成する 43
L2 ICSR 構成を検証する 44
OAM のサポート 45
show コマンドのサポート 45

第 4 章 ダイナミックルール向け ADC 47
機能説明 48
機能の仕組み 48
制限事項 49
OAM のサポート 49
show コマンドの出力 49
show subscribers user-plane-only full all 49
show subscribers user-plane-only callid callid pdr full all 51

第 5 章 APN ACL のサポート 55
機能の概要と変更履歴 55
要約データ 55

更新履歴 56
機能説明 56
ルール 56
アクション 56
基準 57
ルールの順序 58
制限事項 58
ACL の設定 58
ACL 構成を確認する 59
IP ソース違反 59
ゲート制御 60

第 6 章 APN AMBR トラフィックポリシング 61
機能の概要と変更履歴 61
要約データ 61
更新履歴 61
機能説明 62
制限事項 62
APN AMBR トラフィックポリシング機能の設定 62
モニタリングおよびトラブルシューティング 63
show コマンドと出力 63

第 7 章 バルク統計サポート 65
機能の概要と変更履歴 65
要約データ 65
更新履歴 66
機能説明 66

第 8 章 課金サポート 69
機能の概要と変更履歴 69
要約データ 69

更新履歴 70
機能説明 70
N4 経由のオフライン課金イベントレポート 70
N4 経由のオンライン課金レポート 71
機能の仕組み 71
コール フロー 71
PFCP Session Establishment 手順 71
PFCP Session Modification 手順 72
PFCP Session Reporting 手順 73
PFCP Session Deletion 手順 74
オフライン課金レポートでサポートされる IE 75
オンライン課金レポートでサポートされる IE 77
PFCP Modification 応答での使用状況レポート 78
オンライン課金およびオフライン課金の使用状況レポート 79
Rating-Group と Service ID を使用した使用状況レポート 79
QAURR フラグを実装する 80
サポートされる機能と制限事項 80
PTT no-quota Limited Pass 82
PTT クォータ枯渇制限パス 82
タリフ時間のサポート 83
TCP 最大セグメントサイズ 84
使用状況レポートのクレジット制御を構成する 84
使用状況レポートの ACS ルールベースを構成する 85
モニタリングおよびトラブルシューティング 88
show コマンドと出力 88
show-user-plane-service statistics rulebase name <name> 88

第 9 章 **VPP による Cisco Ultra Traffic Optimization 89**
機能の概要と変更履歴 89
要約データ 89
更新履歴 89

機能説明 90
RCM のサポート 91
Cisco Ultra Traffic Optimization への GBR または MBR 値の送信 91
Cisco Ultra Traffic Optimization ライブラリの初期化解除 91
機能の仕組み 91
アーキテクチャ 91
制限事項 93
show コマンドと出力 94
show コマンドと出力 94
バルク統計情報 96
設定例 98

第 10 章 N4 インターフェイス経由の使用状況データの収集とレポート 101
機能の概要と変更履歴 101
要約データ 101
更新履歴 102
機能説明 102
機能の仕組み 102
標準準拠 103
N4 インターフェイス経由でボリューム測定を収集およびレポートするための構成 104
必要な課金情報アクションの課金アクションを構成する 104
課金アクションとルールベースを関連付ける 104

第 11 章 コントロールプレーンが開始する N4 アソシエーションのサポート 107
機能の概要と変更履歴 107
要約データ 107
更新履歴 108
機能説明 108
SMF が開始する N4 Association Setup 手順 108
機能の仕組み 108
コール フロー 108

セッション管理機能が開始する N4 Association Setup 手順 108
CP が開始する N4 アソシエーションのセットアップ機能を構成する 109
CP が開始する N4 アソシエーションのセットアップ機能の OAM サポート 109
show コマンドのサポート 110

第 12 章 コンバージドデータパス 111
機能の概要と変更履歴 111
要約データ 111
更新履歴 112
機能説明 112
アーキテクチャ 112
機能の仕組み 113
SxDemuxMgr 113
SessMgr 114
データパス 114
課金 114
コール フロー 114
SGW-C/cnSGW と SMF/IWF との初期接続 114
Collapsed UPF を使用した 5G から 4G へのハンドオーバー 116
Collapsed UPF を使用した S-GW 内ハンドオーバー 118
Collapsed UPF を使用したアイドル/アクティブ DDN の処理 119
S1 ハンドオーバー中の IDFT 処理 121
同じ SGW-U を使用した S-GW の再配置 122
Wi-Fi から LTE へのハンドオーバー 124
制限事項 127
コンバージドコールに課金する 127
機能説明 128
機能の仕組み 128
制限事項 129
eGCDR を構成する 129
GTPP グループの構成 129

コンバージド Sxa コールのボリュームカウントを含む使用状況レポートの生成します 130
設定例 130
コンバージドデータパスを構成する 130
UPF でコンバージドデータパスを有効にする 130
Sxa および N4 にリモートピアを構成する 131
Sxa および N4 にユーザープレーンサービスを構成する 131
モニタリングおよびトラブルシューティング 131
show コマンドと出力 131
show subscribers user-plane-only all 131
show subscribers user-plane-only full all 131
show user-plane-service statistics all 132

第 13 章 ディープ パケット インスペクションとインラインサービス 133
機能の概要と変更履歴 133
要約データ 133
マニュアルの変更履歴 134
機能説明 134
DNS サーバーアドレス再指定 135
機能の仕組み 136
ダウンリンクおよびアップリンクパケットの DSCP マーキング 136
Transport Level Marking IE 137
Transport Level Marking Options IE 137
Inner Packet Marking IE 138
通信のアドレス再指定またはリダイレクト 138
Redirect Information IE 139
サポートされるインラインサービス 140
アプリケーション検出および制御 140
QUIC IETF の導入 140
QUIC IETF の設定 141
統計情報 141
コンテンツ フィルタリング 141
DNS スヌーピング 142

イベントデータレコード 143
機能説明 143
機能の仕組み 144
イベントデータレコードを構成する 147
モニタリングおよびトラブルシューティング 149
ファイアウォールのサポート 150
機能説明 150
サブスクライバ ファイアウォールの構成 151
モニタリングおよびトラブルシューティング 153
フローアイドルタイムアウトのランダム化 155
ACS でフローアイドルタイムアウトのランダム化を構成する 155
HTTP URL フィルタリング機能 156
IP 再アドレス指定 159
IP アドレス再指定を構成する 160
Show コマンド 161
L7 プロトコル 161
DNS 162
FTP 162
HTTP 162
HTTPS 170
RTP/RTSP 170
SIP 171
モニタリングおよびトラブルシューティング 171
N4 での NAT サポート 172
機能説明 172
NAT の設定 174
モニタリングおよびトラブルシューティング 175
テザリング検出 180
機能説明 180
テザリングサポートを構成する 181
モニタリングおよびトラブルシューティング 182
RTP ダイナミックフローの検出 183

ベアラー固有フィルタのルール照合 183
アップリンクパケットの IP 送信元違反検出の有効化 185
アップリンクパケットの IP 送信元違反の有効化の仕組み 186
アップリンクパケットの IP 送信元違反を確認する 186
URL のブロックリスト登録登録 189
機能説明 189
機能の仕組み 189
URL ブロックリスト登録を構成する 190
モニタリングおよびトラブルシューティング 192
静的ルールと事前定義済みルールを構成する 194
DPI 向け L7 プロトコルの ACS Ruledef を構成する 195
DPI 向け L7 プロトコルの課金アクションの構成 197

第 14 章 EDNS0 レコードのデバイス ID 201
機能の概要と変更履歴 201
要約データ 201
更新履歴 201
機能説明 202
機能の仕組み 202
プロセス フロー 203
EDNS0 パケット形式 204
IP 再アドレス指定を使用した EDNS0 205
動作と制限事項 205
制限事項 206
EDNS フォーマットとトリガーアクションの設定 206
設定例 208
モニタリングおよびトラブルシューティング 209
show コマンドと出力 209
バルク統計 210

第 15 章 ダウンリンク データ通知 211

機能の概要と変更履歴 211
要約データ 211
マニュアルの変更履歴 211
機能説明 212
機能の仕組み 212
ダウンリンクデータ通知：遅延（DDN-D）のサポート 213
5G SMF コール 213
DDN スロットリングのサポート 214
ユーザー接続タイマーのサポートなし 214
DDN コールフロー 215
DDN の成功シナリオ 215
DDN の失敗シナリオ 216
ユーザー接続タイマーのサポートなし 218
DDN 遅延タイマー 219
Sx インターフェイス 221
制限事項 223
リリース 10 非準拠 MME の DDN スロットリング 223
リリース 10 準拠 MME の DDN スロットリング 225
SAE-GW セッションのアイドルタイマー 225
制限事項 226
SAE-GW セッションのアイドルタイマーの設定 226
S-GW セッションのアイドルタイムアウト 226
セッション アイドル タイムアウトの設定 227
show コマンドの入力と出力 227
show subscribers user-plane-only full all 228
show subscribers user-plane-only full callid <call_id> 228

第 16 章 **Collapse コールの DSCP マーキング 229**
機能の概要と変更履歴 229
機能説明 230
5G 通信の DSCP マーキング 230

4G Collapsed データパスコールに対する DSCP マーキング 230
機能の仕組み 230
SessMgr SMF の変更 231
構成 234
モニタリングおよびトラブルシューティング 235
show コマンドの出力 235

第 17 章 ダイナミックおよび静的 PCC ルール 237
機能の概要と変更履歴 237
要約データ 237
更新履歴 238
機能説明 238
機能の仕組み 238
定義済み PCC ルールのサポート 238
定義済み PCC ルールをプロビジョニングする 239
ダイナミック PCC ルールのサポート 240
ポリシング 241
帯域幅ポリシー構成の制限 242
静的ルールおよび事前定義済みルールのレート制限 243
ダイナミックルールのレート制限 243
標準準拠 245
URR ID を構成する 245
しきい値の設定 246

第 18 章 ECS 正規表現 247
機能の概要と変更履歴 247
要約データ 247
更新履歴 248
機能説明 248
機能の仕組み 248
正規表現ルールの設定 250

設定例 250
モニタリングおよびトラブルシューティング 250
show コマンドと出力 251

第 19 章 GTP-U のサポート 253
機能の概要と変更履歴 253
要約データ 253
更新履歴 253
機能説明 254
機能の仕組み 255
コール フロー 255
MME と S-GW 経由の E-UTRAN での初期接続 255
N26 インターフェイスを使用する 5G から EPS へのハンドオーバー 256
UP での Error Indication の処理 258
UP での GTP-U パス障害のサポート 258
S5u/N3 インターフェイスでデュアル スタック サポートを有効にする 259
UDP チェックサムを無効にする 259
UDP チェックサムを無効にする 259

第 20 章 N4/Sx インターフェイスのハートビートサポート 261
機能の概要と変更履歴 261
要約データ 261
マニュアルの変更履歴 262
機能説明 262
機能の仕組み 262
パス障害の検出 262
パスの障害の処理 263
N4/Sx インターフェイスのハートビートを構成する 263
Sx インターフェイスのハートビートを有効にする 263
パス障害の検出ポリシーを構成する 264
モニタリングおよびトラブルシューティング 265

show コマンドや出力 265
show sx-service all 265
show sx-service statistics all 265
切断理由 266
SNMP トラップ 266

第 21 章 アイドルモードのバッファリングとページング 267
機能の概要と変更履歴 267
要約データ 267
更新履歴 268
機能説明 268
機能の仕組み 268
UPF でのバッファリング アクション ルールをプロビジョニングする 268
バッファリング アクション ルールのコールフロー 269
最初の DL パケットのダウンリンクデータレポート 269
ページングポリシー差別化 270
ページング ポリシー インジケータ（PPI） 270
PDU セッション ユーザー プレーン プロトコルのフレームフォーマット 270
QoS フロー識別子（QFI） 270
ページングポリシーの存在 270
ページング ポリシー インジケータ 271

第 22 章 間接転送トンネル 273
マニュアルの変更履歴 273
機能説明 273
機能の仕組み 273
通話フロー 273
サポートされる機能 276
制限事項 277
間接転送トンネルの設定 277
間接転送トンネル機能の有効化 277

間接転送トンネル機能の確認 277
show sgw-service name <service_name> 277
モニタリングおよびトラブルシューティング 278
show コマンドの入力と出力 278
show subscribers saegw-only full all 278
show subscribers user-plane-only callid <call_id> pdr all 278
show subscribers user-plane-only full all 279

第 23 章 **DHCP サーバー経由の IP 割り当て 281**
UPF が DHCP サーバー経由で UE IP を割り当てる方法 282
DHCP サブネット選択基準 285
DHCP 構成の検証基準 286
IPv4 および IPv6 アドレスの検証 287
DHCP ベースの IP 割り当てを有効にする 288
DHCPv4 または DHCPv6 サービスを開始する 289
スロット/ポートを構成して DHCP サーバーの検出を有効にする 290
制限事項 293

第 24 章 **IPv6 向け IPsec サポート 295**
機能の概要と変更履歴 295
要約データ 295
更新履歴 295
機能説明 296
IPsec AH および ESP 296
IPSec の転送およびトンネルモード 296
IPSec 用語 297
暗号アクセス制御リスト 297
トランスフォームセット 297
ISAKMP ポリシー 297
クリプト マップ 297
暗号テンプレート 298

サポートされるアルゴリズム 298
制限事項と制約事項 299
設定例 299
モニタリングおよびトラブルシューティング 300
Show コマンド 300

第 25 章 IPv6 プレフィックス委任 303
IPv6 プレフィックス委任 304
ライセンス 305
IPv6 プレフィックス委任のガイドラインと制限事項 305
IPv6 プレフィックスの委任 305
IPv6 プレフィックスのリリース 307
プレフィックス委任向けに DHCP サーバー名を構成する 307
IPv6 プレフィックス委任を検証する 308
show subscribers user-plane-only full all callid 308
show dhcpv6 statistics 309

第 26 章 LTE：Wi-Fi のシームレスハンドオーバー 311
機能の概要と変更履歴 311
要約データ 311
マニュアルの変更履歴 311
機能説明 311
機能の仕組み 312
EPC から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー 312
非 3GPP 信頼できない Wi-Fi から EPC へのハンドオーバー コール フロー 316
非 3GPP インターワーキング機能 320
ICSR とセッションのリカバリ 321
制限事項 321
標準準拠 321

第 27 章 モニタ サブスクライバ 323

機能の概要と変更履歴 323
要約データ 323
マニュアルの変更履歴 323
機能説明 324
機能の仕組み 325
SMF と UPF の相互作用 325
SMF からのサブスクライバ トレーシングシング 326
fastpath および slowpath パケットキャプチャ 330
UPF SessMgr の機能 331
マルチ PDN マルチトレース 331
MonSub 統計 332
X-Header 332
UPF におけるサブスクライバのモニターの設定手順 332
Monsub CLI オプション 333
モニターサブスクライバのコンテキスト、CDRMOD、および 16 進ダンプのインタラクション 336
PCAP ファイル名の表記法 336
PCAP ファイルの場所 339
制限事項 340
UPF での MonSub の 16 進ダンプモジュールの設定 342
MonSub ポールタイマーの設定 342
MonSub ファイル名の設定 342
モニタリングおよびトラブルシューティング 343
SNMP トラップ 343

第 28 章 **UPF での MPLS のサポート 345**
機能の概要と変更履歴 345
要約データ 345
マニュアルの変更履歴 345
機能説明 346
機能の仕組み 347

PE に接続された MPLS-CE 347
設定例 348
VPN 関連 CLI コマンド 350
モニタリングおよびトラブルシューティング 355
show コマンドと出力 355
show mpls ftn vpp 355

第 29 章 複数の cnSGW のサポート 357
機能の概要と変更履歴 357
要約データ 357
マニュアルの変更履歴 357
機能説明 358
機能の仕組み 358
複数の SMF/cnSGWs を構成する 359
UPF での複数の SMF/cnSGW を構成する 359
モニタリングおよびトラブルシューティング 359
show コマンドと出力 359
show subscribers user-plane-only full all 359
show sx peers 359

第 30 章 複数の N4/Sx インターフェイス 361
機能の概要と変更履歴 361
要約データ 361
マニュアルの変更履歴 362
機能説明 362
機能の仕組み 363
複数の N4/Sx インターフェイスを構成する 363
複数のピアノードを構成する 363
モニタリングおよびトラブルシューティング 364
show コマンドと出力 364
show ip chunks 364

show ipv6 chunks 364
show subscribers user-plane-only full all 364
show sx peers 365
show user-plane-service statistics peer-address <address> 365

第 31 章 ネクストホップ転送サポート 367
更新履歴 367
機能説明 367
機能の仕組み 367
アーキテクチャ 367
制限事項 373
ネクストホップ転送サポートを構成する 374
課金アクションを使用してネクストホップ転送を構成する 374
DNN プロファイル経由でネクストホップ転送を構成する 374
IPv4 アドレスの IPAM プロファイルによる IP プールでのネクストホップ転送の構成 374
IPv6 アドレスの IPAM プロファイル経由で IP プールのネクストホップ転送を構成する 375
設定例 377
ネクストホップ転送を使用した VLAN セグメンテーション 378
機能説明 378
機能の仕組み 379
ネクストホップ転送を使用して VLAN セグメンテーションを有効にする 379
設定例 380
UPF でネットワーク到達可能性サーバーを構成する 380
設定例 382
OAM のサポート 382
モニタリングのサポート 382
モニタリングおよびトラブルシューティング 383
show コマンドと出力 383

第 32 章 N:M 冗長化および冗長化構成マネージャ 385
機能の概要と変更履歴 385

要約データ 385

更新履歴 385

機能説明 386

第 33 章 PDU セッション情報の N3 転送 387

機能の概要と変更履歴 387

要約データ 387

更新履歴 387

機能説明 387

機能の仕組み 388

ダウンリンクデータパケットの PDU セッション情報の転送 388

アップリンクデータパケットの PDU セッション情報の転送 388

PDU Session Information Frame IE 389

標準準拠 390

制限事項 390

第 34 章 3GPP 仕様との N4 インターフェイスの準拠 391

機能の概要と変更履歴 391

要約データ 391

更新履歴 391

機能説明 392

Averaging Window 392

Paging Policy Indicator 392

Outer Header Creation 393

Outer Header Removal 394

第 35 章 N4 インターフェイスの構成 397

機能の概要と変更履歴 397

要約データ 397

更新履歴 398

機能説明 398

N4 および Sx インターフェイスにおける圧縮の統一性 398
N4 インターフェイスを構成する 399
N4 インターフェイスを識別する 400
Sx サービスの N4-type パラメータの変更 400
統計情報 401
show control-plane-group 401
show sx-service all 401
show subscribers user-plane-only all 401
show user-plane-service statistics all 401
show subscribers user-plane-only seid number pdr all 401
show subscribers user-plane-only callid number pdr full all 401

第 36 章 IPSec 経由の N4/Sx 403
機能の概要と変更履歴 403
要約データ 403
マニュアルの変更履歴 403
機能説明 404
推奨タイマー 406
推奨設定 407
SMF の構成例 407
ルータの設定例 410
UPF の構成例 411
SRP の設定例 412
設定例 413
モニタリングおよびトラブルシューティング 415

第 37 章 N4 Session Management、Node Level、および Reporting 手順 417
機能の概要と変更履歴 417
要約データ 417
マニュアルの変更履歴 418
機能説明 418
N4 Session Management、Node Level、および Reporting 手順 418

N4 Node-level 手順 418
N4 Session Management 418
N4 Session/Node-level Reporting 手順 419
関係 419
End Marker サポート 419
UEs IPv4、IPv6 および IPv4v6 サポート 419
機能の仕組み 419
N4 Node-level 手順コールフロー 420
N4 Association Setup 手順のコールフロー 420
N4 Association Update 手順のコールフロー 420
N4 Association Release 手順のコールフロー 421
N4 Heartbeat 手順 422
N4 Session Management 手順のコールフロー 422
N4 Session Establishment コールフロー 422
N4 Session Modification コールフロー 422
N4 Session Delete コールフロー 423
N4 Session/Node-level Reporting 手順コールフロー 424
GTP-u Error Indication コールフローによるセッションレベルのレポート 424
GTP-u パス障害コールフローによる Node-level Reporting 手順 425
PDN Update 手順：eNodeB F-TEIDu 427
UEs IPv4、IPv6 および IPv4v6 サポートコールフロー 428
IPv6 コールフローの N4 Session Establishment と Modification 手順 428
IPv4v6 コールフローの N4 Session Establishment と Modification 手順 429
N4 Session/Node-level Reporting 手順を構成する 431
GTP-u Echo Request 手順を有効にする 431
N4 Session/Node-level Reporting 手順構成を確認する 432
N4 Session Node Level Reporting 手順の OA および M サポート 432
SNMP トラップ 433
グレースフル セッション終了の拡張された PFCP 関連付けのリリース手順 434
UPF が開始した PFCP セッションのリリース 435
UPF でサブスクライバセッションをクリアする 436

原因レベルの統計を確認する 436
UPF によって開始された拡張 PFCP 関連付けの解除 437
EPFAR 機能の有効化 438
Sx サービスのアソシエーション解除を開始する 438
アソシエーションの解除タイマーを有効にする 439

第 38 章 NRF のサポート 441
機能の概要と変更履歴 441
要約データ 441
更新履歴 441
機能説明 442
NRF 管理サービス 442
機能の仕組み 443
UPF 登録 443
UPF ハートビート 443
UFP 登録解除 443
標準準拠 443
NRF 管理サービスを構成する 444
モニタリングおよびトラブルシューティング 446
show コマンドと出力 446

第 39 章 パスワード期限切れ通知 449
機能の概要と変更履歴 449
要約データ 449
更新履歴 449
機能説明 450
Save Configuration コマンドを使用したアップグレードとダウンロードの手順 451

第 40 章 UPF での QCI 80 のサポート 453
機能の概要と変更履歴 453
要約データ 453

更新履歴 453
機能説明 454
機能の仕組み 454
検出された通信に基づくダイナミック QoS フローの確立 454
通話フロー 454
制限事項 456
ADC ルールを構成する 456
モニタリングおよびトラブルシューティング 458

第 41 章 Ruledefs の QoS グループのサポート 459
機能の概要と変更履歴 459
要約データ 459
マニュアルの変更履歴 459
機能説明 460
機能の仕組み 460
制限事項 462
OAM のサポート 462
show コマンドのサポート 463
show subscribers user-plane-only callid call_id far full all 463
show subscribers user-plane-only callid call_id qer full all 463
show subscribers user-plane-only callid call_id qos-group all 463
show subscribers user-plane-only callid call_id qos-group statistics 464
show subscribers user-plane-only full all 464
show user-plane-service qos-group-of-ruledefs 465
show user-plane-service statistics qos-group sessmgr 466

第 42 章 ローミングのサポート 467
機能の概要と 467
要約データ 467
更新履歴 468
機能説明 468
関係性 469

アーキテクチャ 470
PLMN 間モビリティサポート 471
機能の仕組み 472
標準準拠 491
制限事項 491
UPF の HR ローミングサポートを構成する 491
サブパラメータ IE のローミングステータス 493
Source Interface Type IE 493
モニタリングおよびトラブルシューティング 494
show user-plane-service statistics all 494
show subscribers user-plane-only full all 495
show subscribers user-plane-only callid pdr full all 495
show user-plane-service gtpu statistics gtpu-service n9-egress 496
show user-plane-service gtpu statistics gtpu-service n9-ingress 498

第 43 章 セキュリティグループタグ（SGT）ベースのアクセスコントロール 501
SGACL 経由のユーザーアクセスコントロール 502
ISE 統合向け SGACL の仕組み 504
通話フロー 504
制限事項 505
UPF でのセカンダリ ISE サーバーの統合 506
セカンダリ ISE サーバー統合の仕組み 508
セカンダリ ISE サーバー統合の制限事項 509
ISE 統合向け SGACL 構成 510
API Manager を有効にする 510
ISE サーバープロファイルを構成する 510
アクティブな ISE サーバーに手動で切り替える 513
ISE サーバープロファイルを関連付ける 513
D-SGT 列を更新する 514
モニタリングおよびトラブルシューティング 515
SGACL と SGT 統合を確認する 515
show subscribers user-plane-only full callid callid_value 515

show subscribers user-plane-only callid callid_value flows full 515
show user-plane-service sgt-column summary 516
show user-plane-service sgt-column dsgt 516
show user-plane-service sgacl name 516
show user-plane-service statistics sgacl all 517
show user-plane-service statistics drop-counter 517
show apimgr statistics ise-server 517
SNMP トラップ 518
OAM のサポート 518

第 44 章 セッションリカバリ 519
機能の概要と変更履歴 519
要約データ 519
更新履歴 519
機能説明 520
機能の仕組み 520
セッションリカバリをサポートするためのシステムの設定 521
セッションリカバリの有効化 521
アウトオブサービスシステムでのセッションリカバリの有効化 521
インサービスシステムでのセッションリカバリの有効化 522
セッションリカバリ機能の無効化 523
セッション リカバリ ステータスの表示 523
再作成されたセッション情報を表示する 523

第 45 章 Session Report Rejection 手順 527
機能の概要と変更履歴 527
要約データ 527
マニュアルの変更履歴 527
機能説明 527
他の機能との関係 528
通話フロー 528
OAM のサポート 529

Show コマンドや出力 529

第 46 章 ソフトウェア管理の運用 531

機能の概要と変更履歴 531

要約データ 531

更新履歴 532

概要 532

SNMP トラップ 533

制限事項 533

正常性チェック 534

ビルドアップグレード 536

UPF アップグレード 538

UPF のダウングレード 538

第 47 章 標準 QCI のサポート 539

機能の概要と変更履歴 539

要約データ 539

マニュアルの変更履歴 539

機能説明 540

制限事項 540

構成 540

第 48 章 システム ログ 541

機能の概要と変更履歴 541

要約データ 541

更新履歴 542

システムログのタイプ 542

イベントロギングパラメータの設定 543

イベントログフィルタの設定 543

Exec モードのフィルタリング 543

グローバル構成モードのフィルタリング 546

syslog サーバの設定 547
アクティブログの設定 550
ファシリティの指定 550
トレースロギングの設定 560
モニターログの設定 561
モニターログの有効化 561
モニターログの無効化 561
ロギング設定と統計情報の表示 561
CLI を使用したイベントログの表示 562
クラッシュログの設定と表示 563
クラッシュロギングのアーキテクチャ 564
ソフトウェアクラッシュログ接続先の設定 564
CLI を使用して要約されたクラッシュログ情報の表示 565
過剰なイベントロギングの削減 566
ログソースのしきい値の設定 567
ログのチェックポインティング 567
ログファイルの保存 568
イベント ID の概要 570
イベントのシビラティ（重大度） 579
ログ出力のイベント ID 情報の概要 580

第 49 章
UPF 入力インターフェイス 581
機能の概要と変更履歴 581
要約データ 581
更新履歴 582
機能説明 582
UPF 入力インターフェイス種別の構成 583
UPF 入力インターフェイスタイプを構成する 583
設定例 583
N9 インターフェイスの Echo 応答を構成する 583
N3 および N9 BGP ルートを分離する 584

UPF 入力インターフェイス種別の構成を検証する 588
show user-plane-service all 588
複数の GTPU IP アドレスのサポート 589
機能説明 589
機能の仕組み 589
制限事項 590
N3 インターフェイスで複数のバインドアドレスを構成する 590
設定例 591
設定の確認 591
OAM のサポート 592
モニタリングのサポート 592

第 50 章 UPF ローカル構成 597
機能の概要と変更履歴 597
要約データ 597
更新履歴 597
機能説明 598
機能の仕組み 598
UPF のローカル構成サポートを構成する 600

第 51 章 N4/Sx インターフェイス経由の負荷と過負荷の制御 601
機能の概要と変更履歴 601
要約データ 601
更新履歴 602
機能説明 602
負荷および過負荷制御の仕組み 603
負荷および過負荷係数の計算 603
CP-F への負荷および過負荷のレポート 604
CP-F への負荷情報レポート 604
CP-F への過負荷情報レポート 605
自己保護モードでのセッションクリア 606

N4 または Sx インターフェイスでの負荷および過負荷制御を有効にする 606
負荷制御プロファイルを構成する 606
過負制御プロファイルを構成する 607
負荷と過負荷制御プロファイルをユーザープレーンサービスと関連付ける 609
モニタリングおよびトラブルシューティング 610
show コマンドと出力 610
show upf-load-control-profile 610
show upf-overload-control-profile 610
show user-plane-service statistics name 611
show user-plane-service statistics all 612
show user-plane-service name 613
show user-plane-service all 613
show sx-service statistics all 614
バルク統計情報 614
SNMP トラップ 616

第 52 章 PCF 経由の使用状況の監視 617
機能の概要と変更履歴 617
要約データ 617
マニュアルの変更履歴 617
機能説明 618
使用状況レポート 618

第 53 章 CPU サイクルの可変解放 619
VRCC の概要 619
VRCC の利点 620
VRCC の仕組み 620
VRCC を構成する 621

第 54 章 仮想ルーティングおよび転送 623
機能の概要と変更履歴 623
更新履歴 623

機能説明 624
重複するIPプール 624
識別子としての VRF 名 626
制限事項と制約事項 626
VRF の設定 626
VRF を使用した VLAN セグメンテーション 629
機能説明 629
VRF を使用して VLAN セグメンテーションを有効にする 630
設定例 630
モニタリングおよびトラブルシューティング 631
show コマンドと出力 631
show ip chunks 631
show ipv6 chunks 631
show ip bgp vpnv4 632
show ip bgp vpnv6 632
show mpls ilm 633

第 55 章 音声の新しいラジオ 635
機能の概要と変更履歴 635
要約データ 635
更新履歴 635
機能説明 636
機能の仕組み 636
UPF の VoNR コールフロー 636

第 56 章 WPS 優先順位 639
機能説明 639
機能の仕組み 640
制限事項 642
過負荷シナリオでのメッセージの優先順位付け 643
WPS の優先順位を構成する 644

WPS の優先順位を有効にする 644
セッション優先順位プロファイルをマッピングする 644
OAM のサポート 645
show コマンドのサポート 645
show subscribers user-plane-only full all 645
show user-plane-service all 646
show user-plane-service session-priority-profile name | all 646
show user-plane-service statistics all 646
show user-plane-service statistics session-priority-profile 647

第 57 章 X ヘッダーの挿入と暗号化 649
機能の概要と変更履歴 649
要約データ 649
マニュアルの変更履歴 649
機能説明 650
機能の仕組み 650
X-Header の挿入 650
X-Header の暗号化 650
制限事項 651
X-Header の挿入と暗号化の設定 652
X ヘッダーの挿入の設定 652
X ヘッダーの暗号化の設定 652
X-Header の挿入と暗号化の構成を確認する 653
X-Header の挿入および暗号化構成をモニタリングして障害対応する 654
アンチスプーフィングのサポート 654
機能説明 654
制限事項 655
X-Header でのアンチスプーフィングを有効にする 655
OAM のサポート 655

第 II 部 : モニタリングおよびトラブルシューティングの情報 657

第 58 章 UPF 障害対応情報 659
デバッグログ 659
監視 CLI 660
監視プロトコル 661
RAT タイプベースの統計 661
サブスクライバレベルの CLI 666
show subscribers user-plane-only full msid msid_value 667
show subscribers user-plane-only callid callid-value rule-match-info { [full] all | rulename rulename} 672
VPP 統計 674
show subscribers user-plane-only callid callid_value drop-statistics 675
show user-plane-service statistics drop-counter 676
show subscribers user-plane-only callid callid_value flows full 677
show subscribers user-plane-only callid callid_value flows flow-id flow_id 678
SNMP サポート 678
UPF 機能の障害対応 680

第 III 部 : UPF の基本構成例 683

第 59 章 UPF の構成例 685
設定例 685



このガイドについて

（注） コントロールプレーンとユーザープレーンの分離（CUPS）は、StarOS ベースの製品の 3G、4G、および 5G のネットワークでの展開方法におけるアーキテクチャ上の著しい変更を表します。このドキュメントでは、5G ネットワークにデプロイされたこの 5G UPF 製品で特にサポートされている機能に関する情報を提供します。レガシー製品または CUPS 以外の製品で以前サポートされていた機能がこの製品でもサポートされていると想定しないでください。レガシー製品または CUPS 以外の製品または機能への言及は、情報提供のみを目的としています。さらに、このドキュメントで言及されている構成（コマンド、統計、属性、MIB オブジェクト、アラーム、ログ、サービスを含むがこれらに限定されない）が、レガシー製品または CUPS 以外の製品との機能的な同等性を示すと想定しないでください。この製品とレガシー製品または CUPS 以外の製品間のパリティについてのご質問は、シスコのアカウント担当者またはサポート担当者にお問い合わせください。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

この序文では、『*5G* セッション管理機能ガイド』、その構成、および表記法について説明します。

このガイドでは、シスコユーザープレーン機能（UPF）について説明します。これには、インフラストラクチャ、インターフェイス、機能説明、仕様のコンプライアンス、セッションフロー、構成手順、システムの監視および障害対応向けの CLI コマンドが含まれます。

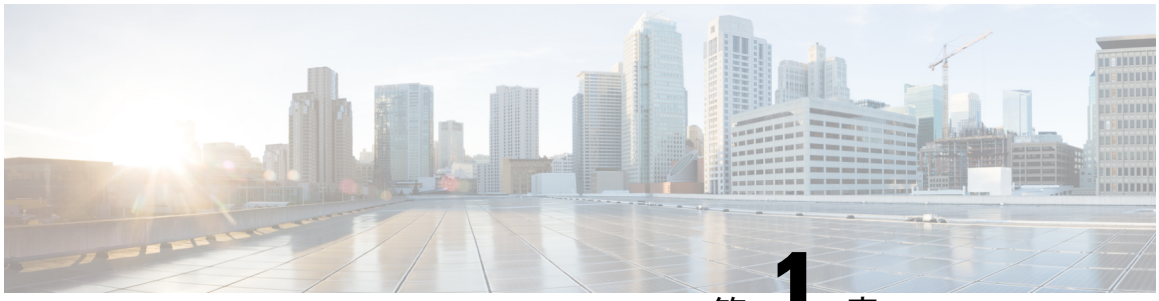
• 使用する表記法 （xxxviii ページ）

使用する表記法

次の表に、このマニュアル全体で使用される表記法を示します。

通知タイプ	説明
情報メモ	重要な機能または手順に関する情報を提供します。
注意	プログラム、デバイス、またはシステムに損傷を与えるおそれがあることを注意喚起します。
警告	人身傷害または死亡事故のおそれがあることを警告します。また、電気的障害のおそれがあることを警告する場合もあります。

書体の表記法	説明
スクリーンディスプレイとして表されるテキスト	この書体は、端末画面に表示されるディスプレイを表します。次に例を示します。 ログイン：
commands として表現されるテキスト	この書体は、入力したコマンドを表します。次に例を示します。 **show ip access-list** このマニュアルでは、コマンドの完全表記に常に小文字を使用しています。コマンドには、大文字と小文字の区別はありません。
command *variable*として表されるテキスト	この書体は、コマンドの一部である変数を表します。次に例を示します。 **show card** *slot_number* *slot_number* は、目的のシャーシのスロット番号を表す変数です。
メニュー名またはサブメニュー名として表されるテキスト	この書体は、ソフトウェアアプリケーション内でアクセスするメニューとサブメニューを表します。次に例を示します。 [File] メニュー、[New] の順にクリックてください。



第 1 章

5G アーキテクチャ

- 機能の概要と変更履歴, on page 1
- アーキテクチャの概要, on page 2
- サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ, on page 4
- コントロール プレーン ネットワーク機能アーキテクチャ, on page 5

機能の概要と変更履歴

要約データ

Table 1: 要約データ

該当製品または機能エリア	• PC-F • SMF • UPF
該当プラットフォーム	SMI
機能のデフォルト設定	N/A
関連資料	該当なし

更新履歴

Table 2: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0 より前

アーキテクチャの概要

Ultra Cloud Core は、5G 新しい無線（NR）スタンドアロン（SA）モードの 3GPP 標準規格をサポートする Cisco のソリューションです。これらの標準規格では、CUPS など、コントロール プレーン（CP）とユーザー プレーン（UP）の分離に基づいてさまざまなネットワーク機能（NF）を定義します。この分離により、ネットワークのパフォーマンスと機能が向上します。

コントロール プレーン ネットワーク機能

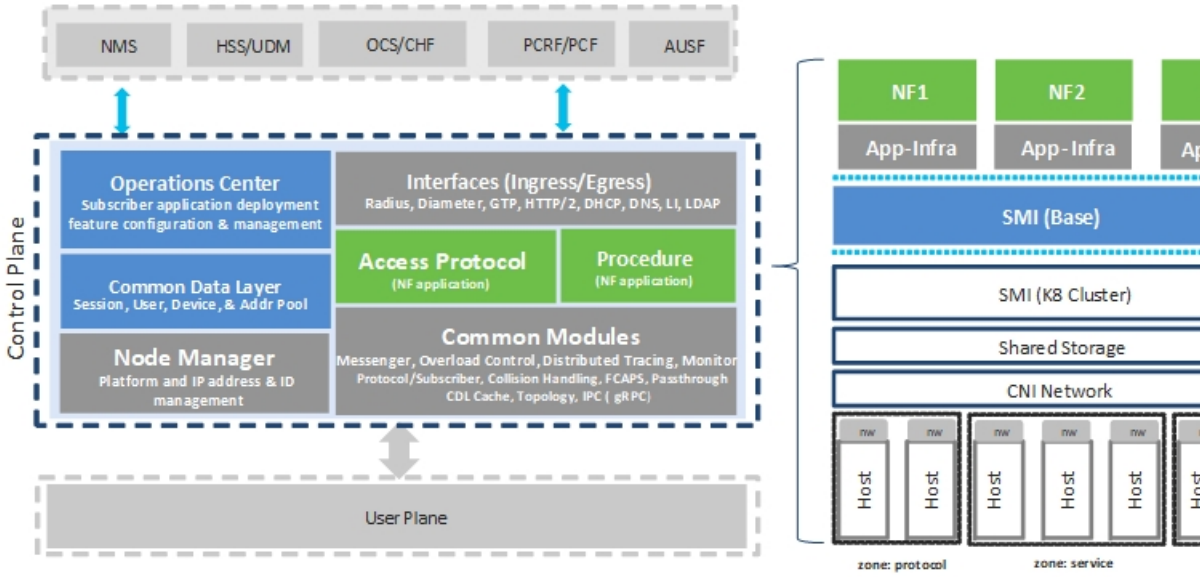
Ultra Cloud Core の CP 関連 NF は、次のテナントを持つ共通アーキテクチャを使用します。

- クラウドスケール：完全に仮想化され、シンプルさ、スピード、柔軟性を実現します。
- 自動化とオーケストレーション：最適化された運用、サービスの構築、およびインフラストラクチャ。
- セキュリティ：インフラストラクチャから NF アプリケーションまで、展開スタック全体における複数のセキュリティ層。
- API 公開：オープンかつ広範で、可視性、制御、およびサービス イネーブルメントが向上します。
- アクセスに依存しない：複数のネットワーク タイプをサポート（5G、4G、3G、Wi-Fi など）。

コントロールプレーン NF は、マイクロサービスなどのコンテナ化されたアプリケーションとして設計されています。Subscriber Microservices Infrastructure (SMI) を介して展開されます。

SMI は、ライフサイクル管理（LCM）、運用と管理（OAM）、パッケージングなど、NF の機能面の共通アプリケーション レイヤを定義します。

Figure 1: Ultra Cloud Core CP アーキテクチャ コンポーネント



ユーザー プレーン ネットワーク機能

Ultra Cloud Core 内の 5G UP NF は、ユーザー プレーン機能（UPF）です。CP 関連の NF とは異なり、5G UPF は、Cisco 4G CUPS アーキテクチャと同じベクトル パケット処理（VPP）テクノロジーを使用します。この共通性により、4G と 5G の間で次のような一貫した機能のセットが提供されます。

- 超高速パケット転送。
- 広範に統合された IP サービス（サブスクライバ ファイアウォール、テザリング、ディープ パケット インスペクション（DPI）、Internet Content Adaption Protocol（ICAP）、アプリケーションの検出および制御（ADC）、ヘッダーエンリッチメント（HE）など）。
- トラフィックおよびTCPを最適化するための統合されたサードパーティ製アプリケーション。

サブスクライバ マイクロサービスのインフラストラクチャのアーキテクチャ

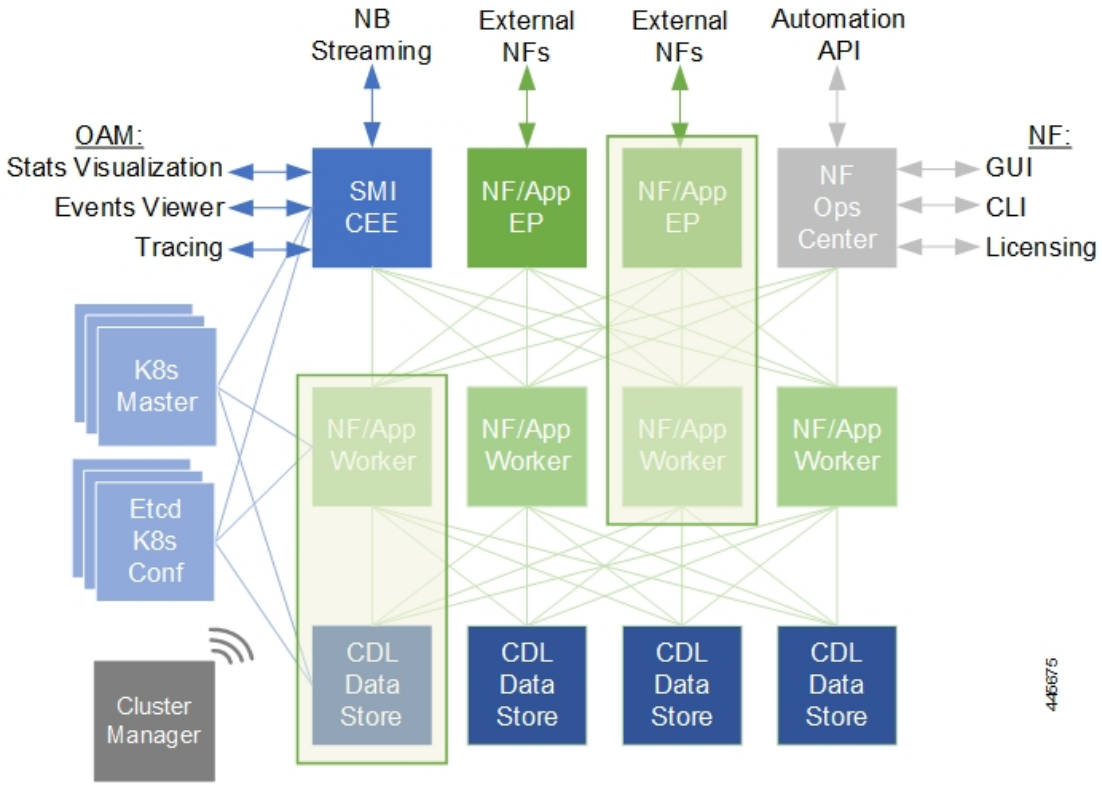
Ultra Cloud Core（UCC）サブスクライバマイクロサービス インフラストラクチャ（SMI）は、クラウド テクノロジーの階層化されたスタックです。マイクロサービスベースのアプリケーションの迅速な展開とシームレスなライフサイクル運用を可能にします。

SMI スタックは、次のコンポーネントで構成されています。

- SMI クラスタ マネージャ：Kubernetes（K8s）クラスタを作成し、ソフトウェア リポジトリを作成して、展開、アップグレード、拡張を含むクラスタの継続的な LCM を提供します。
- Kubernetes 管理：クラスタに展開される NF アプリケーションに LCM を提供する K8s プライマリおよび etcd 機能が含まれます。このコンポーネントは、クラスタ ヘルス モニタリングとリソース スケジューリングも提供します。
- 共通実行環境（CEE）：Cisco Cloud ネイティブ NF およびアプリケーションにユーティリティおよび OAM 機能を提供します。これには、ライセンスおよび権限付与機能、構成管理、テレメトリが含まれます。また、アラームの可視化、ログ管理、およびトラブルシューティング ユーティリティも提供します。また、これらのツールと展開されたアプリケーションに関連するすべてのお客様との接触ポイントと統合ポイントで、一貫した対話とエクスペリエンスを提供します。
- Common Data Layer（CDL）：5G およびサブスクライバ アプリケーション向けに特別に設計された、高性能で低遅延のステートフルなデータストアを提供します。この次世代データストアは、ローカルまたは地理的冗長性の展開で高可用性を提供します。
- サービス メッシュ：アプリケーション コンテナ間の高度なメッセージ ルーティングを提供し、管理された相互接続性、追加のセキュリティ、および低リスクの方法で新しいコードと新しい構成を展開する機能を実現します。
- NB ストリーミング：課金および課金システムに「ノースバウンド データ ストリーミング」サービスを提供します。
- NF またはアプリケーション ワーカー ノード：NF アプリケーションポッドを構成するコンテナ。
- NF またはアプリケーション エンドポイント（EP）：NF またはアプリケーションと、それらのネットワーク上の他のエンティティへのインターフェイス
- アプリケーションプログラミングインターフェイス（API）：展開、構成、および管理の自動化のためのさまざまな API を提供します。

次の図は、これらのコンポーネントがどのように相互接続し、マイクロサービスベースの NF またはアプリケーションを構成するかを示しています。

Figure 2: SMI コンポーネント



SMI コンポーネントの詳細については、『Ultra Cloud Core サブスクライバ マイクロサービス インフラストラクチャ』および『展開ガイド』の 「概要」の 章にある関連ドキュメントを参照してください。

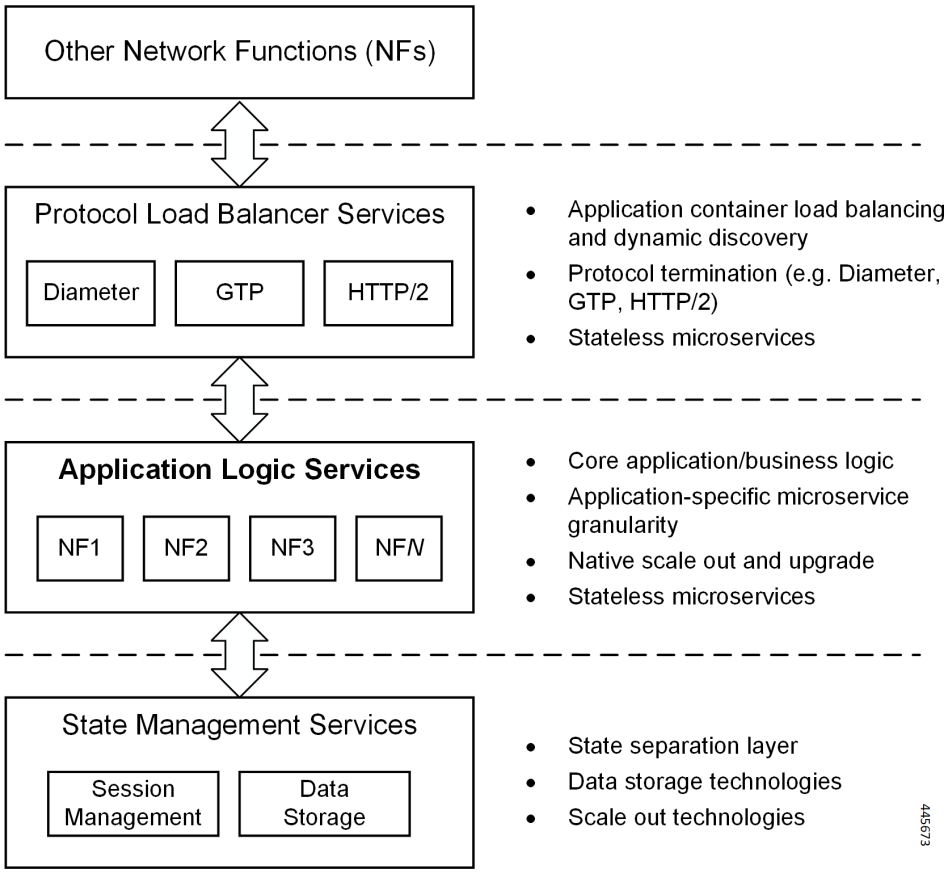
コントロールプレーンネットワーク機能アーキテクチャ

コントロールプレーン（CP）NFは、3階層アーキテクチャを使用します。このアーキテクチャは、クラウドネイティブ環境でステートフルまたはステートレス機能を活用します。アーキテクチャ層は次のとおりです。

- プロトコル ロード バランサ サービス：このサービスは、アプリケーション コンテナの動的な検出と、プロトコルのプロキシと終了を主な役割とするステートレスマイクロサービスです。これには、従来の 3GPP プロトコルと、5G で導入された新しいプロトコルが含まれます。
- アプリケーション サービス：コア アプリケーションまたはビジネス ロジックの実装を行い、受信した情報に基づいて実際のアプリケーションをレンダリングするステートレス サービスです。このレイヤには、さまざまなレベルのマイクロサービスの粒度が含まれる場合があります。アプリケーション サービスはステートレスです。

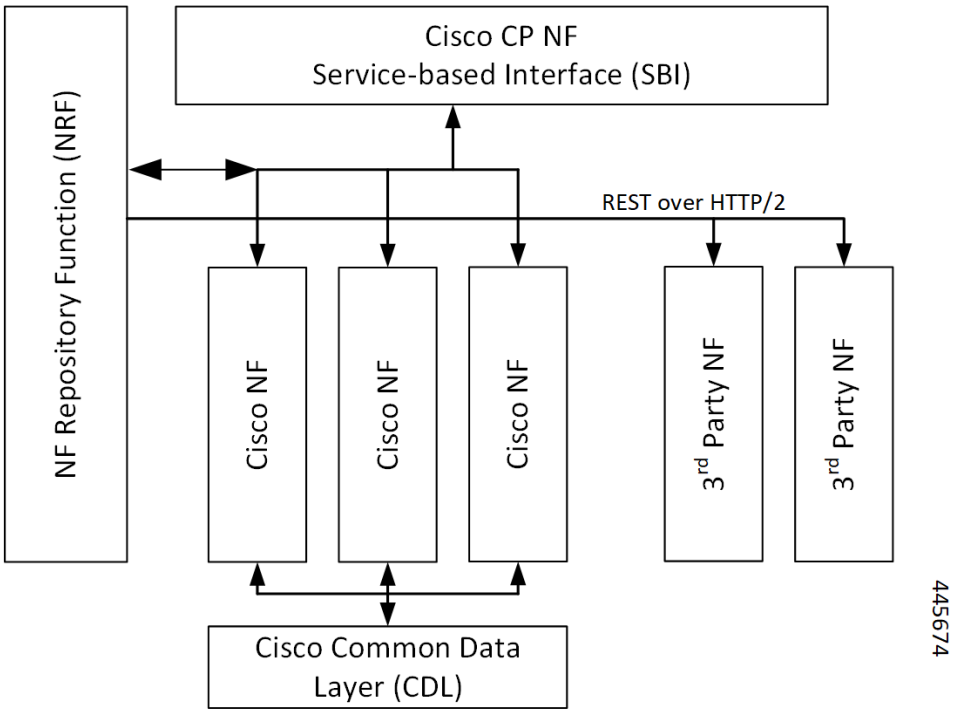
- ステート管理サービス：ステートレス アプリケーション サービスは、セッション データやサブスクライバデータなどのステート情報を保存またはキャッシュするための共通データ層（CDL）を提供します。この層は、インメモリ キャッシュから本格的なデータベースまで、さまざまなデータ ストレージ テクノロジーをサポートします。

Figure 3: 制御プラン、ネットワーク機能階層型アーキテクチャ

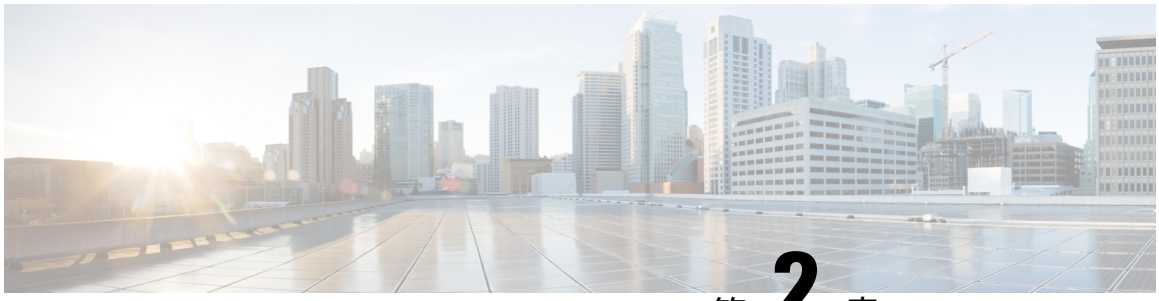


Cisco CP NF が設計されている 3 階層アーキテクチャは、3GPP で定義されている 5G コア（5GC）のサービスベース アーキテクチャ（SBA）を完全にサポートしています。これらの NF は、サービスベースのインターフェイス（SBI）を使用して通信します。3GPP で定義されているように、TCP 経由の HTTP/2 を使用します。

Figure 4: Cisco CP NF サービスベース アーキテクチャのサポート



Cisco のネットワーク機能の詳細については、対応するネットワーク機能のマニュアルを参照してください。



第 2 章

5G-UPF の概要

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 9
- 製品の説明, on page 10
- ユースケースと機能, on page 11
- 展開アーキテクチャおよびインターフェイス, on page 15
- 標準準拠, on page 19

機能の概要と変更履歴

要約データ

Table 3: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 4: マニュアルの変更履歴

改訂の詳細	リリース
UPF クラウドネイティブ デプロイメントのサポートが追加されました。	2023.01.0
最初の導入。	2020.02.0

製品の説明

ユーザープレーン機能（UPF）は、5G コアネットワーク（5GC）のネットワーク機能（NF）の 1 つです。UPF は、5G アーキテクチャにおける、パケットルーティングと転送、パケットインスペクション、QoS 処理、およびデータネットワーク（DN）の相互接続を担当します。

UPFは、ユーザー通信に高性能な転送エンジンを提供する別個の仮想ネットワーク機能（VNF）です。ベクトルパケット処理（VPP）テクノロジーを使用して、UPFは、すべてのユーザープレーン機能との互換性を維持しながら、超高速パケット転送を実現します。たとえば、シャロー パケット インスペクション（SPI）/ディープ パケット インスペクション（DPI）、通信最適化、インラインサービス（NAT、ファイアウォール、DNS スヌーピングなど）が挙げられます。UPF は現在、統合ディープ パケット ベース インスペクション（DPI）サービスを提供するように設計されています。

UPF の 1 つのインスタンスで次の機能の一部またはすべてが提供されます。

- RAT 内および RAT 間モビリティのアンカーポイント（該当する場合）。
- データネットワークへのインターコネクトの外部 PDU セッションポイント。
- パケットのルーティングと転送。
- パケットインスペクションたとえば、service data flow テンプレートと、追加で SMF から受信したオプションの PFD に基づくアプリケーション検出です。
- ポリシールール適用のユーザープレーン部分。たとえば、ゲーティング、リダイレクト、通信ステアリングなどです。
- 合法的傍受（UP コレクション）
- 通信使用状況レポート。
- ユーザープレーンのQoS処理。たとえば、アップリンク（UL）およびダウンリンク（DL）のレートの適用、DL でのリフレクティブ QoS マーキングなどです。
- アップリンク通信の検証（SDF からQoS フローへのマッピング）。
- アップリンクおよびダウンリンクでのトランスポートレベルのパケットマーキング。

- ダウンリンク パケット バッファリングとダウンリンクデータ通知のトリガー。
- 1 つ以上の「End Marker」を送信元 NG-RAN ノードに送信および転送します。

UPF は、モバイル仮想ネットワークオペレータ（MVNO）モデルをサポートします。これにより、モバイルネットワークオペレータ（MNO）は、リースされた MVNO サブスクライバのセカンダリ認証を実行できます。

ユースケースと機能

UPF の構成と導入要件

5G デプロイメントでは、Cisco UPF と Cisco 以外の SMF、および Cisco SMF と Cisco 以外の UPF 間での相互運用性が必要です。また、SMF と UPF 間の構成関連のメッセージの分離には、次の利点があります。

- ユーザープレーンとコントロールプレーン間の設定分岐に関する 3GPP 標準に準拠しています。
- SMF での構成管理の複雑さを軽減します。
- ユーザープレーン関連の構成における構成および変更管理を簡素化、効率化できます。これは、SMF が構成を管理および分散する必要がないためです。
- シスコ以外の SMF と UPF 間のインターワーキングを実現するように拡張できます。

Cisco UPF は、N4 インターフェイスで 3GPP 指定の属性をサポートします。現在のアーキテクチャでは、UPF のみが SMF に関連付けられます。

次の機能は、このユース ケースに関連しています。

- UPF デプロイメント アーキテクチャ （15 ページ）
- UPF ローカル構成 （597 ページ）
- N4 Session Management、Node Level、および Reporting 手順 （417 ページ）
- セッションリカバリ （519 ページ）
- 1:1 冗長性 （23 ページ）
- UPF 入力インターフェイス （581 ページ）

RAT 内および RAT 間モビリティのアンカーポイント

UPF は、モバイル インフラストラクチャとデータネットワーク（DN）間のアンカーポイントです。つまり、ユーザープレーン（GTP-U）の GPRS トンネリングプロトコルのカプセル化とカプセル化解除です。このユースケースでは、Xn ハンドオーバーなどの RAT 内モビリティ

と、4G から 5G や 5G から 4G へのハンドオーバーなどの RAT 間モビリティがサポートされています。

GTP-U のサポート 機能は、このユース ケースに関連しています。

データネットワークにインターコネクトする外部PDUセッションポイント

UPF は、データネットワークにインターコネクトする外部 PDU セッションポイントとして機能し、N3、N4、およびN6インターフェイスをサポートします。PDU レイヤは、PDUセッション中に UE と PDN の間で転送される PDU に対応します。PDU セッションのタイプは、IP パケットを転送するための IPv4 または IPv6 です。ユーザープレーン（GTP-U）の GPRSトンネリングプロトコルは、コアネットワークの N3 インターフェイス（5G アクセスノードと UPF 間）経由でユーザーデータをトンネリングすることにより、異なる PDU セッションからの通信の多重化をサポートします。GTP は、すべてのエンドユーザー PDU をカプセル化し、PDU セッションごとにカプセル化します。このレイヤは、QoS フローに関連付けられているマーキングも転送します。5G カプセル化レイヤは、N9インターフェイス（異なる UPF 間のインターフェイス）を介した異なる PDU セッションからの通信の多重化をサポートします。PDU セッションごとにカプセル化し、QoS フローに関連付けられたマーキングを反映します。

次の機能は、このユース ケースに関連しています。

- コントロールプレーンが開始する N4 アソシエーションのサポート
- PDU セッション情報の N3 転送
- N4 Session Management、Node Level、および Reporting 手順
- N4/Sx インターフェイス経由の負荷と過負荷の制御

パケットインスペクション

Cisco UPF は、受信したユーザー通信の L3/L4 および L7 インスペクションを実行します。L3/L4 インスペクションには、IP アドレス/ポートの照合が含まれ、ディープ パケット インスペクションには、L7ヘッダーフィールドの照合が含まれます。

ディープ パケット インスペクションとインラインサービス 機能は、このユース ケースに関連しています。

ポリシールールの適用のユーザープレーン部分

Cisco UPF は、SMF から受信したポリシーに基づいてさまざまな適用メカニズムを提供します。UPF は、アクセスドメインとIPドメイン間の境界であり、ポリシーベースの適用を実装するのに最適な場所です。PCF が指定する pcc ルールと SMF で事前定義されたルールは、N4 インターフェイス経由でアップロードされ、DNN ごとに UPF にインストールされます。これにより、差別化された課金と QoS 適用を有効にするダイナミックポリシーが許可されます。

- ダイナミックおよび静的 PCC ルール
- 音声の新しいラジオ

合法的傍受

合法的傍受（LI）は、裁判所または行政機関による命令を根拠として、LEA が個人（ターゲット）に対して電子監視を実施できるようにするプロセスです。合法的傍受プロセスを容易にするために、特定の法律および規制によって、サービスプロバイダーおよびインターネットサービスプロバイダーに対して、認可された電子監視を明示的にサポートするようにネットワークを実装することが定められています。サービスプロバイダーが実行するアクションには、ネットワーク内でターゲットアイデンティティをプロビジョニングして、ターゲットの通信の分離（他のユーザーの通信からの分離）を可能にすること、コピーを LEA に送信するための通信の複製、および傍受製品を LEA に配送することが挙げられます。

UPF による合法的傍受のサポートについては、シスコのアカウント担当者にお問い合わせください。

通信使用状況レポート（課金）

UPF の使用状況の測定とレポート機能は、SMF によって制御されます。SMF は、次の方法でこれらの機能を制御します。

- サービスデータフロー、アプリケーション、ベアラー、またはセッション（まだ存在していない場合）を表すために必要な PDR を作成します。
- Charging Key、および Charging Key と Service ID の組み合わせの URR を作成します。また、Charging Key、Sponsor ID および Application Service Provider ID の組み合わせに対する URR を作成します。

  静的ルールの場合、UPF が URR ID を作成することに注意します。URR ID は、UPF で構成されているオンライン/オフラインおよび Content ID + Service ID の組み合わせに基づいて作成されます。
- SDF、セッション、またはアプリケーションレベルでの使用状況レポートのために、PFCP セッションで定義された関連する PDR に URR を関連付けます。
- オンライン課金では、オンライン課金サーバー（OCS）からボリュームと時間クォータを受信した場合、SMF は、それらをプロビジョニングします。

課金サポート 機能は、このユース ケースに関連しています。

ユーザープレーンの QoS 処理

5G QoS モデルでは、サブスクリプション関連および呼び出し関連の優先順位メカニズムに基づいて、特定のサービスの分類と差別化を行うことができます。これらのメカニズムは、優先

順位が のQoS フローを呼び出す、変更、維持、リリースしたり、ネットワーク輻輳条件でのQoS特性に従ってQoS フローパケットを配信したりする機能を提供します。

ダイナミックおよび静的 PCC ルール 機能は、このユース ケースに関連しています。

ダウンリンク パケット バッファリングおよびデータ通知トリガー処理

バッファリング アクションルール（BAR）は、UPF のバッファリング動作を制御する指示を提供します。BAR は、パケット転送制御プロトコル（PFPC）セッションのすべての転送アクションルール（FAR）のバッファリング動作を制御します。この制御は、パケットをバッファリングしそれぞれの BAR に関連付けることを要求する Apply Action パラメータを PFCP セッションが設定している場合に適用されます。

アイドルモードのバッファリングとページング機能は、このユース ケースに関連しています。

エンドマーカーをソース NG-RAN ノードに転送する

ハンドオーバー手順の時点で、UPF ノードで構成される UE のPDU セッションは、PDU セッションアンカーおよび中間の UPF 終端 N3 参照ポイントとして機能します。SMF は、NG-RAN の新しい AN トンネル情報を含む N4 Session Modification 要求メッセージを送信し、N3 パスに切り替える UPF を指定します。さらに、SMF は、古い N3 ユーザープレーンパスで End Marker パケットを送信する UPF も指定します。UPF が指示を受信すると、End Marker が作成され、古いパスの最後の PDU を送信した後、送信元 NG-RAN に向けて各 N3 GTP-U トンネルに送信されます。

N4 Session Management、Node Level、および Reporting 手順 機能は、このユース ケースに関連しています。

MVNO サポート

SMF は、エンタープライズ MVNO モデルをサポートします。モバイル ネットワーク オペレータは、リースされた MVNO サブスクライバのセカンダリ認証を実行でき、AAA サーバーに関連する追加の機能もサポートできます。

次の機能は、このユース ケースに関連しています。

- APN ACL のサポート （55 ページ）

  選択的なサブスクライバセッションに通信分類とポリシーの適用を適用するための設定可能なメカニズム。

- ダイナミックおよび静的 PCC ルール （237 ページ）

  帯域幅ポリシーあたりのグループ最大数を増加します。

- 仮想ルーティングおよび転送 （623 ページ）

  重複する IP プールと IP プールチャンクをサポートします。

スマートライセンシング

UPF は、Cisco Smart Licensing をサポートします。これは、クラウドベースのライセンスモデルでシスコのソフトウェアアセットの購入、デプロイメント、管理を簡単にします。詳細については、「Smart Licensing」コレクションページを参照してください。

展開アーキテクチャおよびインターフェイス

Cisco UPF は、共通の Mobile Core Platform アーキテクチャを使用する 5GC ネットワーク機能ポートフォリオ（AMF/SMF/NRF/PCF/NSSF/UPF）の一部です。

UPF アーキテクチャ

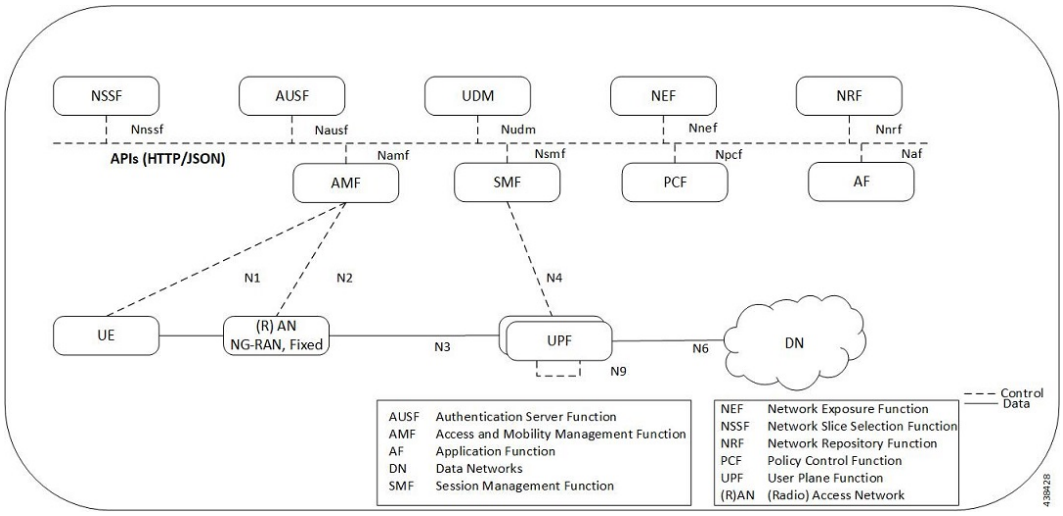
ユーザープレーン機能（UPF）は、3GPP 5G コア インフラストラクチャ システム アーキテクチャの基本的なコンポーネントです。UPF は、コントロールプレーンとユーザープレーンの分離（CUPS）戦略のデータプレーンの進化を表し、最初は 3GPP のリリース 14 仕様の既存の Evolved Packet Cores（EPC）の拡張として導入されました。CUPS 分離パケットゲートウェイ（P-GW）制御およびユーザープレーン機能により、データ転送コンポーネント（PGW-U）の分散化を可能にします。これにより、ネットワークエッジに近い場所でパケット処理と通信集約を実行できるため、ネットワーク負荷を軽減しながら帯域幅の効率性を高めることができます。P-GW 処理シグナリング通信（PGW-C）は、モビリティ マネージメント エンティティ（MME）のノースバウンドのコアに残ります。

CUPS の主な目標は、5G 新しい無線（NR）の実装をサポートし、早期 IoT アプリケーションとより高いデータレートを可能にすることです。CUPS の完全な実装にコミットすることは、ネットワークスライシングを提供する 5G ユーザープレーン機能（5G-UPF）を採用するオペレータにとっては一部の利点しか得られないため、複雑な提案です。仮想マシン（VM）としてデプロイされるユーザープレーン機能は、サービスベースアーキテクチャ（SBA）のパケット処理基盤を提供します。

UPF は、N4 参照ポイント経由で SMF から受信した情報に基づいて、ユーザープレーン通信フローを識別します。N4 インターフェイスは、CUPS のサポートにおいて Sx/N4 参照ポイントで使用するために 3GPP 技術仕様 29.244 で定義されているパケット転送制御プロトコル（PFPC）を採用しています。PFCP は、OpenFlow に似ていますが、モバイルネットワークのサポートに必要な機能のみに制限できます。UPF で確立される PFCP セッションは、パケットの識別方法（パケット検出ルール/ PDR）、転送（転送アクションルール/FAR）、処理（バッファリング アクション ルール/BAR）、マーク（QoS 適用ルール/QER）およびレポート（使用状況レポートルール/URR）を定義します。

UPF デプロイメント アーキテクチャ

次の図は、UPF の大まかなデプロイメント アーキテクチャとその他の NF を示しています。



VM の展開

仮想化パケットコア：単一インスタンス（VPC-SI）

VPC-SI は、StarOS を実行している物理的な Cisco ASR 5500 シャーシの動作を、既製品の（COTS）サーバー上で実行できる 1 つの仮想マシン（VM）に統合します。これは、企業内、リモートサイト内、または顧客のデータセンター内のスタンドアロンの単一仮想マシンとして使用できます。また、VPC-SI を大規模なサービスプロバイダーオーケストレーションソリューションの一部として統合することもできます。

VPC-SI は、サポートされているハイパーバイザ KVM（カーネルベースの仮想マシン）と VMware ESXi とのみ連携します。物理的なデバイスの知識はほとんどないか、まったくありません。

UPF は、5G ベースの VNF デプロイメントでユーザープレーンノードとして機能します。UPF は、StarOS の 1 つのスタンドアロンインスタンスを実行する VNFC としてデプロイされます。展開要件に基づいて拡張性を得るために、複数の UPF VNFC を展開できます。

ハイパーバイザ要件

VPC-SI は、次のハイパーバイザで実行する資格があります。

- カーネルベースの仮想マシン（KVM）：QEMU エミュレータ 2.0 VPC-SI StarOS インストールビルドには、Ubuntu Server 18.04 の仮想マシン作成用の libvirt XML テンプレートと ssi_install.sh が含まれます。

（注） UPF のポートがシャットダウンされ、その後起動した場合、ポートインターフェイスは Ubuntu バージョン 18.04 および NIC ドライバ i40e バージョン 2.12.6 で表示されます。これらのインターフェイスの BGP は自動的に回復しません。

UPF を完全に復元するには、UPF をリロードする必要があります。Ubuntu バージョン 20.04 および NIC ドライバ i40e バージョン 2.17.15 では、ポートインターフェイスと BGP の両方が自動的に回復します。

- KVM：Red Hat Enterprise Linux 7.2：VPC-SI StarOS インストールビルドには、qvpc-si_install.sh というインストールスクリプトが含まれています。
- VMware ESXi 6.7：VPC-SI StarOS インストールビルドには、ESXi GUI を介した VM の作成用の OVF（オープン仮想化フォーマット）と OVA（オープン仮想アプリケーション）のテンプレートが含まれています。

vNIC のオプション

サポートされている vNIC オプションは次のとおりです：

- VMXNET3：VMware 用の準仮想 NIC
- VIRTIO：KMV 用の準仮想 NIC
- ixgbe：Intel 10 ギガビット NIC 仮想機能
- enic：Cisco UCS NIC
- SR-IOV：シングルルート I/O 仮想化。

SR-IOV の仕様は、1 つのルート機能（1 つのイーサネットポートなど）を複数の個別の物理デバイスのように表示できるメカニズムを提供します。Intel 82599 10G は、SR-IOV 対応デバイスであり、PCI 構成スペースで複数の機能（PF および VF）として表示するように（通常はハイパーバイザによって）設定できます。仮想機能（VF）は、Nova 仮想マシンに割り当てることができます。これにより、仮想マシンからの通信がハイパーバイザをバイパスして、ファブリックインターコネクトに直接送信されます。この機能により、仮想マシンへの通信スループットが増加し、UCS サーバーの CPU 負荷が軽減されます。

キャパシティ、CEPS、およびスループット

VPC-SI インスタンスのサイズ変更には、予想されるコールモデルのモデリングが必要です。

サービスタイプの多くは、他よりも多くのリソースを必要としています。パケットサイズ、セッションあたりのスループット、CEPS（コールイベント/秒）レート、IPSec の使用率（サイト間、サブスクライバ、LI）、その他の VM との競合、および基盤となるハードウェアのタイ

プ（CPU の速度、vCPU の数）によって、サブスクライバの最大有効数がさらに制限されます。同等のハードウェアとハイパーバイザ設定でのコールモデルの認定が必要です。

VPP の構成例

5G-UPF の場合、FORWARDER_TYPE は「vpp」です。

次に、VPP 構成の出力例を示します。

```
show cloud configuration
Thursday January 30 12:18:10 UTC 2020
Card 1:
  Config Disk Params:
-------------------------
FORWARDER_TYPE=vpp
VNFM_INTERFACE=MAC:fa:11:3e:22:d8:33
MGMT_INTERFACE=MAC:fa:11:3e:44:af:9e
VNFM_IPV4_ENABLE=true
VNFM_IPV4_DHCP_ENABLE=true
SERVICE1_INTERFACE=MAC:fa:11:3e:11:9d:23
SERVICE2_INTERFACE=MAC:fa:11:3e:99:ec:7b
VPP_CPU_WORKER_CNT=8
VPP_DPDK_TX_QUEUES=9
VPP_DPDK_RX_QUEUES=8
CHASSIS_ID=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

  Local Params:
-------------------------
    No local param file available
```

（注） VPC-SI ビルドコンポーネント、boot パラメータ、VPC-SI boot パラメータの設定、仮想マシンの構成、vCPU と vRAM のオプション、VPP 構成パラメータなどの詳細については、『*VPC-SI* システム アドミニストレーション ガイド』を参照してください。

VPC-SI を使用した UPF のデプロイメント

VPC-SI のその他の情報、サポートされているオペレーティングシステム、ハイパーバイザパッケージ、プラットフォーム構成、ソフトウェアのダウンロードとインストール、UPF デプロイメントの詳細については、シスコのアカウント担当者にご連絡ください。

リリースパッケージの詳細については、このビルドに含まれている対応するリリースノートを参照してください。

SMI Cluster Manager を使用した UPF デプロイメント

Ultra Cloud Core Subscriber Microservices Infrastructure（SMI）は、Cisco Cloud-Native Network Function（CNF）のデプロイおよび管理のためにランタイム環境を提供します。これは、アプリケーションとも呼ばれます。

これは、Kubernetes（K8s）、Docker、Helm、etcd、confd、gRPC などのオープンソースプロジェクトに基づいて構築されており、デプロイした cNF が使用する共通のサービス一式を提供します。

SMIは、マイクロサービスベースのアプリケーションの迅速なデプロイメントとシームレスなライフサイクル運用を可能にするクラウドテクノロジーの階層化されたスタックです。

SMI スタックは、Kubernetes（K8s）クラスターを作成する SMI Cluster Manager とソフトウェアリポジトリで構成されます。SMI Cluster Managerは、デプロイメント、アップグレード、拡張を含むクラスターに対して、継続的なライフサイクル管理（LCM）を行います。

SMI Cluster Manager は、仮想化テクノロジーであるカーネルベースの仮想マシン（KVM）を使用して、ユーザープレーン機能（UPF）仮想マシンをデプロイします。

詳細については、『*UCC SMI* 運用ガイド』を参照してください。

SAEGW-C と SMF の同じ UP プール

SAEGW と SMF は、UP の同じプールを使用できます。ユーザープレーンは、UP と UPF として同時に機能できます。Sx インターフェイス経由で SAEGW に、N4 インターフェイス経由で SMF にサービスを提供できます。SAEGW と SMF の同じサブスクライバ IP プールは、異なる VRF でのみサポートされます。

この機能は、UP および UPF として機能するユーザープレーンに適合しており、5G コール用の 2G、3G、4G RAT、および SMF N4 インターフェイスの CUPS および SAEGW Sx インターフェイス（Sxa、Sxb、および Sxab）を同時にサポートします。

（注） UP と UPF を組み合わせたコールは、このリリースでは認定されません。

サポートするインターフェイス

この項では、UPF と 5GC の他のネットワーク機能との間でサポートされるインターフェイスについて説明します。

- N3：RAN（gNB）と（最初の）UPF 間のインターフェイス。3GPP TS 29.281 および 3GPP TS 38.415（2018 年 10 月）に準拠しています。
- N4：セッション管理機能（SMF）と UPF 間のインターフェイス。3GPP TS 29.244（2018 年 12 月）に準拠しています。
- N6：データネットワーク（DN）と UPF 間のインターフェイス。3GPP TS 29.561（2018 年 12 月）に準拠しています。
- Sx：Evolved Packet Core（EPC）の分割型 P-GW、S-GW、および TDF アーキテクチャでのコントロールプレーンとユーザープレーン間のインターフェイス。3GPP TS 23.214 および 3GPP TS 33.10 に準拠しています。

標準準拠

Cisco UPF は、以下の基準に準拠しています：

- コントロールプレーンとユーザープレーンノード間のインターフェイス：3GPP TS 29.244 バージョン 15.4.0。（2018 年 12 月）
- General Packet Radio System (GPRS) Tunneling Protocol User Plane（GTPv1-U）：3GPP TS 29.281 バージョン 15.5.0（2018 年 12 月）。
- NG-RAN：PDU Session User Plane protocol：3GPP TS 38.415（2018 年 12 月）
- 5G システム：5G ネットワークおよび外部データネットワーク間のインターワーキング、ステージ 3：3GPP TS 29.561（2018 年 12 月）

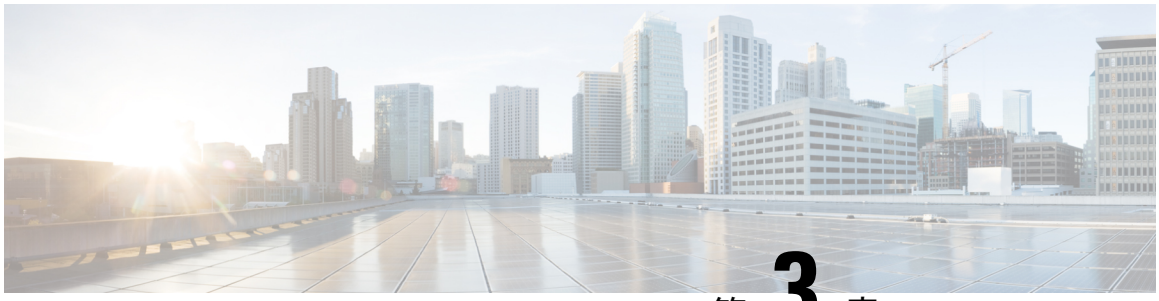


第 部

特長と機能

- 1:1 冗長性 （23 ページ）
- ダイナミックルール向け ADC （47 ページ）
- APN ACL のサポート （55 ページ）
- APN AMBR トラフィックポリシング （61 ページ）
- バルク統計サポート （65 ページ）
- 課金サポート （69 ページ）
- VPP による Cisco Ultra Traffic Optimization （89 ページ）
- N4 インターフェイス経由の使用状況データの収集とレポート （101 ページ）
- コントロールプレーンが開始する N4 アソシエーションのサポート （107 ページ）
- コンバージドデータパス （111 ページ）
- ディープ パケット インスペクションとインラインサービス （133 ページ）
- EDNS0 レコードのデバイス ID （201 ページ）
- ダウンリンク データ通知 （211 ページ）
- Collapse コールの DSCP マーキング （229 ページ）
- ダイナミックおよび静的 PCC ルール （237 ページ）
- ECS 正規表現 （247 ページ）
- GTP-U のサポート （253 ページ）
- N4/Sx インターフェイスのハートビートサポート （261 ページ）
- アイドルモードのバッファリングとページング （267 ページ）
- 間接転送トンネル （273 ページ）
- DHCP サーバー経由の IP 割り当て （281 ページ）

- IPv6 向け IPsec サポート （295 ページ）
- IPv6 プレフィックス委任 （303 ページ）
- LTE：Wi-Fi のシームレスハンドオーバー, on page 311
- モニタ サブスクライバ, on page 323
- UPF での MPLS のサポート （345 ページ）
- 複数の cnSGW のサポート （357 ページ）
- 複数の N4/Sx インターフェイス （361 ページ）
- ネクストホップ転送サポート （367 ページ）
- N:M 冗長化および冗長化構成マネージャ （385 ページ）
- PDU セッション情報の N3 転送 （387 ページ）
- 3GPP 仕様との N4 インターフェイスの準拠 （391 ページ）
- N4 インターフェイスの構成 （397 ページ）
- IPSec 経由の N4/Sx （403 ページ）
- N4 Session Management、Node Level、および Reporting 手順 （417 ページ）
- NRF のサポート （441 ページ）
- パスワード期限切れ通知 （449 ページ）
- UPF での QCI 80 のサポート （453 ページ）
- Ruledefs の QoS グループのサポート （459 ページ）
- ローミングのサポート, on page 467
- セキュリティグループタグ（SGT）ベースのアクセスコントロール （501 ページ）
- セッションリカバリ （519 ページ）
- Session Report Rejection 手順 （527 ページ）
- ソフトウェア管理の運用 （531 ページ）
- 標準 QCI のサポート, on page 539
- システム ログ （541 ページ）
- UPF 入力インターフェイス （581 ページ）
- UPF ローカル構成 （597 ページ）
- N4/Sx インターフェイス経由の負荷と過負荷の制御 （601 ページ）
- PCF 経由の使用状況の監視 （617 ページ）
- CPU サイクルの可変解放 （619 ページ）
- 仮想ルーティングおよび転送 （623 ページ）
- 音声の新しいラジオ （635 ページ）
- WPS 優先順位 （639 ページ）
- X ヘッダーの挿入と暗号化 （649 ページ）



第 3 章

1:1 冗長性

- 機能の概要と変更履歴 （23 ページ）
- 機能説明 （24 ページ）
- 機能の仕組み （24 ページ）
- 1:1 UPF 冗長性を構成する （31 ページ）
- モニタリングおよびトラブルシューティング （37 ページ）
- L2 ICSR のサポート （40 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
L2 ICSR のサポートが追加されました。	2023.01.0

改訂の詳細	リリース
次の機能のサポートが追加されました。 • ユーザープレーン機能の会計上のゼロ損失 • 早期 PDU リカバリ • リカバリ中のセッションの優先順位付け • UPF の状態を Pending-Active から Active に変更するための構成	2021.02.0
最初の導入。	2020.02.0

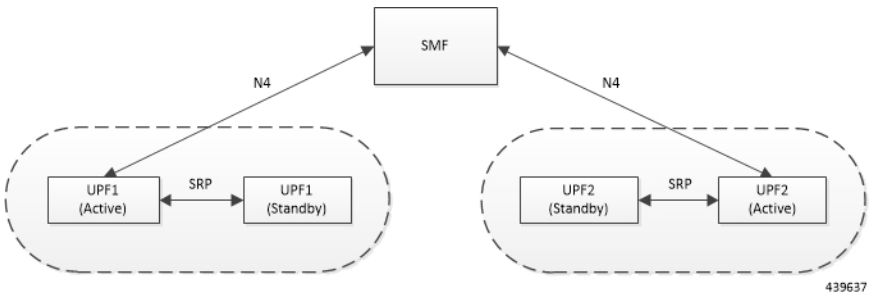
機能説明

5Gデプロイメント向けの1:1 UPF冗長化機能は、障害が発生したユーザープレーン機能（UPF）を検出し、障害が発生した UPF の機能をシームレスに処理します。各アクティブ UPF には専用のスタンバイ UPF があります。1:1 UP 冗長化アーキテクチャは、UPF から UPF へのシャーシ間セッションリカバリ（ICSR）接続に基づいています。

機能の仕組み

次の図に示すように、5G-UPF デプロイメントは、UPF ノードの チェックポイント指定とスイッチオーバーにICSR フレームワーク インフラストラクチャを使用します。アクティブ UPF は、UPF 間でプロビジョニングされた Service Redundancy Protocol（SRP）リンク経由で専用のスタンバイ UPF と通信します。

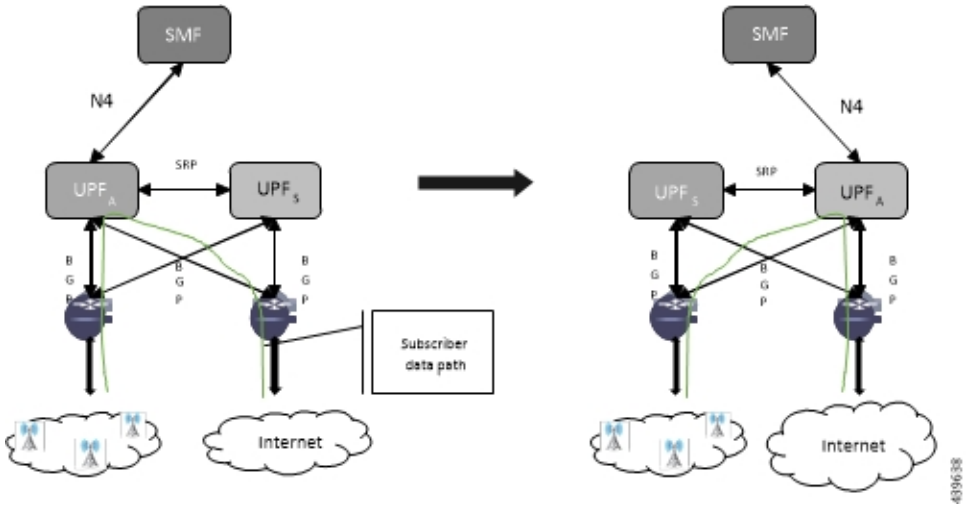
図 *5 : SRP* を使用した *UPF* の *1:1* 冗長化



セッション管理機能（SMF）ノードには、UPF グループ構成で使用可能なスタンバイ UPF 情報がありません。このため、SMF は、UPF の冗長性構成と UPF 間のスイッチオーバーイベントを認識しません。

アクティブ UPF は、UPF で構成された N4 インターフェイスアドレス経由で SMF と通信します。スタンバイ UPF は、スイッチオーバーイベント中に Active に移行する際に、同じ Sx インターフェイスアドレスを引き継ぎます。これは、Sx/N4 インターフェイスが SRP によってアクティブ化され、既存の設定メソッドに準拠していることを意味します。したがって、UPF スイッチオーバーは SMF に対して透過的です。

図 *6 : UPF* の *1:1* 冗長化スイッチオーバー



1:1 の冗長性に完全に準拠するため、5G 環境の SRP ベースの ICSR に対する次の依存関係に対応します。

- 構成の同期（または、スタンバイ UPF でのレプリカ構成）
- Sx/N4 アソシエーション チェックポイント
- Sx/N4 リンクモニタリング

上記の依存関係に加えて、UPF は UPF ノードに固有の Data Collection 手順および Checkpoint 手順を実装します。たとえば、IP プールチャンクのチェックポイント指定などです。UPF は、これらの手順を既存の ICSR チェックポイント指定フレームワークに統合します。

スタンバイ UPF の独立した構成

UPF が基本構成（サービス、コンテキスト、インターフェイスなど）で起動した後、残りの構成（たとえば、ACS やポリシー関連の構成）は、Ops-Center または冗長化および構成マネージャ（RCM） Pod 経由で行われます。この構成は、SMF ポリシーと UPF ポリシーの両方に共通です。SRP の冗長性を機能させるため、アクティブ UPF とスタンバイ UPF の間で SRP 接続が確立される SRP 関連の設定を除き、アクティブ UPF とスタンバイ UPF の設定は同じです。RCM は、アクティブ UPF とスタンバイ UPF を個別に設定します。

アクティブ UP とスタンバイ UP 間の BFD モニター

Bidirectional Forwarding Detection（BFD）は、迅速にエラー検証とスイッチオーナーを行うために、アクティブ UPF とスタンバイ UPF 間の SPR リンクを監視します。スタンバイ UPF がこのリンクで BFD 障害を検出すると、アクティブ UPF を引き継ぎます。

BFD リンクは、シングルホップまたはマルチホップが可能です。

アクティブ UP と スタンバイ UP 間に BFD モニターを構成するには、「アクティブ *UPF* と スタンバイ *UPF* 間に *BFD* モニタリングを構成する」を参照してください。

マルチホップ BFD モニタリングの設定例

プライマリ UPF：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.225 chassis-to-chassis
      peer-ip-address 209.165.200.225
      bind address 209.165.201.1
    #exit
    interface srp
      ip address 209.165.201.1 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.201.1 209.165.200.225
    ip route 209.165.201.1 255.255.255.224 209.165.201.1 srp
  #exit
end
```

バックアップ UPF：

```
config
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.201.1 interval 50 min_rx 50 multiplier 20
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.201.1 chassis-to-chassis
      peer-ip-address 209.165.201.1
      bind address 209.165.201.1
    #exit
    interface srp
      ip address 209.165.201.1 255.255.255.224
    #exit
    ip route static multihop bfd bfd1 209.165.200.225 209.165.201.1
    ip route 209.165.201.1 255.255.255.224 209.165.200.225 srp
  #exit
End
```

プライマリ UPF とバックアップ UPF 間のルータ：

```
config
  context one
    interface one
      ip address 209.165.201.1 255.255.255.224
    #exit
    interface two
      ip address 209.165.200.225 255.255.255.224
    #exit
```

```
  #exit
end
```

シングルホップ BFD モニタリングの構成例

プライマリ UPF：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.201.1 chassis-to-chassis
      peer-ip-address 209.165.201.1
      bind address 209.165.201.4
    #exit
    interface srp
      ip address 209.165.201.1 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 209.165.201.4
  #exit
end
```

バックアップ UPF：

```
config
  context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      monitor bfd context srp 209.165.200.225 chassis-to-chassis
      peer-ip-address 209.165.201.4
      bind address 209.165.201.7
    #exit
    interface srp
      ip address 209.165.201.4 255.255.255.224
      bfd interval 50 min_rx 50 multiplier 10
    #exit
    ip route static bfd srp 209.165.201.7
  #exit
end
```

VPP モニター

SRP VPP モニターが構成されている場合、UPF シャーシは SRP アクティブであり、VPP サブシステムに障害が発生すると、SRP はスタンバイ UPF へのスイッチオーバーを開始します。現在、VPP ヘルスモニタリングは、NPUMgr タスクと VPP プロセス間のハートビートメカニズムに限定されています。

VPP モニターを構成するには、「アクティブ *UPF* および スタンバイ *UPF* に *VPP* モニターを構成する」を参照してください。

Sx/N4 アソシエーション チェックポイント

アクティブ UPF が、SMF に対して Sx/N4 アソシエーションを開始すると、スタンバイ UPF は、このデータをチェックポイントします。これにより、UPF スイッチオーバー後もアソシエーション情報が保持されます。

Sx/N4 Heartbeat メッセージが送信され、アクティブ UPF 、連続して UPF のスイッチオーバーが発生した後も応答します。

Sx/N4 モニター

UPF と SMF 間の Sx/N4 インターフェイスを監視することは重要です。SRP モニタリングは Sx/N4 インターフェイスで有効になり、既存の Sx/N4 ハートビートメカニズムを利用してモニター障害を検出します。アクティブ UPF の Sx/N4 モジュールは、障害を検出すると、SRP VPNMgr に UPFスイッチオーバーイベントをトリガーし、スタンバイ UPF が引き継ぐようにします。

（注） Sx/N4 モニタリングは UPF でのみ使用できます。

SMF Sx/N4 ハートビートタイムアウトが、UPF Sx/N4 ハートビートタイムアウトと UPF ICSR スイッチオーバ—タイムとり高いことが重要です。これは、UPF Sx/N4 監視エラーが原因で、SMF が、UPF スイッチオーバ—中に Sx/N4 パスを検出しないためです。

スタンバイ UPF 自体に SMF との独立した接続はありません。アクティブ UPF Sx/N4 コンテキストが スタンバイ UPF に複製されることで、SRP スイッチオーバー時のテイクオーバー準備が整います。これは、Sx/N4 監視エラーが原因でアクティブ UPF がスタンバイに切り替わった場合、新しいスタンバイは UPF から SMF へのリンクが機能しているかどうかを把握できないことを意味します。新しいアクティブ UP での Sx モニター障害が原因で、新しい スタンバイ UP が再びアクティブ状態にスイッチバックされないようにするには、新たな **monitor sx** CLI コマンドで **disallow-switchover-on-peer-monitor-fail** キーワードを使用します。

Sx/N4 監視エラーが原因でシャーシがスタンバイになった後、Sx/N4 チェックポイントが新しいアクティブ UPF から受信されても、Sx/N4 監視エラーはリセットされません。これは、前回のスイッチオーバーを引き起こしたそもそもの原因が Sx/N4 監視エラーであった場合に、Sx/N4 監視エラーによって、再び新しいアクティブの計画外のスイッチバックが起こるのを防ぐためです。これにより、SMF の停止時に、連続したスイッチオーバーが起こるのを防ぎます。Sx/N4 監視エラー状態は、ネットワーク接続が正常であるという確信が得られたら、オペレータが手動でリセットする必要があります。リセットするには、スタンバイシャーシで新しい **srp reset-sx-fail** CLI コマンド（「*Sx* モニター障害のリセット」を参照）を使用します。

Sx/N4 モニターを構成するには、「アクティブ *UPF* およびスタンバイ *UPF* での *Sx/N4* モニタリングの構成」を参照してください。

Sx/N4 モニター：Pending-Active

UPF シャーシは、次のいずれかの理由で Pending-Active 状態になることがあります。

- SMF アップグレード中に Sx/N4 ハートビートがタイムアウトすると、Sx/N4 接続は終了します。したがって、Sx/N4 監視エラーにより、UPF で ICSR スイッチオーバーがトリガーされます。このスイッチオーバーにより、古いスタンバイ UPF が Pending-Active 状態に移行します。Pending-Active 状態の UPF は、SMF から Sx/N4 ハートビートもサブスクライバ通信も受信しません。その結果、UPF は無期限に Pending-Active 状態のままになり、手動での介入なしでは使用できません。

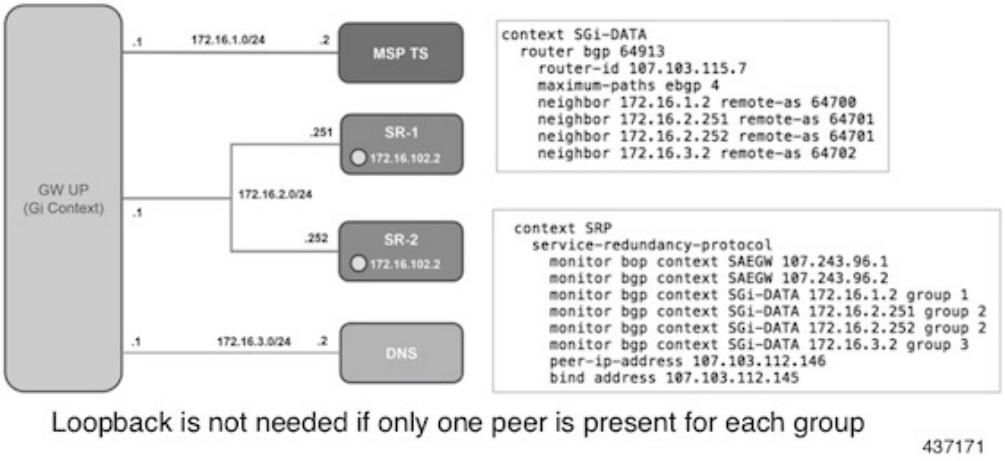
- UPF をアップグレードするための適切な手順に従わない場合、UPF の 1 つが Pending-Active 状態になる可能性があります。また、UPF のアップグレード中に SMF が停止した場合、または UPF のスイッチオーバーに SMF ハートビートタイムアウトよりも長い時間がかかる場合、UPF の 1 つが無期限に Pending-Active 状態のままになります。
- ネットワークの問題が原因で SMF と UPF の間で Sx/N4 セッションがタイムアウトし、UPF ICSR スイッチオーバーがほぼ同時に発生した場合（二重障害シナリオ）、Pending-Active 状態の UPF はアクティブ状態に移行しません。

UPF シャーシが Pending-Active 状態になるたびに、UPF を Pending-Active 状態から Active 状態に強制的に移行するコールバックでタイマーを開始します。移行を強制する前に、SRP リンクが稼働していて、SRP ピアがスタンバイ状態であるかを確認します。そうでない場合は、タイマーを再起動します。タイマーの期間は、**force-pactv-to-actv-timeout** *value_seconds* CLI コマンドを使用すると構成できます（構成の詳細については、「*Pending-Active* 状態から *Active* 状態に *UPF* 状態を変更する」項を参照してください。）。この CLI コマンドが構成されていない場合、UPF は無期限に Pending-Active 状態のままになります。

BGP モニター

UPF（Gi 側と Gn 側の両方）からネクストホップルータの BGP ピアモニターとピアグループモニターを構成します。これは既存の ICSR 設定です。BGP は、迅速な BGP ピア障害の検出のため、BFD によるサポートと併せて実行できます。

図 *7: BGP* ピアグループと回送



BGP モニタリングを設定し、BPG モニタリング障害にフラグを立てるには、「各 *UP* とネクストホップルータ間の *BGP* 状態モニタリングを構成する」を参照してください。

UPF セッションチェックポイント

アクティブシャーシは、次のシナリオで、UPF データのコレクションをチェックポイントとしてピアスタンバイシャーシに送信します。

- 新しいコールのセットアップ時

- コールの状態が変化するたびに
- アカウンティングバケット用に定期的に

これらのチェックポイントを受信すると、スタンバイシャーシはデータに基づいて動作し、コール、ノードまたはインスタンスレベルで必要な情報を更新します。

VPN IP プールのチェックポイント

Sx/N4 アソシエーション中に、各 UPF に割り当てられた IP プールは、SMF によってそれぞれの UPF に送信されます。VPNMgr はこのメッセージを UPF で受信して、SRP が構成された場合、スタンバイ UPF で同じ情報をチェックポイントします。

IP プール情報は、SRP VPNMgrR の再起動中、および SRP リンクのダウンおよびアップシナリオ中にも送信されます。

スイッチオーバーの前に、スタンバイに IP プール情報が存在することを検証することが重要です。IP プール情報が存在しない場合、ルートアドバタイズメントができないため、通信は UPF に到達しません。

外部監査と PFD 設定監査のインタラクション

外部監査管理は、アクティブ UPF で行われます。セッションマネージャが、構成監査の開始通知と完了通知を受け取ります。構成監査が進行していない場合、セッションマネージャは、外部監査を開始しません。外部監査の実行中に構成監査の開始通知が到着した場合、セッションマネージャはフラグを設定し、外部監査の完了後に外部監査が再開されるようにします。構成監査がすでに実行中の場合、外部監査を実行しても目的を達成できないため、外部監査を再開する必要があります。

ユーザープレーン機能における会計上のゼロ損失

ユーザープレーン機能（UPF）に会計上のゼロ損失機能が実装されました。これにより会計データまたは請求ロスを、Active UPF から Standby UPF へのデフォルトのチェックポイント時間である 18 秒、または構成された課金チェックポイント時間から削減します。

これは、Gz、Gy、VoGx、および RADIUS URR をサポートするために UPF で変更されました。会計上のゼロ損失/URR データカウンタ損失では、計画的スイッチオーバーのみがサポートされます。この機能は、現行の ICSR フレームワークや、チェックポイント指定およびリカバリ方法には影響しません。

Sx/N4 使用状況レポートは、シャーシが Pending Active 状態からアクティブになるまでブロックされます。

UPF セッションリカバリに向けた早期 PDU リカバリ

早期 PDU リカバリ機能は、これまでのセッションリカバリ機能が抱えていた、リカバリ対象として選択された CRR に優先順位が行われないという制限を克服します。これまでは、すべての CRR が AAAMgr から取得され、コールが順番に回復されていました。すべての CRR を取得するのにかかる時間が、セッションリカバリ中に認識される遅延の主な要因でした。障害が発生した際に、セッションマネージャに多数のセッションがあると、遅延が非常に長くなる

ことがありました。また、コールのリカバリに特定の順序がないため、アクティブセッションよりも前にアイドルセッションが回復されることもありました。

（注） 早期 PDU リカバリ機能は、最大 5% のセッションを回復できます。

リカバリ中のセッションの優先順位付け

この機能がないと場合、セッションリカバリ機能はリカバリ対象として選択されたセッションに優先順位を付けず、コールリカバリリスト内のすべてのコールをループ処理し、セッションリカバリがトリガーされると順番に回復していました。

リカバリにおけるセッション優先の一環として、優先コールのみを対象に別途スキップリストを保持します。該当するレコードがループ処理によらず、AAAMgrからすぐに送信できるようにするためです。その結果、優先コールの迅速なリカバリとデータ停止時間の短縮につながります。

ユーザープレーンには、優先セッションと通常セッションの2種類のセッションがあります。セッションが優先セッションかどうかは、SMFから受信したメッセージの優先順位フラグに基づいて判別され、優先セッションがまず回復され、その後に通常のコールが続きます。これらの優先セッションは、早期 PDU 処理でも優先されます。通常コールの早期 PDF のリカバリは、すべての優先セッションがリカバリされてから、開始されます。

クリティカルフラッシュ（GR）の場合、まず優先セッションのチェックポイントが送信され、その後に通常のコールが送信されます。スイッチオーバー中は、すべてのコール（通常コールと優先コールの両方）のデータが許可されます。

（注） SMF がすべてのコールに優先順位フラグを設定します。UPF は、SMF から受信した優先コールの詳細を、セッション優先機能に使用します。

1:1 UPF 冗長性を構成する

次の項では、この機能のサポートで利用可能な CLI コマンドの情報について説明します。

アクティブ UPF とスタンバイ UPF 間の BFD モニタリングを構成する

アクティブ UPF とスタンバイ UPF で Bidirectional Forwarding Detection（BFD）の 監視を構成するには、次の構成を使用します。このコマンドは、SRP 構成モードで構成します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bfd context context_name { ipv4_address | ipv6_address
```

```
} { chassis-to-chassis | chassis-to-router }
        end
```

注：

- **no**：アクティブ UPF とスタンバイ UPF で BFD 監視を無効にします。
- **context** *context_name* ：使用するコンテキストを指定します。BFD ピアが設定されているコンテキスト（SRP コンテキスト）を参照します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- *ipv4 _address* | *ipv6_address*：モニターする BFD ネイバーの IP アドレスを定義します。これは、IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

  設定された BFD（ICSR）ピアの IP アドレスを参照します。
- **chassis-to-chassis** | **chassis-to-router**：

  chassis-to-chassis：非 SRP リンク上のプライマリシャーシとバックアップシャーシの間で BFD を実行できるようにします。

  chassis-to-router：BFD はシャーシとルータの間で動作します。



注意　アクティブ UPF とスタンバイ UPF 間の SRP リンクで BFD 監視に対して **chassis-to-router** キーワード使用しないでください。

- このコマンドはデフォルトでは無効になっています。

各 UPF とネクストホップ ルータ間の BGP 状態モニタリングを構成する

次のコマンドを使用して、各 UPF とネクストホップルータ間にボーダー ゲートウェイ プロトコル（BGP）を構成します。このコマンドは、SRP 構成モードで構成されます。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp context bgp-session-context-name [
nexthop-router-ipv4-address | nexthop-router-ipv6-address ] { vrf
bgp-session-vrf-name } { group group-number  }
        end
```

注：

- **no**：UPF で BGP 状態モニタリングを無効にします。

- **bgp context** *bgp-session-context-name*：BGP ピアが構成されているコンテキストを指定します。*bgp-session-context-name* は、コンテキスト文字列を指定します。
- **nexthop-router-ipv4-address | nexthop-router-ipv6-address**：監視する構成済みの BGP ピア IPv4 または IPv6 アドレスを指定します。
- **vrf** *bgp-session-vrf-name*：BGP VPN Routing and Forwarding (VRF) インスタンスを指定します。*bgp-session-vrf-name* は、VRF 名を指定します。
- **group** *group-number* ：BGP ピアを含める BGP ピアグループを指定します。*group-number* は、グループ番号を指定します。

  このキーワードを実装すると、動作は次のようになります。

  - そのグループの BGP ピアが稼働すると、BGP ピアグループも稼働します。

    BGP モニターのグループ構成を省略すると、そのモニターはグループ 0 に含まれます。

    BGP グループ 0 は、暗黙的なグループからのコンテキストでモニターされました。各コンテキストは、個別の BGP グループ 0 の暗黙的モニターグループを形成します。

    いずれかの BGP ピアグループが停止している場合、BGP モニターは停止します。

- このコマンドは、デフォルトでディセーブルになっています。

BGP モニタリングのエラーにフラグを立てるための代替アルゴリズム

このリリースでは、代替（新規）アルゴリズムが導入され、BGP監視エラーにフラグを立てられるようになりました。

次のコマンドを使用して、単一BGPピア（ユーザープレーン機能）エラーが発生した際にBGP監視エラーにフラグを立てます。このコマンドは、SRP 構成モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor bgp exclusive-failover
      end
```

注：

- **no**：単一の BGP ピア障害時の BGP モニター障害のフラグ設定を無効にします。
- 新しい **exclusive-failover** キーワードを実装すると、動作は次のようになります。
  - BGP ピアグループ内のいずれかの BGP ピアが稼働している場合、BGP ピアグループは稼働します。
  - BGP ピアをグループ 0 に含めることは、非グループ化（グループを省略する）と同じです。
  - いずれかの BGP ピアグループまたは非グループ BGP ピアがダウンすると、BGP モニターはダウンします。

- このコマンドはデフォルトでは無効になっています。

アクティブ UPF およびスタンバイ UPF で Sx/N4 モニタリングを構成する

アクティブ UPF およびスタンバイ UPF で Sx/N4 モニタリングを構成するには、次の構成を使用します。このコマンドは、SRP 構成モードで設定します。

```
configure
  context context_name
    service-redundancy-protocol
      [ no ] monitor sx [ { context context_name | bind-address
{ipv4_address |ipv6_address } | { peer-address { ipv4_address | ipv6_address }
} ]
      end
```

注：

- **no**：アクティブおよび スタンバイ UPF で Sx/N4 モニタリングを無効にします。
- **context***context_name*：Sx/N4 サービスのコンテキストを指定します。

  context_name は、1 ～ 79 文字の英数字で表される既存のコンテキストである必要があります。
- **bind-address {** *ipv4 _address* **|** *ipv6_address* **}**：Sx/N4 サービスのサービス IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。

（注） **bind-address** および **peer-address** の IP アドレスファミリは同じである必要があります。

- **peer-address {** *ipv4 _address* **|** *ipv6_address* **}**：Sx/N4 ピアの IP アドレスを定義します。IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記を使用して入力します。
- **disallow-switchover-on-peer-monitor-fail**:

  UPF から SMF へのリンクの動作状態が不明な場合に、UPF が [アクティブ（Active）] 状態にスイッチバックされるのを防止します。
- 複数の Sx/N4 接続をモニタリングする場合には、この CLI コマンドを複数回実装できます。
- モニター対象の Sx/N4 接続のいずれかが停止すると、Sx/N4 のモニター状態も停止します。
- このコマンドは、デフォルトでディセーブルになっています。
- 最大 18 のピアノードを構成できます。

アクティブ UPF およびスタンバイ UPF で VPP モニターを構成する

次の構成を使用して、Vector Packet Processing（VPP）を構成し、VPP が停止した場合に、アクティブ UPF で UPF スイッチオーバーがトリガーされるようにします。このコマンドは、SRP 構成モードで設定します。

```
configure
   context context_name
      service-redundancy-protocol
        monitor system vpp delay-period seconds
        end
```

注：

- 以前に構成されている場合は、**no monitor system vpp** CLI コマンドを使用して、アクティブおよびスタンバイ UPF で VPP モニタリングを無効にします。
- **vpp delay-period** *seconds* ：VPP 障害後のスイッチオーバーの遅延時間を秒単位で指定します。*seconds* は、0 ～ 300 の値を指定する必要があります。

  遅延時間が 0 より大きい値の場合、VPP に障害が発生すると、指定された遅延時間の後にスイッチオーバーが開始されます。遅延時間内の最後の VPP ステータス通知が、スイッチオーバーアクションの最終トリガーです。デフォルト値は 0 秒で、すぐにスイッチオーバーが開始されます。

  遅延は、VPP が一時的にダウンし、回復が進行中のシナリオに対処するために必要です。これは、スイッチオーバーが不要な場合があることを意味します。
- このコマンドはデフォルトでは無効になっています。

ユーザープレーンのスイッチバックを防止する

次の構成を使用して、新しいアクティブ UPF で Sx/N4 の監視に失敗したことによって、新しいスタンバイ UPF が再びアクティブ状態にスイッチバックするのを防ぎます。

```
configure
   context context_name
      service-redundancy-protocol
        monitor sx disallow-switchover-on-peer-monitor-fail timeout
seconds
        end
```

次のいずれかの CLI を使用して、新しいスタンバイ UPF からアクティブ状態へのスイッチバックを許可します。

```
no monitor sx disallow-switchover-on-peer-monitor-fail
```

または

```
monitor sx disallow-switchover-on-peer-monitor-fail timeout 0
```

注：

- **no**：スイッチオーバー防止を無効にします。
- **disallow-switchover-on-peer-monitor-fail [timeout** *seconds* **]** ：UPF から SMF へのリンクの動作状態が不明な場合に、UPF がアクティブ状態にスイッチバックされるのを防止します。

  timeout *seconds*：スタンバイピアで Sx/N4 エラー状態がリセットされない場合でも、このタイムアウトの経過後にスイッチバックを許可します。有効な値の範囲は、0 ～ 2073600（24 日）です。

（注） タイムアウトを 0 秒に指定すると、計画外のスイッチオーバーが可能になります。

timeout キーワードが指定されていない場合、アクティブシャーシはスタンバイピアで Sx/N4 エラー状態がリセットされるまで無期限に待機します。

- デフォルト設定では、あらゆる条件において、Sx/N4 モニターエラーによる計画外のスイッチオーバーが許可されます。

（注） 手動による計画的スイッチオーバーは、この CLI が設定されているかどうかに関係なく許可されます。

デュアル アクティブ エラー シナリオの防止

CP で次の CLI 設定を使用して、UPF 1:1 冗長性のデュアル アクティブ エラー シナリオを回避します。

```
configure
    user-plane-group group_name
       sx-reassociation disabled
       end
```

注：

- **sx-reassociation disabled**：CP との関連付けがすでに存在する場合、UP Sx の再関連付けを無効にします。

Sx/N4 モニター障害をリセットする

次の構成は、Service Redundancy Protocol (SRP) Sx/N4 モニター障害情報をリセットする際に、スタンバイシャーシのみで使用します。このコマンドは、EXEC モードで設定します。

```
srp reset-sx-fail
```

UPF 状態を保留アクティブからアクティブに変更する

次の構成を使用して、UPF シャーシの状態を Pending-Active から Active に変更します。

```
configure
   context context_name
      service-redundancy-protocol
         force-pactv-to-actv-timeout value_seconds
```

注：

- *value_seconds*：タイムアウト値を秒単位で指定します。1 ～ 300 の範囲で指定する必要があります。
- **show config context** *context-name* CLI コマンドを使用知って、構成を確認します。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できるCLIコマンドに関する情報を提供します。

show コマンドや出力

この項では、この機能のサポートにおけるshowコマンドまたはその出力について説明します。

show srp monitor bfd

この CLI コマンドの出力には、5G UPF 1:1 UP 冗長性機能に関する次のフィールドが含まれます。

- 次のように入力します。
  - (A) - Auth. probe
  - (B) - BGP
  - (D) - Diameter
  - (F) - BFD
  - (E) - EGQC
  - (C) - Card
  - (V) - VPP
- 状態：
  - (I) - Initializing
  - (U) - Up
  - (D) - Down

- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp monitor bgp

この CLI コマンドの出力には、5G UPF 1:1 UPF 冗長性機能に関する次のフィールドが含まれます。

- 次のように入力します。
  - (A) - Auth. probe
  - (B) - BGP
  - (D) - Diameter
  - (F) - BFD
  - (E) - EGQC
  - (C) - Card
  - (V) - VPP
  - (S) - Sx
- 状態：
  - (I) - Initializing
  - (U) - Up
  - (D) - Down
- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp monitor sx

この CLI コマンドの出力には、Sx/N4 監視状態をサポートする次のフィールドが含まれます。

- 次のように入力します。
  - (A) - Auth. probe

- (B) - BGP
- (D) - Diameter
- (F) - BFD
- (E) - EGQC
- (C) - Card
- (V) – VPP
- (S) - SX

- 状態：
  - (I) - Initializing
  - (U) - Up
  - (D) - Down

- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp monitor vpp

この CLI コマンドの出力には、5G UPF 1:1 UPF 冗長性機能に関する次のフィールドが含まれます。

- 次のように入力します。
  - (A) - Auth. probe
  - (B) - BGP
  - (D) - Diameter
  - (F) - BFD
  - (E) - EGQC
  - (C) - Card
  - (V) - VPP

- 状態：
  - (I) - Initializing
  - (U) - Up

- (D) - Down

- GroupId
- IP Addr
- Port
- Context (VRF Name)
- Last Update

show srp statistics

この CLI コマンドの出力には、Sx/N4 モニター - Pending-Active 機能の次のフィールドが含まれます。

- Pending-active タイマーの開始
- Pending-active タイマーの停止
- Pending-active から Active forced
- Pending-active から Active force-failed
- Pending-active から Active force-skipped - peer-not-sby
- Pending-active から Active force-skipped - not-PActv

L2 ICSR のサポート

機能説明

UPF は、アクティブ UPF とスタンバイ UPF 間のパケット転送を明確にするために、2 サーバーアーキテクチャでレイヤ 2 ベース（L2）ICSR をサポートします。UPF は、Gratuitous Address Resolution Protocol（GARP）Unsolicited Neighbor Advertisement メッセージを使用して L2 ICSR を実現します。

SRP ピア間の L2 ICSR は、SRP コンテキストで設定できます。UPF は、物理インターフェイスと同じサブネットの下にループバック インターフェイスも設定します。UPF は、アクティブからアクティブへのシナリオを回避するために SRP BFD モニタリングをサポートしています。

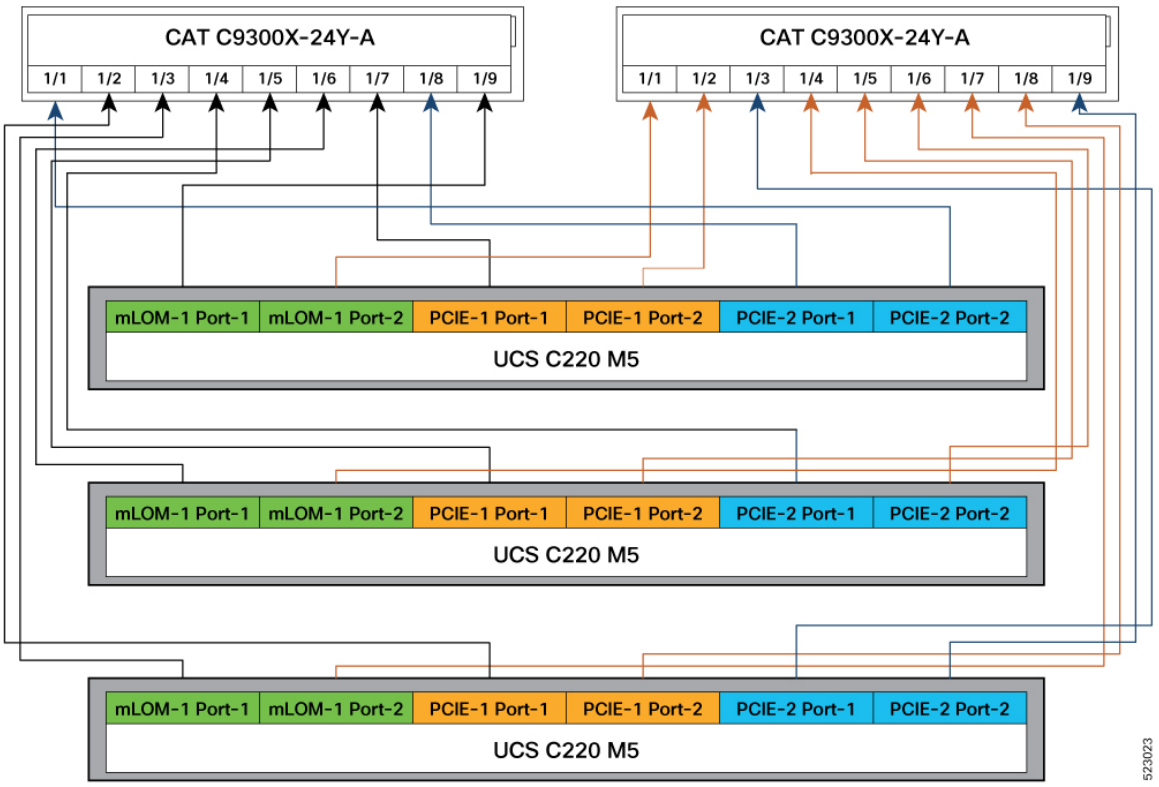
SRP ループバック インターフェイス

SRP ループバック インターフェイスは、サービス IP（N3）のループバック インターフェイスまたは IP プール（N6）のネクストホップ IP です。これらのループバック インターフェイスの IP アドレスは、コンテキストのイーサネット インターフェイスと同じサブネットにある必要があります。SRP ループバック インターフェイスは、アクティブおよびスタンバイの両方の UPF で同じ IP アドレスを持ちます。

- UPF が Standby の場合、SRP ループバック インターフェイスは ARP 応答または GARP パケットを送信しません。IPv6 の場合、UPF は Solicited または Unsolicited Neighbor Advertisement メッセージで応答しません。
- UPF がスタンバイの場合、SRP ループバック インターフェイスは、Boxer 内で IP アドレスが接続された状態で有効になります。これにより、これらのインターフェイスにバインドされた UPF サービスは、実行状態のままになります。
- UPF が別の状態からアクティブ状態に移行する際、SRP ループバック インターフェイスは、GARP パケットを送信します。IPv6 の場合、UPF は Unsolicited Neighbor Advertisement メッセージを送信します。

次の図は、非結合インターフェイスの 3RU 配線図を示しています。

図 *8* : 非結合インターフェイスの *3RU* 配線



機能の仕組み

UPF は、同じサブネット内の N3 ルータ上の gNB または N6ルータ上のサーバーに直接接続します。UPF ICSR は、gNB/N3 およびサーバー/N6 には表示されません。

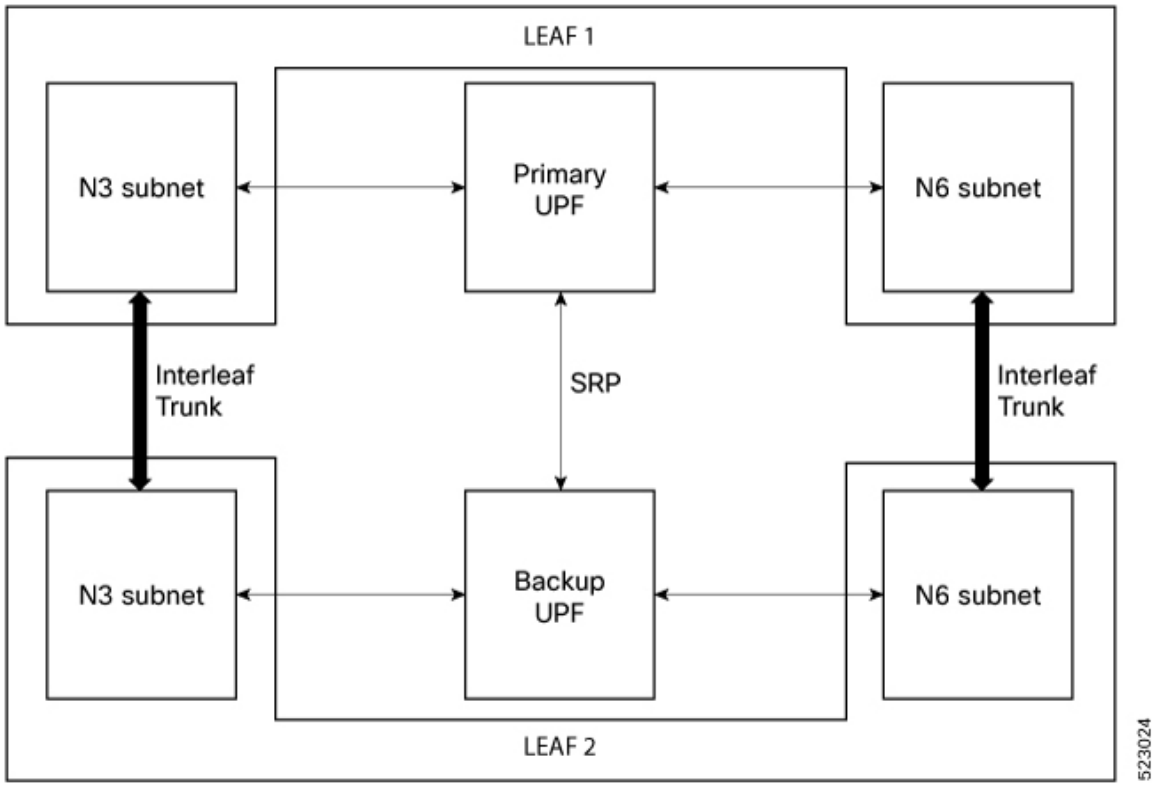
L2 スイッチは、BFD をサポートします。すべての N3 および N6 サブネットで、スイッチには IP アドレスが必要です。

UPF は、L2 ICSR ソリューションを機能させるために、Chassis-Chassis (C-R) BFD および Chassis-Router (C-R) BFD を必要とします。Active-Active 状態を回避するには、C-C および C-R 間で BFD を実行します。BFD には、C-R BFD より高いタイムアウト値を設定する必要があります。

2 リーフネットワーク設計および非結合 UPF インターフェイスの場合、各 UPF は個別のリーフに接続します。L2 スイッチの IP アドレスは、リーフの一部です。

次の図は、非結合インターフェイスの L2 スイッチ配線の概要を示しています。

図 *9:* 非結合インターフェイスの *L2* スイッチ配線



ステートマシン

この表には、UPF の状態に関する情報が表示されています。

表 *5:* ステートマシン

番号	前の状態	内部障害	C-R BFD	C-C BFD	SRP リンク状態	次の状態	BFD のプルダウン
1	X	はい	X	X	X	スタンバイ	はい

番号	前の状態	内部障害	C-R BFD	C-C BFD	SRP リンク状態	次の状態	BFD のプルダウン
2	X	X	Any-Down	X	X	スタンバイ	はい
3	X	いいえ	All-Up	Any-Down	X	アクティブ	いいえ
4	X	いいえ	All-Up	All-Up	ダウン	No-Change	いいえ
5	X	いいえ	All-Up	All-Up	アップ	SRP-Protocol-Decided	いいえ

注：

- C-R BFD が「Not-All-Up」から「All-Up」に移行する場合、SRP 状態処理に遅延が発生し、すべての C-C BFD が安定した状態になります。
- デュアルアクティブシナリオを回避するには、上記の表の 3 行目の状態が両方の UPF で発生しないようにします。これは、正しく動作し構成されたシステムでは発生しません。

SRP コンテキストで L2 ICSR を構成する

SRP ピア間で L2 ICSR を有効または無効にするには、次の構成を使用します。

```
configure
   context context_name
      service-redundancy-protocol
         l2-icsr [ disable | enable ]
         end
```

注：

- **disable**：SRP ピア間の L2 ICSR を無効にします。これがデフォルト設定です。
- **enable**：SRP ピア間の L2 ICSR を有効にします。

プライマリシャーシとバックアップシャーシからの C-C および C-R BFD を構成する

次の手順を実行して、プライマリシャーシとバックアップシャーシからの C-C および C-R BFD を構します。C-C BFD は、マルチホップを構成して、C-R BFD とは異なるタイムアウト値を指定します。

```
context SAEGW
bfd-protocol
  bfd multihop-peer 209.165.200.227 interval 50 min_rx 50 multiplier 6
#exit
interface S5_SGW_PGW
  ip address 209.165.200.226 255.255.255.0
  ipv6 address 2001:DB8:A:B::1/64 secondary
  bfd interval 50 min_rx 50 multiplier 3
```

```
#exit
ip route static bfd S5_SGW_PGW 209.165.200.225
ip route static multihop bfd bfdcc 209.165.200.226 209.165.200.227
ip igmp profile default
#exit
```

L2 ICSR 構成を検証する

設定を確認するには、次のコマンドを使用します。

- **show config context srp**
- **show srp monitor all**
- **show srp info**

次に、**show config context srp** コマンドの出力例を示します。

```
[local]upf# show config context srp
    context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      checkpoint session duration non-ims-session 0
      checkpoint session duration ims-session 0
      force-pactv-to-actv-timeout 1
      l2-icsr enable
      [output truncated]
```

次に、**show srp monitor all** コマンドの出力例を示します。

```
[local]upf# show srp monitor all
+----- Type: (A) - Auth. probe (B) - BGP (D) - Diameter (F) - BFD (E) - EGQC (C) - Card
| (V) - VPP (S) - Sx
|
|+---- State: (I) - Initializing (U) - Up (D) - Down
||
||+--- GroupId
|||
vvv IP Addr Port Context(VRF Name) Last Update
-------------------------------------------------------------------------------
FU0 209.165.200.225 3785 SAEGW Thu Jan 05 01:13:08 2023
FU0 209.165.200.227 3785 SAEGW Thu Jan 05 01:13:08 2023
FU0 209.165.200.230 3785 ISP Thu Jan 05 01:13:08 2023
FU0 209.165.200.231 3785 ISP Thu Jan 05 01:13:08 2023
-------------------------------------------------------------------------------
[local]upf#
[local]upf# context SAEGW
[SAEGW]upf# show bfd neighbors >>>>>
All the time intervals are in ms
OurAddr NeighAddr LD/RD DtctTime State Intf
209.165.200.226 209.165.200.225 1/1090519046 150 Up S5_SGW_PGW
209.165.200.226 209.165.200.227 2/1 300 Up
Total Sessions 2
Sessions in UP state 2
```

次に、**show srp info** コマンドの出力例を示します。

```
sample o/p:
[local]l10-ru34-up1# show srp info
Service Redundancy Protocol:
-------------------------------------------------------------------------------
Context: srp
```

```
Local Address: 209.165.201.234
Chassis State: Active
Chassis Mode: Primary
Chassis Priority: 47299
Local Tiebreaker: 00-50-56-AE-EE-8D
Route-Modifier: 33

Peer Remote Address: 209.165.201.235
Peer State: Standby
Peer Mode: Backup
Peer Priority: 1673325643
Peer Tiebreaker: 00-00-00-00-00-00
Peer Route-Modifier: 0
Last Hello Message received: Tue Jan 10 04:40:43 2023 (2 seconds ago)
Peer Configuration Validation: Complete
Last Peer Configuration Error: None
Last Peer Configuration Event: Tue Jan 10 04:32:31 2023 (494 seconds ago)
Last Validate Switchover Status: None
Connection State: Connected
Next Peer Audit Scheduled:
Periodicity Audit Scheduled : -
Daily-Start-time Audit Scheduled : -
Cron-Job Audit Scheduled : -
Peer Audit State: Unknown
Last Peer Audit Type: Unknown
Last Peer Audit Successful: -
DSCP Configuration:
Control flow : be
Session flow : be
Feature Configured-status Operational-status
allow-volte-data-traffic: Disabled Enabled
allow-all-data-traffic: Disabled Enabled

[local]l10-ru34-up1#
```

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

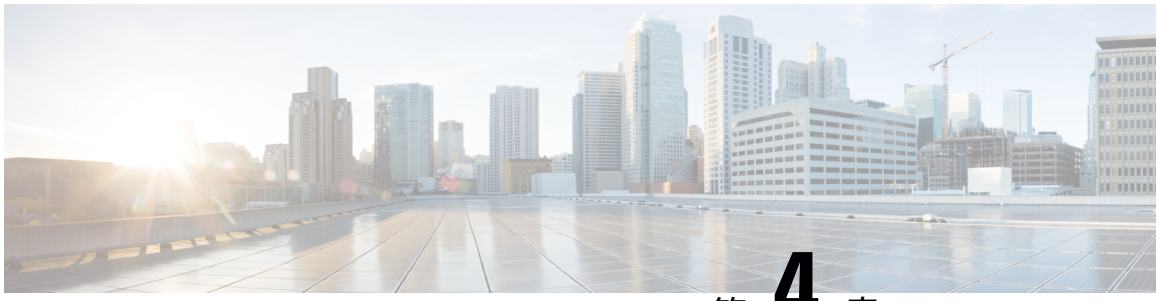
show コマンドのサポート

show ip interface または **show ipv6 interface** を使用して、GARP 統計を表示します。

次に、このコマンドの出力例を示します。

```
[EPC2]l10-ru32-up1# show ip interface
Interface Name                    : S5_SGW_PGW
Interface Type                    : Broadcast
Description                       :
VRF                               : None
IP State                         : UP (Bound to 1/10 vlan id 2141, 802.1P prior 0, ifIndex
 17432595)
IP Address                        : 209.165.200.226
Subnet Mask                       : 255.255.255.0
Bcast Address                     : 209.165.200.255
MTU                               : 1500
Resoln Type                       : ARP
ARP timeout                       : 1200 secs
L3 monitor LC-port switchover     : Disabled
Number of Secondary Addresses     : 1
    IPv6 Address: 2001:DB8:A:B::1/64
```

```
GARP sent through this interface : 45
GARP sent for this interface     : 0
GARP sent for/through this interface successfully: 45
Last GARP sent for/through this interface: Tue Dec 06 18:40:26 2022
```



第 4 章

ダイナミックルール向け ADC

表 *6* : 機能の履歴

機能名	リリース情報	説明
ToS 値を使用した IoT アプリケーション通信の優先順位	2025.01.0	この機能により、ダイナミックルール経由で cnPGW から受信した ToS 値を使用して、IoT アプリケーション通信に優先順位を付けることができます。UPF は、これらの値を適用して、データパケット通信を効率的に管理します。この変更は、**show subscribers user-plane-only full all** コマンドで確認できます。 **[デフォルト設定（Default Setting）]**：有効 – 常時オン
Gx を介した ADC ダイナミックルール	2024.02.0	UPF は、通信の照合と課金にダイナミック ADC ルールを使用します。この機能により、サービスプロバイダーはコネクテッドカーなどの IoT デバイスを管理し、SMF または UPF で分類された通信フローに基づいて回線に請求できます。このトラフィック分類により、サービス プロバイダーはサービスの収益化を可能にします。 要約すると、SMF は最初に、TDF-App-Identifier、Service ID および Rating Group を使用して PCF から受信したダイナミック ADC ルールを処理します。次に、SMF はこの情報を UPF に送信して、ruledef を分類し、課金を実行します。 **[デフォルト設定（Default Setting）]**：有効 – 常時オン

- 機能説明 （48 ページ）
- 機能の仕組み （48 ページ）
- 制限事項 （49 ページ）
- OAM のサポート （49 ページ）

機能説明

UPF は、SMF から受信した N4 メッセージを処理し、ダイナミック ADC ルールのメッセージエンティティ（PDR /URR/FAR/QER）をインストール、削除、および変更します。

UPF は、SMF からの PDR インストールの一部として、ダイナミック ADC ルールで受信した TDF-App-Identifier AVP を、構成された ruledef と照合します。一致した場合、UPF はパケットを分類し、ダイナミックルール PDR の Rating Group と Service ID に従ってサブスクライバに課金します。

[TosTrafficClass] フィールドは、PCRF から SMF および UPF へのダイナミックルールで受信されます。これは、ネットワーク輻輳時に通信フローの優先順位をサポートします。

機能の仕組み

PCRF は、課金ルールの定義を含むダイナミック ADC ルールを SMF にインストールします。UPF は、ダイナミック ADC ルール関連の PDR、URR、QER、および FAR を含む N4 メッセージを SMF から受信します。ダイナミック ADC ルール PDR には、PCRF から受信した TDF-App-Identifier およびミュート通知に対応するアプリケーション ID が含まれます。Mute が有効になっているため、UPF はアプリケーションの開始/停止トリガーを有効にしません。

N4 メッセージを受信すると、Application ID/TDF-App-Identifier を使用して指定された ruledef と照会します。次に、UPF は、この ruledef と一致するパケットを受信した URR に対して課金し、ダイナミック ADC ルール PDR で受信した QER に基づいて帯域幅ポリシングを適用します。

UPF は、ダイナミック ADC ルールをサポートするために、次の 3 つのユースケースをサポートしています。

- **サブスクリプションごとのダイナミック ADC ルールをインストールする**：PCRF からダイナミック ADC ルールを受信すると、SMF はルールをインストールし、N4 Session Establishment 要求を UPF に送信して、PDR、QER、FAR、および URR を作成します。このダイナミック ADC ルールの Create PDR 要求には、TDF-App-Identifier が含まれ、すべてのダイナミック ADC ルールに対して Mute AVP が有効になります。

  TosTrafficClass は CCA-I メッセージ経由で SMF で受信される任意の値です。

  TOS 値と対応するマスクは、N4 Establishment 要求の DL FAR の TRANSPORT LEVEL MARRING IE と UL FAR の INNER PACKET MARCMING IE にそれぞれ入力されます。

  UPF は、構成された ruledef を TDF-App-Identifier と照合し、ダイナミック ADC ルールで受信した RG/SI に従ってパケットに課金します。ルールのインストール中に SMF の PCRF から Mute 通知が有効になるため、UPF は APP-START/STOP に対して N4 セッションレポートを生成しません。

- **PCRF/SMF からのダイナミック ADC ルールを変更する**：PCRF は、Dynamic ADC Rule Modification 要求とともに、Re-authorization request（RAR）を SMF に送信します。次に、

SMF は Session Modification 要求を UPF に送信し、更新されたゲートウェイ状態と MBR 値を含む QER を更新します。

UPF が、AVP の変更を実行し、N4 Session Modification 応答を SMF に送信します。UPF では、セッション中に、RAR 経由で QoS のオフラインおよびオンライン課金と変更を有効または無効にすることもできます。

（注） 既存の ADC ルール向けの TOS の変更は適用されません。ADC ルールをインストールする際、このルールは、異なる TOS 値でインストールできますが、インストールが正常に完了すると、ルールの TOS 値は、コールが有効な期間は変更されません。

- **PCRF/SMF からダイナミック ADC ルールを削除する**：UPF は、ダイナミック ADC ルールに対応する Remove PDR および QER と一緒に N4 Modify 要求を受信します。UPF は、Rating-Group/Service-ID の最後のルールである場合、Remove URR を受信することがあります。

  N4 Modify 要求を受信すると、UPF は、Session Modification 要求から受信した TDF-App-Identifier が指定した ruledef のルールとの照合を停止します。

ダイナミック ADC ルールの詳細については、リリースに該当する『*UCC 5G SMF* 構成およびアドミニストレーション ガイド』を参照してください。

制限事項

次に、この機能の既知の制限事項を示します：

- ダイナミック ADC ルールのセッション中の RAR を使用してオフライン課金が有効になっている場合、デフォルトのベアラー URR は、サブスクライバの使用量を表示しません。

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

show コマンドの出力

この項では、この機能でサポートされる show コマンドについて説明します。

show subscribers user-plane-only full all

show コマンド **show subscribers user-plane-only full all** の出力が強化され、関連付けられた ADC PDR の数と ToS カウンタが表示されるようになりました。

```
[local]UPF1# show subscribers user-plane-only full all

  Local SEID      : [0x0004000000000002] 1125899906842626
  Remote SEID     : [0x00000004bebf6665] 20380083813
  State           : Connected
  Connect Time    : Wed Apr  3 12:45:51 2024
  Idle time       : 00h00m07s
  Access Type: uplane-ipv4v6             Network Type: IP
  user-plane-service-name: user-plane-service
  active-service-scheme-name:
  Callid: 00004e23
  Rulebase: adc1
  Interface Type: N4
  eMPS Session: No
  eMPS Session Priority: 0
  Session-Type: normal
  Precedence-order: 0
  Data Queue: 0
  Card/Cpu: 1/0                          Sessmgr Instance: 1
  IP address: 2001:cb0:0:3::4e:2301,11.11.0.4
  Next Hop Ip Address: N/A,
  Source context: EPC2-UP                Destination context: ISP
  PDN-Instance: cnpgw
  User-plane-Sx-addr: 20.20.20.106
  Control-plane-Sx-addr: 20.20.20.3
  Number of associated PDRs : 4
  Number of associated ADC PDRs : 2
  Number of associated FARs : 4
  Number of associated QERs : 3
  Number of associated BARs : 0
  Number of associated URRs : 5
  Number of associated BLIs : 1
  Uplink APN AMBR (bps) : 100000       Downlink APN AMBR (bps) : 100000
  active input acl: n/a                active output acl: n/a
  active input ipv6 acl: n/a             active output ipv6 acl: n/a
  Bandwidth Policy: n/a
  FW-and-NAT Policy: n/a
  FW-and-NAT Policy ID: n/a
  Firewall Policy IPv4: n/a
  Firewall Policy IPv6: n/a
  NAT Policy NAT44: n/a
  NAT Policy NAT64: n/a
  Converged Session: No                  Converged Peer Callid:      n/a
  Visited Call: No
  Subscriber Parameters:
  IMSI: 123456781300001
  IMEI: 123456781312381
  MSISDN: 22331101101010
  Rat Type: 6
  Old Rat Type: n/a
  MCC MNC: 123456
  SGSN Address: 20.20.20.15
  ULI: TAI+ECGI=21635400152163540000000d00
  CF Policy ID: n/a
  GX CF Policy ID: n/a
  S-NSSAI: 0x01000002
  Roaming Status:  Homer
  Old Roaming Status: n/a
  input pkts: 5                                  output pkts: 5
  input bytes: 5200                              output bytes: 200
  input bytes dropped: 0                         output bytes dropped: 0
  input pkts dropped: 0                          output pkts dropped: 0
  CF Buffered Uplink Packets: 0                  CF Buffered Downlink Packets: 0
  CF Buffered Uplink Bytes: 0                    CF Buffered Downlink Bytes: 0
```

```
  Uplink Packets in Buffer: 0                    Downlink Packets in Buffer: 0
  Buff Over-limit Uplink Pkts: 0                 Buff Over-limit Downlink Pkts: 0
  DDN buffered pkts : 0                          DDN buffered bytes : 0
  DDN buffer overflow drop pkts : 0              DDN buffer overflow drop bytes : 0
  pk rate from user(bps): 0                      pk rate to user(bps): 0
  ave rate from user(bps): 0                     ave rate to user(bps): 0
  sust rate from user(bps): 0                    sust rate to user(bps): 0
  pk rate from user(pps): 0                      pk rate to user(pps): 0
  ave rate from user(pps): 0                     ave rate to user(pps): 0
  sust rate from user(pps): 0                    sust rate to user(pps): 0
  ipv4 bad hdr: 0                                ipv4 ttl exceeded: 0
  ipv4 fragments sent: 0                         ipv4 could not fragment: 0
  ipv4 bad length trim: 0
  input pkts dropped (0 mbr): 0                  output pkts dropped (0 mbr): 0
  ipv4 input acl drop: 0                         ipv4 output acl drop: 0
  ipv6 input acl drop: 0                         ipv6 output acl drop: 0
  ip source violations: 0                        ipv4 output no-flow drop: 0
  ipv6 bad hdr: 0                                ipv6 bad length trim: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Uplink Pkts Drop: 0                    APN AMBR Downlink Pkts Drop: 0
  APN AMBR Uplink Bytes Drop: 0                   APN AMBR Downlink Bytes Drop: 0
  APN AMBR Uplink Pkts IP pref lowered: 0        APN AMBR Downlink Pkts IP pref lowered:
 0
  APN AMBR Uplink Bytes IP pref lowered: 0         APN AMBR Downlink Bytes IP pref
lowered: 0
  ITC Uplink Pkts Drop: 0                         ITC Downlink Pkts Drop: 0
  ITC Uplink Bytes Drop: 0                        ITC Downlink Bytes Drop: 0
  ITC Uplink Pkts IP pref lowered: 0              ITC Downlink Pkts IP pref lowered: 0
  ITC Uplink Bytes IP pref lowered: 0             ITC Downlink Bytes IP pref lowered:
0
  ITC Terminated Flows:: 0                        ITC Redirected Flows: 0
  Flow Action Terminated Flows: 0                 Flow Action Redirected Flows: 0
  ToS marked Uplink Pkts: 0                       ToS marked Downlink Pkts: 0
  CC Dropped Uplink Pkts: 0                       CC Dropped Downlink Pkts: 0
  CC Dropped Uplink bytes: 0                      CC Dropped Downlink Bytes: 0
  Uplink Inflight Pkts: 0                         Downlink Inflight Pkts: 0
  QFI Mismatch Uplink Pkts Drop: 0                QFI Mismatch Downlink Pkts Drop: 0
  Total QoS-Group(s) Active: 0
  DNS-to-EDNS Uplink Pkts: 0                     DNS-to-EDNS Uplink Bytes: 0
  EDNS Response Received: 0

  Flow information:
    Current Active Flows:
      TCP: 1
      UDP: 0
    Total Flows:
      TCP: 1
      UDP: 0
      FP:  1
```

show subscribers user-plane-only callid *callid* pdr full all

show コマンド **show subscribers user-plane-only callid** *callid* **pdr full all** の出力が変更され、次の新しいフィールドが表示されるようになりました。

- TDF アプリケーション ID
- TDF 通知
- 検出された ADC PDR の総数

```
[local]UPF1# show subscribers user-plane-only callid 00004e21 pdr full all

Callid: 00004e21
Interface Type: N4
IP address: 2001:cb0:0:3::4e:2301,11.11.0.4
PDR-ID:                    0x0003
 Rule Name:                port-2000
 TDF App Id:         port-2000
 TDF Notifications:  Disabled
 Hits:                      1 Match Bypassed:             4
 Matched Bytes:           200 Matched Packets:            5
 Precedence:               55
 Source Interface:        Core
 Source Interface Type: N/A
 SDF Filter(s):
  No SDF filters present
 Local F-TEID:            0x0
 Local F-TEID IP Addr:
  IPv4:                  N/A
  IPv6:                  N/A
 Outer header removal:
 Application ID:          N/A
 Associated FARID:        0x80000001
  Destination Interface: Access
  Apply Action:           FORWARD
  Outer Header Creation: GTP-U/UDP/IPv4
  Remote TEID:            0x3000000
  Transport Level Marking:        0X88 0XFC
  Transport Level Marking Options:
    Copy Inner:                    No
    Copy Outer:                    No
  Inner Packet Marking:            N/A
  Remote IP Address:     20.20.20.15
 Remote Port:            N/A
 Associated QERIDs:      2
  QER-IDs                Correlation-ID
   0x00000003                    n/a
   0x00000001               0x0000000E
 Associated URRIDs:      4
  URR-IDs                Parent URR-ID
   0x00000011            0x80000002
   0x00000027                 n/a
   0x80000002                 n/a
   0x80000009                 n/a
 Activation Time:         N/A
 Deactivation Time:       N/A
 Bearer Level Info-id:         1
    5QI:                      5
    ARP:                      20
    Charging Id:              4

PDR-ID:                    0x0004
 Rule Name:                port-2000
 TDF App Id:         port-2000
 TDF Notifications:  Disabled
 Hits:                      1 Match Bypassed:             4
 Matched Bytes:          5200 Matched Packets:            5
 Precedence:               55
 Source Interface:     Access
 Source Interface Type: S5U(1)
 SDF Filter(s):
  No SDF filters present
 Local F-TEID:            0x8001
 Local F-TEID IP Addr:
```

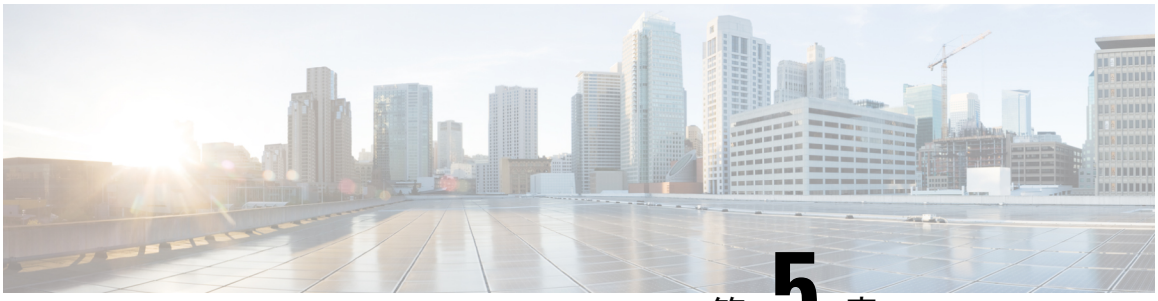
```
  IPv4:                 20.20.20.46
  IPv6:                 N/A
 Outer header removal:   GTP-U/UDP/IPv4
 Application ID:         N/A
 Associated FARID:       0x80000002
  Destination Interface: Core
  Apply Action:          FORWARD
  Outer Header Creation:
  Remote TEID:           0x0
  Transport Level Marking:         N/A
  Transport Level Marking Options:
    Copy Inner:                    No
    Copy Outer:                    No
  Inner Packet Marking:            0X88 0XFC
  Remote IP Address:
 Remote Port:            N/A
 Associated QERIDs:      2
  QER-IDs                Correlation-ID
   0x00000003                     n/a
   0x00000001                 0x0000000E
 Associated URRIDs:      4
  URR-IDs                Parent URR-ID
   0x00000011            0x80000002
   0x00000027                 n/a
   0x80000002                 n/a
   0x80000009                 n/a
 Activation Time:        N/A
 Deactivation Time:      N/A
 Bearer Level Info-id:        1
    5QI:                    5
    ARP:                    20
    Charging Id:            4

PDR-ID:                    0x0005
 Rule Name:                ipv6rsradl
 TDF App Id:              N/A
 TDF Notifications:       N/A
 Hits:                     3 Match Bypassed:             0
 Matched Bytes:          312 Matched Packets:            3
 Precedence:               1
 Source Interface:CP-function
 Source Interface Type: N/A
 SDF Filter(s):
  No SDF filters present
 Local F-TEID:           0x8000a001
 Local F-TEID IP Addr:
  IPv4:                 20.20.20.46
  IPv6:                 N/A
 Outer header removal:   GTP-U/UDP/IPv4
 Application ID:         N/A
 Associated FARID:       0x0003
  Destination Interface: Access
  Apply Action:          FORWARD
  Outer Header Creation: GTP-U/UDP/IPv4
  Remote TEID:           0x3000000
  Transport Level Marking:         N/A
  Transport Level Marking Options:
    Copy Inner:                    No
    Copy Outer:                    No
  Inner Packet Marking:            N/A
  Remote IP Address:     20.20.20.15
 Remote Port:            N/A
 Associated QERIDs:      1
  QER-IDs                Correlation-ID
```

```
  0x00000002                    n/a
 Associated URRIDs:      0
 Activation Time:        N/A
 Deactivation Time:      N/A
 Bearer Level Info-id:   N/A

PDR-ID:                   0x0006
 Rule Name:               ipv6rsraul
 TDF App Id:              N/A
 TDF Notifications:       N/A
 Hits:                     0 Match Bypassed:            0
 Matched Bytes:            0 Matched Packets:           0
 Precedence:               1
 Source Interface:     Access
 Source Interface Type: S5U(1)
 SDF Filter(s):
  Filter 1
    Protocol:            ICMPV6
    Src IP Addr:         ANY
    Src Port:            ANY
    Dst IP Addr:         ff05::2/128
    Dst Port:            ANY
    SPI:                 0
  Filter 2
    Protocol:            ICMPV6
    Src IP Addr:         ANY
    Src Port:            ANY
    Dst IP Addr:         ff02::2/128
    Dst Port:            ANY
    SPI:                 0
  Filter 3
    Protocol:            ICMPV6
    Src IP Addr:         ANY
    Src Port:            ANY
    Dst IP Addr:         ff01::2/128
    Dst Port:            ANY
    SPI:                 0
 Local F-TEID:           0x8001
 Local F-TEID IP Addr:
  IPv4:                 20.20.20.46
  IPv6:                 N/A
 Outer header removal:   GTP-U/UDP/IPv4
 Application ID:         N/A
 Associated FARID:       0x0004
  Destination Interface: CP-function
  Apply Action:          FORWARD
  Outer Header Creation: GTP-U/UDP/IPv4
  Remote TEID:           0x4
  Transport Level Marking:         N/A
  Transport Level Marking Options:
    Copy Inner:                    No
    Copy Outer:                    No
  Inner Packet Marking:            N/A
  Remote IP Address:     20.20.20.3
 Remote Port:            N/A
 Associated QERIDs:      0
 Associated URRIDs:      0
 Activation Time:        N/A
 Deactivation Time:      N/A
 Bearer Level Info-id:   N/A

Total ADC PDRs found:  2
Total PDRs found:      4
```



第 5 章

APN ACL のサポート

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 55
- 機能説明, on page 56
- IP ソース違反, on page 59
- ゲート制御, on page 60

機能の概要と変更履歴

要約データ

Table 7: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 8: マニュアルの変更履歴

改訂の詳細	リリース
ゲートウェイ制御機能が拡張され、ダイナミックルールの PDRごとに追加の QER を介して有効/無効としてゲート状態が表示できるようになりました。	2024.01.1
選択的なサブスクライバセッションに通信分類とポリシーの適用を適用するために設定可能なメカニズムが導入されました。	2021.01.0
最初の導入。	2020.02.0

機能説明

IPアクセスリスト（一般にアクセス制御リスト（ACL）と呼ばれる）は、システムに出入りするパケットのフローを制御します。この構成はコンテキストごとに設定され、「ルール」（ACL ルール）または、フィルタ条件に一致するパケットに適用するアクションを制御するフィルタで構成されます。構成が完了すると、ACL を個々のサブスクライバに適用できます。IPv4 と IPv6 のアクセスルートに個別の ACL を作成できます。

次に、ACL の 2 つの重要な側面を示します。

- ルール
- ルールの順序

ルール

単一の ACL は、1 つ以上の ACL ルールで構成されます。各ルールは、パケットが特定の基準に一致した場合に、特定のアクションを実行するように設定されたフィルタです。

各ルールは、指定された基準にパケットが一致した場合に、実行するアクションを指定します。この項では、システムでサポートされているルールアクションと基準について説明します。

アクション

ACLは、指定された基準に一致するパケットに対して、次のいずれかのアクションを実行できるように指定します。

- **Permit**：パケットが受け入れられ、分類とポリシーの適用のために処理されます。
- **Deny**：パケットは拒否されます。

- **Redirect CSS**：許可アクションと同じ動作をします。

注：

- UPF では、Redirect CSS の代わりに Permit オプションを使用することを推奨します。機能的には、UPF では、両方のオプションは同じです。Redirect CSS オプションのサポートは、後方互換性のみを目的としており、後方互換性関連シナリオでのみ使用する必要があります。
- ルールなしで構成されている設定済み ACL は、「deny any」ルールを示します。これは、空の ACL のデフォルトの動作です。
- UPF では、ACL が APN に関連付けられていない場合、コールは起動します。デフォルトでは、通信は、分類およびポリシー適用のために処理されます。UPF 以外のアーキテクチャの場合、Redirect CSS が必須であるため、コールは失敗します。
- 特定の通信に対して ACL で Deny オプションのみが指定されている場合、残りの通信を通過させるには、その通信に対して Permit オプションを明示的に指定する必要があります。
- 特定の通信に対して ACL で Permit オプションのみが指定されている場合、残りの通信を通過させるには、その通信に対して Permit を明示的に指定する必要があります。
- Router Advertisement/Router Solicitation（RA/RS）パケットは、ACL の候補です。したがって、IPv6 ACL を指定する際には注意が必要です。
- ACL の構成変更は、既存のコールではなく、新しいコールに適用されます。

基準

各 ACL は、パケットの比較基準を指定する 1 つまたは複数のルールで構成されます。

サポートされる基準は次のとおりです。

- **Any**：すべてのパケットをフィルタ処理します。
- **Host**：送信元ホストの IP アドレスに基づいてパケットをフィルタ処理します。
- **ICMP**：Internet Control Message Protocol（ICMP）のパケットをフィルタ処理します。
- **IP**：Internet Protocol（IP）パケットをフィルタ処理します。
- **Source IP Address**：1 つ以上の送信元 IP アドレスに基づいてパケットをフィルタ処理します。
- **TCP**：Transport Control Protocol（TCP）パケットをフィルタ処理します。
- **UDP**：User Datagram Protocol （UDP）パケットをフィルタ処理します。

上記の基準それぞれについては、以降の項で詳述します。

- **Any**：すべてのパケットにルールが適用されます。
- **Host**：IP アドレスによって決定される特定のホストにルールが適用されます。

- **ICMP**：特定の Internet Control Message Protocol（ICMP）パケット、タイプ、またはコードにルールが適用されます。ICMP のタイプとコードの定義については、*www.iana.org*（RFC 3232）を参照してください。
- **IP**：特定のIP パケットまたはフラグメントにルールが適用されます。
- **Source IP Address**：特定の送信元アドレスまたは送信元アドレスのグループから発信される特定のパケットにルールが適用されます。
- **TCP**：任意の TCP 通信にルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。TCP ポート番号の定義については、*www.iana.org* を参照してください。
- **UDP**：任意の UDP 通信にルールが適用され、送信元/接続先の IP アドレス、特定のポート番号、またはポート番号のグループの任意の組み合わせでフィルタ処理されます。UDP ポート番号の定義については、*www.iana.org*を参照してください。

ルールの順序

複数のルールで 1 つの ACL を構成できます。各パケットは、一致が見つかるまで、各 ACL ルールを入力した順序で比較されます。一致が特定されると、後続のすべてのルールは無視されます。

制限事項

UPF の APN ACL 機能の既知の制限を次に示します。

- ACL のアドレス再指定オプションは、サポートされていません。
- コンテキストおよびネクストホップのリダイレクト ACL は、サポートされていません。
- ログオプションは、ACL ではサポートされていません。
- ACL ドロップ（IPv4 のみ）の APN レベルのバルク統計は、サポートされています。

ACL の設定

ACL を APN 経由で個々のサブスクライバに適用するには、次の構成を使用します。

```
configure
  context dest_context_name [ -noconfirm ]
    { ip | ipv6 } access-list acl_list_name
      { permit | deny | redirect }acl
      end
configure
  apn apn_name
    { ip | ipv6 } access-group acl_list_name [ in | out ]
    end
```

（注）

- 適用する ACL は、APN の接続先コンテキスト内にある必要があります（APN が設定されているコンテキストとは異なる場合があります）。
- **in** キーワードも **out** キーワードも指定しなかった場合、ACL はインバウンドとアウトバウンドのすべてのパケットに適用されます。
- 各 APN に対して 4 つのアクセスグループを適用できます。次に例を示します。

  ip access-group acl_list_name_1 in

  ip access-group acl_list_name_2 out

  ipv6 access-group acl_list_name_3 in

  ipv6 access-group acl_list_name_4 out

ACL 構成を確認する

Exec モードで次の CLI コマンドを使用して、ACL リストが適切に適用されたかどうかと、ACL が原因で削除されたパケットをチェックします。

- **show subscriber user-plane-only full all**
- **show subscribers user-plane-only full callid** *call_id*
- **show user-plane-service pdn-instance statistics** *name*

IP ソース違反

送信元検証では、受信パケットの送信元アドレスがセッション中のサブスクライバの IP アドレスと一致する必要があります。これにより、ハンドオフのシナリオでユーザーが 2 つのゲートウェイ間を何度も行き来する際に問題が発生するのを防ぐよう、ネットワークを構成できます。

UPF が送信元 IP アドレス違反のあるサブスクライバパケットを受信すると、システムは IP 送信元違反ドロップ制限カウンタをインクリメントし、IP 送信元違反期間のタイマーを開始します。IP 送信元違反期間中に不正な送信元アドレスで受信された後続の各パケットにより、ドロップ制限カウンタがインクリメントされます。たとえば、ドロップ制限を 10 に設定すると、10 の送信元違反が発生するとコールはドロップされます。検出期間タイマーは、このプロセス全体でカウントし続けます。

ユーザープレーン APN 構成で、以下を構成する必要があります。

```
ip source-violation { ignore | check [ drop-limit limit ] } [
exclude-from-accounting ]
```

Note IP source violation CLI コマンドの詳細については、「*CLI*（コマンドライン インターフェイス）のリファレンス」を参照してください。

ゲート制御

Table 9: 機能の履歴

機能名	リリース情報	説明
追加の QER を使用したゲート制御	2024.01.1	このリリースでは、UPF でサポートされる PDR あたりの QER の数が 2 から 3 に増えています。 すべてのルールとフィルタは、PDR経由でUPFに送信されます。SMFは、デフォルトのQFI/ベアラーにインストールされたダイナミックルールに対して追加のQERを送信します。Gate Status IE は、ゲートが開いているか閉じているかを示します。 **デフォルト設定**： 該当なし

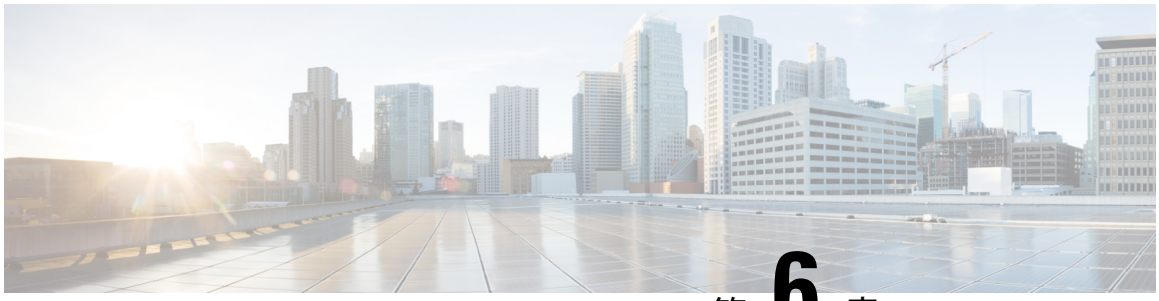
UPF のゲート制御は、サービスデータフローに属する IP パケットまたは、検出されtあアプリケーションの通信の転送を有効または無効にし、目的のエンドポイントにパススルーします。「3GPP TS 23.203、subclause 4.3.2」を参照してください。

SMF は、サービスデータフローまたは検出するアプリケーションの通信向けに PDR に関連付けられている QER を作成して UPF でゲート状態を制御します。Gate Status IE に関連付けられている QER は、サービスデプロイフローまたは検出されたアプリケーション通信が、転送可能か（ゲートが開いているか）、またはアップリンクやダウンリンク方向で破棄されるか（ゲートウェイが閉じているか）を示します。

デフォルト PDR の 2 つの QER は、デフォルト QFI/ベアラーのダイナミックルールの PDR に関連付けられます。したがって、SMF は、その他の QER を作成し、デフォルトの QFI/ベアラーのダイナミックルールに関する GATE 状態を表示します。その他の QER は、ダイナミックルールの PDR に関連付けられます。したがって、UPF は、PDR アソシエーションごとに最大 3 つの QER をサポートします。

UPF は、PDR の PDI の Source Interface IE または FAR の接続先 Interface IE ごとに UL と DL のフローを識別します。UPF は、それに応じて、UL と DL ゲーティングを適用します。

SMF は、QER の Gate Status IE にある [ゲート（Gate）] フィールドを [クローズ（CLOSED）] に設定することで、PDR で受信したパケットを博するように UPF にリクエストします。



第 6 章

APN AMBR トラフィックポリシング

- 機能の概要と変更履歴, on page 61
- 機能説明 （62 ページ）
- APN AMBR トラフィックポリシング機能の設定 （62 ページ）
- モニタリングおよびトラブルシューティング （63 ページ）

機能の概要と変更履歴

要約データ

Table 10: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

表 *11* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.01.0

機能説明

APN-AMBR は、HSS の APN ごとに保存されるサブスクリプション パラメータです。S-GW は、デフォルトベアラーの確立手順において APN-AMBR を提供します。APN-AMBR により、すべての GBR 以外のベアラーと同じ APN のすべての PDN 接続にわたって提供されることが予想される集約ビットレートが制限されます。これらの GBR 以外のベアラーのそれぞれが APN-AMBR 全体を利用する可能性があります。たとえば、他の GBR 以外のベアラーが通信を伝送しない場合などです。P-GW は、ダウンリンクおよびアップリンク方向に APN-AMBR を適用します。

制限事項

token-replenishment-interval および **violate-action shape** CLI コマンドはサポートされていません。

APN AMBR トラフィックポリシング機能の設定

ここでは、APN-AMBR トラフィックポリシングの設定方法について説明します。

```
configure
         context context_name
           apn apn_name
      apn-ambr rate-limit direction { downlink | uplink } [ burst-size
 { auto-readjust duration { milliseconds msecs | seconds } |
violate-action { drop | lower-ip-precedence | transmit }
               end
```

注：

- **rate-limit direction { downlink | uplink }**：ダウンリンク（ネットワークからサブスクライバ）トラフィック、アップリンク（サブスクライバからネットワーク）トラフィックのどちらにレート制限を適用するかを指定します。
- **burst-size { auto-readjust duration milliseconds msecs | seconds }**：このパラメータは、トラフィックのショートバーストが許容データレートを超えないようにするために、ポリシングアルゴリズムで使用されます。トークンバケットの最大サイズです。
  - **auto-readjust duration***seconds*：バーストサイズの計算（バーストサイズ = ピークデータレート/8 * 自動再調整期間）で使用される期間（秒単位）。
    - 秒は 1 ー 30 の整数値である必要があります。デフォルトは 1 秒です。
  - **milliseconds**：*msecs* は 100 ～ 900 の整数値で、100 ミリ秒単位で指定する必要があります。たとえば、100、200、300 などです。

- **violate-action { drop | lower-ip-precedence | transmit }**：ベアラーコンテキストのデータレートが AMBR を超えた場合に P-GW が実行するアクション。
  - **drop**：違反パケットをドロップします。
  - **lower-ip-precedence**：違反パケットの DSCP 値をゼロ（「ベストエフォート」）に設定します。
  - **transmit**：違反パケットを送信します。これは、この機能のデフォルト動作です。
- この機能が導入される前は、デフォルト動作では違反パケットはドロップされました。

モニタリングおよびトラブルシューティング

この項では、APN-AMBR トラフィックポリシング機能のモニターや障害対応に使用できるコマンドについて説明します。

show コマンドと出力

この項では、APN-AMBR トラフィックポリシング機能のモニタリングや障害対応に使用できる show コマンドについて説明します。

- **show user-plane-service pdn-instance name <apn_name>**

  UPF でこの show コマンドを使用して、レート制限が有効または無効になっているか、バーストサイズ、およびダウンリンクとアップリンク通信のその他のパラメータを確認します。

  - APN-AMBR
    - [Downlink Apn Ambr]：ダウンリンクトラフィックのレート制限が有効か無効かを示します。
      - [Burst Size]：ダウンリンクトラフィックのバーストサイズを示します。
      - [Auto Readjust]：ダウンリンクバーストサイズの自動再調整が有効か無効かを示します。
      - [Auto Readjust Duration]：ダウンリンクバーストサイズの計算に使用される期間を示します。
      - [Burst Size(bytes)]：バーストサイズをバイト単位で示します。
      - [Violate Action]：ベアラーコンテキストのデータレートがダウンリンクトラフィックの AMBR を超えた場合に P-GW が実行するアクションを示します。
    - [Uplink Apn Ambr]：アップリンクトラフィックのレート制限が有効か無効かを示します。
      - [Burst Size]：アップリンクトラフィックのバーストサイズを示します。

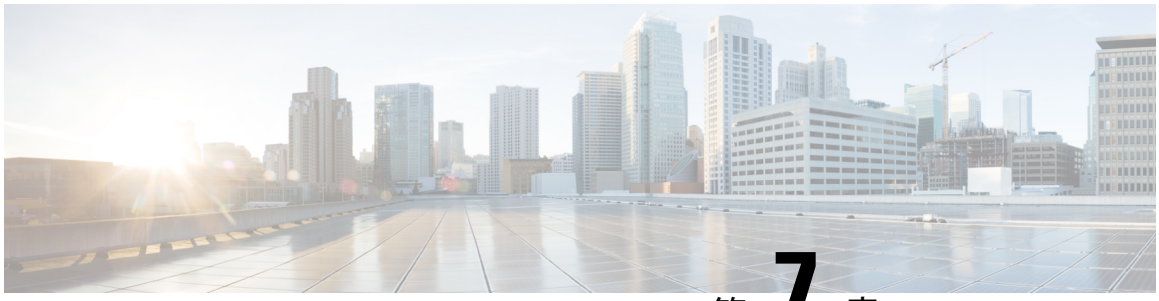
- [Auto Readjust]：アップリンクバーストサイズの自動再調整が有効か無効かを示します。
- [Auto Readjust Duration]：アップリンクバーストサイズの計算に使用される期間を示します。
- [Burst Size(bytes)]：バーストサイズをバイト単位で示します。
- [Violate Action]：ベアラーコンテキストのデータレートがアップリンクトラフィックのAMBRを超えた場合にP-GWが実行するアクションを示します。

- [Token Replenishment Interval]：トークンの補充間隔を示します。

- **show sub user-plane-only full all**

  UPFでこのshowコマンドを使用すると、ドロップされたパケットの数と、APN-AMBRポリサーが原因でIPプレシデンスが低下したことを確認できます。この機能をサポートするために、次のフィールドが導入されました。

  - [APN AMBR Uplink Pkts Drop]：アップリンクトラフィックでドロップされたAPN-AMBRパケット数を示します。
  - [APN AMBR Uplink Bytes Drop]：アップリンクトラフィックでドロップされたAPN-AMBRバイト数を示します。
  - [APN AMBR Uplink Pkts IP pref lowered]：IPプレシデンスが低下するAPN-AMBRアップリンクパケット数を示します。
  - [APN AMBR Uplink Bytes IP pref lowered]：IPプレシデンスが低下するAPN-AMBRアップリンクのバイト数を示します。
  - [APN AMBR Downlink Pkts Drop]：ダウンリンクトラフィックでドロップされたAPN-AMBRパケット数を示します。
  - [APN AMBR Downlink Bytes Drop]：ダウンリンクトラフィックでドロップされたAPN-AMBRバイト数を示します。
  - [APN AMBR Downlink Pkts IP pref lowered]：IPプレシデンスが低下するAPN-AMBRダウンリンクパケット数を示します。
  - [APN AMBR Downlink Bytes IP pref lowered]：IPプレシデンスが低下するAPN-AMBRダウンリンクバイト数を示します。



第 7 章

バルク統計サポート

- 機能の概要と変更履歴, on page 65
- 機能説明 （66 ページ）

機能の概要と変更履歴

要約データ

Table 12: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 13: マニュアルの変更履歴

改訂の詳細	リリース
次の新しいバルク統計スキーマがサポートされるようになりました。 • P2P スキーマ • SX スキーマ • システムスキーマ • ユーザープレーンスキーマ	2021.01.0
最初の導入。	2020.02.0

機能説明

この章では、Cisco Ultra Cloud 5G ユーザープレーン機能（UPF）ソフトウェアリリースのバルク統計スキーマについて説明します。

バルク統計は、ソフトウェア機能とフレームワークの集合体で、パケットコアノードに関する重要なパフォーマンス関連統計と正常性関連統計を収集して、下部ノードにエクスポートします。これらの統計は、オペレータが以下の機能を実行するための効率的な方法を指定します。

- ノードの全体的な正常性とパフォーマンスをモニターします。
- 是正措置を行うために支援します。
- パケットコアネットワークを最適化して、使用性を向上させます。
- 全体的な運用コスト（OpEx）を削減します。

各統計は、「スキーマ」と呼ばれるグループで収集されるように設定されます。

システムでサポートされているバルク統計により、オペレータは重要な統計を選択し、プレゼンテーション形式を構成できます。これにより、外部のバックエンドプロセッサによる解析を容易にするデータフォーマットが可能になるため、統計データの後処理が簡素化されます。

統計またはバルク統計レポートは、モバイルパケットコアノードで重要です。製品をネットワークにデプロイするには、キャリアグレードの要件を満たす統計をサポートする必要があります。

バルク統計は、次の目的でオペレータによって使用されます。

- パフォーマンス KPI のモニタリング
- ネットワーク障害の分析とデバッグ

- ネットワーク最適化
- トラフィックパターン分析
- ノードの正常性分析

エレメント管理システム（EMS）とともに使用すると、データを解析、アーカイブ、グラフ化できます。

5G接続環境では、次のネットワーク機能に対して収集を行うようにシステムを設定できます。

- アクセスおよびモビリティ管理機能（AMF）
- ネットワークリポジトリ機能（NRF）
- ネットワークスライス選択機能（NSSF）
- ポリシー制御機能（PCF）
- セッション管理機能（SMF）
- ユーザープレーン機能（UPF）

システムは、最大 4 セット（プライマリ/セカンダリ）の受信機の設定をサポートします。各セットは、サポートされているスキーマのリストから特定の統計セットを収集するように設定できます。統計は、システムから手動で取得することも、設定された間隔で送信することも可能です。バルク統計は、受信側のファイルに保存されます。

ユーザーは、バルク統計データファイルの形式を設定できます。次の項目を指定できます。

- ファイル名のフォーマット
- 日付、システムホスト名、システム稼働時間などの情報を含むファイルヘッダーおよびフッター。
- 統計を生成するシステムの IP アドレス（ヘッダーとフッターでのみ使用可能）
- ファイルが生成された時刻。

EMS は、XML 解析、アーカイブ、グラフ化によって統計データをさらに処理できます。EMS のバルク統計サーバーのコンポーネントは、収集された統計を解析し、その情報を PostgreSQL データベースに保存します。また、XML 出力を生成し、さらなる処理のためにノースバウンド NMS か代替のバルク統計サーバーに送信することもできます。

さらに、バルク統計サーバーは、サーバー上の代替ディレクトリにファイルをアーカイブすることが可能です。ディレクトリは、ローカルファイルシステム上、または EMS サーバー上の NFS マウントファイルシステム上に配置できます。

5G におけるバルク統計の実装は次のとおりです。

- NF は、統計を個別に収集して、5G アーキテクチャのアグリゲータノードにエクスポートします。

- 受信側は、node-namesまたはバルク統計構成の一環として構成されたその他の情報を使用してNFから統計を相互に関連付けます。どのEMSツールでも、スタンドアロンシステムからレンダリングするのと同じようにこのデータをレンダリングできます。

サポートされているスキーマ

このリリースでは、5Gアーキテクチャで次のスキーマがサポートされています。

APN スキーマ

APN スキーマは、アクセスポイント名（APN）統計を提供します。

カードスキーマ

カード好きは、カードレベルの統計を提供します。

ECS スキーマ

ECS スキーマは、Enhanced Charging Service の統計を提供します。

GTP-U スキーマ

GTP-U スキーマは、GPRS Tunneling Protocol- User メッセージ統計を提供します。

P2P スキーマ

P2P スキーマは、ポイントツーポイント統計を提供します。

P-GW スキーマ

P-GW スキーマは、ユーザープレーンサービスの統計を提供します。

ポートスキーマ

ポートスキーマは、ポートレベルの統計を提供します。

Rulebase

Rulebase スキーマは、rulebase の統計を提供します。

SX スキーマ

Sx スキーマは、N4 関連のメッセージの統計を提供します。

システムスキーマ

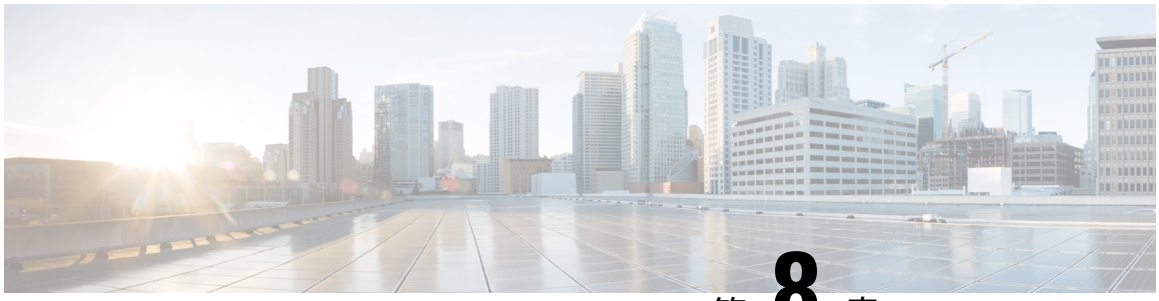
システムスキーマは、システムレベルの統計を提供します。

ユーザープレーンスキーマ

ユーザープレーンスキーマは、ユーザープレーンの統計を提供します。



重要 バルク統計の設定の詳細については、『ASR 5500 システム アドミニストレーション ガイド』の「Bulk Statistics」の章を参照してください。



第 8 章

課金サポート

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 69
- 機能説明, on page 70
- 機能の仕組み, on page 71
- 使用状況レポートのクレジット制御を構成する （84 ページ）
- 使用状況レポートの ACS ルールベースを構成する, on page 85
- モニタリングおよびトラブルシューティング （88 ページ）

機能の概要と変更履歴

要約データ

Table 14: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 15: マニュアルの変更履歴

改訂の詳細	リリース
この機能は、N4 インターフェイスの Recalculate IE をサポートするように拡張されています。	2023.04.0
この機能は、次の機能をサポートするように拡張されています。 • PTT クォータなし制限パス • PTT クォータ枯渇制限パス • タリフ時間 • TCP 最大セグメントサイズ	2021.02.0
Rating-Group と Service ID を使用した使用状況レポートが導入されました。	2020.02.5
最初の導入。	2020.02.0

機能説明

ユーザープレーン機能（UPF）UPF 2.0 の使用状況の測定およびレポート機能は、セッション管理機能（SMF）が制御します。SMF は、次の方法でこれらの機能を制御します。

- サービスデータフロー、アプリケーション、ベアラー、またはセッション（まだ存在していない場合）を表すために必要な PDR を作成します。
- Charging Key、および Charging Key と Service ID の組み合わせの URR を作成します。また、Charging Key、Sponsor ID および Application Service Provider ID の組み合わせに対する URR を作成します。
- SDF、セッション、またはアプリケーションレベルでの使用状況レポートのために、PFCP セッションで定義された関連する PDR に URR を関連付けます。
- オンライン課金では、オンライン課金サーバー（OCS）からボリュームと時間クォータを受信した場合、SMF は、それらをプロビジョニングします。

N4 経由のオフライン課金イベントレポート

ユーザープレーン機能（UPF）は、セッションベースのオフライン課金、URR における PDU セッションレベルのレポートトリガー（ボリュームおよび時間のしきい値）、PFCP session

report 手順、および Session-AMBR の変更、QoS、ユーザー位置情報のトリガーに対する PFCP 変更応答の使用量レポート IE をサポートします。

N4 経由のオンライン課金レポート

UPF は、フローベースのオンライン課金サポートをサポートしています。これには、PFCP Modify 応答の Volume and Time quota and Usage reporting IE の URR 拡張機能が含まれます。さらに、UPF は、使用状況レポート IE による PFCP Session Report 要求のサポートを含む、オンライン課金トリガーをサポートします。

機能の仕組み

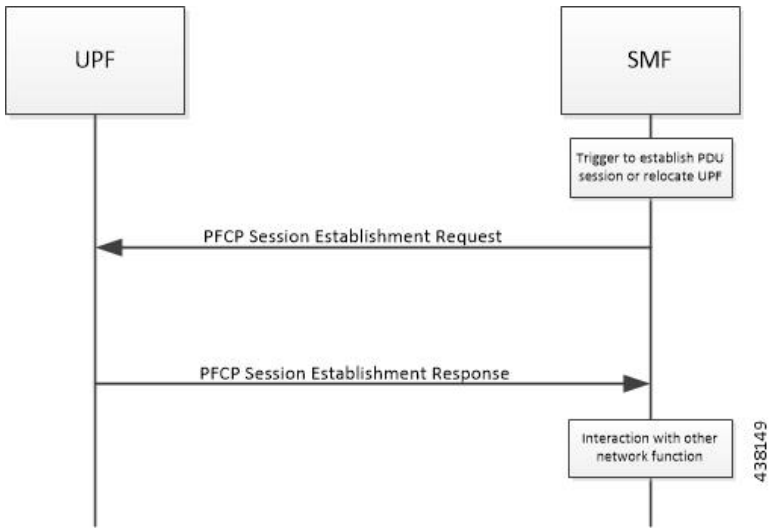
コール フロー

以下の項では、PFCP セッション管理向け SMF および UPF 間のコールフローについて説明します。

PFCP Session Establishment 手順

PFCP Session Establishmentn 手順では、SMF と UPF の間に PFCP セッションを確立します。また、受信パケットを処理するためのルールを UPF で構成します。さらに、SMF は、レポートを対象としたトリガーとしきい値で構成される Create URR Information Element（IE）を送信します。

次のコールフローは、PFCP Session Establishment 手順を示しています。

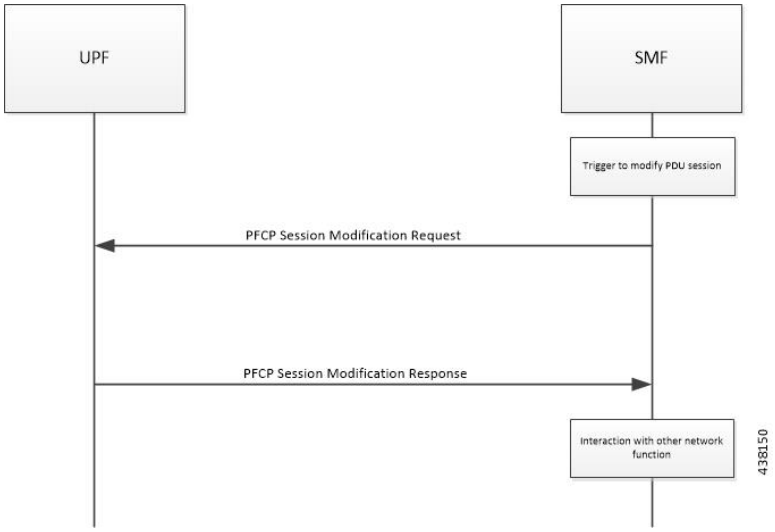


ステップ	説明
1	SMF は、新しい PDU セッションを確立するか、または確立された PDU セッションの UPF を変更するトリガーを受信します。
2	SMF は、N4 Session Establishment 要求メッセージを UPF に送信します。このメッセージには、UPF の動作を定義する構造化された制御情報が含まれます。
3	SMF は Create URR IE を使用して URR をプロビジョニングします。Create URR は、Create PDR IE に URR-ID IE を追加することで PDR に関連付けられます。これには、使用状況レポートのさまざまなトリガーとしきい値が含まれます。
4	同じ URR が複数の PDR に関連付けられている場合、URR は別の URR とリンクされます。したがって、URR のレポートが送信されると、リンクされた URR も報告されます。
5	UPF は N4 Session Establishment 応答メッセージで SMF に応答します。たとえば、データ通信の GTP-u カプセル化の gNB に UPF Flow-TEID が送信される Created PDR IE などです。
6	SMF は、この手順をトリガーしたネットワーク機能と相互作用します。たとえば、AMF や PCF などです。

PFCP Session Modification 手順

SMF は、PFCP Session Modification 手順を使用して、UPF 上の既存の PFCP セッションを変更します。たとえば、新しいルールの設定、既存のルールの変更、既存のルールの削除などです。SMF は、Create URR IE、Update URR IE（トリガーまたはしきい値を更新するため）、および Remove URR IE（Session Establishmentn 手順中に SMF によって以前に作成された既存の URR を削除するため）を同じメッセージで送信します。

次のコールフローは、PFCP Session Modification 手順を示しています。

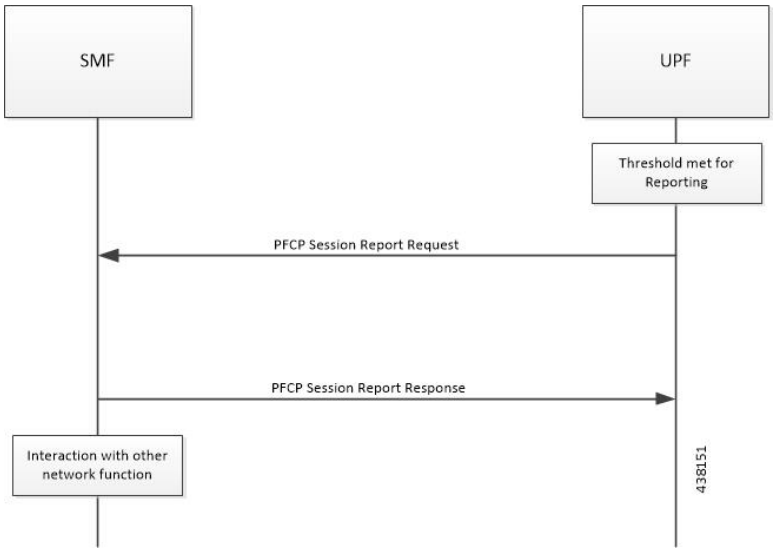


ステップ	説明
1	SMF は、既存の PDU セッションを変更するトリガーを受信します。
2	SMF は、N4 Session Modification 要求メッセージを UPF に送信します。このメッセージには、UPF の動作を定義する構造化された制御情報が含まれます。
3	UPF は、セッション ID が変更する PFCP セッションコンテキストを識別します。SMF から送信されたパラメータのリストに従って、このセッションコンテキストのパラメータを更新します。次に、PFCP Session Modification 応答メッセージで応答します。メッセージには、UPF が（受信した制御情報の応答で）SMF に提供する必要がある情報が含まれます。
4	• SMF が PFCPSMReq-Flag IE または URR ID で設定された QAURR フラグを Query URR IE (e) を使用して送信する場合、UPF は PFCP Session Modification 応答とともに対応する URR に関する usage report IE を送信します。 • 再計算測定と呼ばれるカスタム Information Element（IE）が Update-URR IE（URR-ID:Gz-Bearer）に追加され、N4 Session Modify 要求での最大 LOSDV 状態による PGWCDR の生成をサポートします。IE を受信した後、UPF は、IE 内に存在する URR-ID に従って、URR のボリュームと期間を調整します。
5	UPF は、SMF から送信された Create URR、Update URR、または Remove URR IE に基づいてプロビジョニングし、機能します。
6	SMF は、この手順をトリガーしたネットワーク機能と相互作用します。たとえば、AMF や PCF などです。

PFCP Session Reporting 手順

UPF は、PFCP Session Reporting 手順を使用して、PFCP セッションに関連する情報を SMF に報告します（usage report IE）。しきい値がボリューム、時間、またはイベントの測定値に達し、レポートに対応するトリガーを設定すると、UPF がメッセージを SMF に送信します。

次のコールフローは、PFCP Session Reporting 手順を示しています。

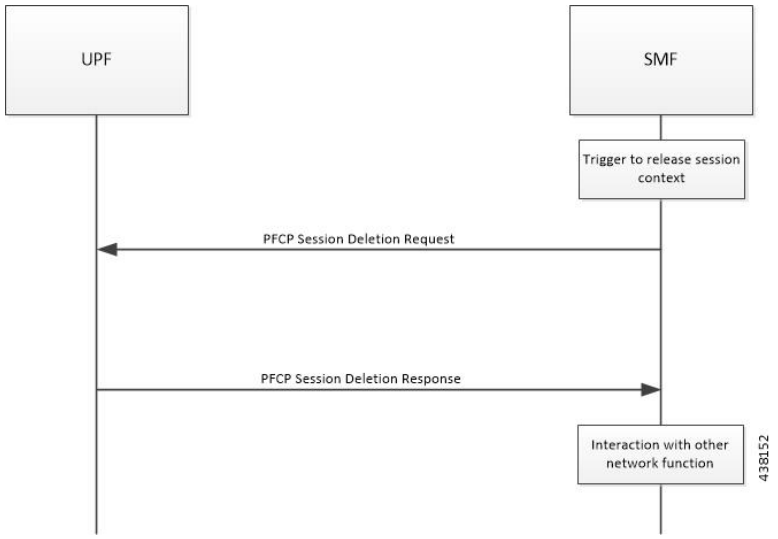


ステップ	説明
1	• プロビジョニングされたしきい値（時間、ボリュームまたはイベントの場合、およびレポートにトリガーが設定された場合）が満たされると、UPF は、ボリューム、時間、またはしきい値の usage report IE と使用状況の詳細を含む PFCP Session Report 要求を送信します。 • 再計算測定と呼ばれるカスタム Information Element（IE）が Update-URR IE（URR-ID:Gz-Bearer）に追加され、N4 Session Modify 要求での最大 LOSDV 状態による PGWCDR の生成をサポートします。IE を受信した後、UPF は、IE 内に存在する URR-ID に従って、URR のボリュームと期間を調整します。
2	SMF は、成功またはエラーメッセージで、PFCP Session Modification 応答に応答します。UPF では、エラーハンドリグは不要です。
3	SMF は、この手順をトリガーしたネットワーク機能と相互作用します。たとえば、AMF や PCF などです。

PFCP Session Deletion 手順

PFCP Session Deletion 手順では、SMF と UPF 間の既存の PFCP セッションが削除されます。SMF は、既存の PFCP セッションを削除するために、UPF に対して PFCP Session Deletion 手順を開始します。UPF は、以前にプロビジョニングされたすべての URR の使用状況レポートを含む Session Deletion 応答を送信します。

次のコールフローは、PFCP Session Deletion 手順を示しています。



ステップ	説明
1	SMF は、PDU セッションの PFCP セッションコンテキストを削除するトリガーを受信します。
2	SMF は PCRF Session Deletion 要求メッセージを UPF に送信します。
3	UPF は、削除するセッション ID の PFCP セッションコンテキストを識別します。その後、セッションコンテキスト全体を削除します。さらに、UPF は、UPF が SMF に提供する情報を含む PFCP Session Deletion 応答メッセージで応答します。たとえば、UPF は、このセッション用にプロビジョニングされたすべての URR の使用状況レポートを送信します。
4	SMF は、この手順をトリガーしたネットワーク機能と相互作用します。たとえば、AMF や PCF などです。

オフライン課金レポートでサポートされる IE

Table 16: 機能の履歴

機能名	リリース情報	説明
N4 インターフェイスの Recalculate Measurement IE	2023.04	UPF は、N4 インフォメーション経由で受信した Recalculate Measurement custom IE をサポートします。この IE は、Update-URR プロセス（URR-ID：Gz-Bearer）に追加され、max_LOSDV 変更条件による PGW-CDR 生成をサポートします。

次のトリガー Information Elements（IEs）は、N4 経由でオフライン課金レポートをサポートします。

- 定期レポート：このトリガーが設定されている場合、UPF はリソース使用状況レポートをセッション管理機能（SMF）に定期的に送信します。定期的なレポートに必要な間隔は、measurement period IE とともに送信されます。
- ボリュームしきい値（ボリュームしきい値が UL、DL、および合計に達した場合）：このトリガーは、ボリュームベースの測定が必要な場合に設定されます。SMF はボリュームしきい値IE とともに通信量の値を送信し、UPF は、特定の使用状況レポートルール（URR）の通信量に達すると通信使用状況レポートを送信します。
- 時間しきい値（時間しきい値に達した場合）：このトリガーは、時間ベースの測定が設定されている場合に設定されます。SMF は、time threshold IE とともに時間しきい値を送信し、時間しきい値が、具体的な URR に達すると、UPF は、リソース使用状況レポートを送信します。
- リンクされた使用状況レポート：このトリガーが設定されている場合、UPF はこの特定の URR の使用状況レポートを送信します。さらに、このトリガーが設定されている場合、使用状況レポートは UPF にリンクされているすべての URR に送信されます。UPF は、リンクされた URR-Id IE とともにリンクされた URR-Id を送信します。
- パケット転送制御プロトコル（PFPC）セッションの削除：PFCP セッションの終了により、URR に関する使用状況レポートが（PFCP Deletion 応答で）生成されます。同様に、具体的な URR の削除により、URR に関する使用状況レポートが（PFCP modification 応答で）生成されます。
- URR の更新：このトリガーは、URR リクエストを受信したときに設定されます。
- Recalculate Measurement：Recalculate Measurement と呼ばれるカスタム Information Element（IE）が、Update-URR プロセス（URR-ID：Gz-Bearer）に追加され、Max-LOSDV 状態による PGWCDR 生成がサポートされます。IE を受信した後、UPF は、IE 内に存在する URR-ID に従って、URR のボリュームと期間を調整します。



Note

- 指定された URR-ID の合計使用量がリセットされ、リンクされた URR がある場合は使用量が再計算されます。
- first-pkt-time、last-pkt-time、および期間のタイムスタンプもそれに応じて調整されます。
- しきい値は変更されません。

- Recalculate Interface：N4 Modify 要求経由で「Recalculate Interface」と呼ばれるカスタム IE が SMF によって送信されます。同じ Sx Modify 要求で、Query URR(s) または Update URR(s) IE と一緒に Recalculate Interface IE を受信した場合、Recalculate Interface IE は、最後に個別に処理されます。IE を受信したら、UPF は、すべての URR を反復し、SMF が言及したぐ

らぐに基づいて URR のみをフェッチし、再計算機能を実行します。その後、UPF は、取得したすべての URR のボリュームと期間を調整します。

Note

- URR に関して累積された使用量は破棄され、リンクされた URR がある場合は、それらの使用量が調整されます。
- first-pkt-time、last-pkt-time、および期間のタイムスタンプは、それに応じて調整されます。
- リンクされた URR のしきい値は変更されません。

オンライン課金レポートでサポートされる IE

次の IE は、オンライン課金をサポートします。

- ボリュームクォータ：SMF は、この IE でのパケットの転送を停止するか、（UPF のオペレータポリシーに基づいて）一部の制限されたユーザープレーン通信の転送を許可するように UPF に要求します。使用状況レポートを生成するためのボリュームしきい値がプロビジョニングされていない場合、測定された通信がクォータに達すると、この IE が使用されます。
- 時間クォータ：SMF は、この IE でのパケットの転送を停止するか、（UPF のオペレータポリシーに基づいて）一部の制限されたユーザープレーン通信の転送を許可するように UPF に要求します。使用状況レポートを生成するためのボリュームしきい値がプロビジョニングされていない場合、測定された通信がクォータに達すると、この IE が使用されます。
- モニタリング時間：この IE は、UPF がボリュームまたは時間のしきい値を再適用できる時刻（UTC 形式）を送信するために SMF が使用します。また、SMF は後続のボリューム、時間、ボリュームクォータ、時間クォータ、およびクォータ IE のいずれかを送信し、これらは、モニタリングタイムスタンプで再適用されます。
- クォータアクションの FAR（転送アクションルール）ID：この IE は、ボリューム、時間、またはクォータのいずれかが使い果たされたときに、URR に関連付けられている通信に対して UPF が適用される代替 FAR を識別するために SMF が使用します。この FAR では、UPF がパケットをドロップするか、通信をリダイレクト接続先にリダイレクトする必要があります。
- 後続のボリュームしきい値：ボリュームベースの測定が使用され、Monitoring Time IE が利用可能な場合、この IE も存在します。この IE の存在は、この具体的な URR に関する通信ボリューム値（UPF が SMF に報告するネットワークリソース使用状況）と監視時間後の期間があることを示します。
- 後続のボリューム：時間ベースの測定が使用され、Monitoring Time IE が利用い可能な場合、この IE も存在します。この IE の存在は、この具体的な URR に関する通信ボリュー

ム値（UP機能がCP機能に報告するネットワークリソース使用状況）と監視時間後の期間があることを示します。

- リンクされたURR ID：リンクされた使用状況レポートが必要な場合、このIEが使用されます。複数のURR-IDを1つのURRにリンクすることができます。また、リンクされた使用状況レポートもReporting Trigger IEで送信されます。
- 測定メソッド：このIEが存在する場合、SMFは、ネットワーク使用状況の測定メソッドを指定します。測定方法は、ボリュームと期間に基づきます。
- 測定期間：このIEは、測定期間を変更するために存在します。
- 定期レポート：このトリガーが設定されている場合、UPFはリソース使用状況レポートをSMFに定期的に送信します。定期的なレポートに必要な間隔は、measurement period IEとともに送信されます。トリガーが1に設定されている場合は、定期的なレポートのリクエストが送信されます。
- ボリュームのしきい値：このトリガーは、ボリュームベースの測定が必要な場合に設定されます。SMFはボリュームしきい値IEとともに通信量の値を送信し、UPFは、特定の使用状況レポートルール（URR）の通信量に達すると通信使用状況レポートを送信します。トリガーが1に設定されている場合、レポートのリクエスト（データボリューム使用量がボリュームしきい値に達したとき）が送信されます。
- 時間しきい値：このトリガーは、時間ベースの測定が設定されている場合に設定されます。SMFは、time threshold IEとともに時間しきい値を送信し、時間しきい値が、具体的なURRに達すると、UPFは、リソース使用状況レポートを送信します。トリガーが1に設定されている場合、レポートのリクエスト（時間使用量が時間しきい値に達したとき）が送信されます。
- 通信の開始：このトリガーが設定されている場合、アプリケーションに対して通信が開始されると、UPFは使用状況レポートを送信します。
- リンクされた使用状況レポート：このトリガーが設定されている場合、UPFはこの特定のURRの使用状況レポートを送信します。さらに、このトリガーが設定されている場合、使用状況レポートはUPFにリンクされているすべてのURRに送信されます。UPFは、リンクされたURR-Id IEとともにリンクされたURR-Idを送信します。トリガーが1に設定されている場合は、リンクされている使用状況レポートのリクエストが送信されます。

PFCP Modification 応答での使用状況レポート

UPFは、リクエストメッセージで受信したIEに基づいて、Session Modification要求を受信した後にSession Modification応答を送信します。UPFは、次のシナリオで、Session Modification応答にusage report IEを含めます。

- URR処理をクエリする：SMFが、Session Modification応答（具体的なIE内でSession Modification応答が存在する場合）のUPFから即時使用状況レポートをリクエストした際に、URR-Id IEが含まれます。

- すべての URR （QAURR）処理をクエリする：UPF は、SMF からの PFCPSMReq-Flags IE で設定された QUARR フラグを受信すると、この PFCP セッション向けに SMG が事前にプロビジョニングしたすべての URR に対して Session Modification 応答を使用して、使用状況レポートを送信します。
- URR を更新する：SMF は、Session Modification 手順中に古い値で既存の ID の新しい値を更新します。
- URR を削除する：Session Modification 手順中に、SMF は、未受信だが、以前い利用可能であった IE を削除します。

オンライン課金およびオフライン課金の使用状況レポート

オンラインおよびオフライン課金の使用状況レポートは、次の方法でサポートされています。

- Service ID が Charging-Action に存在する場合でも、Rating-Group レベルに基づくオンライン課金の URR。この動作は、クレジット制御グループで diameter ignore-service-id が設定されている場合に発生します。
- Charging-Action で構成されている静的ルールおよび事前定義済みルールの Rating-Group レベルと Service ID の組み合わせに基づくオフライン課金の URR。

両方の URR は SMF によってリンクされています。これらの URR は、オンライン URR が報告されるとオフライン URR も報告されるようにリンクされています。

（注） Update URR に時間またはボリュームのしきい値が含まれていない場合、そのしきい値はそのポイント以降は監視されません。

Rating-Group と Service ID を使用した使用状況レポート

この機能は、Session Report 要求の Usage Report IE で入力された Rating-Group（RG）または Service ID（SI）が記載された使用状況を SMF に報告します。

RG と SI は、独自の PFCP IE を使用して入力され、静的および事前定義の設定済みルールにのみ関連付けられた URR の使用状況レポートに適用されます。この値は、ruledef に関連付けられている構成された charging-action から派生し、静的ルールの場合、事前定義されたアクティベーション時または通信ヒット時に URR が作成されます。

charging-action の RG/SI プロパティの変更は、新しい URR にのみ反映されます。このような charging-action に関連付けられている既存の URR は、以前の RG + SI 値で使用状況を報告し続けます。

UPF は、オンライン URR とオフライン URR の使用状況レポートを区別せず、charging-action で構成された RG + SI/RG/SI 値を報告し、結果として URR が作成されます。

注：SMF がこの機能を処理する方法については、『*UCC 5G SMF* 構成およびアドミニストレーション ガイド』の「*SMF* 課金」章の「ダイナミック構成変更のサポート」項を参照してください。

QAURR フラグを実装する

SMF は PFFCPSMReq-Flags IE の QAURR フラグを設定して、以前にプロビジョニングされたすべての URR の即時使用状況レポートを要求します。または、SMF クエリは、Query URR IE で URR-ID を送信することにより、選択した URR のレポートを実行します。SMF が、PFCPSMReq-Flag IE または URR-Id with Query URR IE で設定された QAURR フラグを送信する際、UPF は、PFCP Session Modification 応答と共に対応する URR に関する usage report IE を送信します。

サポートされる機能と制限事項

ボリュームクォータ メカニズムを使用した基本的なコールフローは、以下の制限付きでサポートされます。

- セッションセットアップ時およびセッション中のどちらでも、[Dynamic Rules with Online Enabled] がサポートされます。
- セッションセットアップ時およびセッション中のどちらでも、[Predefined Rules]（ダイナミックのみ）がサポートされます。「プリエンプティブな要求」の設定に制限はありません。
- オンライン課金を使用する静的ルールがサポートされます。
- Ignore-service-id がサポートされます。
- ボリュームクォータ/ボリュームしきい値メカニズムがサポートされます。
- イベントトリガー（クエリ URR が発生するもの）、および OCS への使用状況情報の送信がサポートされます。
- OCS が新しいクォータを許可する Sx/N4-Session-Modification 手順を介した「updateURR」手順がサポートされています。
- Pending-Traffic-Treatment（PTT）の [Drop] / [Pass] は、次の制限付きでサポートされます。
  - 現在サポートされているシナリオは、「クォータなし」および「クォータ枯渇」です。
  - トリガーまたは再承認シナリオはサポートされていません。
  - PTT アクション（[Forward] / [Drop]）は、クォータ取得で取得できるクォータが枯渇した後に考慮されます。
- 実測時間クォータメカニズムがサポートされます。
- その他の時間クォータメカニズム（離散期間および連続期間）はサポートされません。

- Final-Unit-Indication Terminate メカニズムがサポートされます。
- [FUI-Restrict] はサポートされません。
- Server-Unreachable（SU）メカニズムがサポートされたことにより、非 5G UPF P-GW と比較して動作が若干変更されました。
  - URR が UPF でクォータを必要とする場合、使用状況レポートが SMF に生成され、SMF がリンクされた SU_URR で応答するまで、この URR に一致するパケットは [Pending-Traffic-Treatment] 設定で処理されます。
  - SU 時間クォータを使用する場合、クォータの枯渇が SMF に報告され、セッションが再びサーバー到達不能状態になると、前回の使用状況レポートからの経過時間が使用状況に計上されます。
- Pending-Traffic-Treatment バッファメカニズムはサポートされません。
- [Quota-Hold-Time] がサポートされます。
- Quota-Consumption-Time メカニズムはサポートされません。
- [Quota-Validity-Time] がサポートされます。
- [rated-group] 値では、「content-id」以外の値の設定がサポートされます。
  - RG「0」はサポートされません。
- Out-of-Credit、Reallocation-of-Credit イベントの PCF へのトリガーは認定されていません。



重要 PCF に対するイベントトリガーの [Out-of-Credit] は、1 回限りの付与クォータ（合計ボリュームと付与ボリュームが同じ値）という制限付きで検証されます。

- [Service-Specific-Units] はサポートされません。
- [Tariff-Time] の変更は、3GPP 仕様に従ってサポートされます。
- [FUI-Redirect] は、次の制限付きでサポートされます。
  - HTTP のリダイレクトはサポートされません。
  - フィルタ ID/フィルタルールを使用した FUI リダイレクトはサポートされません。
  - WSP プロトコルはサポートされません。
  - **redirect-require-user-agent** CLI コマンドはサポートされません。ユーザーエージェントが存在しない場合でも、リダイレクトは引き続き機能します。
  - 元の URL の追加はサポートされません。

- リダイレクトを脱するトークンベースのメカニズムはサポートされません。5G UPF でリダイレクトを終了するには、OCS が Redirect Validity-Time または RAR を送信します。
- FUI リダイレクトは、非 5G UPF アーキテクチャでの動作と同様に、URL に対してのみサポートされます。
- FUI リダイレクト URL のポイント指定の確認はサポートされていません。

PTT no-quota Limited Pass

この機能により、サブスクライバは OCS からの応答を待機している間にネットワークを使用できます。Limited-Pass 設定では、サブスクライバが OCS からのクォータ応答を待機している間に消費できるボリュームを指定できます。使用量はそれぞれの課金バケツでカウントされ、次のクォータ割り当てに対して調整されます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
      pending-traffic-treatment noquota limited-pass volume volume
      end
```

Limited Pass Volume は、**noquota** のケース（クォータを初めて要求する評価グループ（RG））にのみ使用され、**quota-exhausted** には使用されません。Limited Pass Volume は、後続のクレジット要求には使用されません。

Limited Pass Volume が使い果たされるまで、トラフィックの通過が許可されます。使用量はそれぞれの課金バケットでカウントされ、付与された「クォータ」に対して調整されます。「クォータ」割り当てが実際の使用量よりも少ない場合、使用状況レポートを使用した OCS への即時レポートが発生し、より多くのクォータ割り当てが要求されます。後続の着信パケットは、「quota-exhausted」PTT 設定に従って処理されます。

OCS がクォータの拒否で応答する前に Limited Pass Volume が使い果たされていない場合、トラフィックは OCS 応答後にブロックされます。ゲートウェイは、次の SX_SESSION_REPORT_REQUEST で Limited Pass Volume の使用状況を報告します。

OCS が応答する前に Limited Pass Volume が使い果たされた場合、OCS からクォータが付与されるまで、セッションの後続の着信パケットはドロップされます。

noquota のデフォルトの pending-traffic-treatment は Drop です。**default pending-traffic-treatment noquota** コマンドは、設定されたすべての Limited Pass Volume サイズを削除します。

PTT クォータ枯渇制限パス

クォータ枯渇制限パスは、高速ネットワークにおける現実的な問題により、クォータ枯渇バッファの代替策として提案されます。バッファリングでは、ゲートウェイでの多数のパケットに応じたパケットバッファリングが必要です。パケットの数が多いと、帯域幅の速度に影響するメモリ不足のリスクが発生します。したがって、Limited Pass は Buffer オプションの代替手段

です。Limited Pass では、クォータ枯渇シナリオで設定された制限に達するまで、通信を通過させます。

この機能を有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    credit-control
     pending-traffic-treatment quota-exhausted limited-pass volumevolume

      end
```

（注） 上記の CLI は、5G UPF アーキテクチャにのみ適用されます。

Limited-Pass ボリュームを使い果たすと、クォータが割り当てられるまで、以降のパケットはドロップされます。

Limited Pass は、Limited-Pass ボリュームを使いきるまで通信を許可します。Limited Pass は、付与された「クォータ」を基準に、それぞれの charging-bucket の使用状況を計算して調整します。「クォータ」割り当てが実際の使用量よりも少ない場合は、usage-report を通じてすぐに OCS に報告し、追加のクォータ割り当てを要求します。

OCS がクォータの拒否に応答する前に、Limited-Pass ボリュームが枯渇しなければ、OCS 応答後に通信がブロックされます。ゲートウェイは、SX_SESSION_REPORT_REQUEST で使用状況を報告します。

OCS からの応答前に Limited-Pass ボリュームが枯渇した場合、OCS からクォータが付与されるまで、セッションでは以降の受信パケットがドロップされます。

quota-exhausted に対する pending-traffic-treatment のデフォルトは、Drop です。デフォルトの pending-traffic-treatment quota-exhausted コマンドにより、設定済みの Limited-Pass ボリュームのサイズは削除されます。

タリフ時間のサポート

タリフ切り替え時間機能は、サブスクライバが、あるタリフプランから別のタリフプランに切り替わるときに適用されます。

Tariff-Time-Change AVP はタリフ切り替え時間を決定するために使用され、Monitoring-Time IE はタリフ時間サポート機能をサポートするために使用されます。

タリフタイマーが終了すると、ゲートウェイは別途、使用量を課金バケットに累積し、引き続き元のクォータ値から消費します。次回のレポート時（クォータの枯渇またはその他の制御イベント発生時）に、ゲートウェイはこの課金バケツの 2 つの使用量（タリフ時間変更の前後）をレポートします。

この課金バケツの 1 つ目のレポートには [Reporting-Reason] として Monitoring Time が含まれ、2 つ目のバケツには前回のレポート理由と、タリフタイマー終了後のクォータの使用状況が含まれます。

データトラフィックの使用状況は、タリフ切り替え前のリソース使用量とタリフ切り替え後のリソース使用量に分けられます。Tariff-Change-Usage AVP は、Used-Service-Units AVP 内で使用され、レポートされた使用状況をタリフ時間変更の前と後で区別します。

制限事項

この機能には次の既知の制限事項があります。

- RG/サービス ID の各組み合わせに対してサポートされるタリフ時間は 1 つのみです。
- タリフ時間の変更の前後で異なるクォータの割り当てはサポートされません。この機能は、3GPP 標準規格に準拠していません。

TCP 最大セグメントサイズ

TCP/IP スタックは、常にヘッダーに最大セグメントサイズ（MSS）フィールドを挿入します。これにより、TCP プロキシを使用する場合と使用しない場合の MSS 挿入動作に違いが生じます。

TCP SYN パケットにすでに TCP MSS が存在する場合、**tcp mss** 構成を使用すると、TCP MSS を制限できます。IP ヘッダーまたは TCP 必須ヘッダーでエラーが検出されず、メモリ割り当てエラーも発生していない場合、TCP オプションヘッダーが解析されます。TCP MSS がオプションヘッダーに存在し、その値が設定された MSS 値より大きい場合、TCP パケットの値は、設定されている値で置き換えられます。

TCP オプションヘッダーが SYN パケットに存在せず、すでに存在する TCP ヘッダーにエラーがない場合、現在のパケットの送信時に、設定された TCP MSS 値が挿入されます。

使用状況レポートのクレジット制御を構成する

この構成により、Diameter ディクショナリで定義された Service-Identifier AVP で Service ID を受け入れたり無視したりできます。

```
configure
  require active charging
  active-charging service service_name
    credit-control group group_name
      diameter ignore-service-id
      end
```

- **diameter ignore-service-id** ：このコマンドを使用すると、いずれかの Diameter ディクショナリが Service-Identifier AVP をサポートしている場合でも、Gy インターフェイスの実装で Service-Identifier AVP の使用を無効にできます。また、この AVP を Gy のやり取りでは使用せず、GCDR/eGCDR には含める必要がある場合にも使用できます。

使用状況レポートの ACS ルールベースを構成する

このセクションでは、ACSルールベースを作成、設定、または削除する方法について説明します。ルールベースは、フローと一致するプロトコルルール、および一致したフローに対して実行される関連アクションのコレクションです。サブスクライバ/APN に使用する特定のルールベースが設定されていない場合、デフォルトのルールベースが使用されます。

ルールベースの設定は、指定されたすべての設定を組み合わせて静的および事前定義された PCC ルールを構築する設定です。

```
configure
   active-charging service service_name
      rulebase rulebase_name
         action priority action_priority { [ dynamic-only ] |
static-and-dynamic | timedef timedef_name ] { group-of-ruledefs
ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name
 [ monitoring-key monitoring_key ] [ description description ] }
         cca quota { holding-time holding_time content-id content_id |
retry-time retry_time [ max-retries retries ] }
         credit-control-group cc_group_name
         dynamic-rule order { always-first | first-if-tied }
        egcdr threshold { interval interval [ regardless-of-other-triggers
 ] | volume { downlink | total | uplink } bytes }
         route priority route_priority ruledef ruledef_name analyzer { dns |
 file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 |
 mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http |
sip [ advanced | basic-and-advanced ] | smtp | tftp | wsp-connection-less
 | wsp-connection-oriented } [ description description ]
         tcp check-window-size
         tcp mss tcp_mss { add-if-not-present | limit-if-present |
limit-if-present add-if-not-present }
         tcp packets-out-of-order { timeout timeout_duration | transmit [
 after-reordering | immediately ] }
         end
```

注：

- **rulebase** *rulebase_name*：ACS rulebase の名前を指定します。*rulebase_name* は、1 ～ 63 文字の英数字の文字列で指定する必要があります。
- **action priority** *action_priority* **{ [dynamic-only] | static-and-dynamic | timedef** *timedef_name* **] { group-of-ruledefs** *ruledefs_group_name* **| ruledef** *ruledef_name* **} charging-action** *charging_action_name* **[monitoring-key** *monitoring_key* **] [description** *description* **] }**：ruledef が一致し、charging action が関連付けられている優先順位を構成します。
  - *priority* は、1 ～ 65535 の整数値で指定する必要があります。
  - *monitoring_key* は、100000 ～ 4000000000 の整数値で指定する必要があります。

- **cca quota { holding-time** *holding_time* **content-id** *content_id* **| retry-time** *retry_time* **[max-retries** *retries* **] }**：オンライン課金のクォータを構成します。
  - *holding_time*：1 ～ 4000000000 の整数値で指定する必要があります。
  - *content_id*：1 ～ 2147483647 の整数値で指定する必要があります。
  - *retry_time*：1 ～ 86400 の整数値で指定する必要があります。
  - *retries*：1 ～ 65535 の整数値で指定する必要があります。
- **credit-control-group***cc_group_name*：この rulebase で使用されるオンライン課金のパラメータを設定します。 *cc_group_name* は は、1 ～ 63 文字の英数字の文字列である必要があります。
- **dynamic-rule order**：rulebase 内で、ダイナミックルールと静的ルールを照合する順序を構成します。
- **egcdr threshold { interval** *interval* **[regardless-of-other-triggers] | volume { downlink | total | uplink } bytes }**：オフライン課金のしきい値を構成します。
  - **interval**：60 ～ 40000000 の整数値で指定する必要があります。
  - **downlink**:：100000 ～ 4000000000 の整数値で指定する必要があります。デフォルト：4000000000。
  - **uplink**:：100000 ～ 4000000000 の整数値で指定する必要があります。デフォルト：4000000000。
  - **total**:：100000 ～ 4000000000 の整数値で指定する必要があります。
- **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [advanced | basic-and-advanced] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [description** *description* **]**：このコマンドは、UPF のみで使用します。
  - *route_priority* は、0 ～ 65535 の整数値で指定する必要があります。
  - *ruledef_name* は、1 ～ 63 の英数字の文字列で指定する必要があります。
- **tcp check-window-size**：このコマンドは UPF でのみ使用されます。
- **tcp mss** *tcp_mss*：このコマンドは、UPF でのみ使用します。*tcp_mss* は、496 ～65535 の整数値で指定する必要があります。
  - **add-if-not-present** ：パケットに TCP MSS が存在しない場合に、追加するよう指定します。
  - **limit-if-present** ：パケットに TCP MSS が存在する場合に、制限するよう指定します。
  - **limit-if-present add-if-not-present** ：TCP MSS が存在する場合は制限するように指定し、存在しない場合は、パケットに追加します。

Note The **tcp mss** *tcp_mss* **limit-if-present add-if-not-present** CLI コマンドは、2021.02.0 以降のリリースで使用可能です。

- **tcp packets-out-of-order { timeout** *timeout_duration* **| transmit [after-reordering | immediately] }**：このコマンドは UPF のみで使用します。
  - *timeout_duration* は、100 ～ 30000 の整数値で指定する必要があります。デフォルト値は 5000 です。

設定例

```
active-charging service acs
    ruledef ip-any-rule
      ip any-match = TRUE
    #exit
    urr-list upf
      rating-group 10 ser 10 urr-id 10
      rating-group 10 urr-id 50
    #exit
    charging-action starent
      content-id 10
      service-identifier 10
      billing-action egcdr
      cca charging credit rating-group 10
    exit
    credit-control group CCG
      diameter ignore-service-id
    #exit
    rulebase starent
      billing-records egcdr
      action priority 30 ruledef ip-any-rule charging-action starent
      egcdr threshold interval 3600
      egcdr threshold volume total 200000
      egcdr threshold volume downlink 100000 uplink 100000
      dynamic-rule order first-if-tied
      credit-control-group CCG
    #exit
#exit

context ISP
    apn starent.com
      accounting-mode gtpp
      gtpp group my_grp accounting-context ISP
      ip context-name ISP
    #exit
    gtpp group my_grp
      gtpp egcdr service-data-flow threshold interval 1200
      gtpp egcdr service-data-flow threshold volume downlink 13000
      gtpp egcdr service-data-flow threshold volume uplink 17000
      gtpp egcdr service-data-flow threshold volume total 22222
    #exit
end
```

モニタリングおよびトラブルシューティング

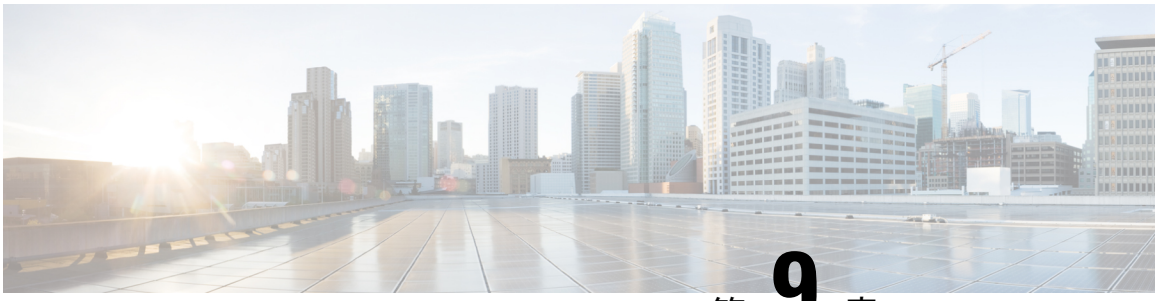
show コマンドと出力

この項では、この機能をサポートするために使用可能な show CLI コマンドについて説明します。

show-user-plane-service statistics rulebase name <name>

このCLIコマンドを使用して、TCP最大セグメントサイズ（MSS）機能のサポートで使用可能な次のフィールドを表示します。

- TCP MSS 挿入パケッ：MSS 挿入パケットの総数を表示します。
- TCP MSS 限定パケット：TCP MSS 限定パケットの総数を表示します。



第 9 章

VPP による Cisco Ultra Traffic Optimization

- 機能の概要と変更履歴 （89 ページ）
- 機能説明 （90 ページ）
- RCM のサポート （91 ページ）
- Cisco Ultra Traffic Optimization への GBR または MBR 値の送信 （91 ページ）
- 機能の仕組み （91 ページ）
- show コマンドと出力 （94 ページ）
- 設定例 （98 ページ）

機能の概要と変更履歴

要約データ

表 *17* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

表 *18* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.1

機能説明

UPF は、Vector Packet Processing（VPP）で Cisco Ultra Traffic Optimization（CUTO）をサポートしています。

Cisco Ultra Traffic Optimization とは、軋轢状態のセルのサブスクライバ接続速度を向上させることにより、セル容量を大幅に増やす RAN 最適化テクノロジーです。これにより、RAN の最適化が実現します。モバイルネットワーク事業者（MNO）はネットワーク品質の目標を達成する一方で、展開するセルの数を継続的に削減したり、トラフィックの増加に対応したりできます。

アダプティブビットレート（ABR）ビデオなどの大規模なトラフィックフローは、無線リソースを飽和させ、eNodeB スケジューラのメモリを大量に消費します。Cisco Ultra Traffic Optimization は、機械学習アルゴリズムを使用してネットワーク内の大量の通信フロー（ビデオなど）を検出します。また、これらのフローの配信を最適化し、ユーザーの品質を変えることなくネットワークの輻輳を軽減します（つまり、ビデオの動作が同じになります）。つまり、Cisco Ultra Traffic Optimization は、ネットワークの中核部分にソフトウェア インテリジェンスを取り入れることで、ビデオが RAN に与える多大な影響を軽減します。

その結果、輻輳した状態のネットワークでも Web サイトの閲覧が可能になります。Cisco Ultra Traffic Optimization：

- 平均ユーザースループットが向上します。
- 輻輳状態にあるセルサイトのキャパシティを増やします。
- スケジューラの遅延を削減します。
- セルを共有するユーザーやトラフィックが増えた場合にも、ユーザーエクスペリエンスの品質を維持します。
- eNodeB パフォーマンスカウンタ（平均 UE スループット、スケジューラ遅延）で直接測定されます。これらは、ネットワーク キャパシティ プランニングに使用される重要業績評価指標（KPI）です。
- RAN の投資要件を永続的に節約します。
- Cisco StarOS P-GW に統合されます。
- 新しいハードウェアやケーブル配線の煩雑な作業は必要ありません。すぐに利用できます。
- HTTP または HTTPS および QUIC 通信をサポートします。

ライセンス

VPP を使用した Cisco Ultra Traffic Optimization は、シスコのライセンスソリューションです。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。ライセンスのインストールと確認の詳細については、『*VPC-SI* システム管理ガイド』の「ソフトウェア管理操作」章の「ライセンスキーを管理する」項を参照してください。

RCM のサポート

この機能により、Cisco Ultra Traffic Optimization（CUTO）の Redundancy and Configuration Management（RCM）のサポートが有効になります。サービススキーマおよび CUTO プロファイルまたは UPF のポリシーのアプリケーションを使用して CUTO を有効にするすべての関連構成は、RCM を使用してサポートされます。

Cisco Ultra Traffic Optimization への GBR または MBR 値の送信

フローレベルの MBR が GBR ベアラー以外の APN-AMBR より大きい場合、トラフィックは APN-AMBR でスロットリングされます。このような場合、APN-AMBR が上限値として CUTO ライブラリに送信されます。フロー固有の有効なフローレベルの MBR がない場合、APN-AMBR は、上限値として CUTO ライブラリに送信されます。

GBR ベアラーの場合、CUTO ライブラリにはフローレベルの GBR が下限値として、フローレベルの MBR が上限値として 送信されます。

Cisco Ultra Traffic Optimization ライブラリの初期化解除

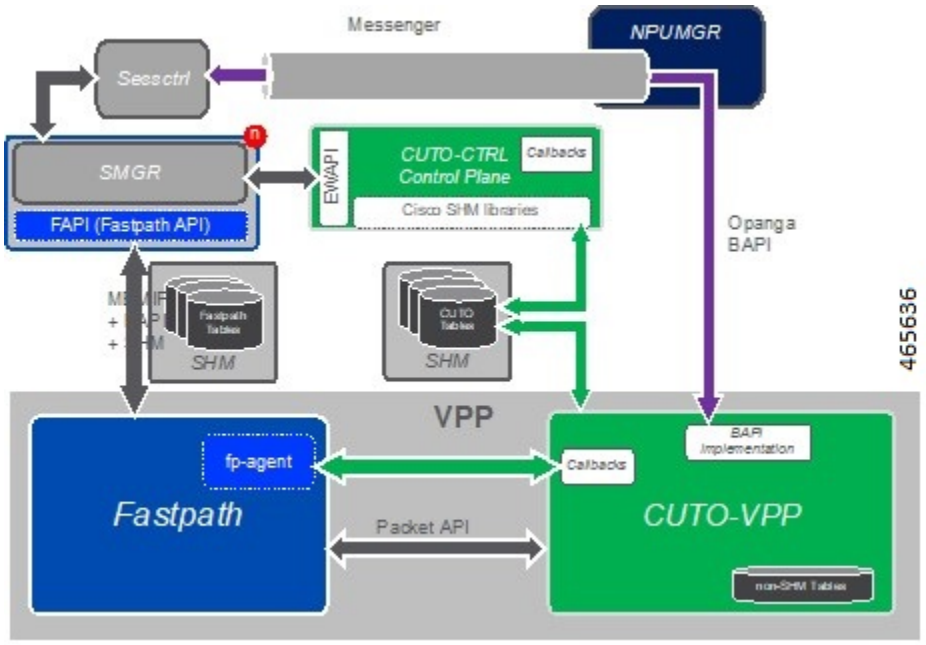
この機能は現在、初期化解除をサポートしていません。初期化解除は、Cisco Ultra Traffic Optimization（CUTO）ライセンスがシステムから削除されたときに発生します。

機能の仕組み

アーキテクチャ

次の図は、VPP の Cisco Ultra Traffic Optimization のアーキテクチャを示しています。

図 *10* : アーキテクチャ



CUTO-CTRL

- CUTO-CTRL は、East-West API（EWAPI）経由で SMGR からガイダンスと 要求を受信します。その結果、クライアント（SMGRインスタンス）が登録および登録解除され、新しいストリームやフローが作成および終了されます。
- CUTO-CTRL は、シスコが提供する SHM インフラストラクチャで構成される North-South API（NSAPI）を使用して、一連の共有メモリ（SHM）テーブルを管理します。
- CUTO-VPP は、この SHM 環境を通じて、CUTO-VPP と CUTO-CTRL の両方に表示されるコンテンツを読み取りおよび書き込みできます。
- SHM は、VPP での CUTO ソリューションの高性能設定と管理に必要な、すべての大容量かつスケーラブルで変更可能なコンテンツに使用されます。

NPUMGR

NPUMGR は、VPP 操作全体を担当する管理層です。これは、初期化、グローバルランタイム構成、ポリシー構成に向けて Binary API (BAPI) 要求を CUTO-VPP に送信します。

SMGR

SMGR は、メインのサブスクライバ コントロール プレーンです。N SMGR インスタンスがあり、すべてのインスタンスは、SessCtrl によって管理されます。VPPMOB/Fastpath のコンテキストでは、SMGR インスタンスは「クライアント」とも呼ばれ、各クライアントには一意の ID があります。

SMGR は、Messenger トンネル経由でポリシー指示を SessCtrl に発行し、更新された Policy ガイダンスを Binary API 経由で CUTO- VPP に送信します。

SMGR は、一連の MEMIF、Binary API 、および共有メモリ（SHM）インフラストラクチャを使用して、既存の機能について Fastpath と通信します。

セッション制御（SessCtrl）

セッション制御は、一連の SMGR インスタンスを監視する管理レイヤです。

BAPI 要求は、Messenger 経由で SessCtrl から NPUMGR にトンネリングされます。

高速パス（Fastpath）

VPP はパケット処理を担当します。fastpath は、VPP 環境内でサブスクライバに関連するパケット処理を実行します。サブスクライバフローは単方向ストリームに分割されます。ストリームコンジットは、パケットが変換され、サブスクライバの処理から変換され、送信されるまでに通過する機能のパイプラインです。

fastpath と CUTO- VPP 間の packet API により、fastpath コンジットを通過するパケットの交換が容易になります。

CUTO-VPP

- CUTO-VPP は、UPF のパケット処理エンジンです。
- fastpath では、Cisco Ultra Traffic Optimization は、その動作で設定されたストリーム上のパケットに適用されます。
- パケットはストリームコンジットから特定の CUTO-VPP 操作に送信され、潜在的な遅延（0 ～ N ミリ秒）の後、同じコンジットにトラフィックが返されます。
- Cisco Ultra Traffic Optimization ライブラリは、パケットをドロップすることはありません。

CUTO-TODR

Traffic Optimization Data Records（TODR）は、イベントのみを生成でき、構成が利用可能になった場合のみ有効化されます。

制限事項

Cisco Ultra Traffic Optimization 機能には、以下の制限があります。

- サービススキーマで行われた CUTO 設定の変更は、既存のフローに対してはすぐに有効になりません。
- Cisco Ultra Traffic Optimization VPP のグローバルな初期化解除はサポートされていません。
- Cisco Ultra Traffic Optimization を有効にするためのベアラー関連のトリガーはサポートされていません。

- ルール照合変更トリガーは、UPC の CUTO に対して設定する必要があります。
- 通信最適化の有効化や無効化は、「loc-update」トリガーではサポートされていません。
- CUTO ライセンスを削除しても、全体的な初期化解除はトリガーされません。新しいフローの CUTO 機能を解除するには、CUTO 設定を削除する必要があります。

show コマンドと出力

この項では、CUPS での Cisco Ultra Traffic Optimization のサポートにおける show コマンドおよびその出力について説明します。

その他のサポートされている show コマンドの詳細については、P-GW アドミニストレーション ガイド [英語] の「Cisco Ultra Traffic Optimization」の章にある「Monitoring and Troubleshooting」の項を参照してください。

show コマンドと出力

show user-plane-service traffic-optimization counters sessmgr all

このコマンドの出力には、次のフィールドが含まれています。

TCP トラフィック最適化フロー：

- Active Normal Flow Count
- Active Large Flow Count
- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Total Normal Flow Count
- Total Large Flow Count
- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

UDP トラフィック最適化フロー：

- Active Normal Flow Count
- Active Large Flow Count

- Active Managed Large Flow Count
- Active Unmanaged Large Flow Count
- Total Normal Flow Count
- Total Large Flow Count
- Total Managed Large Flow Count
- Total Unmanaged Large Flow Count
- Total IO Bytes
- Total Large Flow Bytes
- Total Recovered Capacity Bytes
- Total Recovered Capacity ms

show user-plane-service traffic-optimization info

このコマンドの出力には、次のフィールドが含まれています。

- CUTO Ctrl Library Version
- CUTO VPP Library Version
- Mode
- Configuration
  - Data Records (TODR)
  - Statistics Options
  - EFD Flow Cleanup Interval
  - Statistics Interval

show user-plane-service traffic-optimization policy all

このコマンドの出力には、次のフィールドが含まれています。

- Policy Name
- Policy-Id
- Bandwidth-Mgmt
  - Backoff-Profile
  - Min-Effective-Rate
  - Min-Flow-Control-Rate
- Curbing-Control：
  - Time

- Rate
- Max-Phases
- Threshold-Rate

- Heavy-Session：
  - Threshold
  - Standard-Flow-Timeout
  - Seed-Time

- Detection-Mode
- Link-Profile：
  - Initial-Rate
  - Max-Rate
  - Peak-Lock

- Session-Params：
  - Tcp-Ramp-Up
  - Udp-Ramp-Up

- 検出された通信最適化ポリシーの総数

バルク統計情報

UPF の Cisco Ultra Traffic Optimization では、次の既存のバルク統計がサポートされています。

バルク統計	説明
cuto-uplink-drop	CUTO ライブラリによってドロップされたアップリンクパケットの合計数を示します。
cuto-uplink-hold	CUTO ライブラリによって保持されているアップリンクパケットの合計数を示します。
cuto-uplink-forward	CUTO ライブラリによって転送されたアップリンクパケットの合計数を示します。
cuto-uplink-rx	CUTO ライブラリが受信したアップリンクパケットの合計数を示します。
cuto-uplink-tx	CUTO ライブラリが送信したアップリンクパケットの合計数を示します。

バルク統計	説明
cuto-dnlink-drop	CUTO ライブラリによってドロップされたダウンリンクパケットの合計数を示します。
cuto-dnlink-hold	CUTO ライブラリによって保持されているダウンリンクパケットの合計数を示します。
cuto-dnlink-forward	CUTO ライブラリによって転送されたダウンリンクパケットの合計数を示します。
cuto-dnlink-rx	CUTO ライブラリが受信したダウンリンクパケットの合計数を示します。
cuto-dnlink-tx	CUTO ライブラリが送信したダウンリンクパケットの合計数を示します。
cuto-todrs-generated	生成された TODR の合計数を示します。
tcp-active-normal-flow-count	Cisco Ultra Traffic Optimization の TCP active-normal-flow カウントの数値を示します。
tcp-active-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-large-flow カウントの数値を示します。
tcp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-managed-large-flow カウントの数値を示します。
tcp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP active-unmanaged-large-flow カウントの数値を示します。
tcp-total-normal-flow-count	Cisco Ultra Traffic Optimization の TCP total-normal-flow カウントの数値を示します。
tcp-total-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-large-flow カウントの数値を示します。
tcp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-managed-large-flow カウントの数値を示します。
tcp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の TCP total-unmanaged-large-flow カウントの数値を示します。
tcp-total-io-bytes	Cisco Ultra Traffic Optimization の TCP total-IO のバイト数を示します。
tcp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の TCP total-large-flow のバイト数を示します。

バルク統計	説明
tcp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティのバイト数を示します。
tcp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の TCP total-recovered キャパシティをミリ秒単位で示します。
udp-active-normal-flow-count	Cisco Ultra Traffic Optimization の UDP active-normal-flow カウントの数値を示します。
udp-active-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-large-flow カウントの数値を示します。
udp-active-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-managed-large-flow カウントの数値を示します。
udp-active-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP active-unmanaged-large-flow カウントの数値を示します。
udp-total-normal-flow-count	Cisco Ultra Traffic Optimization の UDP total-normal-flow カウントの数値を示します。
udp-total-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-large-flow カウントの数値を示します。
udp-total-managed-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-managed-large-flow カウントの数値を示します。
udp-total-unmanaged-large-flow-count	Cisco Ultra Traffic Optimization の UDP total-unmanaged-large-flow カウントの数値を示します。
udp-total-io-bytes	Cisco Ultra Traffic Optimization の UDP total-IO のバイト数を示します。
udp-total-large-flow-bytes	Cisco Ultra Traffic Optimization の UDP total-large-flow のバイト数を示します。
udp-total-recovered-capacity-bytes	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティのバイト数を示します。
udp-total-recovered-capacity-ms	Cisco Ultra Traffic Optimization の UDP total-recovered キャパシティをミリ秒単位で示します。

設定例

CUTO 機能を有効にする構成例：

```
configure
  active-charging service ACS
    trigger-action TA1
       traffic-optimization policy custom1
    #exit
    trigger-condition TC1
      rule-name = dynamic-rule2
    #exit
    service-scheme SS1
      trigger rule-match-change
        priority 5 trigger-condition TC1 trigger-action TA1
      #exit
    subs-class SB1
      rulebase = cisco
    #exit
    subscriber-base default
      priority 5 subs-class SB1 bind service-scheme SS1
    #exit
    traffic-optimization-profile
      mode active
      data-record
    #exit
    traffic-optimization-policy custom1
      bandwidth-mgmt min-effective-rate 800 min-flow-control-rate 250
      heavy-session threshold 200000
      link-profile max-rate 20000
    #exit
    traffic-optimization-policy default
    #exit
end
```

CUTO-TODR

CUTO-TODR 機能を有効にする構成例：

```
context ISP
edr-module active-charging-service
file name EDR directory TODR_CUTO rotation volume 51200 headers
cdr use-harddisk
```



第 10 章

N4 インターフェイス経由の使用状況データの収集とレポート

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 101
- 機能説明, on page 102
- 機能の仕組み, on page 102
- N4 インターフェイス経由でボリューム測定を収集およびレポートするための構成, on page 104

機能の概要と変更履歴

要約データ

Table 19: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 20: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入	2020.02.0

機能説明

このリリースでは、ユーザープレーン機能（UPF）は、N4 インターフェイスを介したオフライン課金と使用状況データのレポートをサポートします。

ここで、SMF は、必要な PDR と URR を作成することで使用状況データの収集とレポートを制御し、PFCP セッションに定義された関連する PDR に URR を関連付けます。また、IP-CAN ベアラーレベル、IP-CAN セッション、TDF セッション、SDF、またはアプリケーションレベルでのデータ使用状況のレポートを制御します。

URR は、使用状況測定方法、レポートトリガー、しきい値、およびクォータ値で構成されます。

Important このリリースでは、PFCP セッション確立中の URR の作成のみがサポートされます。

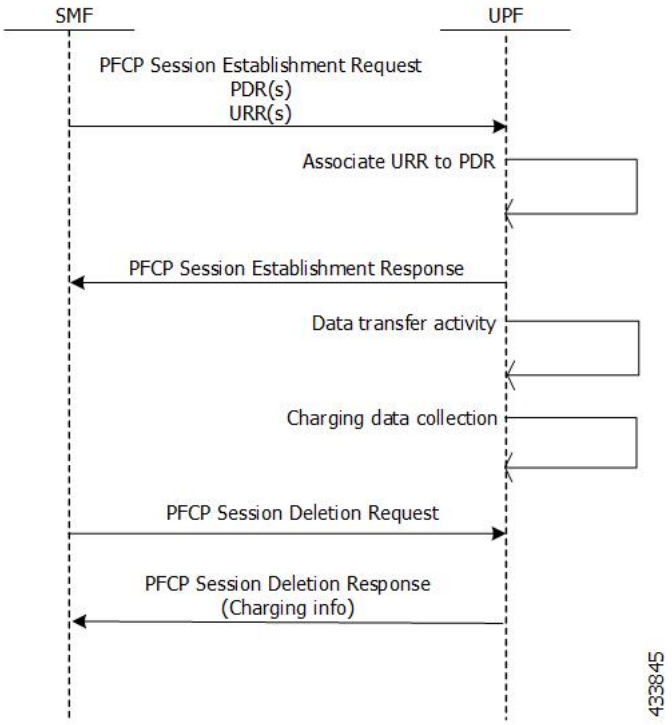
機能の仕組み

この項では、UPF が使用量データのオフライン課金をサポートする方法について説明します。

オフライン課金を実装する場合、課金情報は PFCP セッションの削除中にのみ SMF に送信されます。

時間および使用量ベースのレポートは、オフラインの課金実装でサポートされます。次のコールフローは、UPF でのオフライン課金を示しています。

Figure 11: UPF でのオフライン課金



PFCP セッションの削除中に、UPF は次の課金情報を SMF に転送します。

- 最初と最後のデータパケットのタイムスタンプ
- Duration measurement：この IE は、URR の作成と使用状況レポートの時間差を指定します。
- Volume measurement：この IE は、アップリンクデータ、ダウンリンクデータ、および UPF から gNodeB に転送された合計バイト数を指定します。

標準準拠

データの収集とレポートのための UPF サポートは、次の標準に準拠しています。

- 3GPP TS 29.244：LTE、EPC ノードのコントロールプレーン t とユーザープレーン間のインターフェイス
- 3GPP TS 23.501：5G、5G システムのシステムアーキテクチャ
- 3GPP TS 23.502v：5G、5G システムの手順

N4インターフェイス経由でボリューム測定を収集およびレポートするための構成

この項では、ボリューム測定（使用状況データ）を収集して報告するために必要な構成について説明します。ただし、これを実現するには、ボリューム測定に関する SMF ベースの構成を行う必要があります。

UPF によって URR のボリューム測定データを送信するには、次の SMF ベースの構成が必要です。

必要な課金情報アクションの課金アクションを構成する

次の構成を使用して、必要な課金アクションに対して課金アクションを構成します。

```
configure
   require active-charging
   active-charging service service_name
      charging-action charging_action_name
         billing-action interface_name
         end
```

注：

- **billing-action**：指定した請求タイプを有効にします。サポートされているインターフェイスは次のとおりです。
  - **egcdr**：GGSN 課金データレコードを有効にします。

課金アクションとルールベースを関連付ける

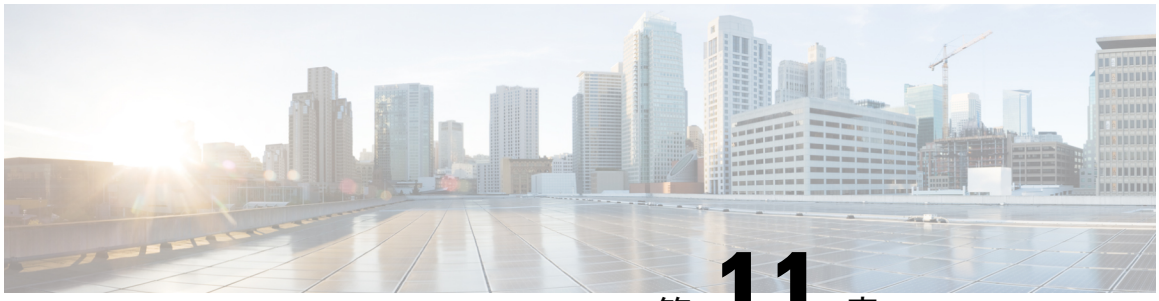
次の構成を使用して、charging action と rulebase を関連付けます。

```
configure
   require active-charging
   active-charging service service_name
      rulebase rulebase_name
         billing-records interface_name
         action priority priority_value ruledef ruledef_name charging-action
 charging_action_name
         end
```

注：

- **rulebase**：Active Charging Service Rulebase 構成を有効にします。

- **billing-records**：請求レコードの生成を有効にします。サポートされているインターフェイスは、**egcdr** です。
- **action**：ruledef で実行されるアクションを決定します。
- **priority**：rulebase 内の ruledef に優先順位を割り当てます。優先順位は、1 ～ 65535 の範囲の一意の整数値で指定する必要があります。
- **ruledef**：ruledef を指定します。
- **charging-action**：課金アクションを指定します。



第 11 章

コントロールプレーンが開始する N4 アソシエーションのサポート

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 107
- 機能説明, on page 108
- 機能の仕組み, on page 108
- CP が開始する N4 アソシエーションのセットアップ機能を構成する, on page 109

機能の概要と変更履歴

要約データ

表 *21* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 22: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

SMF が開始する N4 Association Setup 手順

N4 Association Setup 手順では、セッション管理機能（SMF）とユーザープレーン機能（UPF）の間に N4 アソシエーションを設定します。これにより、SMF が UPF リソースを使用して N4 セッションを確立できるようになります。SMF と UPF は、この手順中にそれぞれの側でサポートされている機能を交換します。

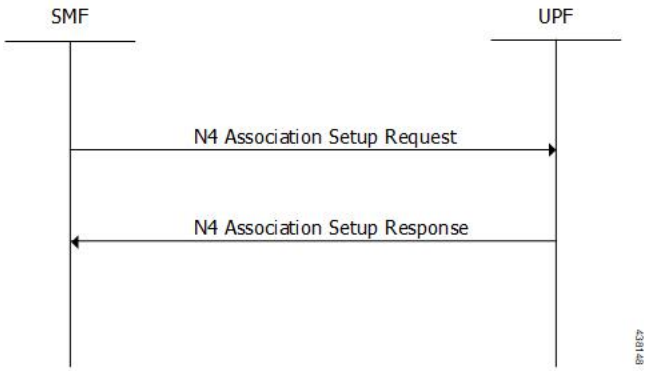
機能の仕組み

N4 Association Setup は、SMF によって開始されます。N4 Association Setup 手順の設定は、コントロール プレーン グループ構成モードの **sx-association initiated-by-cp** CLI コマンドによって制御されます。デフォルトでは、UPF によって開始された N4 Association Setup 手順をサポートするように構成が設定されています。

コール フロー

セッション管理機能が開始する N4 Association Setup 手順

次のコールフローは、SMF が開始する N4 Association Setup 手順を示しています。



ステップ	説明
1	SMF は、N4 Association Setup 手順を開始して、この UPF で最初の N4 セッションを確立する前に、UPF に対する N4 アソシエーションのセットアップを要求します。
2	N4 Association Setup 要求を受信した後、UPF は N4 Association Setup 応答を送信します。

CP が開始する N4 アソシエーションのセットアップ機能を構成する

この項では、CP が開始する N4 アソシエーション セットアップ機能の構成方法について説明します。

この機能を構成するには、コントロールプレーン構成モードで、**sx-association initiated-by-cp**" CLI コマンドを使用します。デフォルト構成は、UPF が開始する N4 Association Setup 手順です。

N4 アソシエーション セットアップ機能を構成するには、次の構成を使用します。

```
configure
   context
      control-plane-group group_name
         peer-node-id ipv4-address ip_address interface n4
         sx-association { initiated-by-cp | initiated-by-up }
         end
```

注：

- **initiated-by-cp:** このキーワードは、コントロールプレーン経由で Sx Association 要求を開始するために使用されます。
- **initiated-by-up:** このキーワードは、ユーザープレーン経由で Sx Association 要求を開始するために使用されます。
- デフォルトでは、UPF が開始する N4 Association Setup 手順が構成されています。
- デフォルト設定に戻すには、**no sx-association** コマンドを使用します。

CP が開始する N4 アソシエーションのセットアップ機能の OAM サポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

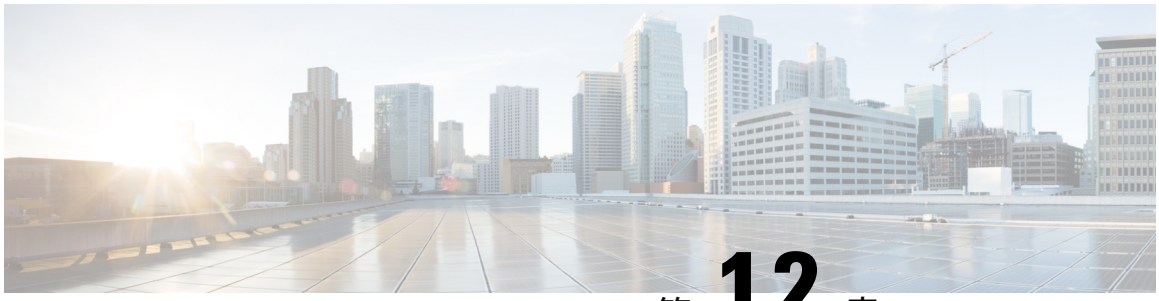
show コマンドのサポート

次の show コマンドを使用して CP が開始する N4 アソシエーション セットアップ機能構成を表示します。

show control-plane-group all

以下は show コマンドの出力例です。

```
show control-plane-group all
Control Plane Group
---------------------------------
Name           : default
Sx-Association : initiated-by-up
Name           : default
Sx-Association : initiated-by-up
Node-Id        : 209.165.200.230
Interface      : N4
```



第 12 章

コンバージドデータパス

- 機能の概要と変更履歴, on page 111
- 機能説明 （112 ページ）
- 機能の仕組み （113 ページ）
- コンバージドコールに課金する （127 ページ）
- コンバージドデータパスを構成する （130 ページ）
- モニタリングおよびトラブルシューティング （131 ページ）

機能の概要と変更履歴

要約データ

Table 23: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 24: マニュアルの変更履歴

改訂の詳細	リリース
Wi-Fi から LTE へのハンドオーバーのサポートが追加され、UPF でコンバージドデータパス機能を有効にする構成が追加されました。	2021.02.0
最初の導入。	2021.01.0

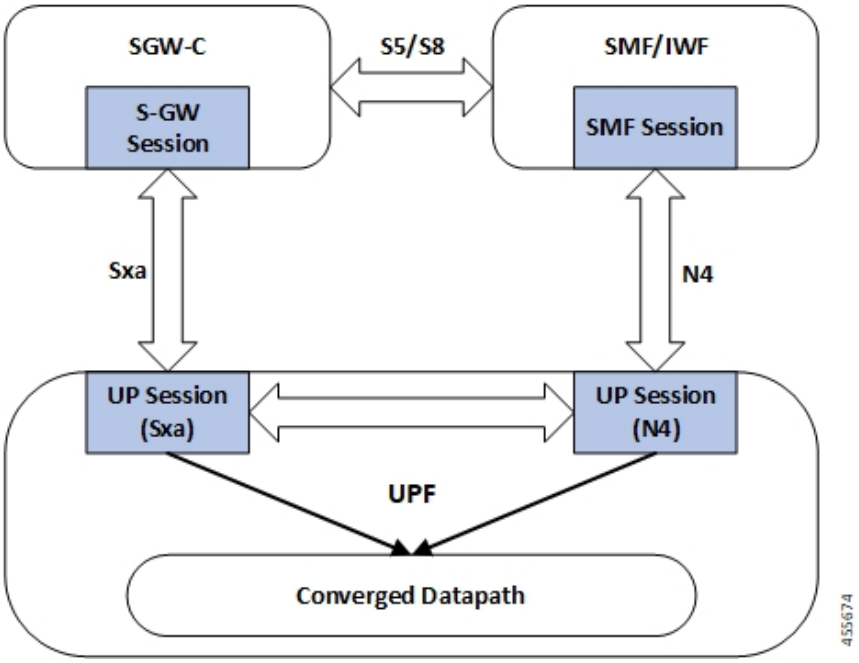
機能説明

コンバージドデータパス機能により、SGW-C/cnSGWおよびセッション管理機能（SMF）/インターワーキング機能（IWF）を使用してUPFインスタンスの同じUEのセッションを相互接続でき、コンバージド/折りたたみデータパスを構築し、より高いスループットを実現できます。この機能の目的は次のとおりです。

- UP/UPF の選択ロジックは、SGW-C/cnSGW と SMF での同じノードの選択を支援するように拡張されています。
- SxDemux は、それぞれ N4 または Sxa の既存のセッションに基づいて同じセッションマネージャ（SessMgr）インスタンスを選択します。
- Sxa セッションと N4 セッションの関連付けは、SessMgr で行われます。
- データパスは、転送プレーンで折りたたむことができます。
- サブスクライバのデータパスの余分なホップが排除され、遅延が減少し、ユーザー体験が向上します。

アーキテクチャ

この機能の一部として、SGW-C/cnSGW と SMF によって確立された同じ UPF インスタンスに 2 つのセッションがあります。確立されると、ソフトウェアロジックがピアセッションを決定し、パケット処理用のコンバージド/折りたたみデータパスが UPF ノードで可能になるようにします。



機能の仕組み

ここでは、この機能の仕組みを説明します。

SxDemuxMgr

UP/UPF の分散アーキテクチャでは、セッション（Sxa または N4）は異なる SessMgr インスタンスで実行されます。単一の SessMgr へのセッションの縮小またはコンバージをサポートするために、SessMgr インスタンスは確立時に両方のセッションによって選択されます。

SxDemux で、SessMgr インスタンスの選択に Sx Establishment 要求（Sxa または N4）を受信すると、リモート F-TEID から SessMgr インスタンスを検索するために解析され、対応するセッション（それぞれ N4 または Sxa）が確立されます。SessMgr インスタンスに組み込まれているトンネル識別子を含む F-TEID が抽出されます。

UPF は SxDemux で IMSI エントリも維持します。IMSI エントリには、現在のセッションがホストされている SessMgr ID の情報が含まれます。Sx Session Establishment 要求受信時に、コンバージドデータパス機能を有効にすると、SxDemux は最初に、F-TEID を使用して、SessMgr ID の検索を試行します。F-TEID が存在しない場合は、IMSI ルックアップが行われます。F-TEID と IMSI の両方が存在しない場合、SxDemux は Sxa/N4 レッグに対して同じ SessMgr ID を選択しません。

SessMgr

同じ SessMgr インスタンスに、Sxa と N4 の 2 つのセッションがあります。これらをコンバージするには、以下のロジックを使用してセッションを識別します。

- アップリンクパケットの場合：Egress FARs F-TEID は Ingress PDRs F-TEID と一致します。
- ダウンリンクパケットの場合：Ingress FAR の F-TEID が Egress PDR の F-TEID と一致するはずです。

F-TEID には、トンネル識別子とエンドポイント IP アドレスの両方が含まれます。セッションが識別されると、データパスで必要な情報を使用してコンバージドデータパスが構築されます。

データパス

SessMgr でセッションのコンバージェンスが発生すると、SessMgr は、Sxa セッション用にインストールされている高速パスから既存のベアラーストリーム（3 タプル）を削除します。これは、受信パケットに基づくフローレベルのストリーム（6 タプル）が分析される場合にのみ確立されます。

アップリンクパケットは、S-GW イングレス PDR エンドポイントごとに受信されます。ダウンリンクパケットは、S-GW イングレス FAR ベースの外部ヘッダーを使用して転送されます。

課金

UPF は、SMF レッグ（N4 レッグ）および S-GW の課金をサポートします。

コール フロー

この項では、コンバージドデータパス機能関連のコールフローについて説明します。

SGW-C/cnSGW と SMF/IWF との初期接続

次の図は、折りたたまれた UPF を使用した初期接続コールフローを示しています。

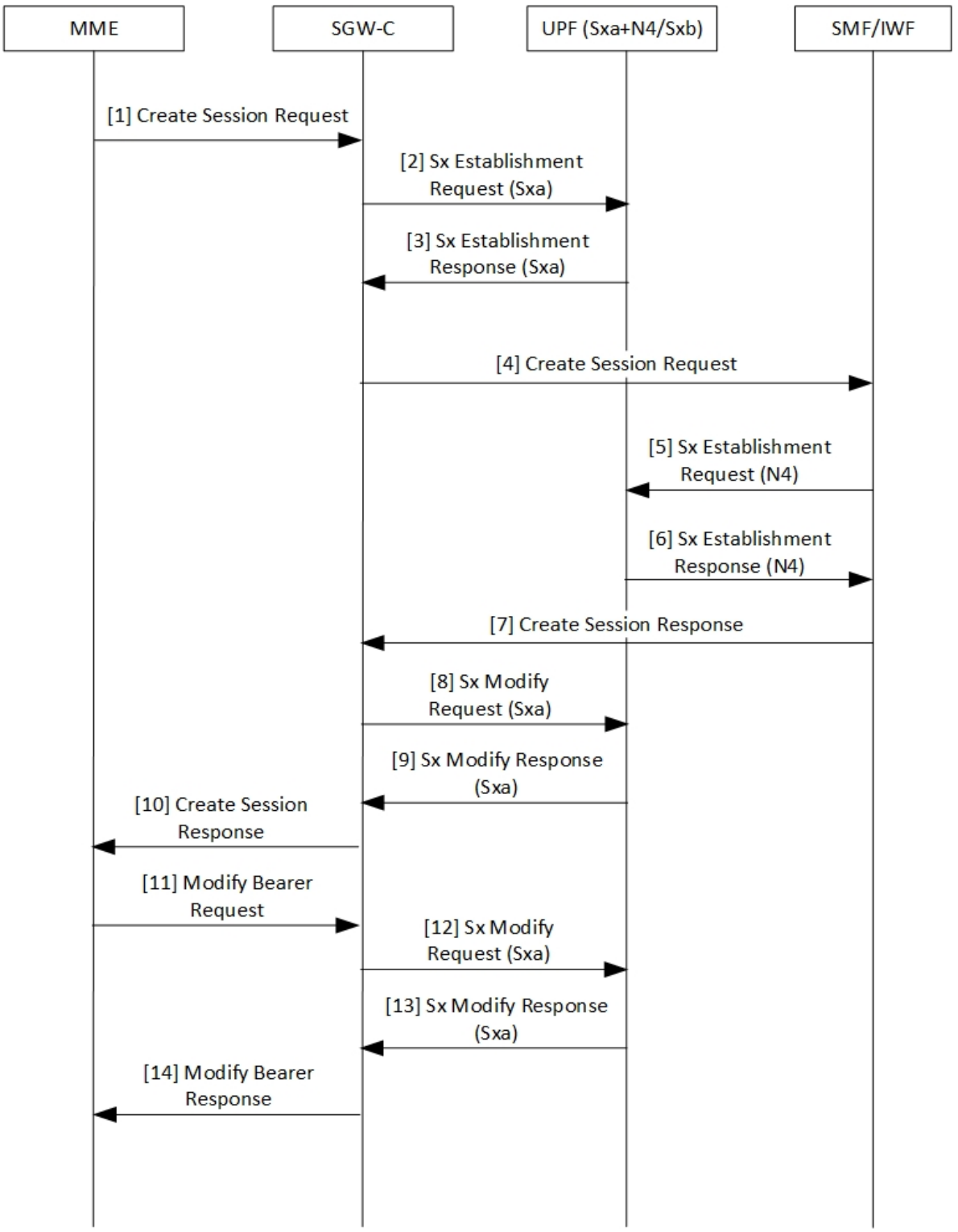

MME
SGW-C
UPF (Sxa+N4/Sxb)
SMF/IWF
[1] Create Session Request
[2] Sx Establishment Request (Sxa)
[3] Sx Establishment Response (Sxa)
[4] Create Session Request
[5] Sx Establishment Request (N4)
[6] Sx Establishment Response (N4)
[7] Create Session Response
[8] Sx Modify Request (Sxa)
[9] Sx Modify Response (Sxa)
[10] Create Session Response
[11] Modify Bearer Request
[12] Sx Modify Request (Sxa)
[13] Sx Modify Response (Sxa)
[14] Modify Bearer Response

表 *25 : SGW-C/cnSGW* と *SMF/IWF* との初期接続コールフローの説明

ステップ	説明
1	Create Session Request（CSReq）は、SGW-C/cnSGW が受信し、UPF を選択します。
2	SGW-C/cnSGW は、Sx Establishment Request（Sxa）を UPF に送信します。 UPF： • Sxa セッションを割り当てます。 • S-GW イングレスとエグレスローカル F-TEID を割り当てる
3	UPF は、Sx Establishment 応答（Sxa）を SGW-C/cnSGW に送り返します。
4	SGW-C/cnSGW は CSReq を SMF/IWF に送信します。 SMF/IWF は、SGW-C/cnSGW が選択した UPF と同じ UPF を選択します。
5	SMF/IWF は、Sx Establishment Request（Sxa）を UPF に送信します。
6	UPF は、Sx Establishment 応答（N4）を SMF/IWF に送信します。
7	SMF/IWF は、Create Session 応答を SGW-C/cnSGW に送信します。
8	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。 UPF は、エグレス FAR の一部として P-GW data F-TEID を更新します。 また、UPF は、内部ロジックを使用して Sxa と N4 セッションを相互接続し、すでに作成されているベアラーストリーム（3 タプル）を削除します。
9	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
10	SGW-C/cnSGW は、Create Session 応答を MME に送信します。
11	MME は、Modify Bearer 要求を SGW-C に 送信します。
12	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。 UPF は、イングレス FAR の一部として eNodeB F-TEID を更新します。
13	UPF は、Sx Modify 応答を SGW-C/cnSGW に送信します。
14	S-GW は、Modify Bearer 応答を MME に送信します。

Collapsed UPF を使用した 5G から 4G へのハンドオーバー

次の図は、Collapsed UPF による 5G から 4G へのハンドオーバーコールフローを示しています。

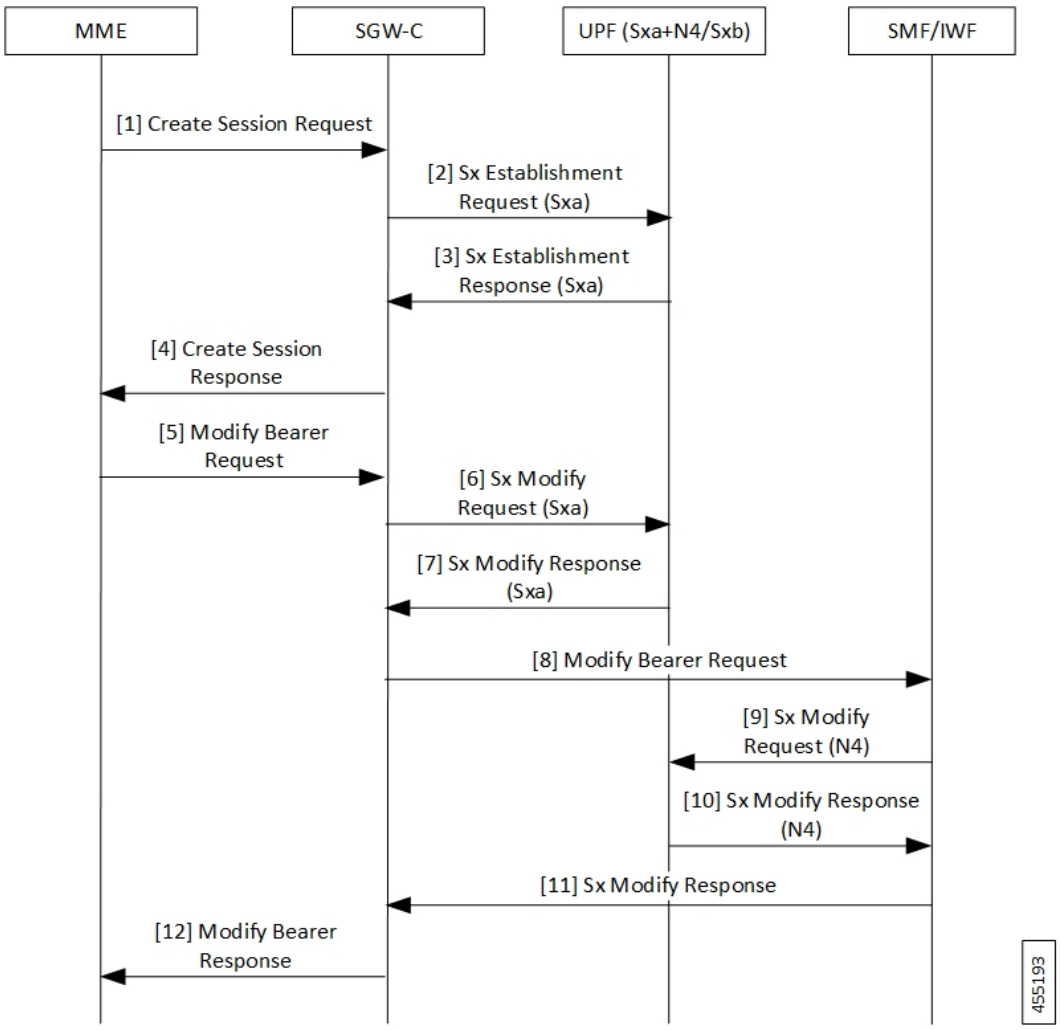


表 *26 : Collapsed UPF* による *5G* から *4G* へのハンドオーバーコールフローの説明

ステップ	説明
1	UE の初期接続の一部として、N4 セッションは SMF と UPF ですでに確立されています。 MME は、Create Session Request（CSReq）を SGW-C/cnSGW に送信します。ハンドオーバー要求の場合、SGW-C/cnSGW は、SMF が選択したものと同じ UPF を選択します。

ステップ	説明
2	SGW-C/cnSGW は、Sx Establishment Request（Sxa）を UPF に送信します。UPF で： • SxDemux は、FAR で受信した P-GW F-TEID から抽出された同じ SessMgr インスタンスを選択します。Sxa と N4 セッションの両方が同じ SessMgr 上にあります。 • Sxa セッションを割り当てます。 • S-GW イングレスとエグレスローカル F-TEID を割り当てる • 内部ロジックを使用して Sxa と N4 セッションをインターコネクトしますが、ベアラーストリーム（3 タプル）はインストールされません
3	UPF は、Sx Establishment 応答（Sxa）を SGW-C/cnSGW に送り返します。
4	SGW-C/cnSGW は、Create Session 応答を MME に送信します。
5	MME は、Modify Bearer 要求を SGW-C に 送信します。
6	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。 UPF は、ダウンリンクデータの eNodeB F-TEID を更新します。
7	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
8	SGW は、Modify Bearer 要求を SMF/IWF に送信します。
9	SMF/IWF は、Sx Modify Bearer 要求（N4）を UPF に送信します。UPF： • F-TEID を使用して S-GW への N4 session FAR を更新します • 新しい F-TEID を使用して VPP での TEP エントリを更新する
10	UPF は、Sx Modify 応答（N4）を SMF/IWF に送信します。
11	SMF/IWF は、Sx Modify 応答を SGW-C/cnSGW に送信します。
12	S-GW は、Modify Bearer 応答を MME に送信します。

Collapsed UPF を使用した S-GW 内ハンドオーバー

次の図は、Collapsed UPF による SGW 間ハンドオーバーコールフローを示しています。

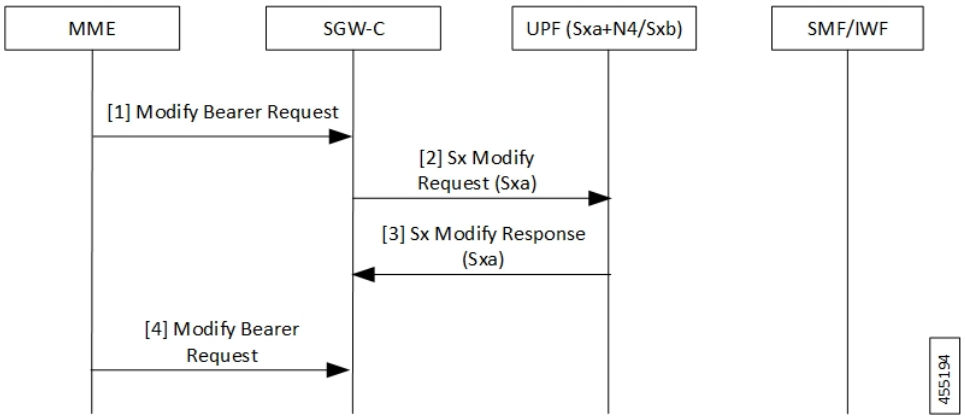


表 *27 : Collapsed UPF* による *SGW* 間ハンドオーバーコールフローの説明

ステップ	説明
1	UE の初期接続の一部として、N4 および Sxa セッションは SMF および UPF ですでに確立されています。UPF で、N4+Sxa セッションが存在し、相互接続されています。 MME は、Modify Bearer 要求を SGW-C に 送信します。 SGW-C/cnSGW は FAR で eNodeB F-TEID を更新します。
2	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。UPF： • ダウンリンクデータの eNodeB F-TEID を更新する • 新しい Remove TEID を使用して VPP で TEP エントリを更新する
3	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
4	S-GW は、Modify Bearer 応答を MME に送信します。

Collapsed UPF を使用したアイドル/アクティブ DDN の処理

次の図は、Collapsed UPF を使用したアイドル/アクティブ DDN の処理について説明しています。

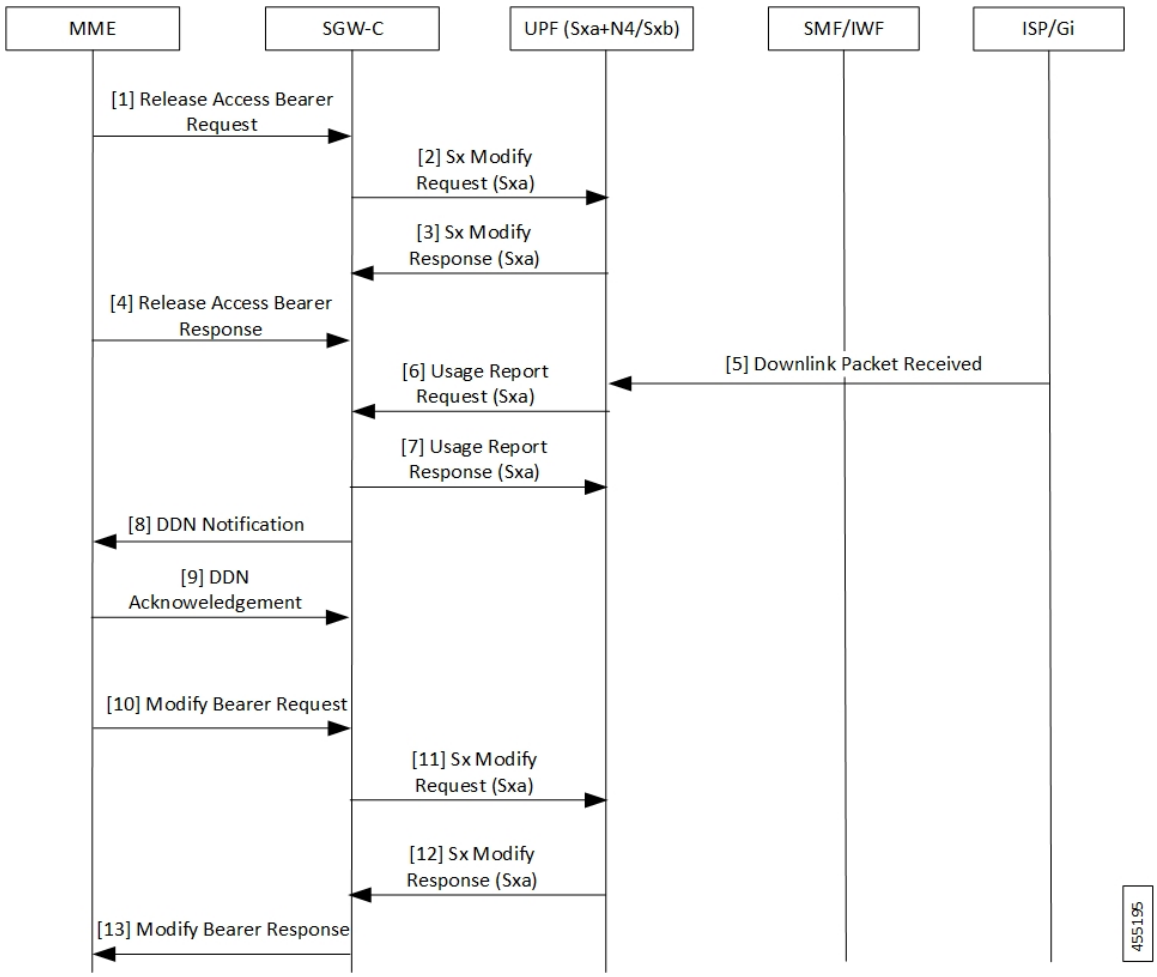


表 *28 : Collapsed UPF* を使用したアイドル/アクティブ *DDN* の処理のコールフロー説明

ステップ	説明
1	UE の初期接続の一部として、N4 および Sxa セッションは SMF および UPF ですでに確立されています。UPF で、N4+Sxa セッションが存在し、相互接続されています。MME では、UE はアクティブ状態からアイドル状態に移行します。 MME は、Release Access Bearer 要求を SGW-C/cnSGW に送信します。SGW-C/cnSGW は、パケットをバッファするように UPF に通知します。
2	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。UPF は、eNodeB に対する FAR アクションをバッファ状態に更新します。バッファリング用に 6 タプルフローがオンロードされます。
3	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
4	SGW-C は、Release Access Bearer 応答を SGW-C/cnSGW に送信します。

ステップ	説明
5	ISP/Gi は、受信したダウンリンクパケットを UPF に送信します。N4 セッションで UPF が受信したパケットは、バッファリングのためにインターコネクト Sxa セッションに渡されます。
6	UPF は、Usage Report Request（Sxa）を SGW-C/cnSGW に送信します。
7	SGW-C/cnSGW は、Usage Report Respons（Sxa）を UPF に送信します。
8	SGW-C/cnSGW は、DDN 通知を MME に送信します。
9	MME は、DDN Acknowledgment を SGW-C/cnSGW に返送します。
10	MME では、UE はアイドル状態からアクティブ状態に移行します。MME は、Modify Bearer 要求を SGW-C に 送信します。SGW-C/cnSGW： • FAR で eNodeB F-TEID を更新する • FAR アクションを Forward に更新する
11	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。UPF： • ダウンリンクデータの eNodeB F-TEID を更新する • 新しい Remove TEID を使用して VPP で TEP エントリを更新する • 各 6 タプルストリームを見つけて、バッファリングされたパケットを解放します
12	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
13	S-GW は、Modify Bearer 応答を MME に送信します。

S1 ハンドオーバー中の IDFT 処理

次の図は、Collapsed UPF を使用した S1 ハンドオーバー中の IDFT の処理を示しています。

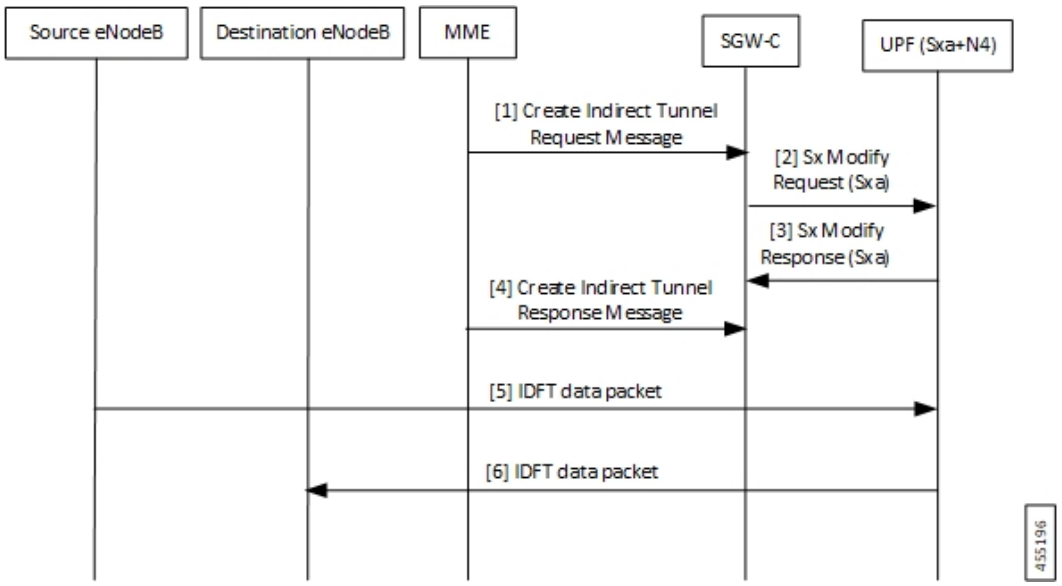


表 *29 : S1* ハンドオーバー中の *IDFT* 処理コールフローの説明

ステップ	説明
1	初期接続の一部として、N4 および Sxa セッションは SMF および UPF ですでに確立されています。S1 ハンドオフがトリガーされます。 MME は、Indirect Tunnel 要求メッセージを SGW-C/cnSGW に送信します。
2	SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。UPF で： • IDFT PDR が SessMgr で検出される • 新しい F-TEID が IDFT トンネルに割り当てられる • コンバージドデータパスが不要で、Slowpath 経由で通信される
3	UPF は、Sx Modify 応答（Sxa）を SGW-C/cnSGW に送信します。
4	SGW-C/cnSGW は、Create Indirect Tunnel 応答をMME に送信します。
5	送信元 eNodeB は、IDFT データパケットを UPF に送信します。UPF で一致する 3 タプルストリームがない場合、パケットは SessMgr に転送されます。
6	UPF は、IDFT データパケットを、接続先 eNodeB に送信します。

同じ SGW-U を使用した S-GW の再配置

次の図は、接続先 S-GW が同じ UPF を選択する S-GW 再配置を示しています。

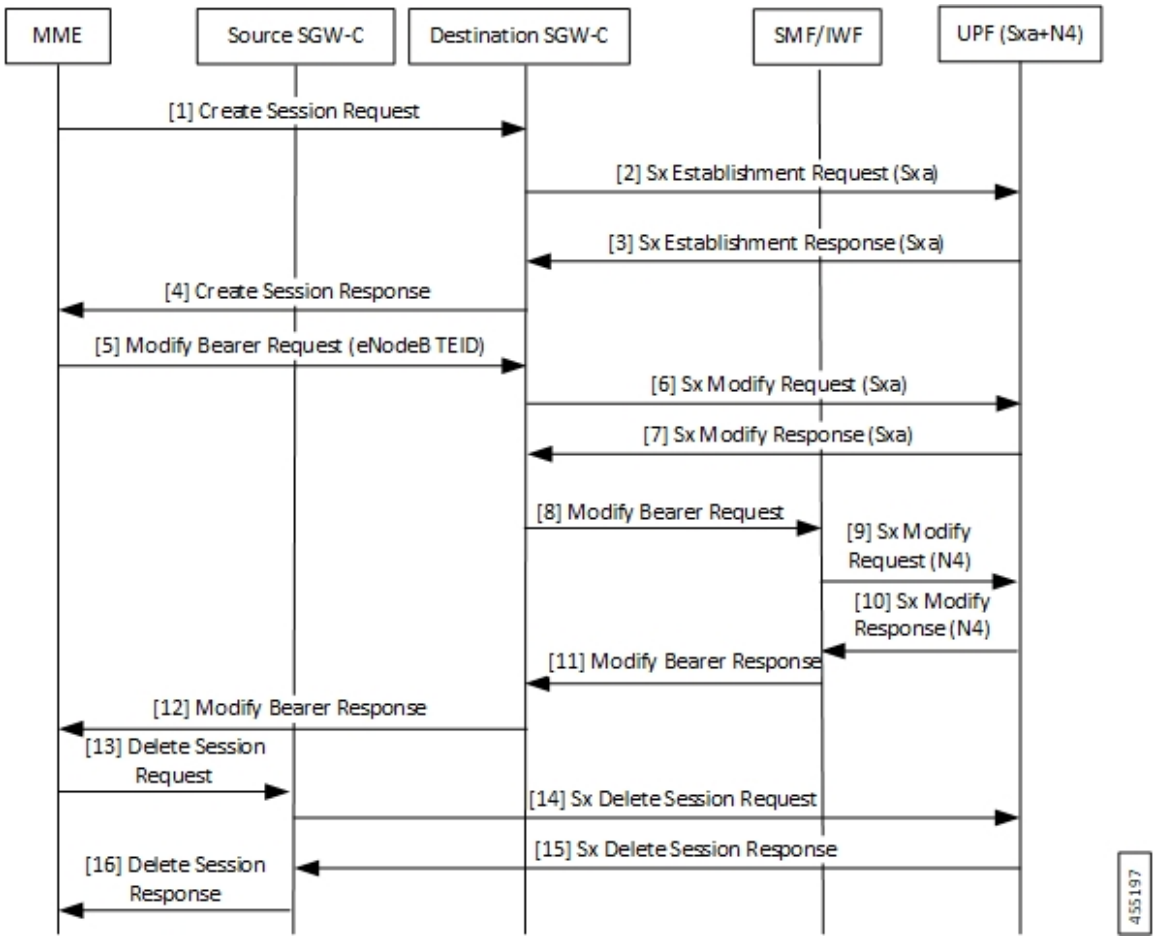


表 *30* : 同じ *SGW-U* が設定された *SGW* 再配置コールフローの説明

ステップ	説明
1	初期接続の一部として、N4 および Sxa セッションは、送信元 SGW-C/cnSGW、SMF/IWF および UPF ですでに確立されています。 MME は、Create Session 要求を接続先 SGW-C/cnSGW に送信します。
2	接続先 SGW-C/cnSGW は、Sx Establishment 要求（Sxa）を UPF に送信します。UPF は、アップリンクパケット（Slowpath）に関する新しい Sxa セッションを N4 セッションにリンクします。
3	UPF は、Sx Establishment 応答（Sxa）を 接続先 SGW-C/cnSGW に送信します。
4	接続先 SGW-C/cnSGW は、Create Session Response を MME に送信します。
5	MME は、Modify Bearer Request（eNodeB F-TEID）を接続先 SGW-C/cnSGW に送信します。
6	接続先 SGW-C/cnSGW は、Sx Modify 要求（Sxa）を UPF に送信します。
7	UPF は、Sx Modify 応答（Sxa）を 接続先 SGW-C/cnSGW に送信します。

ステップ	説明
8	接続先 SGW-C/cnSGW は、Modify Bearer 要求を SMF/IWF に送信します。
9	SMF/IWF は、Sx Modify 要求（N4）を UPF に送信します。UPF はダウンリンクトンネルを切り替え、N4 セッションを新しい Sxa セッションにリンクします。
10	UPF は、Sx Modify 応答（N4）を SMF/IWF に送信します。
11	SMF/IWF は、Modify Bearer 応答を接続先 SGW-C/cnSGW に送信します。
12	接続先 SGW-C/cnSGW は、Modify Bearer 応答を MME に送信します。
13	MME は、Delete Session 要求を 送信元 SGW-C/cnSGW に送信します。
14	送信元 SGW-C/cnSGW は、Sx Delete Session 要求を UPF に送信します。
15	UPF は、Sx Delete Session 応答を送信元 SGW-C/cnSGW に送信します。
16	送信元 SGW-C/cnSGW は、Delete Session 要求を MME に送信します。

Wi-Fi から LTE へのハンドオーバー

ここでは、Wi-Fi から LTE へのハンドオーバー コール フローについて説明します。

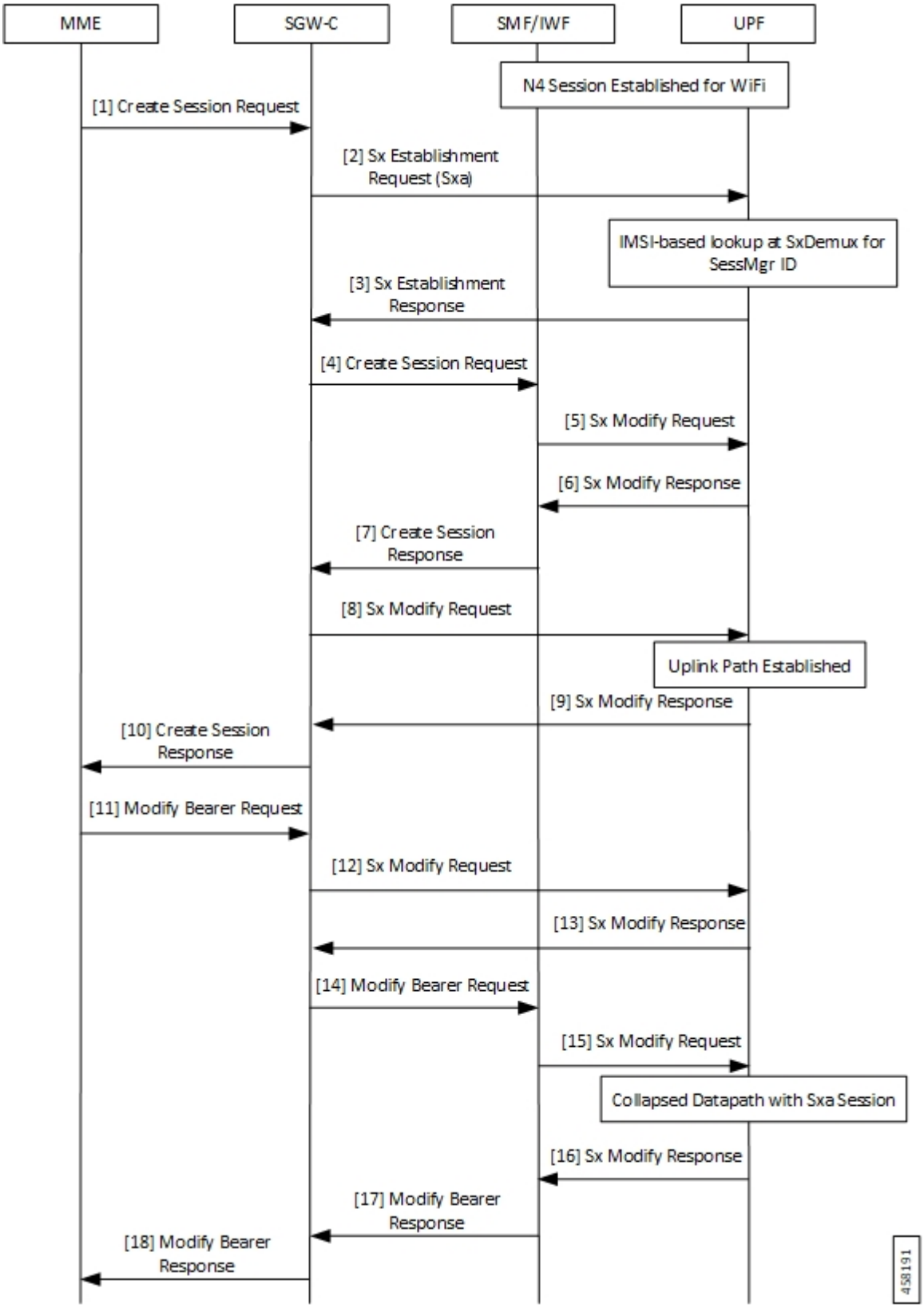

MME
SGW-C
SMF/IWF
UPF
N4 Session Established for WiFi
[1] Create Session Request
[2] Sx Establishment Request (Sxa)
IMSI-based lookup at SxDemux for SessMgr ID
[3] Sx Establishment Response
[4] Create Session Request
[5] Sx Modify Request
[6] Sx Modify Response
[7] Create Session Response
[8] Sx Modify Request
Uplink Path Established
[9] Sx Modify Response
[10] Create Session Response
[11] Modify Bearer Request
[12] Sx Modify Request
[13] Sx Modify Response
[14] Modify Bearer Request
[15] Sx Modify Request
Collapsed Datapath with Sxa Session
[16] Sx Modify Response
[17] Modify Bearer Response
[18] Modify Bearer Response
458191

表 *31 : Wi-Fi* から *LTE* へのハンドオーバー コール フローの説明

ステップ	説明
1	SMF/IWF と UPF 間の Wi-Fi に対して N4 セッションが確立されます。 MME は、Create Session 要求を（4G に移動）SGW-C/cnSGW に送信します。
2	SGW-C/cnSGW は、Sx Session Establishment 要求（F-TEID なし）を UPF に送信します。
3	IMSI ベースのルックアップは、SessMgr ID の SxDemux で行われます。 UPF は、Sx Establishment 要求を SGW-C/cnSGW に送信します。
4	SGW-C/cnSGW は、Create Session 要求を SMF/IWF に送信します。
5	SMF/IWF は、新しい Uplink RB PDR を使用して Sx Modify 要求を UPF に送信します。
6	UPF は、Uplink データの新しい TEID を使用して Sx Modify を SMF/IWF TEID に送信します。
7	SMF/IWF は、Create Session 応答を SGW-C/cnSGW に送信します。
8	SGW-C/cnSGW は、更新された Uplink FAR を使用して Sx Modify 要求を UPF に送信します。
9	アップリンクパスが確立されます。 UPF は、Sx Modify 応答を SGW-C/cnSGW に送信します。
10	SGW-C/cnSGW は、Create Session 応答を MME に送信します。
11	MME は、Modify Bearer 要求を SGW-C に 送信します。
12	SGW-C/cnSGW は、eNodeB TEID を使用して Sx Modify 要求を UPF に送信します。
13	UPF は、Sx Modify 応答を SGW-C/cnSGW に送り返します。
14	SGW は、Modify Bearer 要求を SMF/IWF に送信します。
15	SMF/IWF は、tunnel switch Sx Modify 要求を UPF に送信します。
16	Sxa セッションとの Collapsed データパスが UPF で確立されます。 UPF は、Sx Modify 応答を SMF/IWF に送信します。
17	SMF/IWF は、Modify Bearer 応答を SGW-C/cnSGW に送信します。
18	S-GW は、Modify Bearer 応答を MME に送信します。

制限事項

この機能には次の既知の制限事項があります。

- Sxa レッグが 1 つのユーザープレーンサービスに属し、N4 レッグが別のユーザープレーンサービスに属している場合、データパスは折りたたまれません。
- Sxa レッグが 1 つのコンテキストの下にあり、N4 レッグが別のコンテキストにある場合、データパスを折りたたむことはできません。
- **show subscribers user-plane-only full all** CLI 出力の S-GW 部分には、ToS マーク付きのアップリンクおよびダウンリンクパケットは表示されません。
- **show user-plane-service statistics rat all** CLI 出力の S-GW 部分では、Unknown のセッション統計が増分されますが、データ統計は RAT-type Unknown で増分されません。
- S-GW の合法的傍受は、サポートされていません。
- S-GW ベアラの非アクティブタイムアウトは適用されません。これは、S-GW URR によって決定されるものであり、Collapsed Datapath ではその処理が行われないためです。
- コールの S-GW レッグは、ローカルでコンバージドセッションをパージし、UPF は、引き続き eNodeB にデータを送信します。

コンバージドコールに課金する

表 *32 :* 機能の履歴

機能名	リリース情報	説明
コンバージド コールの課金サポート	2024.02.0	UPF は、コンバージドコールの S-GW 課金データレコード（CDR）ボリュームレポートをサポートしています。この機能により、インバウンド LBO ローミングシナリオで、これらの CDR をレポートや課金に使用できます。 この機能により、ACS サービス構成に新しい CLI コマンド **converged-sxa-usage-reporting** が導入され、ボリューム数が記載された使用レポートを生成できます。 **デフォルト設定**：無効：有効にするには設定が必要。

機能説明

コンバージドコールの場合、SGW-U は、SGW-C が、それに基づいて CDR を生成する使用状況レポートを SGW-C に送信します。この機能は、**converged-sxa-usage-reporting** CLI コマンドを使用して有効にできます。有効にすると、SGW-U は、ボリュームアカウンティングを含む使用状況レポートを SGW-C に送信し、それに基づいて SGW-C が CDR を生成します。

機能の仕組み

SGW-Uがボリュームレポートを更新する場合、URR リンクはSGW-Uベアラー URR と PGW-U、UPF ベアラー、または SDF レベルの URR の間で発生します。UPF での課金の調整中に、Sxa での課金の調整も同時に行われます。しきい値トリガーに応じて、SGW-U は使用状況レポートを生成します。しきい値トリガーの例として、時間しきい値、ボリュームしきい値、クエリ URR などが挙げられます。その後 SGW-U は、使用状況レポートを SGW-C に送信し、それに基づいて、SGW-C が CDR を生成します。

コンバージドコール向けのPGW-UまたはUPF URR と一緒にSGW-Uベアラー URR のボリュームカウントを更新するには、次のプロセスを発生させます。

- SGW-U のデフォルトのベアラー URR の参照ポインタは、PGW-U または UPF のデフォルトのベアラー URR に保存されます。
- SGW-U 専用ベアラーの URR の参照ポインタは、PGW-U または UPF の対応する専用ベアラーの SDF レベルの URR に保存されます。

LC 数の調整中に、PGW-U または UPF と SGW-U ベアラーの URR が通過されます。次に、両方のコール ID URR のボリュームカウントが更新されます。

（注）

- コールがコンバージドコールとして確立される場合、SGW-Uベアラー URR の参照ポインタは、コールコンバージェンス中に PGW-U、UPF ベアラー、または SDF レベルの URR に保存されます。
- 非コンバージドコールからコンバージドコールに S-GW を再配置する場合、URR のリンクが発生します。URR リンクは、SGW-Uベアラー URR の参照ポインタが、PGW-U、UPF ベアラー、または SDF レベルの URR に保存されることを意味します。
- コンバージドコールから非コンバージドコールに S-GW を再配置する場合、URR のリンク解除が発生します。URR のリンク解除は、SGW-U ベアラー URR の参照ポインタが、PGW-U、UPF ベアラー、または SDF レベルの URR から削除されることを意味します。
- リカバリの場合、リンクの再作成が発生します。これは、一貫した動作を維持するために、リカバリ中に SGW-U URR の参照ポインタが PGW-U または UPF URR に保存されることを意味します。

制限事項

コンバージドコールの課金機能には、次の制限があります。

- S-GW URR のボリュームレポートは、対応する PGW-U または UPF の URR の使用数に基づいています。たとえば、P-GW 処理が原因でドロップされたアップリンクパケットは、Sxa コールでは考慮されません。
- RA または RS パケットの課金は UPF では発生しません。Sxa 使用状況レポートは UPF に依存するため、RA または RS パケットは Sxa コールの課金対象にはなりません。
- 同じ URR ID を使用する複数のベアラーは、Sxa として生成される使用状況レポートに不整合が生じます。
- コンバージドコールの場合、パケットが N4 レッグで課金されない場合、これらのパケットは Sxa でも課金されません。
- 専用ベアラーで事前定義されたルールに対する課金は、コンバージドコールではサポートされません。
- コールがコンバージされると、既存のコールの接続時間まで、この機能の設定は有効または無効のままです。構成の変更は、新しいコール以降に適用されます。この機能が有効になっている場合、既存の URR と新しい URR に対して課金が継続されます。ただし、この機能が無効になっている場合、既存および新しい URR に対して課金は行われません。

eGCDR を構成する

PGW-U または UPF でデフォルトベアラー URR を作成するには、PGW-U または UPF に eGCDR 構成が必要です。

以下に設定サンプルを示します。

```
config
   active-charging service ACS
       rulebase starent
           billing-records egcdr
   end
```

GTPP グループの構成

PGW-U または UPF でデフォルトベアラー URR を作成するには、PGW-U または UPF に GTPP グループ構成が必要です。

以下に設定サンプルを示します。

```
config
   context ISP
      apn intershat
          gtpp group my_grp
   end
```

コンバージド Sxa コールのボリュームカウントを含む使用状況レポートの生成します

Sxa コールのボリュームカウントを含む使用状況レポートを生成するには、次の構成例を使用します。

```
config
  active-charging service service_name
    converged-sxa-usage-reporting
      end
```

注：

- **converged-sxa-usage-reporting**：統合 SxA コールの使用状況レポートの生成を有効にします。この機能を無効にするには、**no converged-sxa-usage-reporting** シンタックスを追加します。デフォルト値は **no converged-sxa-usage-reporting** です。

設定例

次に、統合 Sxa コールの使用状況レポート生成の構成例を示します。

```
config
  active-charging service ACS
     converged-sxa-usage-reporting
  end
```

コンバージドデータパスを構成する

この項では、この機能をサポートするために使用可能な CLI コマンドについて説明します。

UPF でコンバージドデータパスを有効にする

次の構成を使用して、UPF でコンバージドデータパスを有効にします。

```
configure
  user-plane converged-mode
  end
```

注：

- **user-plane**：構成に関連する UPF を指定します。
- **converged-mode**：Sxa コールおよび N4 コールの Collapse データパスを指定します。
- デフォルトでは、CLI は無効になっています。
- 起動設定に CLI を追加することをお勧めします。

Sxa および N4 にリモートピアを構成する

次の CLI コマンドを使用して、Sxa および N4 インターフェイスのリモートピアを構成します。

```
configure
  control-plane-group group_name
    peer-node-id ipv4-address ipv4_address interface n4
    peer-node-id ipv4-address ipv4_address
    end
```

Sxa および N4 にユーザープレーンサービスを構成する

次のコマンドを使用して、Sxa および N4 インターフェイスに対して UP サービスを構成します。

```
configure
  user-plane-service service_name
    associate gtpu-service gtpu_service upf-ingress
    associate gtpu-service gtpu_service sgw-ingress
    associate gtpu-service gtpu_service sgw-egress
    associate gtpu-service gtpu_service cp-tunnel
    associate sx-service sx_service
    associate control-plane-group group_service
    end
```

モニタリングおよびトラブルシューティング

show コマンドと出力

この項では、コンバージドデータパス機能をサポートするために利用可能な show CLI コマンドおよび出力について説明します。

show subscribers user-plane-only all

この CLI コマンドの出力が強化され、セッションがコンバージドされているかされていないかを示す次のフィールドが表示されるようになりました。

- コンバージド
- 非コンバージド

show subscribers user-plane-only full all

この CLI コマンドの出力が強化され、以下のフィールドが表示されるようになりました。

- コンバージドセッション
- コンバージドピアコール ID

show user-plane-service statistics all

この CLI コマンドの出力が強化され、以下のフィールドが表示されるようになりました。

- コンバージド データ セッション PDN：
  - アクティブ
  - 設定
  - リリース日



第 13 章

ディープ パケット インスペクションとインラインサービス

- 機能の概要と変更履歴, on page 133
- 機能説明, on page 134
- 機能の仕組み （136 ページ）
- サポートされるインラインサービス （140 ページ）
- 静的ルールと事前定義済みルールを構成する, on page 194
- DPI 向け L7 プロトコルの ACS Ruledef を構成する （195 ページ）
- DPI 向け L7 プロトコルの課金アクションの構成 （197 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
• N4 インターフェイスの NAT サポートが追加されました。 • TCP アイドルタイムアウトのサブスクライバ ファイアウォールのサポートが追加されました。 • 2 つの新しい属性を使用してデータストールの問題をキャプチャするためのサポートが追加されました。	2023.04.0
次の機能に対してサポートが追加されました。 • IP 再アドレス指定 • RTP ダイナミックフローの検出 • ベアラー固有フィルタのルール照合 • QUIC IETF の導入	2021.02.0
ディープ パケット インスペクション（DPI）んお一部として、新しい L7 プロトコルが導入されました。	2021.01.0
TCP 用に次の EDR 属性が追加されました。 • SYN および SYN-ACK パケット • SYN-ACK および ACK パケット	2021.01.0
EDR に新しい DNS 属性が導入されました。	2021.01.0
最初の導入。	2020.02.0

機能説明

Cisco 5G-UPF の主要な製品機能の 1 つとして、統合されたディープ パケット インスペクション（DPI）ベースのサービスが挙げられます。DPI は、Uniform Resource Identifier（URI）情報を含むレイヤ 7（L7）の検査です。場合によっては、トリガー条件を識別するレイヤ 3（L3）およびレイヤ 4（L4）アナライザは、課金目的では不十分であるため、レイヤ 7（L7）検査が使用されます。

DPI は、L4 検査よりも後のパケットインスペクションを実行し、通常、L7 で URI 情報（DNS、HTTP、HTTPS、RTP、RTSP URL など）を検出するためにデプロイされます。

DNS サーバーアドレス再指定

不正な DNS サーバーを使用する場合は常に、要求を変更して DNS IP のアドレスを再指定し、許可されたサーバーを使用することができます。ruledef は、パケットが DNS クエリに属するかどうかを判別します。また、DNS クエリが一連の許可 DNS サーバーに属しているかどうかも判別します。DNS クエリが許可された DNS サーバーに属していない場合、フローアクションは、アドレス再指定サーバーリストから DNS サーバーを取得します。

active-charging サービスで **readdress-server-list** コマンドを構成できます。フローが、**ruledef** と一致すると、フローアクションを構成して、**readdress-server-list** からサーバーを使用できます。

次の構成を使用して、active-charging サービスでアドレス再指定サーバーリストを構成します。

```
configure
  active-charging service service_name
    readdress-server-list name_of_list
      server ipv4_address [ port ]
      server ipv6_address [ port ]
```



（注） アドレス再指定サーバーリストには、最大 10 のサーバーを構成でき、active-charging サービスには、最大 10 のアドレス再指定サーバーリストを構成できます。同じ **readdress-server-list** 内に、IPv4 アドレスと IPv6 アドレスの両方を設定できます。

次のいずれかのメソッドを使用して、リストから **readdress-server-list** を選択します。

- ラウンドロビン：新しいフローごとにラウンドロビン方式でサーバーが選択されます。選択時に、リスト内の非アクティブサーバーは考慮されません。

  このメソッドが、デフォルトの選択です。

- 階層型：このアプローチでは、サーバーは **readdress-server-list** で定義されている順序に応じて、プライマリ、セカンダリ、ターシャリというようにタグ付けされます。すべてのフローのアドレス再指定先は、プライマリサーバーが使用可能である限り、プライマリサーバーです。プライマリサーバーがダウンした場合は、フローのアドレス再指定先はセカンダリサーバーとなり、その後も同じロジックが繰り返されます。プライマリサーバーが再びアクティブになると、フローのアドレス再指定先はプライマリサーバーに戻ります。

DNS アドレス再指定サーバーリストを設定するには、active-charging サービスで次の CLI 構成を使用します。

```
configure
  active-charging service service_name
    readdress-server-list name_of_list
      server ipv4_address [ port ]
      server ipv6_address [ port ]
      consecutive-failures integer_value
      response-timeout integer_value
```

```
reactivation-time integer_value

charging-action action_name
  flow action readdress server-list name_of_list
  exit
```

注：

- **consecutive-failures**：1 ～ 10 の整数を指定します。デフォルト値は *5* です。
- **response-timeout**：1 ～ 10000 ミリ秒の整数を指定します。デフォルト値は *1000* です。
- **reactivation-time**：1 ～ 1800 秒の整数を指定します。デフォルト値は *300* です。

アドレス再指定先サーバーの状態

この項では、アドレス再指定サーバーの状態について説明します。

- アクティブ状態：一度設定すると、すべてのサーバーが [Active] としてマークされます。
- 非アクティブ状態：アドレス再指定先サーバーからの応答が受信されない場合、サーバーは [Inactive] としてマークされます。
- アクティブ保留状態：サーバーが [Active-Pending] 状態になると、アドレス再指定要求を受け付け可能となります。この状態の場合、リクエストがこのサーバーにアドレス再指定されると、レスポンスが返り、サーバー状態が、[アクティブ（Active）] に変わります。それ以外の場合は、[Inactive] 状態に戻ります。

機能の仕組み

この項では、以下の DPI の機能について説明します。

- ダウンリンクおよびアップリンクパケットの DSCP マーキング。
- 通信のアドレス再指定またはリダイレクト

ダウンリンクおよびアップリンクパケットの DSCP マーキング

トランスポートレベルのマーキングは、Differentiated Services Code Point（DSCP; DiffServ コードポイント）値を使用して UPF で通信をマーキングするプロセスです。QoS フローごとに実行されるトランスポートレベルのマーキングは、5QI からのマッピングと、SMF からのオプションの割り当ておよび保持ポリシー（ARP）構成に基づいています。

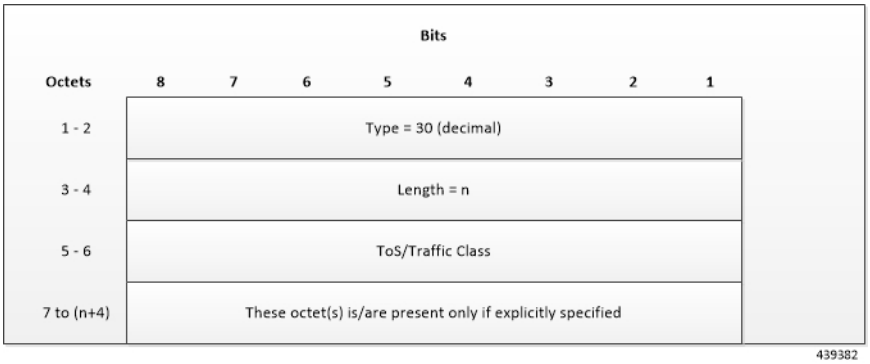
SMF は、マークされる通信と一致する PDR に関連付けられている FAR の Transport Level Marking IE の ToS（IPv4）または Traffic Class（IPv6）の DSCP を指定することで、通信レベルのマーキングを制御します。UPF は、検出された通信に対して、トランスポートレベルのマーキングを実行し、マークされたパケットをピアエンティティに送信します。SMF は、関連する FAR の Transport Level Marking IE を変更して、トランスポートレベルのマーキングを変更できます。

UPF は次の IE をサポートしています。

- Inner Packet Marking IE：内部パケットマーキングのトンネルパケットをマークします。
- Transport Level Marking Options IE：内部パケットから外部 IP パケットに DSCP をコピーします。

Transport Level Marking IE

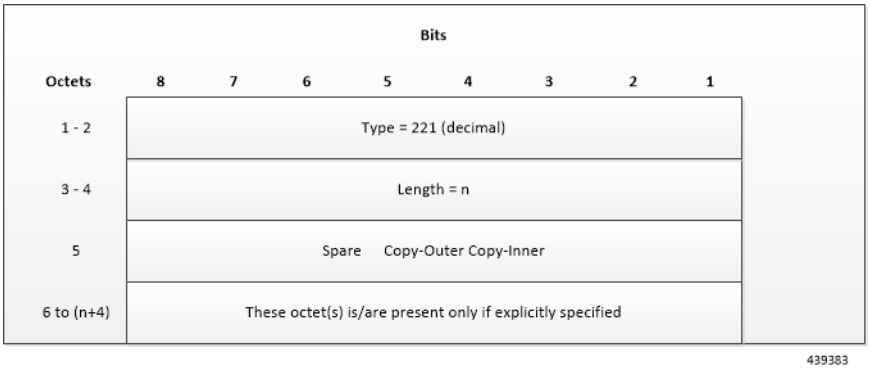
「Transport Level Marking」 IE のタイプは、以下の図に示すようにエンコードされています。これは、downlink transport-level marking の DSCP 値を示しています。



Type-of-Service（ToS）または Traffic Class のエンコーディングは、OctetString として 2 つのオクテット形式で実行されます。最初のオクテットには、[IPv4 Type-of-Service] フィールドまたは [IPv6 Traffic-Class] フィールドの DSCP 値が含まれ、2 番目のオクテットには、*0xFC*に設定されてる [ToS/Traffic Class] マスクフィールドが含まれます。

Transport Level Marking Options IE

「Transport Level Marking Options」 IE のタイプは、以下の図に示すようにエンコードされています。ダウンリンクトランスポート レベル マーキングの DSCP は、内部パケットからコピーされます。

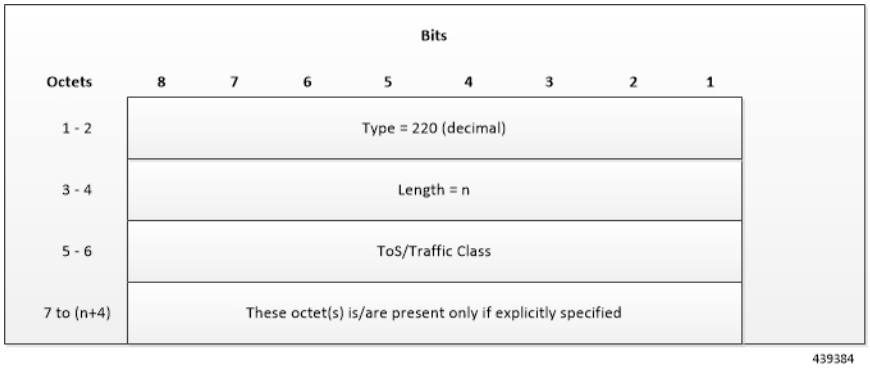


Copy-Inner および Copy-Outer フラグは、オクテット 5 のビット 0 とビット 1 に存在します。ISP から受信するパケットには外部ヘッダーが存在しないため、ダウンリンクパケットには

Copy-Outer フラグが使用されません。Copy-Inner フラグが存在する場合、UPF は内部パケットの DSCP 値を使用してトランスポートレベルの IP ヘッダーをマークします。

Inner Packet Marking IE

次の図に示すように、「Inner Packet Marking」IE タイプがエンコードされます。ダウンリンクの Inner Packet Marking の DSCP 値を示します。



ToS/通信クラスのエンコーディングは、OctetString として 2 つのオクテットの形式で実行されます。最初のオクテットには IPv4 ToS または IPv6 Traffic Class フィールドの DSCP 値が含まれ、2 番目のオクテットには ToS/Traffic Class マスクフィールドが含まれます。このフィールドは、*0xFC* に設定されています。

注：

- ユーザープレーンパケットの IP ヘッダー内の元の ECN ビットは、Transport Level Marking または Inner Packet Marking の適用後は変更されません。
- 「Transport Level Marking」IE、「Inner Packet Marking」IE または両方の IE が、アップリンク FAR に関連付けられている場合、次のリリースがアップリンクパケットマーキングに適用されます。
  - 「Transport Level Marking」IE または「Inner Packet Marking」IE が存在する場合、その DSCP 値が使用されます。
  - 「Transport Level Marking」IE および「Inner Packet Marking」IE の両方が存在する場合、アップリンクパケットマーキングには、「Transport Level Marking」IEからの値が使用されます。

通信のアドレス再指定またはリダイレクト

通信リダイレクトは、アップリンクアプリケーション通信をリダイレクト接続先にリダイレクトするプロセスです。たとえば、一部の HTTP フローをサービス プロビジョニング ページにリダイレクトします。リダイレクト接続接続先は、PCF によって提供されるか、SMF または UPF で事前設定済みです。

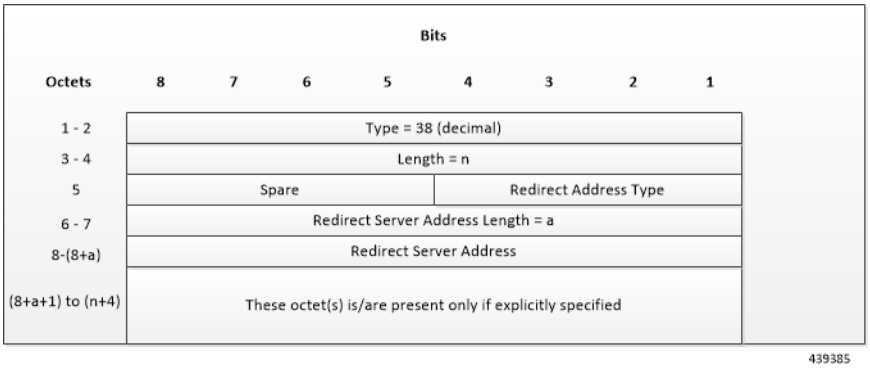
通信リダイレクトの適用は、SMF または UPF がサポートする通信が、通信リダイレクトの対象となる場合、UPF で適用されます。UPF は、「UP-Function Features」IE 経由で UPF での通信リダイレクトの適用をサポートしているかどうかを SMF に報告します。

UPF で通信リダイレクトを適用するために、SMF は次のアクションを実行します。

- 通信リダイレクトを表すために必要な PDR が存在しない場合は、作成します。
- 次を使用して FAR を作成します。
  - リダイレクト接続先を含む「Redirect Information」IE（通信が SMF によって提供されるリダイレクト接続先へのリダイレクトが必要な場合）。SMF からのリダイレクト接続先は、UPF で事前設定済みのリダイレクト接続先よりも優先されます。
    - HTTP 通信リダイレクトの場合、リダイレクトアドレスタイプは「URL」に設定され、SMF は FAR の「Destination Interface」IE を（リダイレクトを示す状態コードとともに HTTP 応答メッセージを転送する）「Access」に設定します。他のタイプの通信リダイレクトの場合、FAR の「Destination Interface」IE は「Core」に設定されます。
- FAR を PFCP セッションの上記の PDR に関連付けます。

Redirect Information IE

リダイレクト情報は、次のようにエンコードされます。



リダイレクトアドレスのタイプを示す「Redirect Address Type」：

Redirect Address Type	値（10 進数）
IPv4 アドレス	0
IPv6 アドレス	1
URL	2
SIP URI	3
スペア（将来使用向け）。	4 ～ 15

「リダイレクトサーバーアドレス長」は、「リダイレクトサーバーアドレス」の長さを示します。「リダイレクトサーバーアドレス」は、UTF8Stringフォーマットでエンコードされており、エンドユーザーと接続するリダイレクトサーバー（例：HTTPリダイレクトサーバー、SIPサーバー）のアドレスが含まれます。

Important このリリースでは、FARがクォータ期限切れのURRと関連付けられている場合に、ダイナミックルールに対して、リダイレクトアドレスタイプURLがサポートされます。

サポートされるインラインサービス

アプリケーション検出および制御

ADCインラインサービスは、通信を分析することでピアツーピアプロトコルを検出するために使用されます。ソーシャルネットワーキングやゲームミングアプリケーションなど、大量のインターネット通信を生成するその他の一般的なアプリケーションも検出できます。

ADCと呼ばれるインライン サービスは、「P2P」とも呼ばれます。ピアツーピア（P2P）とは、2つのわずかに異なるコンテキストで使用される用語です。機能レベルでは、クライアント/サーバー方式とは対照的に、ピアリング方式で対話するプロトコルを意味します。ノードの機能の間に明確な区別はありません。どのノードもクライアント、サーバー、またはその両方として機能できます。プロトコルはこの2つを明確に区別しない場合があります。たとえば、ピアリング交換には、クライアントとサーバーの機能や情報の送受信が同時に含まれることがあります。

（注） ADCのサポートは、ライセンスが必要な機能です。ライセンスの入手方法の詳細については、シスコのアカウントまたはサポート担当者にお問い合わせください。

QUIC IETFの導入

現在のフレームワークでは、プラグイン到達時に、フロー内のすべてのパケットに対してディープパケットインスペクション（DPI）が実行されます。DPIは、パケットを分析し、確定的なパターンを抽出することによって実行されます。DPIは順番に実行され、アプリケーションの検出とそのサブタイプの分類を行います。プラグインは、DPI後のフローを除外します。フローは検出後にオフロードされます。QUIC IETFの一部として、初回のQUICハンドシェイクパケット（Client Hello/Server Hello）はネットワーク上で暗号化されます。したがって、アプリケーションの検出に使用できる確定的なパターンはありません。p2pプラグインによる、検出用SNI（Server Name Indication）の復号と取得が新たにサポートされるようになりました。

QUIC IETF の設定

QUIC IETF 復号を有効または無効にするには、次の設定を使用します。

```
configure
  active-charging service acs_service_name
    p2p-detection debug-param protocol-param p2p_quic_ietf_decrypt 1
    end
```

（注）
- デフォルトでは、CLI は無効になっており、TLS 復号によるパフォーマンスへの影響は最小限です。
- ランタイム変更の構成は、既存のフローに影響しません。変更は、新しいフローにのみ適用されます。

統計情報

show user-plane-service statistics analyzer name p2p

この show CLI コマンドを使用して、QUIC とアプリケーションに関して分析するパケットを判断します。

コンテンツ フィルタリング

コンテンツフィルタリングは、3GPP および 3GPP2 ネットワークで使用可能なインラインサービスです。HTTP リクエスト内の URL に基づいてモバイルサブスクライバからの HTTP リクエストをフィルタ処理します。これにより、オペレータは個々のサブスクライバがアクセスできるコンテンツをフィルタ処理して制御できるため、サブスクライバが常識的に容認されないコンテンツや望まないコンテンツに思いがけずさらされることはありません。

コンテンツフィルタリングの構成

コンテンツフィルタリングを有効にするには、次の追加設定を使用します。

```
configure
  require user-plane content-filtering
    content-filtering category database directory path path_address
    content-filtering category database max-version version_number
    end
```

（注）
コンテンツフィルタリングを有効にするには、ブート時に上記の構成を UPF で構成する必要があります。ユーザープレーン設定後に上記の設定を定義すると、エラーや不整合が発生します。

show コマンドの入力と出力

show subscribers user-plane-only callid *call_id* full all

SMF は、Session Establishment/Modification 要求で、コンテンツ フィルタリング ポリシー ID を指定します。この機能をサポートするために、次のフィールドが表示されます。

- SUBSCRIBER パラメータ
  - コンテンツ フィルタリング ポリシー ID

DNS スヌーピング

課金

DNS スヌーピングの課金は SM-P で実行されます。

ルール定義

ルール定義のホスト名（domain-names）とホスト名の一部を指定するには、次の CLI コマンドを使用します。

```
ruledef <ruledef_name>
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
        multi-line-OR enabled
```

ip server-domain-name のルールラインを削除するには、この CLI の no バージョンを使用します。

```
ruledef <ruledef_name>
  no ip [server-domain-name {contains|=|ends-with|starts-with}
<url_string>]
  exit
```

ECS レベルで DNS エントリについて設定可能なタイマーには、次の CLI を使用します。

```
configure
         active-charging service service_name
            ip dns-resolved-entries timeout <value_secs>
            end
```

ip server-domain-name キーワードを含む ruledef が定義され、ルールベースで使用されるたびに、インスタンス単位でルールベースごとに ip-table が作成されます。

ルールの照合

この機能は、非 CUPS アーキテクチャの機能と同じです。

show CLI

次の CLI を使用して、DNS IP エントリ：**show user-plane-service [statistics dns-learnt-ip-addresses {summary | sessmgr instance <id> |all [verbose] }]** のテーブルを確認します。

バルク統計情報

DNS スヌーピング機能をサポートするために、次のバルク統計情報を使用できます。

- ecs-dns-learnt-ipv4-entries
- ecs-dns-flushed-ipv4-entries
- ecs-dns-replaced-ipv4-entries
- ecs-dns-overflown-ipv4-entries
- ecs-dns-learnt-ipv6-entries
- ecs-dns-flushed-ipv6-entries
- ecs-dns-replaced-ipv6-entries
- ecs-dns-overflown-ipv6-entries

前述のバルク統計情報は、非 CUPS アーキテクチャと同様に ECS スキーマに追加されます。

（注） SNMP トラップ生成コマンドは、CUPS DNS スヌーピング機能ではサポートされていません。

イベントデータレコード

表 *33 :* 機能の履歴

機能名	リリース情報	機能説明
EDR の最終アップリンクおよびダウンリンクパケット時間属性	2023.04	EDR 設定では、データ停止の問題を特定するために、2 つの新しい属性 **sn-last-uplink-pkt-time** と **sn-last-downlink-pkt-time** がサポートされています。

機能説明

Event Data Records（EDR）は、システム管理ユーザーによるコンテンツ情報、形式、および生成トリガーの構成をサポートする、使用状況レコードです。

フローが終了すると、UPF は終了したフローの詳細情報を使用して EDR を生成します。

機能の仕組み

EDRは、フロー終了時にユーザープレーンから生成されます。コールセットアップとコール変更中、EDR 生成に必要なすべてのコール固有属性は、Sx Establishment/Modification 要求メッセージの 「Subscriber Params」IE の一環として、SMF から UPF に送信されます。

フローの終了時に、VPP から課金カウンタが取得されます。EDR 形式の設定で設定されたすべてのコールレベル属性は、課金やボリュームカウンタの属性とともに CDRMOD proclet に送信されます。この proclet により、該当レコードがファイルまたはディスクに書き込まれ、設定された外部サーバーに転送されます。

TCP Fast Open

TCP Fast Open（TFO）は、2 つのエンドポイント間の連続する TCP 接続をより迅速に開始するための拡張機能です。そのためにこの機能では、クライアントに保存され、サーバーとの初回接続時に設定される暗号化 Cookie である TFO Cookie（TCP オプション）を使用します。クライアントが再接続する際、認証のために初回 SYN パケットとともに TFO Cookie データも送信します。認証が成功すると、サーバーは、3 ウェイハンドシェイクの最後の ACK パケットを受信する前であっても、クライアントへのデータ送信を開始できます。このため、EDR の TCP フローの制御パケット間の時間差を計算して記録するために、次のパケット間の差が記録されます。

- SYN および SYN-ACK パケット
- SYN-ACK および ACK パケット

EDR 内の情報をキャプチャするために追加されるルール変数の詳細については、「その他の *TCP* フィールドを構成する」項を参照してください。

トランザクション完了 EDR

HTTP トランザクションが完了すると、HTTP EDR に対してTransaction Complete EDR が生成されます。完了すると、VPP から課金カウンタがフェッチされます。EDR 形式の設定で設定されたすべてのコールレベル属性は、課金やボリュームカウンタの属性とともにCDRMOD proclet に送信されます。この proclet により、該当レコードがファイルまたはディスクに書き込まれ、設定された外部サーバーに転送されます。

次の EDR 属性がサポートされています。

- sn-start-time
- sn-end-time
- sn-start-time format MM/DD/YYYY-HH:MM:SS:sss
- sn-end-time format MM/DD/YYYY-HH:MM:SS:sss
- radius-calling-station-id
- radius-called-station-id
- bearer 3gpp imsi

- bearer 3gpp imei
- bearer 3gpp rat-type
- bearer 3gpp user-location-information
- ip subscriber-ip-address
- ip dst-address
- sn-ruledef-name
- sn-subscriber-port
- sn-server-port
- sn-app-protocol
- sn-volume-amt ip bytes uplink
- sn-volume-amt ip bytes downlink
- sn-flow-start-time format seconds
- sn-flow-end-time format seconds
- sn-volume-amt ip pkts uplink
- sn-volume-amt ip pkts downlink
- sn-direction
- traffic-type
- p2p protocol
- p2p app-identifier tls-cname
- p2p app-identifier tls-sni
- p2p app-identifier quic-sni
- bearer 3gpp sgsn-address
- sn-rulebase
- sn-charging-action
- flow tethered-ip-ttl
- flow ttl
- flow ip-control-param
- bearer qci
- tcp flag
- ip server-ip-address
- sn-flow-id
- sn-closure-reason

- sn-duration
- ip src-address
- IP プロトコル
- sn-charge-volume ip bytes uplink
- sn-charge-volume ip bytes downlink

次の HTTP EDR 属性がサポートされています。

- http url length 2000
- http request method
- http content type
- http user-agent length 255
- http reply code
- http referer
- http host
- http cookie
- http header-length
- transaction-uplink-bytes
- transaction-downlink-bytes

次の DNS EDR 属性がサポートされています。

- dns answer-ip-list
- dns answer-name
- dns previous-state
- dns query-name
- dns query-type
- dns return-code
- dns state
- dns tid

データの停滞を特定する EDR 属性

EDR は、データ停滞の問題を特定するために、次の属性をサポートしています。

- **sn-last-uplink-pkt-time**
- **sn-last-downlink-pkt-time**

アップリンクまたはダウンリンク報告の最後のパケットと**sn-end time**（フローリリース時間）間で平均差が大きい場合、これは、データの停滞を示しています。

これらのEDR変数は、制御パケット（FIN/RST/FIN-ACK/TCP TEAR DOWN ACK）のパケット時間はキャプチャしません。これらのパケットのパケット時間は、**sn-end time**を使用してセッションマネージャでキャプチャされます。

オフロードされたフローの場合、属性**sn-last-uplink-pkt-time**と**sn-last-downlink-pkt-time**は、fastpathを通過するパケットに対して更新されます。

制限事項

UPDのEDR機能には、次の制限があります。

- EDRは、フロー終了条件（アイドルタイムアウト、HAGR、通常フロー終了、およびセッション終了中）に対してのみ生成されます。
- 課金アクションベースのEDR設定はサポートされません。
- EDRのレポートはサポートされません。
- コントロールプレーンのパケット時間は、EDRのlast_uplink_packet_time and last_downlink_packet_time except mid session TCP ACKには更新されません。

イベントデータレコードを構成する

UPFでEDRを構成する

UPFでEDR属性を構成するには、次の構成を使用します。

```
active-charging service service_name
   rulebase rulebase_name
      flow end-condition { timeout | normal-end-signaling | session-end
 | hagr } charging-edr charging_edr_format_name
      edr transaction-complete { http | dns } charging-edr
charging_edr_format_name
      exit
      edr-format format_name
         attribute attribute_name format time_format priority priority_val
```

注：

- **flow end-condition**：このコマンドを使用すると、ユーザーセッションに関連するセッションフローの終了条件を設定し、EDR生成をトリガーできます。
- **timeout**：タイムアウト条件が原因でフローが終了するたびに、指定されたEDR形式でEDRを作成します。
- **normal-end-signaling**：フロー終了が正常に通知されるたびに、指定されたEDR形式でEDRを作成します。たとえば、TCPフローのFINとACKを検出し、指定されたEDR形式を使用してフローのEDRを作成します。

- **session-end**：サブスクライバセッションが終了するたびに、指定された EDR 形式で EDR を作成します。このオプションを使用すると、セッションマネージャは、セッション終了時にフローに対して最後の EDR が作成されてからアクティビティがあったすべてのフローに対して、指定された形式名で EDR を作成します。
- **charging-edr** *charging_edr_format_name*：課金 EDR 形式を指定します。
- **hagr**：シャーシ間 Session Recovery アクションによりフローが終了するたびに、指定された EDR 形式で EDR を作成します。
- **http**：HTTP プロトコル関連の設定を指定します。
- **dns**：DNS プロトコル関連の設定を指定します。
- **edr-format** *format-name*：構成する必要がある EDR を指定します。
- **attribute** *attribute_name* **format** *time_format* **priority** *priority_val*：EDR でキャプチャする具体的な属性を指定します。**format** *time_format*は、タイムスタンプ形式を指定します。次の時間形式をサポートしています。
  - MM/DD/YY-HH:MM:SS
  - MM/DD/YY-HH:MM:SS:sss
  - MM/DD/YYYY-HH:MM:SS
  - MM/DD/YYYY-HH:MM:SS:sss
  - YYYY/MM/DD-HH:MM:SS
  - YYYY/MM/DD-HH:MM:SS:sss
  - YYYYMMDDHHMMSS
  - YYYYMMDDHHMMSSsss
  - 秒

  priority *priority_val* は、EDR レコード内の値の位置の優先順位を指定します。値は、1 ～ 65535 の整数で指定する必要があります。

EDR モジュールを有効にするための構成

EDR モジュールを有効にするには、次の構成を使用します。

```
configure
  context context_name
    edr-module active-charging-service
    end
```

追加の TCP フィールドの設定

次の CLI コマンドを使用して EDR に追加の TCP フィールドを設定する前に、他のすべての EDR 設定が完了していることを確認します。

```
configure
  active-charging service service_name
    edr-format edr_format_name
      rule-variable tcp syn-synack-rtt priority priority_value
      rule-variable tcp synack-ack-rtt priority priority_value
      end
```

モニタリングおよびトラブルシューティング

show user-plane-service statistics rulebase name *rulebase_name*

この機能をサポートするために、次のフィールドが表示されます。

- ルールベース名
  - EDR
  - Charge Volume
    - Uplink Pkts
    - Uplink Bytes
    - Downlink Pkts
    - Downlink Bytes
  - Charging EDRs
    - Total Charging EDRs generated
    - EDRs generated for handoff
    - EDRs generated for timeout
    - EDRs generated for normal-end-signaling
    - EDRs generated for session end
    - EDRs generated for rule match
    - EDRs generated for hagr
    - EDRs generated for flow-end content-filtering
    - EDRs generated for flow-end url-blacklisting
    - EDRs generated for content-filtering
    - EDRs generated for url-blacklisting
    - EDRs generated for any-error packets
    - EDRs generated for firewall deny rule match
    - EDRs generated for transaction completion
    - EDRs generated for voip call end
    - EDRs generated for dcca failure handling

- EDRs generated for TCP optimization on
- EDRs generated for tethering signature change
- EDRs generated for interim interval
- Total Flow-Overflow EDRs
- Total zero-byte EDRs suppressed

show user-plane-service edr-format all

EDR 機能の追加の TCP フィールドをサポートするために、次のフィールドが表示されます。

- Service Name
  - EDR 形式名
    - rule-variable tcp syn-synack-rtt priority 1
    - rule-variable tcp synack-ack-rtt priority 2

ファイアウォールのサポート

表 *34 :* 機能の履歴

機能名	リリース情報	説明
ファイアウォール TCP アイドル タイムアウト アクション	2023.04	ファイアウォール機能は、IP セッションベースのアクセス制御を実行するサブスクライバ通信を検査して、セキュリティ攻撃からサブスクライバを保護します。 UPF は、サブスクライバフローをドロップするか、TCP タイムアウトの期限切れ時にリセットを送信する TCP アイドル タイムアウト アクションをサポートします。

機能説明

UPF 2.0のファイアウォール機能は、サブスクライバ通信を検査し、サブスクライバセッションの IP セッションベースのアクセスコントロールｗｐ実行して、悪意のあるセキュリティ攻撃からサブスクリプションを保護します。UPF 2.0 は、サブスクライバフローをドロップする

か、TCP タイムアウトの期限切れ時にリセットを送信する TCP アイドル タイムアウト アクションをサポートします。

ファイアウォールの設定により、システムはサブスクライバ データ セッションの各パケットを検査できます。また、セキュリティ脅威を評価し、アップリンクおよびダウンリンクトラフィックに設定されたポリシーを適用します。ファイアウォールは、フローレベルごとおよびパケットごとの検証をサポートします。

ファイアウォール機能は、次の機能をサポートしています。

- DoS および DDoS 攻撃からの保護
- アプリケーションレベル ゲートウェイ
- ステートフル パケット インスペクションおよびフィルタリング
- ステートレス パケット インスペクションおよびフィルタリング
- SNMP のしきい値設定

サブスクライバ ファイアウォールの構成

ファイアウォール構成は、UPF のアクティブな課金構成で使用できます。

- Access-Ruledefs
- Firewall-NAT Policy

IPv4 および IPv6 のデフォルトファイアウォールを有効にする

次の構成を使用して、IPv4 および IPv6 のデフォルトファイアウォールを構成します。

```
configure
  active-charging service service_name
    fw-and-nat policy policy_name
      firewall policy ipv4-and-ipv6
      end
```

TCP アイドル タイムアウト アクションを構成する

TCP アイドル タイムアウト アクションを構成するには、次の構成を使用します。

```
configure
  active-charging service service_name
    fw-and-nat policy policy_name
      firewall tcp-idle-timeout-action { drop | reset }
      end
```

注：

- **firewall tcp-idle-timeout-action { drop | reset }**：TCP アイドルタイマーの期限切れ時に実行されるステートフル ファイアウォール アクションを指定します。
  - **drop**：サブスクライバフローは、TCP タイムアウトの期限切れ時にリセットを送信せずにクリアまたはドロップされます。

- **reset**：TCP タイムアウトの期限切れ時にリセットを送信するように指定します。これはデフォルト値です。

- **firewall tcp-idle-timeout-action reset** CLI コマンドは、ファイアウォールにのみ適用されます。
- UPF はフローマッピングをサポートしません。

前述のサービス構成に加えて、次の構成は、サービス内のさまざまなファイアウォール関連 CLI のデフォルト CLI 動作です。

```
Dos-Protection:
      Source-Route                          : Disabled
      Win-Nuke                              : Disabled
      Mime-Flood                            : Disabled
      FTP-Bounce                            : Disabled
      IP-Unaligned-Timestamp                : Disabled
      Seq-Number-Prediction                 : Disabled
      TCP-Window-Containment                : Disabled
      Teardrop                              : Disabled
      UDP Flooding                          : Disabled
      ICMP Flooding                         : Disabled
      SYN Flooding                          : Disabled
      Port Scan                             : Disabled
      IPv6 Extension Headers Limit          : Disabled
      IPv6 Hop By Hop Options               : Disabled
      Hop By Hop Router Alert Option        : Disabled
      Hop By Hop Jumbo Payload Option       : Disabled
      Invalid Hop By Hop Options            : Disabled
      Unknown Hop By Hop Options            : Disabled
      IPv6 Destination Options              : Disabled
      Invalid Destination Options           : Disabled
      Unknown Destination Options           : Disabled
      IPv6 Nested Fragmentation             : Disabled

    Max-Packet-Size:
      ICMP                              : 65535
      Non-ICMP                          : 65535
    Flooding:
      ICMP limit                        : 1000
      UDP limit                         : 1000
      TCP-SYN limit                     : 1000
      Sampling Interval                 : 1

    TCP-SYN Flood Intercept:
      Mode                              : None
      Max-Attempts                      : 5
      Retrans-timeout                   : 60
      Watch-timeout                     : 30
    Mime-Flood Params:
      HTTP Header-Limit                 : 16
      HTTP Max-Header-Field-Size        : 4096

    No Firewall Ruledef Match Action:
      Uplink Action                     : permit
      Downlink Action                   : deny

    TCP RST Message Threshold     : Disabled
    ICMP Dest-Unreachable Threshold    : Disabled
    Action upon receiving TCP SYN packet with ECN/CWR Flag set    : Permit
    Action upon receiving a malformed packet  : Deny
```

```
Action upon IP Reassembly Failure   : Deny
Action upon receiving an IP packet with invalid Options : Permit
Action upon receiving a TCP packet with invalid Options : Permit
Action upon receiving an ICMP packet with invalid Checksum: Deny
Action upon receiving a TCP packet with invalid Checksum: Deny
Action upon receiving an UDP packet with invalid Checksum: Deny
Action upon receiving an ICMP echo packet with id zero : Permit
TCP Stateful Checks : Enabled
First Packet Non-SYN Action: Drop
ICMP Stateful Checks: Enabled
TCP Partial Connection Timeout: 30
```

IP リアセンブル

この項では、リアセンブル機能について説明します。

- 非CUPSアーキテクチャでは、デフォルトのファイアウォール構成の場合、フラグメントは最大64Kバイトまでバッファリングされます。64Kを超えると、バッファリングされたすべてのフラグメントと後続のフラグメントがドロップされます。UPF では、最大 9K バイトのパケットサイズを最大 6 つのフラグメントにリアセンブルできます。
- **firewall ip-reassembly-failure** CLI は、ティアドロップ攻撃、ネストされたフラグメンテーション、および一般的な ip-reassembly-failure を構成します。最大 IP パケットサイズは。6 つのフラグメント（9000 バイトまで）に制限されています。
- ファイアウォール統計のカウンタを次に示します。このカウンタは、リアセンブルに関連するすべての攻撃に対して増分されます。
  - IPv4 リアセンブルの失敗が原因でドロップされたダウンリンクパケット数
  - IPv4 リアセンブルの失敗が原因でドロップされたアップリンクパケット数
  - IPv4 リアセンブル失敗時のダウンリンクドロップバイト数
  - IPv4 リアセンブル失敗時のアップリンクドロップバイト数
  - IPv6 リアセンブルの失敗が原因でドロップされたダウンリンクパケット数
  - IPv6 リアセンブルの失敗が原因でドロップされたアップリンクパケット数
  - IPv6 リアセンブル失敗時のダウンリンクドロップバイト数
  - IPv6 リアセンブル失敗時のアップリンクドロップバイト数

モニタリングおよびトラブルシューティング

この項では、この機能をサポートする show コマンドとその出力について説明します。

show config active-charging service name acs verbose

```
fw-and-nat policy SFW_NAT_TEST
      no firewall dos-protection source-router
      no firewall dos-protection winnuke
      no firewall dos-protection mime-flood
      no firewall dos-protection ftp-bounce
      no firewall dos-protection ip-unaligned-timestamp
```

```
  no firewall dos-protection tcp-window-containment
  no firewall dos-protection teardrop
  no firewall dos-protection flooding udp
  no firewall dos-protection flooding icmp
  no firewall dos-protection flooding tcp-syn
  no firewall dos-protection port-scan
  no firewall dos-protection ipv6-extension-hdrs
  no firewall dos-protection ipv6-hop-by-hop
  no firewall dos-protection ipv6-hop-by-hop router-alert
  no firewall dos-protection ipv6-hop-by-hop jumbo-payload
  no firewall dos-protection ipv6-hop-by-hop invalid-options
  no firewall dos-protection ipv6-hop-by-hop unknown-options
  no firewall dos-protection ipv6-dst-options
  no firewall dos-protection ipv6-dst-options invalid-options
  no firewall dos-protection ipv6-dst-options unknown-options
  no firewall dos-protection ipv6-frag-hdr nested-fragmentation
  no firewall dos-protection ip-sweep tcp-syn
  no firewall dos-protection ip-sweep udp
  no firewall dos-protection ip-sweep icmp
  firewall max-ip-packet-size 65535 protocol icmp
  firewall max-ip-packet-size 65535 protocol non-icmp
  firewall flooding protocol icmp packet limit 1000
  firewall flooding protocol udp packet limit 1000
  firewall flooding protocol tcp-syn packet limit 1000
  firewall flooding sampling-interval 1
  firewall tcp-syn-flood-intercept mode none
  firewall tcp-syn-flood-intercept watch-timeout 30
  firewall mime-flood http-headers-limit 16
  firewall mime-flood max-http-header-field-size 4096
  no firewall icmp-destination-unreachable-message-threshold
  access-rule no-ruledef-matches uplink action permit
  access-rule no-ruledef-matches downlink action deny
  firewall tcp-idle-timeout-action reset
  no firewall tcp-reset-message-threshold
  firewall tcp-syn-with-ecn-cwr permit
  firewall malformed-packets drop
  firewall ip-reassembly-failure drop
  no firewall validate-ip-options
  firewall tcp-options-error permit
  firewall icmp-echo-id-zero permit
  firewall icmp-checksum-error drop
  firewall tcp-checksum-error drop
  firewall udp-checksum-error drop
  firewall tcp-fsm first-packet-non-syn drop
  firewall icmp-fsm
  firewall policy ipv4-and-ipv6
  firewall tcp-partial-connection-timeout 30
  no nat policy
  no nat binding-record
  no nat pkts-drop edr-format
  no nat pkts-drop timeout
  default nat suppress-aaa-update
  nat private-ip-flow-timeout 180
  nat check-point-info basic limit-flows 100
  nat check-point-info sip-alg
  nat check-point-info h323-alg
  nat max-chunk-per-realm single-ip
#exit
```

show CLI

この項では、UPF でサポートされている show コマンドについて説明します。

- **show subscribers user-plane-only full all**

- **show subscribers user-plane-only flows**
- **show user-plane-service inline-services firewall statistics verbose**
- **show user-plane-service statistics rulebase all**
- **show alarm outstanding all**
- **show alarm outstanding all verbose**
- **show alarm statistics**
- **show user-plane-service statistics rulebase name** *rulebase_name*

SNMP トラップ

この項では、SNMP トラップについて説明します。トラップを有効にするには、ユーザープレーンでそれぞれの trap CLI を使用します。

- **Dos 攻撃**：DoS攻撃の数が設定されたしきい値を超えると、SNMP トラップが生成されます。設定された時間間隔内に数値がしきい値を下回ると、トラップがクリアされます。
- **パケットドロップ**：ドロップされたパケット数がしきい値を超えると、SNMP トラップが生成されます。設定された時間間隔内に数値がしきい値を下回ると、トラップがクリアされます。
- **拒否ルール**：拒否ルールの数がしきい値を超えると、SNMP トラップが生成されます。設定された時間間隔内に数値がしきい値を下回ると、トラップがクリアされます。
- **ルールなし**：ルールなしの数がしきい値を超えると、SNMP トラップが生成されます。設定された時間間隔内に数値がしきい値を下回ると、トラップがクリアされます。

フローアイドルタイムアウトのランダム化

セッションマネージャは、2秒ごとに、セッションマネージャインスタンスからの最新パケットの時刻、または fastpath ストリームをポーリングして、アイドルフローを判断します。短い距離のフローは、パケット数が少ないため、短時間で 5 ～ 10 秒以内でアイドル状態になります。その結果、所定の2秒のポーリングサイクルでのタイムアウトにより、多数のアイドルフローを削除する必要があります。アイドルフローの削除は、統計の調整、EDRの生成、および高速パスストリームの削除をともなうため、CPUに負荷がかかります。短期フローは積極的にクリアされるため、この機能でより多くのフローに対応できます。

ACS でフローアイドルタイムアウトのランダム化を構成する

アイドルタイムアウトフローをランダム化するには、次の構成を使用します。

```
configure
active-charging service service_name
  idle-timeout randomize-range range
    { default | no } idle-timeout randomize-range
      end
```

注：

- **idle timeout**：フローがアイドル状態を維持できる最大時間を秒単位で指定します。秒は、5～30の整数で指定する必要があります。その後、フローはランダムな値に基づいて終了します。
- **randomize-range**：期間を秒単位で指定します。適用されるアイドルタイムアウトは、フローごとに異なります。

  次に例を示します。

  ```
  idle-timeout randomize-range 20
  ```

  0～20の整数のランダム番号が生成されます。この数値は、設定されたアイドルタイムアウト値に追加され、2秒間のタイマー処理でフローがアイドルになったかどうかを確認します。設定されたアイドルタイムアウトが60秒に設定されている場合、各フローに適用される実際のタイムアウトは *60 + 20* 秒の範囲でランダム化され、フローが段階的に削除されます。
- **no**：アイドルタイムのランダム化を無効にします。このコマンドは、デフォルトでディセーブルになっています。
- **default**：idle timeout randomization コマンドをを秒単位のデフォルト設定で構成します。秒は、0～30の整数で指定する必要があります。デフォルト範囲は、0～30秒です。

  たとえば、**default idle-timeout randomize-range** は、**idle-timeout randomize-range 30** と同じです。

HTTP URL フィルタリング機能

HTTP URL フィルタリング機能は、URL 検出に使用されるルール定義を簡素化します。

HTTP リクエストパケットには、プロキシ（プレフィックス付き）URL と実際の URL を含めることができます。プロキシURLがHTTPリクエストパケットで見つかった場合、HTTP URL フィルタリング機能は解析された情報からこのURLを切り捨て、実際のURLのみがルール照合とイベントデータレコード（EDR）の生成に使用されます。

HTTP URL フィルタリング機能の設定

ここでは、HTTP URL フィルタリング機能の設定方法について説明します。

プレフィックス付き URL のグループの設定

プレフィックス付き URL のグループを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
    end
```

プレフィックス付き URL のグループ内 URL の設定

プレフィックス付き URL のグループでフィルタリング対象の URL を設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    group-of-prefixed-urls prefixed_urls_group_name
      prefixed-url url_1
      ...
      prefixed-url url_10
      end
```

ルールベースでのプレフィックス付き URL のグループの有効化

プレフィックス付き URL を処理するためにルールベースでプレフィックス付き URL のグループを有効にするには、次の CLI コマンドを使用します。

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_1
      ...
      url-preprocessing bypass group-of-prefixed-urls
prefixed_urls_group_name_64
      end
```

コントロール プレーン シャーシのこの設定は、「group-of-prefixed-urls」と「rulebase-url-preprocessing」の PFD メッセージを使用してユーザープレーンにプッシュされます。

プレフィックス付き URL のグループにはプロキシ URL のリストがあり、このリストは削除する必要があります。rulebase には、プレフィックス付き URL の複数のグループが含まれており、フィルタリングする必要があります。課金 ruledef には、プレフィックス付き URL グループ内の URL を削除してから検索する必要がある実際の URL のルールが含まれています。

（注）
- プレフィックス付き URL の 1 グループあたり、最大 10 個のプレフィックス付き URL を追加できます。
- 最大 64 のプレフィックス付き URL グループを作成および設定できます。

Show コマンド

show user-plane-service group-of-prefixed-urls all | name *group_name*

この show コマンドをユーザープレーンで使用すると、プレフィックス付き URL のグループがプッシュされているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of the group of prefixed URLs
- Prefixed URLs

- Total number of prefixed URLs found

show user-plane-service rulebase name *rbase_name*

このshowコマンドをユーザープレーンで使用すると、プレフィックス付きURLのグループがrulebaseで設定されているかどうかを確認できます。このコマンドの出力は次のとおりです。

- Name of rulebase
- Name of the groups of prefixed Urls for URL pre-processing

show user-plane-service statistics analyzer name http

このコマンドの出力は次のとおりです。

- Total HTTP Sessions
- Current HTTP Sessions
- Total Uplink Bytes
- Total Downlink Bytes
- Total Uplink Pkts
- Total Downlink Pkts
- Uplink Bytes Retrans
- Downlink Bytes Retrans
- Uplink Pkts Retrans
- Downlink Pkts Retrans
- Total Request Succeed
- Total Request Failed
- GET Requests
- POST Requests
- CONNECT Requests
- PUT requests
- HEAD requests
- Websocket Flows
- Invalid packets
- Wrong FSM packets
- Unknown request method
- Pipeline overflow requests
- Corrupt request packets
- Corrupt response packets

- Unhandled request packets
- Unhandled response packets
- Partial HTTP Header Anomaly prevented
- New requests on closed connection
- Memory allocation failures
- Packets after permanent failure
- Prefixed Urls Bypassed
- FastPath Statistics
- Total FP Flows
- Uplink (Total FP Pkts)
- Downlink (Total FP Pkts)
- Uplink (Total FP Bytes)
- Downlink (Total FP Bytes)

（注） パフォーマンス測定指標として、[Prefixed URLs Bypassed] カウンタが http アナライザ統計に追加されました。削除済みのプレフィックス付き URL 数を表示します。

IP 再アドレス指定

IP アドレス再指定機能により、パケットの宛先 IP アドレスに基づいて、不明なゲートウェイ通信を既知のゲートウェイや信頼できるゲートウェイにリダイレクトできます。

IP アドレス再指定は、課金アクションで定義されたフローアクションで設定されます。IP アドレス再指定は、特定の ruledef に一致する通信に対して機能し、そのため課金アクションが適用されます。IP アドレス再指定は、アップリンクとダウンリンク通信の両方に適用されます。拡張された課金サブシステムでは、アップリンクパケットは、パケット検査やルール照合などの後に変更され、接続先 IP またはポートが決定され、送信される直前にアドレス再指定された IP またはポートに置き換えられます。ダウンリンクパケット（アドレス再指定された IP またはポートを含む）は、受信した時点でパケットインスペクションの前に変更され、送信元 IP またはポートが、元のサーバー IP またはポート番号に置き換えられます。

MS からの 1 つのフローで、1 つのパケットのアドレスが再指定されると、そのフローに含まれるすべてのパケットのアドレスが同じサーバーに再指定されます。DPI や rule-matching などの機能は影響を受けません。各 IP アドレスとポートの組み合わせは、ruledef として定義されます。

IP フラグメンテーションの場合、IP リアセンブルに成功したパケットのアドレスが再指定されます。ただし、IP フラグメンテーションに失敗したパケットのアドレスは、再指定されません。

server-list が charging-action で構成された場合、アドレス再指定サーバーを選択するために、2 つの異なるアプローチがあります。

- **round-robin**：round-robin アプローチでは、サーバーは、新しい各フローで round-robin 方式で選択されます。round-robin では、リスト内のアクティブなサーバーのみが選択対象と見なされます。
- **階層型アプローチ**：階層型アプローチでは、アドレス再指定 server-list で定義されている順に応じて、サーバーがプライマリ、セカンダリ、ターシャリなどでタグ付けされます。すべてのフローは、プライマリサーバーが稼働状態になるまで、プライマリサーバーにアドレス再指定されます。プライマリサーバーがダウンした場合は、フローのアドレス再指定先はセカンダリサーバーとなり、その後も同じロジックが繰り返されます。プライマリサーバーが再びアクティブになると、フローのアドレス再指定先はプライマリサーバーに戻ります。

ユーザーがサーバーの選択に階層型か round-robin アプローチを指定できるその他の CLI が提供されます。round-robin および階層型のサーバー選択アプローチはどちらも、IPv4 ベースおよび IPv6 ベースのサーバーの両方に適用できます。

IP アドレス再指定を構成する

パケットの宛先 IP アドレスに基づいてパケットをアドレス再指定することで、道のゲートウェイ通信から既知または信頼されているゲートウェイにリダイレクトできます。これは、課金アクションでサーバーのアドレス再指定を構成することによって実装されます。

IP アドレス再指定機能を構成するには、次の構成を使用します。

```
configure
  active-charging service  acs_service_name
    charging-action  charging_action_name
      flow action readdress server ipv4_address/ipv6_address [
discard-on-failure ]  [ dns-proxy-bypass ]  [ port port_number [
discard-on-failure ] [ dns-proxy-bypass ] ]
      end
```

アドレス再指定 server-list が charging-action で定義されている場合に、IP アドレス再指定機能を構成するには、次の構成を使用します。

```
configure
  active-charging service  acs_service_name
    charging-action  charging_action_name
      flow action readdress server-list server_list_name [ hierarchy ] [
 round-robin ] [ dns-proxy-bypass ] [ discard-on-failure ]
      end
```

次に、server-list の構成例を示します。

```
readdress-server-list DRE
consecutive-failures 1
response-timeout 10000
server 209.165.200.225 port 53
server 209.165.200.226 port 53
server 2001:420:54fe::1019 port 53
server 2001:420:54fe::1039 port 53
```

```
server 2001:420:54fe::1049 port 53
server 2001:420:54fe::1059 port 53
server 209.165.201.30 port 8080
#exit
```

（注） リストには、最大 10 のサーバーを構成でき、active-charging サービスには、最大 10 のリストを構成できます。

Show コマンド

この項では、IP のアドレス再指定機能のサポートに使用可能な show CLI コマンドについて説明します。

CLI コマンド	説明
show user-plane-service readdress-server-list statistics all **show user-plane-service readdress-server-list statistics instance** *instance* **show user-plane-service readdress-server-list statistics name** *name*	これらの show コマンドを使用して、リアドレスサーバーリストの統計を表示します。
show user-plane-service readdress-server-list statistics	

clear user-plane-service readdress-server-list statistics all CLI を使用して、再アドレスサーバーリスト統計をクリアします。

show user-plane-service statistics charging-action all CLIを使用して、「再アドレスされた」カウンタを確認します。

L7 プロトコル

次の L7 プロトコルが DPI の一部としてサポートされています。

- DNS
- FTP
- HTTP
- HTTPS
- RTP/RTSP
- SIP

DNS

UPF は、L7 アナライザの一部として DNSプロトコルをサポートします。

FTP

UPF 2.0 は、L7 アナライザの一部として FTP プロトコルをサポートします。

HTTP

HTTP リクエストまたは HTTP 応答が完了すると、次の場合に、アップリンクまたはダウンリンクのデータパケットが、VPP にオフロードされます。

- コンテンツ長：ボリュームベースのオフロードは、GETやPOSTなどのメソッドでサポートされます。チャンクエンコーディングによるデータ転送メカニズムを使用したHTTPフローは、HTTP で定義されているメソッドに関係なくオフロードされません。ストリームがコンテンツ長に基づいてオフロードされた場合、もう一方のストリームも、前者がオンロードされなくなるまでオフロードされます。
- CONNECTメソッド：フローがCONNECTにアップグレードされると、アップリンクとダウンリンクの両方のストリームがオフロードされるメソッドです。
- WebSocket メソッド：フローが WebSocket プロトコルとして分類されると、アップリンクとダウンリンクの両方のストリームがオフロードされます。
- ストリームは、次のいずれかの場合に再度、オンロードされます。
  - FIN パケットを受信した場合
  - コンテンツ長に違反している場合
  - PDN の更新

ヘッダー解析

rulebaseに含まれるruledefで定義されているヘッダーフィールドのみが解析されます。X-Header機能の場合は、一部のHTTPヘッダーフィールドと依存関係があるリダイレクトが設定されます。

HTTP 課金

- 完全なパケットは、課金されます。
- 部分的パケットは、完成時に課金されます。部分的パケットを完成させるパケットも、課金されます。
- 連結パケットは、課金されます。
- 遅延課金が有効になっている場合：制御パケットは、遅延課金CLI構成に応じて、アプリケーションベースのルールに対して課金されます。

- 応答ベースの課金が有効になっている場合：HTTP リクエストの応答を受信した後、その HTTP リクエストは応答ルールの CA に対して課金されます。

X-Header の解析とルール照合

x-header ルール行が含まれる ruledef が解析され、照合されます。

WebSocket

HTTP フローが WebSocket フローにアップグレードされた場合、HTTP GET リクエストの後のフローの後続のパケットの課金が関与します。

応答ベースの TRM

トランザクションルールの照合は、HTTP 応答パケットの受信後に行われます。

X-Header の挿入

HTTP リクエストへの X-Header の挿入がサポートされます。

URL ベースのリダイレクト

URL ベースのリダイレクションは、次を実行する UPF 機能です。

- サブスクライバにリダイレクト応答を返し、既存の TCP 接続を終了します。
- サブスクライバの Web ブラウザをトリガーして、元の HTTP パケットを指定された接続先 URL に自動送信します。
- ダイナミックポリシー経由で受信したコンポジット文字列（returnURL など）から特定の接続先 URL を抽出できるようにします。

通信フローが HTTP でない場合、UPF は、リダイレクト URL オプションを無視して、パケットを通常どおり転送します。リダイレクションは、アップリンク方向に送信される特定の HTTP パケット（GET 要求など）についてのみサポートされます。

表 *35 :* 機能の履歴

機能名	リリース情報	説明
リダイレクト URL の暗号化	2024.01	UPF は、Blowfish および AES 暗号化方式を使用したダイナミックフィールドの URL 暗号化をサポートしています。 デフォルト設定：無効：構成が必要

機能名	リリース情報	説明
リダイレクトの書き換えと TCP FIN/RST	2026.01.1	N7 インターフェイスの ADC ダイナミックルールは、リダイレクト URL サポートを実行します。これは、AES 暗号化でのみサポートされます。

ダイナミックフィールドと暗号化：

- **フィールド挿入**： UPF は、リダイレクトされた URL へのダイナミック サブスクライバ データの追加をサポートしています。
- **セキュリティ**：機密性の高いダイナミックフィールドを、対称ブロック暗号を使用して保護できます。
  - **Blowfish**：暗号化と復号に 128 ビットキーを使用します。
  - **AES**：256 ビットキーによる暗号ブロック連鎖（CBC）モードを使用します。UPF は、AES 暗号化にハードコードされた 10 ラウンドの値を使用します。

（注） N7 インターフェイスのリダイレクト URLは、AES 暗号化でのみサポートされます。

N7 インターフェイスを使用した URL リダイレクションの制限事項

- この機能は、UL L7 パケットのみをサポートします。機能要件は、特に UL L7 のサポート向けであるため、DL L7 パケットはサポートしません。
- 既存の課金アクションの設定は変更しないでください。

リダイレクションでサポートされるダイナミックフィールド

UPF は、リダイレクトされた URL に挿入するための次のダイナミックフィールドをサポートしています。アスタリスク（*）付きのフィールドは、暗号化をサポートします。

- #ACSMGR_BEARER_CALLED_STATION_ID#
- #BEARER.IMSI# *
- #BEARER.MSISDN# *
- #HTTP.HOST#
- #HTTP.URL#
- #HTTP.URI#
- #RTSP.URI#

- #RULEBASE#

UPF は、N7 インターフェイスでリダイレクトされた URL に挿入するための次のダイナミックフィールドをサポートしています。

- #BEARER.IMSI# *
- #HTTP.URL#

UPF のリダイレクションと終了の仕組み

UPF は、service-scheme フレームワークを使用して具体的なポリシーイベントを検出します。次に、SMF から N4 インターフェイス経由で受信した ADC ダイナミックルールに基づいて、リダイレクションまたはフロー終了を実行します。

process_summary

このプロセスに関与する主要なコンポーネントは次のとおりです。

- PCF：複合リダイレクト URL またはブロック指示を含むダイナミックポリシーを提供します。
- SMF：N4 インターフェイス経由で UPF にポリシー情報をリレーします。
- UPF：リダイレクトと暗号化を実行し、ダイナミックデータを挿入し、ブロックされた通信の TCP シグナリング（FIN/RST）を管理します。

process_workflow

N7 インターフェイスによるリダイレクトまたは終了を有効にするワークフロー：

1. **service-scheme トリガー**：service-scheme フレームワークは、セッションの確立または変更中に far-received または pdr-received イベントを検出します。
2. **条件照合**：システムは、リダイレクト URL に returnURL や構成に基づいた具体的なキーワードが含まれているかどうかなどをチェックするなど、trigger-conditions を評価します。
3. **アクションの実行**：UPF は、セッションの確立または変更中に発生した adc ルールに基づいて特定の charging-action を指す、マッピングされた trigger-action を実行します。
4. **URL 処理**：リダイレクトの場合、UPF は実際の URL を抽出し、ダイナミックフィールドに入力し、暗号化を適用します。
5. **フロー管理**：終了の場合、UPF はTCP FIN を Web クライアントに送信します。また、TCP RST を Web サーバーに送信して、接続をグレースフルに終了します。

URL 暗号化を構成する

リダイレクトされた URL のダイナミックフィールドの暗号化を有効にするには、次の構成例を使用します。

```
configure
  active-charging service service_name
    charging-action charging_action_name
      flow action redirect-url redirect_url [ encryption { blowfish128
| aes256 } [ encrypted ] key key ]
    end
```

注：

- **flow action redirect-url** *redirect_url*：リダイレクト URL を指定します。最大 16 のダイナミックフィールドを含めることができます。*redirect_url* は、1 ～ 511 文字の英数字で指定する必要があります。
- **encryption { blowfish128 | aes256 } [encrypted] key** *key*：リダイレクト URL のダイナミックフィールドの暗号化を有効にする場合に指定します。
  - **blowfish128**：ダイナミックフィールドの暗号化に 128 ビットキーで Blowfish 暗号化を使用するために指定します。
  - **aes256**：ダイナミックフィールドの暗号化に 256 ビットキーで AES-CBC 暗号化を使用するように指定します。
  - **encrypted**：キーを暗号化する場合に指定します。
  - **key** *key*：ダイナミックフィールドの暗号化に使用するキーを指定します。*key* は、1 ～ 523 文字の英数字で指定する必要があります。
- リダイレクト先の URL でエンコーディングが有効になっている場合、暗号化された URL は、最大 2300 文字をサポートします。この長さを超えると、2301 文字以降の URL は切り捨てられます。

N7 ベースのリダイレクト フロー アクションを構成する

N7 インターフェイスを使用してダイナミックリダイレクト URL を処理し、暗号化を適用するように UPF を設定します。

Before you begin

- L7 アナライザがアクティブであることを確認します（HTTPS のサポートに必要）。
- AES 暗号化を使用する場合は、キーフレーズ（英数字、1 ～ 523 文字）を指定します。
- リダイレクト URL 列が 1 ～ 511 文字であることを確認します。

リダイレクト フロー アクションを構成するには、次の手順を実行します。

手順

ステップ 1 URL ID の ruledef を定義します。

例：

```
[upf] # ruledef rule_name
 [upf] #  http url contains test.html
 [upf] #  http url !contains abc.html
 [upf] #  multi-line-or all-lines
```

ステップ 2 リダイレクト URL の trigger-conditions を構成します。

例：

```
[upf] # trigger-condition TC1
 [upf] #  redirect-url contains "returnURL="
 [upf] #  redirect-url starts-with "https://snap"
```

ステップ 3 リダイレクションの trigger-actions を定義します。

例：

```
[upf] # trigger-action TA1
    [upf] #  execute-charging-action url_redirect_ca
```

ステップ 4 暗号化パラメータを使用して charging-action を作成します。

例：

```
[upf] # charging-action url_redirect_ca
[upf] #  flow action redirect-url <return url recieved over n4 interface with ADC rule>
```

ステップ 5 トリガーを service-scheme にバインドします。

例：

```
[upf] # service-scheme SS1
 [upf] #  trigger far-received
   [upf] #  priority 1 trigger-condition TC1 trigger-action TA1
```

終了フローアクションを構成する

TCP シグナリングを使用して通信ブロックを実装します。

Before you begin

フロー終了を構成するには、次の手順を実行します。

手順

ステップ 1 通信ブロックの ruledef を定義します。

例：

```
[upf] # ruledef terminate_rule
  [upf] #  ip any-match = TRUE
```

ステップ 2 終了の trigger-conditions を設定します。

例：

```
[upf] # trigger-condition TC2
  [upf] # tdf-appid contains <terminate app id recived with ADC dynamic rule over N4 interface>
```

ステップ 3 終了の trigger-actions を定義します。

例：

```
[upf] # trigger-action TA2
   [upf] #   execute-charging-action terminate_all
```

ステップ 4 フロー終了の charging-action を作成します。

例：

```
[upf] # charging-action terminate_all
   [upf] #  flow action terminate-flow
```

ステップ 5 トリガーを service-scheme にバインドします。

例：

```
[upf] # service-scheme SS1
[upf] #   trigger pdr-received
[upf] #   priority 2 trigger-condition TC2 trigger-action TA2
```

フロー統計のリダイレクトと終了

次のコマンドを使用して、機能の状態を確認し、リダイレクトまたは終了したフローの統計を表示できます。

サブスクライバ FAR の詳細

抽出されたリダイレクトURLと具体的なコールに適用された課金アクションを表示するには、次のシンタックスを使用します。

例：

```
[upf] # show subscribers user-plane-only callid [call_id] far full all
```

サンプル出力：

```
Callid: 00004e29
Interface Type: Sxb
 FAR-ID       : 0x0003
 Destination Interface : Core
 Apply Action     : FORWARD
 Outer Header Creation   :
 Remote TEID     : 0x0
 Transport Level Marking    : N/A
 Transport Level Marking Options :
   Copy Inner:                    No
   Copy Outer:                    No
 Inner Packet Marking           : N/A
 Layer2 Marking                 : N/A
 Remote IP Address   :
 Remote Port    : N/A
 Number of Associated PDRs: 1
 Linked Traffic Endpoint : 0x2
 Redirect Info  :
Redirect Address Type  : URL
Redirect Address Value :
https://snap.mobile.att.net/?nonce=ApolloHONDA&returnURL=https://myvehicle.att.com/%23/start%3Foem=honda
```

```
       Charging Action Name           : url_redirect_ca
```

トリガーアクションの構成

具体的なトリガーアクションにマッピングされている課金アクションを確認するには、次のシンタックスを使用します。

例：

```
[upf] # show user-plane-service trigger-action all
```

サンプル出力：

```
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
       Flow-IP-Readdressing         : Disabled
       EDNS-Encode                  : Disabled
       Charging-Action-Map          : none
       Charging-Action-Name         : url_redirect_ca

Trigger-Action: TA2
       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
       Flow-IP-Readdressing         : Disabled
       EDNS-Encode                  : Disabled
       Charging-Action-Map          : none
       Charging-Action-Name         : terminate_all
```

トリガー条件の詳細

課金アクションの選択に使用する条件を確認するには、次のシンタックスを使用します。

例：

```
[upf] # show user-plane-service trigger-condition all
```

サンプル出力：

```
Trigger-Condition: TC1
       redirect-url  contains returnURL=
       redirect-url  starts-with https://snap
       redirect-url  contains nonce=Name
       Multi-line-OR All lines : Disabled
```

```
Trigger-Condition: TC2
       Tdf-AppId  contains terminate_
       Multi-line-OR All lines : Disabled
```

グローバルリダイレクト統計

リダイレクトされたフローのグローバル数を表示するには、次のシンタックスを使用します。

例：

```
[upf] # show user-plane-service statistics all
```

サンプル出力：

```
ADC Redirect Stats:
    ADC Redirected Flows         : 3
```

終了したフロー数

具体的なコールに対して終了したフローの数を表示するには、次のシンタックスを使用します。

例：

```
[upf] # show subscribers user-plane-only full callid <call_id>
```

サンプル出力：

```
Flow Action Terminated Flows: 5
```

PDR 終了の詳細

フローの終了中に一致するパケット数と適用される課金アクションを表示するには、次のシンタックスを使用します。

例：

```
[upf] # show subscribers user-plane-only callid <call_id> pdr full all
```

サンプル出力：

```
Callid: 12345
Interface Type: Sxb
IP address: 11.11.0.1
PDR-ID:                   0x0003
Rule Name:               dynamicfacebook
Charging Action Name:      terminate_all
TDF App Id:   terminate_rule
TDF Notifications:   Enabled
Hits:                     5 Match Bypassed:            0
Matched Bytes:          285 Matched Packets:           5
```

HTTPS

UPF は、L7 アナライザの一部として HTTPS プロトコルをサポートします。

RTP/RTSP

UPF 2.0 は、L7 アナライザの一部として RTP および RTSP プロトコルをサポートします。

SIP

Session Initiation Protocol は、IETF で定義されているシグナリングプロトコルです。Internet Protocol（IP）を介した音声やビデオ通話などの通信セッションの制御に広く使用されています。このプロトコルは、2 者（ユニキャスト）またはマルチパーティ（マルチキャスト）セッションの作成、変更、および終了に使用できます。セッションは、1 つまたは複数のメディアストリームで構成されます。

UPF 2.0 は、L7 アナライザの一部として SIP をサポートしています。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できる CLI コマンドに関する情報を提供します。

show コマンドや出力

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

DNS

DNS 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name dns

FTP

FTP 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name ftp

HTTP

HTTPS 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name http

HTTPS

HTTPS 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name secure-http

RTP

RTP 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name rtp

RTSP

RTSP に関連する統計情報を取得するには、次の CLI コマンドを使用します。

- **show user-plane-service statistics analyzer name rtsp**

- **show user-plane-service statistics analyzer name rtsp verbose**

SIP

SIP 関連の統計を取得するには、次の CLI コマンドを使用します。

show user-plane-service statistics analyzer name sip

N4 での NAT サポート

表 *36 :* 機能の履歴

機能名	リリース情報	説明
N4インターフェイスでのNATサポート	2023.04	ネットワーク アドレス変換（NAT）機能は、ルーティング不可のプライベート IP アドレスをパブリック IP アドレスのプールからのルーティング可能なパブリック IP アドレスに変換します。 UPFFは、ネットワークアドレスを構成するN4インターフェイスの NAT をサポートし、NAT バインディングレコードを N4 に送信します。NAT ポリシーと NAT パブリック IP アドレスの IP プールは、N4 の UPF で構成されます。

機能説明

ネットワーク アドレス変換（NAT）機能は、ルーティング不可のプライベート IP アドレスをパブリック IP アドレスのプールからのルーティング可能なパブリック IP アドレスに変換します。この機能により、ユーザーは外部ネットワークとの通信に必要なパブリックIPアドレスの数を節約できます。この機能により、内部ネットワーク向けIPアドレススキーマとしてセキュリティを確保でき、外部ホストからマスキングされ、各送受信パケットがこの変換プロセスを通過します。

UPF は、N4 インストレーションで NAT をサポートし、ネットワークアドレスを構成します。NAT IP アドレスと NAT ポートを使用して、UE の送信元 IP または送信元ポートアドレスをカプセル化したデータパケットを自動的に転送するようにシステムを構成できます。

サポートされる NAT の組み合わせは次のとおりです。

- NAT44 オンデマンド多対 1

- NAT44 オンデマンド 1 対 1
- NAT64 オンデマンド多対 1
- NAT 64 オンデマンド 1 対 1
- NAT44 非オンデマンド多対 1
- NAT44 非オンデマンド 1 対 1
- NAT64 非オンデマンド多対 1
- NAT64 非オンデマンド 1 対 1

NAT の補足情報については、StarOS の『*NAT* アドミニストレーション ガイド』を参照してください。

注：StarOS の『*NAT* アドミニストレーション ガイド』に記載されているすべての機能が UPF に当てはまるわけではありません。

制限事項

N4 インターフェイスの NAT のサポートには次の制限事項があります。

- 多対 1 およびオンデマンドモードの NAT44 のみがサポートされます。
- すべての NAT プールは、接続先コンテキストの個別のユーザープレーンで設定されます。
- fw-and-nat ポリシーでの CLI アクション拒否を使用した課金アクション、および active-charging-service での flow-any-error 課金アクションはサポートされていません。
- 外部サーバーからの「dynamic-only」および「static-and-dynamic」ルールを使用して構成された access-rules はサポートされません。
- 同じレルムからの複数の IP はサポートされません。
- NAT プールでのネクストホップ転送はサポートされません。
- NAT プールのポート範囲はサポートされません。
- プライベート IP チェック CLI のスキップはされません。
- RADIUS および Gy で返される Fw-and-nat ポリシーベースの NAT ポリシーの適用はサポートされません。
- ベアラー固有のフィルタは、access-ruledef ではサポートされません。
- Access-rules は、fw-and-nat ポリシーでの open-port ポート範囲設定のトリガーをサポートしません。
- SR/ICSR 後の NAT ポートリカバリ（fw-and-nat アクション）はサポートされません。
- active-charging サービスでは、NAT reassembly timeout CLI はサポートされません。代わりに、UP の汎用コンテキストレベル CLI を使用する必要があります。
- NAT フラグメンテーション リアセンブルのエラーはサポートされません。

- NAT flow-mapping タイマーはサポートされません。
- N:M 冗化性の場合、各 UP ホストのインターフェイス設定の一部として RCM から設定される NAT IP プール、およびプール名は、すべてのアクティブなユーザープレーンで一意である必要があります。fw-and-nat ポリシーで参照される同じ NAT レルムをすべてのユーザープレーンに適用できるように、すべてのプールに NAT グループを使用することが必須になります。
- N:M 冗長化の場合、RCM 経由ですべての UP でまとめて設定される NAT IP プールの総数は、IP プールの最大制限数（2,000）に従う必要があります。すべてのアクティブ UP の累積合計が最大値を超えると、スタンバイユーザープレーンの設定は失敗します。

NAT の設定

NAT ポリシー（Firewall-and-NAT ポリシー）と access-ruledef 構成は、UPF の active-charging サービスで実行されます。

NAT 関連の CLI コマンドの詳細については、『*StarOS NAT* アドミニストレーション ガイド』の「*NAT* 構成」章を参照してください。

（注） 『*StarOS NAT* アドミニストレーション ガイド』の「*NAT* 構成」章に記載されているすべての CLI コマンドと構成が UPF に適用できるわけではありません。

設定例

ユーザープレーン

ISP コンテキストのユーザープレーンでは、次のプール関連の設定が必要です。

```
configure
   context ISP1-UP
      ip pool NAT44_PUBLIC1 209.165.200.225 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC2 209.165.200.226 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC3 209.165.200.227 255.255.255.224 napt-users-per-ip-address 2
 on-demand port-chunk-size 8 max-chunks-per-user 1 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC4 209.165.200.228 255.255.255.224 napt-users-per-ip-address 4
 on-demand port-chunk-size 32256 max-chunks-per-user 4 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC5 209.165.200.229 255.255.255.224 napt-users-per-ip-address
8064 on-demand port-chunk-size 8 max-chunks-per-user 2
      end
```

さまざまな NAT プールタイプの NAT プール関連の設定例

```
1-1 on-demand:
----------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_1_1 209.165.200.230 255.255.255.224 nat-one-to-one on-demand
```

```
nat-binding-timer 60
end

N-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_N_1 209.165.200.231 255.255.255.224 napt-users-per-ip-address 2
max-chunks-per-user 2 port-chunk-size 8
end

1-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_NOD_1_1 209.165.200.232 255.255.255.224 nat-one-to-one
end
```

Note コントロールプレーンの構成を追加して、1 つ以上のアクセスルール定義をユーザープレーンで設定された必要な NAT プールまたはグループにマッピングします。

モニタリングおよびトラブルシューティング

NAT 統計の収集

次の表に、NAT 統計の収集に使用できるコマンドを示します。

最初の列には収集する統計、2 つ目の列には使用するコマンドを挙げています。

統計/情報	show コマンド
アクティブまたは休止中のセッションがある、現在のすべてのサブスクライバに関する情報。サブスクライバに関連付けられている IP アドレスを確認します。NAT レルムで使用されているすべての IP アドレスも表示されます。	**show subscribers user-plane-only full all**
NAT サブシステムの統計情報。	**show user-plane-service statistics all**
NAT 関連のすべての統計。	**show user-plane-service statistics nat all**
NAT レルム関連のすべての統計。	**show user-plane-service statistics nat nat-realm all**
NAT IP プールグループ内のすべての NAT IP プールの統計。	**show user-plane-service statistics nat nat-realm** *pool_name*
生成された NAT バインドレコードに関する情報。	**show user-plane-service edr-format statistics all**
UP の APN で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service pdn-instance name** *name*

統計/情報	show コマンド
UP での fw-an-nat ポリシーの設定を確認します。	**show user-plane-service fw-and-nat policy all**
ポートチャンクの割り当ておよび解放のために生成された NAT バインドレコードに関する情報。	**show user-plane-service rulebase name** *name*
アクセス ruledef に関する情報。	**show user-plane-service ruledef all**
UP の rulebase で fw-and-nat ポリシーの関連付けを確認します。	**show user-plane-service rulebase name** *name*

clear コマンド

この機能をサポートする、次の clear CLI コマンドを使用できます。

- **clear user-plane-service statistics nat nat-realm all**
- **clear user-plane-service statistics nat all**

NAT パラメータしきい値の SNMP トラップ

NAT パラメータしきい値に対する次の SNMP トラップがサポートされます。

SNMP トラップ	説明
ThreshNATPortChunks	NAT ポートのチャンク使用率が、しきい値により設定された限度に達すると生成されます。
ThreshClearNATPortChunks	NAT ポートのチャンク使用率が、クリアしきい値により設定された限度に達すると生成されます。
ThreshNATPktDrop	NAT パケットドロップが、しきい値により設定された限度に達すると生成されます。
ThreshClearNATPktDrop	NAT パケットドロップが、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolUsed	IP プールで使用されている IP の数が、しきい値により設定された限度に達すると生成されます。
ThreshClearIPPoolUsed	IP プールで使用されている IP の数が、クリアしきい値により設定された限度に達すると生成されます。
ThreshIPPoolFree	IP プールが解放され、しきい値が定める限度に達すると生成されます。
ThreshClearIPPoolFree	IP プールが使用され、クリアしきい値が定める限度に達すると生成されます。

SNMP トラップ	説明
ThreshIPPoolAvail	IP プールが次のフローで使用可能になり、設定されたしきい値に達すると生成されます。
ThreshClearIPPoolAvail	IP プールが使用され、設定されたしきい値に達すると生成されます。

注：これらのトラップを有効にするには、それぞれのCLIをユーザープレーンで設定する必要があります。

バルク統計

NAT レルムスキーマ

NAT レルムはユーザープレーンで設定され、統計情報はコンテキストごと、レルムごとに保存されます。これらの統計変数（累積とスナップショットの両方）は、NAT レルムスキーマで使用できます。

***Table 37: NAT* レルムスキーマ**

変数名	データ型	カウンタタイプ	説明
Vpnname	文字列	情報	コンテキスト名
Realmname	文字列	情報	レルム名。
nat-rlm-bind-updates	Int64	カウンター	送信された暫定AAA NBUの合計。
nat-rlm-bytes-txferred	Int64	カウンター	レルムによって転送されたNAT44およびNAT64バイトの合計数（アップリンク+ダウンリンク）。
nat-rlm-bytes-nat44-tx	Int64	カウンター	レルムによって転送されたNAT44バイトの合計数。
nat-rlm-bytes-nat64-tx	Int64	カウンター	レルムによって転送されたNAT64バイトの合計数。
nat-rlm-ip-flows	Int64	カウンター	レルムで使用されたNAT44およびNAT64フローの総数。
nat-rlm-nat44-flows	Int64	カウンター	レルムによって処理されたNAT44フローの総数。
nat-rlm-nat64-flows	Int64	カウンター	レルムによって処理されたNAT64フローの総数。

変数名	データ型	カウンタタイプ	説明
nat-rlm-ip-denied	Int32	カウンター	NAT IP アドレスが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-ip-denied-nat44	Int64	カウンター	IP が拒否された NAT44 フローの総数。
nat-rlm-ip-denied-nat64	Int64	カウンター	IP が拒否された NAT64 フローの総数。
nat-rlm-port-denied	Int32	カウンター	ポートが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-port-denied-nat44	Int64	カウンター	ポートが拒否された NAT44 フローの総数。
nat-rlm-port-denied-nat64	Int64	カウンター	ポートが拒否された NAT64 フローの総数。
nat-rlm-memory-denied	Int64	カウンター	メモリが拒否された NAT44 および NAT64 フローの総数。
nat-rlm-memory-denied-nat44	Int64	カウンター	メモリが拒否された NAT44 フローの総数。
nat-rlm-memory-denied-nat64	Int64	カウンター	メモリが拒否された NAT64 フローの総数。
nat-rlm-ttl-ips	Int32	ゲージ	NAT レルムあたりのコンテキストごとの NAT パブリック IP アドレスの総数。スタティック値です。
nat-rlm-ips-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに、現在使用されている NAT IP アドレスの総数。
nat-rlm-current-users	Int32	ゲージ	NAT レルムを現在使用しているサブスクライバの総数。
nat-rlm-ttl-port-chunks	Int32	ゲージ	NAT レルムあたりのコンテキストごとのポートチャンクの総数。スタティック値です。
nat-rlm-chunks-in-use	Int32	ゲージ	NAT レルムあたりのコンテキストごとに現在使用されているポートチャンクの総数。

変数名	データ型	カウンタタイプ	説明
nat-rlm-port-chunk-size	Int32	ゲージ	NAT レルムのポートチャンクのサイズ。
nat-rlm-port-chunk-average-usage-tcp	Int32	ゲージ	割り当てられた TCP ポートの平均 TCP ポート使用率。つまり、割り当てられた TCP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-udp	Int32	ゲージ	割り当てられた UDP ポートの平均 UDP ポート使用率。つまり、割り当てられた UDP ポートのうち、使用された数。パーセンテージ値ではありません。
nat-rlm-port-chunk-average-usage-others	Int32	ゲージ	割り当てられた他のポートでの他の（ICMP または GRE）ポートの平均使用率（つまり、割り当てられた「他の」ポートのうち、使用された数）。パーセンテージ値ではありません。
nat-rlm-max-port-chunk-subs	Int64	カウンター	最大数のポートチャンクを使用したサブスクライバの総数。
nat-rlm-max-port-chunk-used	Int32	カウンター	使用された最大ポートチャンク数。
nat-rlm-max-cur-port-chunk-subs	Int64	ゲージ	ポートチャンクの最大数を使用している現在のサブスクライバ数。
nat-rlm-max-cur-port-chunk-used	Int32	ゲージ	アクティブなサブスクライバによって使用された最大ポートチャンク数。

NAT バインドレコード

NAT IP アドレスまたは NAT ポートチャンクがサブスクライバとの間で割り当てまたは割り当て解除されるたびに、NAT バインドレコード（NBR）を生成できます。NBR の生成は、ファイアウォールと NAT ポリシーの設定で設定できます。

NBR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,
sn-server-port,sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,
sn-nat-realm-name,sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,
```

```
sn-nat-port-chunk-alloc-time-gmt,sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
,,,209.165.200.225,,,,209.165.201.1,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,1,02/18/2020
06:41:08,,,
,,,209.165.200.225,,,,209.165.201.2,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,1,02/18/2020
 06:41:14,,,
,,,209.165.200.225,,,,209.165.201.3,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,0,02/18/2020
06:41:08,02/18/2020 06:42:12,,
,,,209.165.200.225,,,,209.165.201.14,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,0,02/18/2020
 06:41:14,02/18/2020 06:44:24,,
```

EDR

通常の EDR では、次の NAT 固有の属性がサポートされています。

- sn-nat-subscribers-per-ip-address：NAT IP アドレスごとのサブスクライバ
- sn-subscriber-nat-flow-ip：NAT 対応サブスクライバの NAT IP アドレス
- sn-subscriber-nat-flow-port：NAT 対応サブスクライバの NAT ポート番号

EDR の例

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,sn-server-port,
sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,sn-nat-realm-name,
sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,sn-nat-port-chunk-alloc-time-gmt,
sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
02/18/2020 12:11:11:630,02/18/2020
12:11:11:632,1,209.165.200.225,209.165.201.1,0,0,,,,209.165.200.230,1024,,2,,,,,,0,0
02/18/2020 12:11:08:672,02/18/2020
12:11:09:671,6,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.230,1034,,2,,,,,,0,0
02/18/2020 12:11:14:499,02/18/2020
12:11:14:499,17,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.240,1025,,8064,,,,,,0,0
```

パケットドロップ EDR

パケットドロップ *EDR* の例

```
#sn-nat-no-port-packet-dropped,sn-start-time,sn-end-time,sn-subscriber-imsi
2,03/13/2020 08:28:24,03/13/2020 08:28:54,123456789012345
```

テザリング検出

機能説明

テザリングとは、モバイルスマートフォンを USB ドングルまたはモデムとして使用して、スマートフォンのデータプランで実行されている PC デバイス（ラップトップ、PDA、タブレットなど）へのインターネット接続を提供することを指します。通常、スマートフォンユーザーの場合、ほとんどのオペレータが無制限のデータプランを設定しており、その使用量はモバイルデバイスとしてのスマートフォンから行うことを目的としています。ただし、一部のサブスクライバは、低コストまたは無制限の使用量データプランを使用して、ブロードバンドまたは Wi-Fi を介した通常のインターネット接続がコストかかるか、利用できないか、または安全でない場所でラップトップにインターネット接続ています。

テザリング検出機能を使用すると、PC デバイスからモバイルスマートフォンにテザリングされたサブスクライバデータ通信の検出が可能になります。また、サービスプロバイダーがこのような通信量を管理し、それに応じてサブスクライバに請求できるよう、効率的なレポートを提供します。テザリング検出は、IPv4（TCP）および IPv6 通信フローでサポートされています。

このリリースでは、IP-TTL ベースのテザリングがサポートされています。この機能は、rulebase レベルで設定でき、rulebase 内に IP-TTL 設定を持つすべてのサブスクライバのすべてのフローに適用されます。

テザリングサポートを構成する

この項では、テザリングサポート機能の構成方法について説明します。

テザリングサポート機能の構成には、以下の手順が含まれます。

- テザリングの rulebase 構成
- テザリングの Ruledef の構成
- テザリングの EDR の構成

テザリングの rulebase 構成

次のコマンドを使用して、テザリングに向けて rulebase パラメータを構成します。

```
configure
  active-charging service service_name
    rulebase rulebase_name
      tethering-detection ip-ttl valuettl_value
      end
```

注：

- **tethering-detection**：このコマンドを使用すると、現在の rulebase および使用する具体的なデータベースに対してテザリング機能を有効または無効にできます。
- **ip-ttl value** *ttl_value*：IP-TTL 構成を使用して、テザリング検出を実行するかを指定します。*ttl_value* は、1 ～ 255 の整数で指定し、テザリングフローの TTL 値を設定します。

テザリングの Ruledef の構成

次のコマンドを使用して、テザリングに向けて ruldef パラメータを構成します。

```
configure
  active-charging serviceservice_name
    ruledef ruledef_name
      ip any-match operator_condition
      tethering-detection ip-ttl flow-tethered
      end
```

注：

- **ip any-match** *operator_condition*：このコマンドは、すべての IPv4 および IPv6 パケットと一致するようにルール式を定義します。
- **ip-ttl**：各 IP-TTL 値ごとにテザリングされたフローまたはテザリングされていないフローを選択することを指定します。
- **flow-tethered**：テザリングがフローで検出された場合、照合するように指定します。

テザリングの EDR の構成

次のコマンドを使用して、テザリング用に EDR を設定します。

```
configure
  active-charging service service_name
    edr-format format_name
      rule-variable flow tethered-ip-ttl priority priority_value
      rule-variable flow ttl priority priority_value
      end
```

注：

- **edr-format** *format_name*：EDR フォーマットを構成します。
- **flow**：EDR でフィールド関連のフローを構成します。
- **tethered-ip-ttl**：フローで IP-TTL ベースのテザリングが検出されます。
- **ttl**：フローの最初のパケットで受信した Time To Live/最大ホップ数の値。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できる CLI コマンドに関する情報を提供します。

show コマンドや出力

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show user-plane-service statistics tethering-detection

この機能をサポートするために、次のフィールドが表示されます。

- 現在のテザリングされたサブスクライバの数
- テザリングされたサブスクライバの総数
- スキャンされたフローの総数
- 検出されたテザリングフローの総数
- 回復されたテザリングフローの総数
- スキャンのためにバイパスされたフローの総数
- テザリング検出統計（ip-ttl）

- スキャンされたフローの総数
- テザリングされたフローの検出数
- テザリングされたアップリンクパケット
- テザリングされたダウンリンクパケット

show user-plane-service statistics rulebase name rulebase_name

この機能をサポートするために、次のフィールドが表示されます。

- テザリング検出（ip-ttl）
  - スキャンされたフローの総数
  - テザリングされたフローの検出数
  - テザリングされたアップリンクパケット
  - テザリングされたダウンリンクパケット

RTP ダイナミックフローの検出

rtp dynamic-flow-detection CLI コマンドは、[ACS Rulebase Configuration] モードで、Real Time Streaming Protocol（RTSP）および Session Description Protocol（SDP）アナライザが子 RTP および RTCP フローを検出できるようにします。RTSP/SIP および SDP アナライザを設定し、**rtp dynamic-flow-detection** CLI が存在していれば、RTP/RTCP の明示的な設定は必要ありません。**rtp dynamic-flow-detection** CLI コマンドを使用すると、子 RTP または RTCP フローが親 RTSP/SIP-SDP フローと相互に関連付けられます。

親フロー（RTSP/SIP-SDP）がクリアされると、子 RTP/RTCP フローもクリアされます。この CLI がない場合、RTP および RTCP の L7 レイヤ分析には、別途アナライザの設定が必要です。RTP/RTCP フローと RTSP/SIP-SDP フローとの相関関係はありません。

ベアラー固有フィルタのルール照合

ベアラー固有フィルタのルール照合機能には、次のようなものがあります。

- IMSI ベースのルールは、サブスクライバの IMSI に従って照合されます。
- APN ベースのルールを使用すると、ベアラーフローのアクセスポイント名（APN）と一致するルール式を定義できます。
- RAT タイプを使用すると、ベアラーフロー内の無線アクセス技術（RAT）に一致するルール式を定義できます。

IMSI プールを構成する

IMSI プールを設定するには、次の CLI コマンドを使用します。

```
configure
  active-charging service service_name
    imsi-pool pool_name
      imsi { imsi_number | range start_imsi to end_imsi }
```

imsi-pool には、IMSI 値または IMSI の範囲を含めることができます。

Rule-line ACS ruledef を構成する

次の CLI コマンドを使用して、ACS Ruledef で構成モードで rule-line を設定します。

```
configure
  active-charging service service_name
    ruledef ruledef_name
      bearer 3gpp imsi { = imsi_value } | { range imsi-pool pool_name }
      bearer 3gpp apn operator apn_name
      bearer 3gpp rat-type operator rat_type
```

IMSI 範囲は、IMSI プールを使用してルール内で設定できます。

bearer 3gpp rat-type *operator rat_type*：

- *operator* は次のいずれかになります。
  - **!+**：等しくない
  - **=**：等しい
- **注意**：このリリースでは、**wlan** は、適格な *rat_type* です。

HTTP Content-Type を構成する

次の CLI コマンドを使用して、HTTP Content-Type entity-header フィールドの値に一致するルール式を定義します。

```
configure
  active-charging service service_name
    ruledef ruledef_name
      http content type [ case-sensitive ] operator content_type
```

show CLI

UPF で **show user-plane-service imsi-pool name** *pool_name* CLI を使用して、サービスで構成された IMSI プール に関する情報を表示します。

アップリンクパケットの IP 送信元違反検出の有効化

表 *38 :* 機能の履歴

機能名	リリース情報	説明
アップリンクパケットの IP 送信元違反検出を有効にする	2024.03.0	cnSGWc のこの機能により、UPF は、アップリンクパケットの発信元が正しいサブスクライバからのものであるかどうかをチェックできます。 この機能は次をサポートします： • この機能により、権限のない関係者へのデータの漏洩を防止することで、セキュリティとサブスクライバのプライバシーが強化されます。この機能は、合法的傍受要件に準拠することにより、サービスプロバイダーの法的および規制的問題のリスクをさらに軽減します。 • cnSGW がセッションに割り当てたトンネルエンドポイント識別子（TEID）の再利用をセッション終了まで遅延させることで、誤ったサブスクライバのタッピング、パケット誤アソシエーションリスク、および合法的傍受（LI）機関による報告を防止します。 この機能は、既存の CLI コマンド **show subscribers user-plane-only full all | callid** *callid* を使用して、構成された **IP Source Violation Action** オプションを表示します。 **デフォルト設定**：無効：有効にするには設定が必要。

IP 送信元違反検出機能が cnSGW で有効になっています。この情報は、cnSGWc から UPF に伝達されます。パケットを無視または破棄する cnSGW の構成に基づいて、ユーザープレーンはソース違反パケットに対処します。

UE がネットワークに接続したら、cnSGW は新しいセッションに一意のトンネルエンドポイント識別子（TEID）を割り当て、UPF への Create Session 要求メッセージに TEID を含めます。

UPF はセッションの確立を確認し、TEID を使用してユーザー データパケットをルーティングします。

この機能により、cnSGW がサブスクライバごとのセッションに割り当てるトンネルエンドポイント識別子（TEID）は、セッションが終了するまで別のサブスクライバですぐに再利用されません。遅延 TEID 再利用により、LI エージェンシーによる誤ったサブスクライバのタップと報告が回避されます。

ユーザープレーンでの IP 送信元違反は、**show subscribers user-plane-only full all | callid** *call_id* CLI コマンドを使用して確認できます。

IP 送信元違反のアップリンクパケットの検証の詳細については、『*cnSGWc* 構成とアドミニストレーション ガイド』の「IP 送信元違反のアップリンクパケットの検証」を参照してください。

アップリンクパケットの IP 送信元違反の有効化の仕組み

この機能を有効または無効にする場合の重要なポイントは次のとおりです。

- デフォルトでは、この機能はディセーブルになっています。
- この機能が IGNORE オプションとともに有効になっている場合、パケットは無効な送信元 IP アドレスに対して検証されます。対応する統計がそれに応じて増加します。ただし、IP が無効であるため、パケットに対するアクションはありません。
- この機能が DISCARD オプションとともに有効になっている場合、無効な送信元 IP アドレスを持つパケットは廃棄されます。対応する統計がそれに応じて増加します。

アップリンクパケットの IP 送信元違反を確認する

UPF でこの手順を使用して、cnSGWc で構成した値で、IP 送信元違反機能が有効になっているか、無効になっているかを確認します。

手順

show subscribers user-plane-only full all | callid <>を入力します。

例：

```
show subscribers user-plane-only full all | callid <>
```

新しいカウンタ **ip source violations ignored:<>** が追加され、無視または転送された IP 送信元違反パケットの数を表示できるようになりました。

以下は、**show subscribers user-plane-only full all | callid <>** CLI コマンドの出力例です。ここでは、**IP Source Violation Action**、**ip source violations** および **ip source violations ignored** の値が構成されています。

```
show subscribers user-plane-only full all
  Local SEID      : [0x0004000000000000] 1125899906842624
  Remote SEID     : [0x0004000000000005] 1125899906842629
  State           : Connected
  Connect Time    : Wed Jun  5 05:09:22 2024
  Idle time       : 00h11m19s
```

```
Access Type: n/a                        Network Type: IP
user-plane-service-name: UP21
active-service-scheme-name:
Callid: 00004e21
Rulebase:
Interface Type: Sxa
eMPS Session: No
eMPS Session Priority: 0
Session-Type: normal
Precedence-order: 0
Data Queue: 0
Card/Cpu: 1/0                           Sessmgr Instance: 1
IP address: n/a
Next Hop Ip Address: n/a
Source context: EPC2-UP                 Destination context: EPC2-UP
PDN-Instance: n/a
User-plane-Sx-addr: 20.20.20.106
Control-plane-Sx-addr: 20.20.20.101
Number of associated PDRs : 2
Number of associated ADC PDRs : 0
Number of associated FARs : 2
Number of associated QERs : 0
Number of associated BARs : 0
Number of associated URRs : 1
Uplink APN AMBR (bps) : 0       Downlink APN AMBR (bps) : 0
active input acl: n/a                active output acl: n/a
active input ipv6 acl: n/a             active output ipv6 acl: n/a
Bandwidth Policy: n/a
FW-and-NAT Policy: n/a
FW-and-NAT Policy ID: n/a
Firewall Policy IPv4: n/a
Firewall Policy IPv6: n/a
NAT Policy NAT44: n/a
NAT Policy NAT64: n/a
Converged Session: No                  Converged Peer Callid:      n/a
Visited Call: No
IP Source Violation Action: DISCARD
Subscriber Parameters:
IMSI: 404005123456789
IMEI: 112233445566778
MSISDN: 9890098900
Rat Type: 6
Old Rat Type: n/a
CF Policy ID: n/a
GX CF Policy ID: n/a
Roaming Status: n/a
Old Roaming Status: n/a
input pkts: 5                                   output pkts: 0
input bytes: 250                                output bytes: 0
input bytes dropped: 123                        output bytes dropped: 0
input pkts dropped: 3                           output pkts dropped: 0
CF Buffered Uplink Packets: 0                   CF Buffered Downlink Packets: 0
CF Buffered Uplink Bytes: 0                     CF Buffered Downlink Bytes: 0
Uplink Packets in Buffer: 0                     Downlink Packets in Buffer: 0
Buff Over-limit Uplink Pkts: 0                  Buff Over-limit Downlink Pkts: 0
DDN buffered pkts : 0                           DDN buffered bytes : 0
DDN buffer overflow drop pkts : 0               DDN buffer overflow drop bytes : 0
pk rate from user(bps): 0                       pk rate to user(bps): 0
ave rate from user(bps): 0                      ave rate to user(bps): 0
sust rate from user(bps): 0                     sust rate to user(bps): 0
pk rate from user(pps): 0                       pk rate to user(pps): 0
ave rate from user(pps): 0                      ave rate to user(pps): 0
sust rate from user(pps): 0                     sust rate to user(pps): 0
ipv4 bad hdr: 0                                 ipv4 ttl exceeded: 0
```

```
  ipv4 fragments sent: 0                          ipv4 could not fragment: 0
  ipv4 bad length trim: 0
  ipv4 input mcast drop: 0                        ipv4 input bcast drop: 0
  input pkts dropped (0 mbr): 0                   output pkts dropped (0 mbr): 0
  ipv4 input acl drop: 0                          ipv4 output acl drop: 0
  ipv6 input acl drop: 0                          ipv6 output acl drop: 0
  ip source violations: 3                         ipv4 output no-flow drop: 0
  ipv6 bad hdr: 0                                 ipv6 bad length trim: 0
  ip source violations ignored: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Uplink Pkts Drop: 0                     APN AMBR Downlink Pkts Drop: 0
  APN AMBR Uplink Bytes Drop: 0                    APN AMBR Downlink Bytes Drop: 0
  APN AMBR Uplink Pkts IP pref lowered: 0          APN AMBR Downlink Pkts IP pref lowered: 0

  APN AMBR Uplink Bytes IP pref lowered: 0         APN AMBR Downlink Bytes IP pref lowered: 0

  ITC Uplink Pkts Drop: 0                          ITC Downlink Pkts Drop: 0
  ITC Uplink Bytes Drop: 0                         ITC Downlink Bytes Drop: 0
  ITC Uplink Pkts IP pref lowered: 0               ITC Downlink Pkts IP pref lowered: 0
  ITC Uplink Bytes IP pref lowered: 0              ITC Downlink Bytes IP pref lowered: 0
  ITC Terminated Flows:: 0                         ITC Redirected Flows: 0
  Flow Action Terminated Flows: 0                  Flow Action Redirected Flows: 0
  ToS marked Uplink Pkts: 0                        ToS marked Downlink Pkts: 0
  CC Dropped Uplink Pkts: 0                        CC Dropped Downlink Pkts: 0
  CC Dropped Uplink bytes: 0                       CC Dropped Downlink Bytes: 0
  Uplink Inflight Pkts: 0                          Downlink Inflight Pkts: 0
  QFI Mismatch Uplink Pkts Drop: 0                 QFI Mismatch Downlink Pkts Drop: 0
  Total QoS-Group(s) Active: 0
  DNS-to-EDNS Uplink Pkts: 0                     DNS-to-EDNS Uplink Bytes: 0
  EDNS Response Received: 0

  Flow information:
    Current Active Flows:
      TCP: 0
      UDP: 0
    Total Flows:
      TCP: 0
      UDP: 0
      FP:  0

Static & Predef Rule Match stats:
Rule Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------  ------------------

Dynamic Rule Match stats:
PDR Id   Rule Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------- -------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------
0x0002   N/A                         0          0          5        250          0              0
       0/0               5/250

Post-Processing Rule Match stats:
Rule Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------  ------------------

Firewall-NAT Access Rule Match stats:
Firewall-Ruledef Name Pkts-Down Bytes-Down    Pkts-Up   Bytes-Up Dr-Pkts-Dn Dr-Byts-Dn Dr-Pkts-Up
Dr-Byts-Up       Hits
-------------------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
```

```
---------- ----------

QoS-Group Statistics:
QGR Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
--------------------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------  -----------------

SGACL Match stats:
ACL Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
--------------------- ---------- ---------- ---------- ---------- -------------

  CIoT APN Rate Control:
    Allowed UL Limit:   0                          Allowed DL limit:    0
    Remaining UL Limit: 0                          Remaining DL limit:  0
    Allowed Time unit: unrestricted                Status Validity Time: N/A

Total subscribers matching specified criteria: 1
```

URL のブロックリスト登録登録

機能説明

URL ブロックリスト登録機能は、URL または URI がブロックリストに登録されている Web サイトからコンテンツを表示またはダウンロードするためのサブスクライバのアクセスを規制します。この機能では、検出された URL がブロック対象として分類されているかどうかを示す URL のリストを記録するデータベースが使用されます。

機能の仕組み

UFP で URL ブロックリスト登録機能を有効にするには、フラッシュ、SFTP、またはそのサブディレクトリ内に「optblk.bin」という名前の URL ブロックリスト登録データベースが存在する必要があります。このデータベースディレクトリのパスは、ユーザープレーンのサービス起動後に、ユーザープレーンで設定する必要があります。

HTTP アナライザの URL ブロックリスト登録を有効にする必要があります。HTTP アナライザは、受信した HTTP リクエストデータパケットから URL 情報を抽出します。抽出された URL コンテンツが、URL ブロックリスト登録データベースと比較されます。受信した HTTP データパケットの URL がデータベースの URL エントリと一致すると、その URL はブロックリスト登録された URL として扱われ、該当する HTTP パケットに対して次のいずれかのアクションが実行されます。

- フローの終了
- パケットの破棄

URL ブロックリスト登録構成は、コントロールプレーン（CP）の Active Charging Service の Rulebase 設定で構成する必要があります。さらに、Active Charging Service レベルの構成では、Exact と Generic の 2 つのブロックリスト登録メソッドがサポートされています。



重要 ブロックリスト登録データベースは、IWF（Internet Watch Foundation）およびNCMEC（National Center for Missing and Exploited children）によって提供されます。UPF は常に、最適化されたフォーマットでブロックリスト登録データベースを受信します。

URL ブロックリスト登録データベースのアップグレード

次の 2 つの方法による URL データベースのアップグレードがサポートされます。

- タイマーベースのアップグレードまたは自動アップグレード
- CLI ベースのアップグレードまたは手動アップグレード

タイマーベースのアップグレードまたは自動アップグレード

データベースがシャーシに初めてロードされると、5 分間のタイマーが開始されます。このプロセスは、データベースを自動アップグレードするために開始されるものです。

タイマー終了時に、ディレクトリパスに有効なデータベースのより上位のバージョンがある場合には、データベースのアップグレード手順が開始され、新しいバージョンのデータベースが UPF にロードされます。

URLブロックリスト登録データベースをアップグレードするには、「optblk_f.bin」という名前の有効な URL ブロックリスト登録データベースの上位バージョンが、現在のデータベース「optblk.bin」と同じディレクトリ内にある必要があります。

データベースが正常にアップグレードされると、以前の「optblk.bin」ファイルの名前が「optblk_0.bin」に変更され、「optblk_f.bin」ファイルの名前が「optblk.bin」に変更されます。すると、「optblk_0.bin」ファイルは、古いデータベースのバックアップファイルとして扱われます。

追加のアップグレードが実行されると、「optblk_0.bin」ファイルの名前は「optblk_1.bin」に変更され、現在の「optblk.bin」ファイルの名前は「optblk_0.bin」に変更されます。

データベースに保存するバックアップファイルの数を構成するには、「*UPF* で *URL* ブロックリスト登録データベースを読み込む」 項を参照してください。

CLI ベースのアップグレードまたは手動アップグレード

現在のデータベースを新しいバージョンにアップグレードするには、「*URL* ブロックリスト登録 データベースをアップグレードする」項を参照してください。

URL ブロックリスト登録を構成する

UPF で URL ブロックリスト登録データベースを読み込む

次の構成を使用して、UPF で URL ブロックリスト登録データベース読み込みます。

2022.01.0 より前のリリース：

```
configure
  url-blacklisting database directory path database_directory_path
  url-blacklisting database max-versions max_version_value
  end
```

2022.01.0 以降のリリース：

```
configure
  url-blockedlisting database directory path database_directory_path
  url-blockedlisting database max-versions max_version_value
  end
```

注：

- **database directory path**：データベースのディレクトリパスを設定します。

  database_directory_path は、1 ～ 255 文字の文字列です。

- **max-versions**：データベースの最大アップグレードバージョンを設定します。

  max_version_value は 0 ～ 3 の整数です。

URL ブロックリスト登録データベースをアップグレードする

この構成を利用して、URLブロックリスト登録データベースを手動でアップグレードします。

2022.01.0 より前のリリース：

```
upgrade url-blacklisting database
end
```

2022.01.0 以降のリリース：

```
upgrade url-blockedlisting database
end
```

URL ブロックリスト登録を有効にするための構成

次の構成を使用して、UPF で URL ブロックリスト登録機能を有効にします。

2022.01.0 より前のリリース：

```
configure
  active-charging service service_name
    url-blacklisting match-method [ exact | generic ]
    rulebase rulebase_name
      url-blacklisting action [ discard | terminate-flow ]
      end
```

2022.01.0 以降のリリース：

```
configure
  active-charging service service_name
    url-blockedlisting match-method [ exact | generic ]
    rulebase rulebase_name
      url-blockedlisting action [ discard | terminate-flow ]
      end
```

注：

- **match-method [exact | generic]**：URL ブロックリスト登録に使用する一致メソッドを指定します。
  - **exact**：URL ブロックリスト登録が、URL の完全一致を実行します。
  - **generic**：URL ブロックリスト登録が、URL の汎用一致を実行します。
- **url-blockedlisting action [discard | terminate-flow]**:
  - **discard**：受信した HTTP パケットを破棄します。
  - **terminate-flow**：受信した HTTP パケットのフローを終了します。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングとトラブルシューティングのサポートに使用できる CLI コマンドに関する情報を提供します。

show コマンドや出力

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show user-plane-service url-blacklisting database

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト静的評価データベース：
  - 前回のアップグレードステータス
  - パス
    - データベースステータス
    - DB 内の URL の数
    - タイプ
    - バージョン
    - 作成時間
    - ホスト名
    - コメント
    - 最終アクセス時刻
    - 最終変更時刻
    - ステータスの最終変更時刻

show user-plane-service url-blacklisting database url database_directory_path

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト静的評価データベース：
  - 前回のアップグレードステータス
  - パス
    - データベースステータス
    - DB 内の URL の数
    - タイプ
    - バージョン
    - 作成時間
    - ホスト名
    - コメント
    - 最終アクセス時刻
    - 最終変更時刻
    - ステータスの最終変更時刻

show user-plane-service url-blacklisting database facility sessmgr all

この機能をサポートするために、次のフィールドが表示されます。

- URL-Blacklisting SessMgr Instance Based Database Configuration
  - SessMgr Instance
  - BL DB Load Status
  - BL DB Version
  - Number of URLs
  - チェックサム

show user-plane-service rulebase name rulebase_name

この機能をサポートするために、次のフィールドが表示されます。

- URL-Blacklisting Action
- URL-Blacklisting Content ID

show user-plane-service inline-services info

この機能をサポートするために、次のフィールドが表示されます。

- URL ブラックリスト：有効
  - URL ブラックリストの照合方法：汎用

show user-plane-service inline-services url-blockedlisting statistics

この機能をサポートするために、次の情報が表示されます。

- 累積 URL ブロックリスト登録の統計
  - ブロックリストに登録された URL のヒット数
  - ブロックリストに登録されていない URL 数
  - 一致したルールベースの総数

show user-plane-service inline-services url-blacklisting statistics rulebase name rulebase_name

この機能をサポートするために、次のフィールドが表示されます。

- ルールベース名
  - URL ブラックリストの統計情報
  - ブラックリストに登録された URL のヒット数
  - ブラックリストに登録された URL の欠落数
- 一致したルールベースの総数

静的ルールと事前定義済みルールを構成する

この項では、課金アクション構成で静的ルールと事前定義済みルールを構成する方法について説明します。

```
configure
   active-charging service service_name
      charging-action charging_action_name
         flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
         end
```

注：

- **flow action**：ルール定義に一致するパケットで実行するアクションを指定します。

- **discard [downlink | uplink]**：ダウンリンクまたはアップリンクのパケットを破棄することを指定します。
- **redirect-url** *redirect_url*：リダイレクトする URL を指定します。例：http://search.com/subtarg=#HTTP.URL#
- **terminate-flow**：終了するフローを指定します。

• redirect-url の場合は、rulebase で HTTP アナライザを構成します。例：

```
route priority 70 ruledef http-port analyzer HTTP
   ruledef http-port
   tcp either-port = 80
   rule-application routing
   exit
```

DPI 向け L7 プロトコルの ACS Ruledef を構成する

は、プロトコル フィールドと状態情報に基づいた複数の L3 ～ L7 プロトコルにおける一連の一致条件を表します。各 ruledef は、アクティブな課金サービス内の複数のルールベースで使用できます。

（注） UPF では、アクティブなコールおよびデータフロー中に ruledef 内のルール行の追加または削除が行われた場合、この構成変更は現在のフローには適用されません。ただし、構成変更は、新しいコールと同じコールの新しいフローに適用されます。

以下は、ACS ルール定義を作成、構成、または削除する方法を示す構成例です。

```
configure
   active-charging service service_name
      ruledef ruledef_name
        dns { any-match value | query-type query_type | query-name query_name
 }
         ip any-match [ = | != ] [ TRUE | FALSE ]
         ip dst-address { operator { { ipv4_address | ipv6_address } | {
ipv4_address/mask | ipv6_address/mask} | address-group ipv6_address } | { !range
 | range } host-pool host_pool_name }
         ip server-ip-address { operator { { ipv4_address | ipv6_address } |
{ ipv4_address/mask | ipv6_address/mask} | address-group ipv6_address } | { !range
 | range } host-pool host_pool_name }
         multi-line-or all-lines
         rule-application { charging | post-processing | routing }
         { tcp | udp } { either-port port_number }
         end
```

注：

- **ruledef** *ruledef_name*：追加、設定、または削除する ruledef を指定します。 *ruledef_name* は ACS ルールデ の名前である必要があります。また、1 ～ 63 文字の英数字の文字列である必要があり、句読点を含めることができます。各 ruledef には一意の名前を付ける必要があります。ホストプール、ポートマップ、IMSI プール、ファイアウォール、ルーティング、および課金のルール定義には一意の名前を付ける必要があります。
- 指定された ruledef が存在しない場合は作成され、CLI モードは ruledef を設定できる ACS Ruledef 構成モードに変わります。
- 指定された ruledef がすでに存在する場合、CLI モードはその ruledef の AACS Ruledef 構成モードに変わります。ACS Ruledef 構成モードを使用して、個々のルール定義（ruledef）でルール式を作成および管理します。
- **ip any-match [= | !=] [TRUE | FALSE]:** ：このコマンドは、IPv4/IPv6 パケットに一致するルール式を定義します。コマンドの 演算子 と 条件 は、次を指定します。
  - 演算子
    - != : 等しくない
    - <=: 等しい
  - 条件
    - FALSE
    - TRUE
- **ip dst-address {** *operator* **{ {** *ipv4_address* **|** *ipv6_address* **} | {** *ipv4_address/mask* **|***ipv6_address/mask* **} | address-group** *ipv6_address* **} | { !range | range } host-pool** *host_pool_name* **}**：このコマンドは、IP ヘッダー内の IP 宛先アドレスフィールドに一致するルール式を定義します。
  - *ipv4_address* **|** *ipv6_address*：発信通信の宛先ノードの IP アドレスを指定します。 *ipv4_address* **|** *ipv6_address* は、IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記の IP アドレスである必要があります。
  - *ipv4_address/mask* **|** *ipv6_address/mask*：発信通信の宛先ノードの IP アドレスを指定します。 *ipv4_address/mask* **|** *ipv6_address/mask* は、 サブネットマスクビットを含む IPv4 ドット付き 10 進表記または IPv6 コロン区切り 16 進表記の IP アドレスである必要があります。マスク ビットは、サブネット マスクのビット数に対応する数値です。
  - *address-group ipv6_address*：ワイルドカード入力や特殊な範囲入力で設定された IPv6 アドレスのグループを指定します。複数のワイルドカード文字を入力として受け入れることができますが、入力できるのは 1 つの 2 バイト範囲入力だけです。ワイルドカード文字の入力と 2 バイトの範囲の入力の両方を、特定の IPv6 アドレス内で一緒に設定できます。
  - **host-pool***host_pool_name*：ホスト プールの名前を指定します。 *host_pool_name* は、1 ～ 63 文字の英数字の文字列である必要があります。
  - コマンドの 演算子 は、次を指定します。

- != : 等しくない
- < : 次の値以下
- = : 等しい
- >=: 次の値以上

- **multi-line-or all-lines**：このコマンドは、単一の ruledef で複数の URL 式を指定できます。ruledef が評価されるときに、multi-line-or all-lines コマンドが設定されていると、論理 OR 演算子が ruledef 内のすべてのルール式に適用され、ruledef が一致するかどうかが判断されます。multi-line-or all-lines コマンドが設定されていない場合、論理 AND 演算子がすべてのルール式に適用されます。
- **rule-application { charging | post-processing | routing }**：このコマンドは、ルール定義のルール適用を指定します。**.**
  - **charging**：現在の ruledef が課金目的であることを指定します。
  - **post-processing**：現在の ruledef が後処理用であることを指定します。これにより、パケットのルール照合が無効になっている場合でも、パケットを処理できます。
  - **routing**：現在の ruledef がルーティング用であると指定します。アクティブな課金サービスでのルーティングには、最大 256 のルール定義を定義できます。デフォルトで、ディセーブルになっています。
- **dns { any-match** *value* **| query-type** *query_type* **| query-name** *query_name* **}**：このコマンドを使用すると、すべての DNS パケットまたはクエリタイプまたはクエリ名に基づいてパケットを照合するルール式を定義できます。

  ip server-ip-address *ip_address_value*：このコマンドを使用すると、接続の接続先の IP アドレスと一致するルール式を定義できます。
- **{ tcp | udp } { either-port** *port_number* **}**：このコマンドを使用すると、UDP/TCP ヘッダーの接続先または送信元ポート番号のいずれかと一致するルール式を定義できます。

DPI 向け L7 プロトコルの課金アクションの構成

このセクションでは、課金アクションの構成方法を説明します。課金アクションは、構成されたルールに一致したときに実行されるアクションを意味します。アクションの範囲として、アカウンティング レコード（例：EDR）の生成から IP パケットのドロップなどまでが含まれます。また、課金アクションによって、使用量計算の原則を規定します。再送信されたパケットをカウントするかどうか、および課金情報にどのプロトコルフィールド（L3/L4/L7 など）を使用するかがこれに当たります。

課金アクション構成を使用して、ruledef に関連付けられている QoS と課金関連パラメータを定義します。

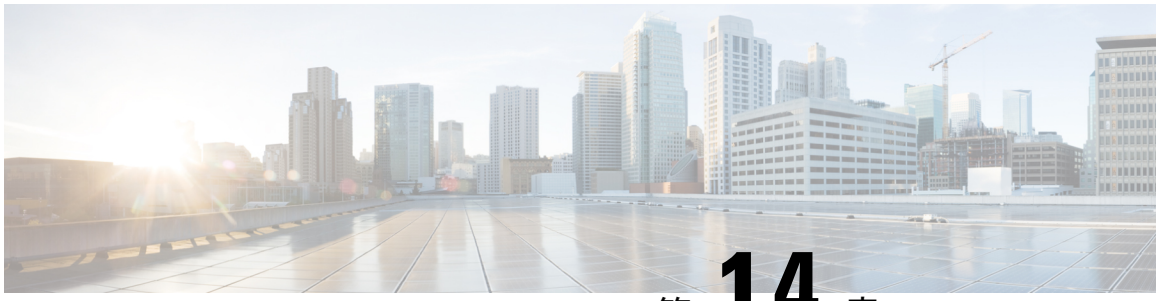
```
configure
   active-charging service service_name
     charging-action charging_action
        allocation-retention-priority priority  [ pci pci_value  | pvi
pvi_value
        billing-action egcdr
        cca charging credit [ rating-group coupon_id ] [
preemptively-request ]
        content-id content_id
        flow action { discard [ downlink | uplink ] | redirect-url
redirect_url | terminate-flow }
        flow limit-for-bandwidth { { direction { downlink | uplink }
peak-data-rate bps peak-burst-size bytes violate-action { discard |
lower-ip-precedence } [ committed-data-rate bps committed-burst-size
bytes [ exceed-action { discard | lower-ip-precedence } ] ] } | { id id
 } }
        nexthop-forwarding-address ipv4_address/ipv6_address
        qos-class-identifier qos_class_identifier
        service-identifier service_id
        tft packet-filter packet_filter_name
        tft-notify-ue
        tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 |
af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value } [ downlink
| uplink ]
```

注：

- **charging-action***charge_action_name*：課金アクションの名前を指定します。*charge_action_name* は、1 ～ 63 文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- 指定された課金アクションが存在しない場合は作成され、CLI モードは課金アクションを構成できる ACS 課金アクション構成モードに変わります。
- 指定された課金アクションが存在する場合、CLI モードはその課金アクションの ACS 課金アクション構成モードに変更されます。
- **allocation-retention-priority** *priority* **[pci** *pci_value* **| pvi** *pvi_value* **]**：割り当て保持優先順位（ARP）を構成します。優先順位 は、1 ～ 15 の範囲の整数で指定する必要があります。
  - **pci** *pci_value* ：**Specifies the Preemption Capability Indication (PCI) value. The options are:**
    - MAY_PREMPT：フローをプリエンプション処理できます。これはデフォルト値です。
    - NOT_PREMPT：フローをプリエンプション処理できません
  - **pvi** *pvi_value*：Preemption Vulnerability Indication（PVI）値を指定します。次のオプションがあります：
    - NOT_PREEMPTABLE：フローをプリエンプション処理できません。これはデフォルト値です。

• PREEMPTABLE：フローをプリエンプション処理できます

- **billing-action**：具体的なルール定義を一致するパケットに請求アクションを構成します。
- **cca charging credit**：クレジットコントロール課金クレジット動作を有効または無効にします。
- **content-id**：Rating Group を構成します。
- **flow action**：ルール定義に一致するパケットで実行するアクションを指定します。
  - **discard [downlink | uplink]**：ダウンリンクまたはアップリンクのパケットを破棄することを指定します。
  - **redirect-url** *redirect_url*：リダイレクトする URL を指定します。
  - **terminate-flow**：終了するフローを指定します。
- **flow limit-for-bandwidth**：MBR や GBR などの QoS パラメータを構成します。
  - Peakdatarate（MBR）：デフォルトは 3000 bps です
  - Peakburstsize：デフォルトは 3,000 バイトです
  - [committedDataRate（GBR）]：デフォルトは 144000 bps です
  - commitedBurstSize：デフォルトは 3000 バイト
- **nexthop-forwarding-address** *ipv4_address/ipv6_address* ：ネクストホップ転送アドレスを構成します。
- **qos-class-identifier** *qos_class_identifier* ：課金アクションの QCI を構成します。*qos_class_identifier* は、1 ～ 9 または 128 ～ 254（オペレータ固有）の範囲の整数で指定する必要があります。
- **service_identifier** *service_id*：生成された請求レコードで使用するサービス識別子を構成します。*service_id* は、1 ～ 2147483647 の範囲の整数で指定する必要があります。
- **tft packet-filter** *packet_filter_name*：現在の課金アクションに追加または削除するパケットフィルタを指定します。*packet_filter_name* は、パケットフィルタ名で、1 ～ 63 文字の英数字の文字列で指定する必要があります。
- **tft-notify-ue**：特定のトリガ条件に基づいて UE に対する TFT 更新を制御します。
- **tos**：Type of Service（ToS）オクテットを構成します。



第 14 章

EDNS0 レコードのデバイス ID

- 機能の概要と変更履歴 （201 ページ）
- 機能説明 （202 ページ）
- 機能の仕組み （202 ページ）
- EDNS フォーマットとトリガーアクションの設定 （206 ページ）
- モニタリングおよびトラブルシューティング （209 ページ）

機能の概要と変更履歴

要約データ

Table 39: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

表 *40 :* マニュアルの変更履歴

改訂の詳細	リリース
TCP のサポートが追加されました。	2021.02.1

改訂の詳細	リリース
最初の導入。	2021.01.2

機能説明

EDNS0 のデバイス ID を使用すると、カスタマイズされたドメインを Cisco Umbrella を介してブロッキングできます。この機能を有効にするには：

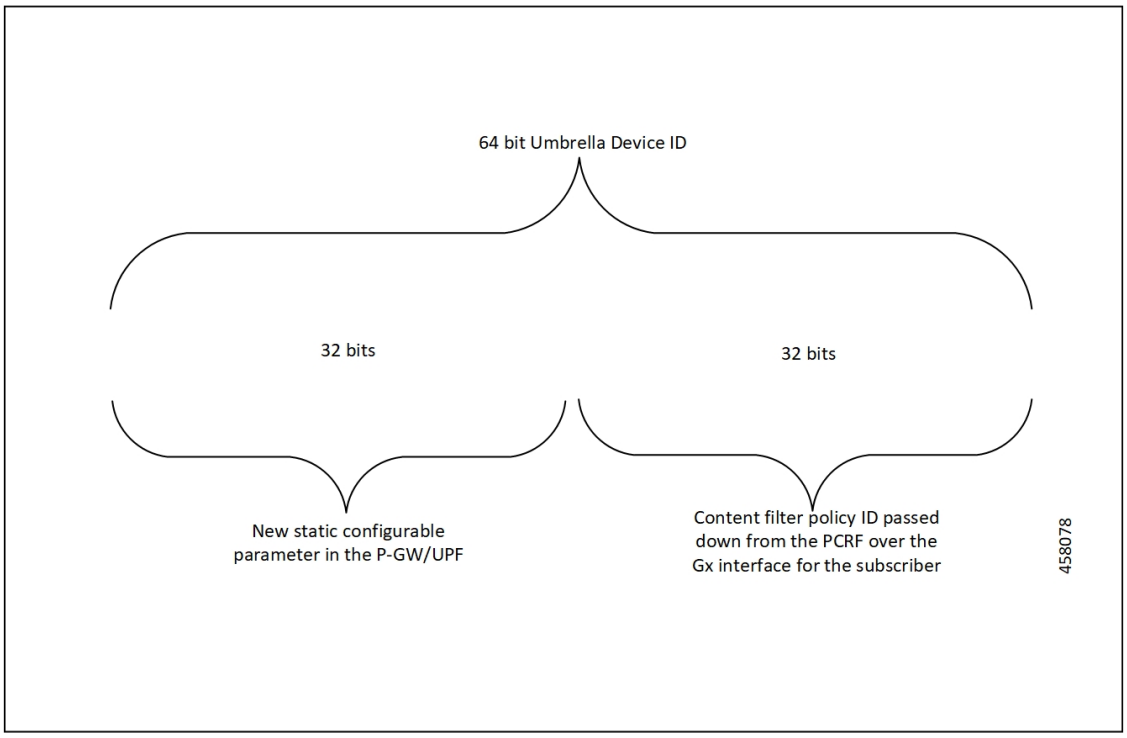
- UP はサブスクライバ DNS 要求を EDNS0 要求に再フォーマットする必要があります。
- UP では EDNS0 パケットに Cisco Umbrella の「デバイス ID」を含める必要があります。そうすることで、Cisco Umbrella DNS リゾルバはデバイス ID を使用して、EDNS0 パケット内のデバイス ID に関連付けられた、または設定されたドメインフィルタを適用できます。

現在、セッション管理機能（SMF）は PCRF/PCF からドメインフィルタリング ポリシー ID を受信します。SMF は、サブスクライバパラメータでドメイン フィルタリング ポリシー ID をユーザープレーン機能（UPF）に渡します。UP はドメイン フィルタリング ポリシー ID を使用して、ドメインフィルタリング機能をサブスクライバに適用します。

機能の仕組み

EDNS0 機能を設定してトリガーする新しい CLI が導入されました。

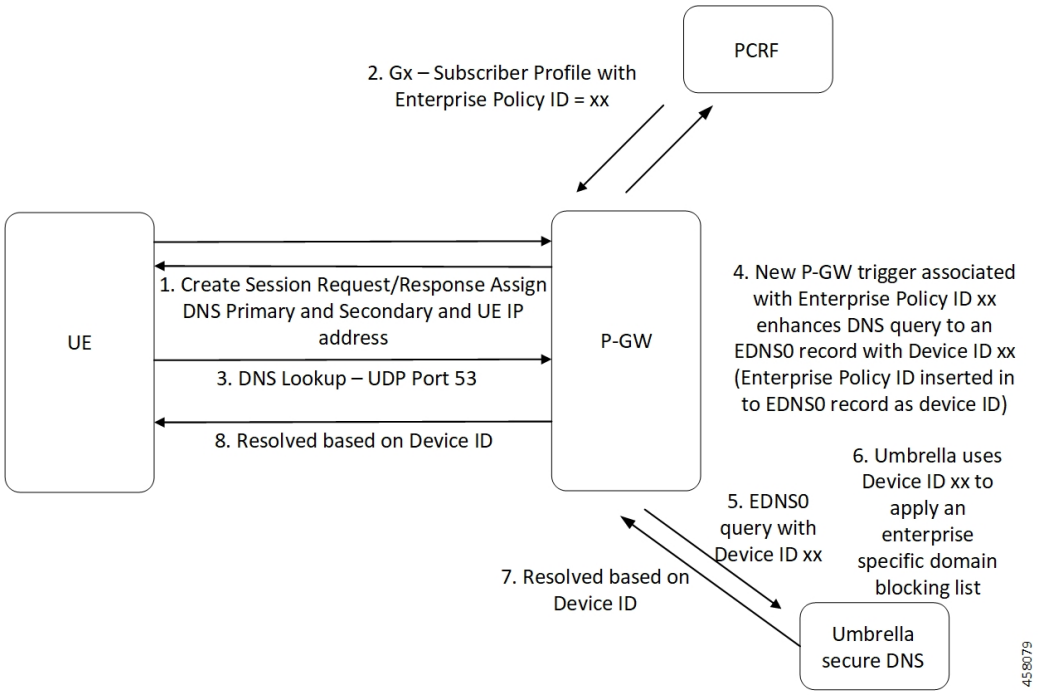
EDNS0 パケットが OPT RR データとして 64 ビットのデバイス ID を受信します。すべてのデバイス ID の最初の 32 ビットは、UPF で設定された固定値です。サブスクライバデバイス ID の最後の 32 ビットは、PCRF や PCF から受信したコンテンツフィルタ ID 値です。UPF はこの 2 つの 32 ビット値を連結して、サブスクライバ EDNS0 クエリに入力するための 64 ビットからなる完全なデバイス ID を作成します。新しい CLI は、静的 device-id 値の最初の 32 ビットを設定するのに役立ちます。32-bit static prefix CLI コマンドを設定しない場合、発信パケットには device-id = 32-bit CF PolicyID が表示されます。



EDNS0 レコードのデバイス ID 番号により、Cisco Umbrella DNS システムは EDNS0 クエリにドメインフィルタのカスタムセットを適用できます。

プロセス フロー

次のプロセスフローは、EDNS0 レコードにデバイス ID を挿入するためのコンテンツフィルタリングの拡張機能を示しています。



EDNS0 パケット形式

PCRF からのエンタープライズポリシー ID（CF_POLICY_ID）は、デバイス ID の作成に役立ちます。SMF はデバイス ID を UPF に送信します。DNS パケットにデバイス ID を追加すると、EDNS0 パケットの作成に役立ちます。EDNS0 パケットの形式は RFC2671 で指定されています。次に、いくつかの詳細を示します。

- 次に、OPT RR の固定部分の構造を示します。

```
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
```

- 次に、RDATA でエンコードされた OPT RR の可変部分を示します。

```
      +0 (MSB)                            +1 (LSB)
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  0: |                         OPTION-CODE                           |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  2: |                         OPTION-LENGTH                         |
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
  4: |                                                               |
    /                         OPTION-DATA                           /
    /                                                               /
    +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
```

  - OPTION-CODE：IANA によって割り当て済み

- OPTION-LENGTH：OPTION-DATA のサイズ（オクテット単位）
- OPTION-DATA：OPTION-CODE によって異なる

例：PCF/PCRF から受信した policy-id が「1234」で、UPF で構成された静的プレフィックスが「5678」の場合。

64 ビットのデバイス ID は「0000162e000004d2」となります。

- 0000162e：5678（10 進数）
- 000004d2：1234（10 進数）

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（文字列）
- 0000162e：5678（MSB）
- 000004d2：1234（LSB）

IP 再アドレス指定を使用した EDNS0

トリガーアクション内で設定された新しい CLI コマンドにより、DNS 通信は Umbrella DNS に再びアドレス指定されます。この CLI は、ACS サービスの既存のアドレス再指定サーバーリスト設定を使用します。パケットの宛先 IP アドレスに基づいてパケットをアドレス再指定することで、アドレス再指定されたサーバーリスト内の設定済みサーバー/ポートにゲートウェイ通信をリダイレクトできます。

動作と制限事項

この機能に適用される動作と制約事項は以下のとおりです。

- フロー作成時にトリガー条件を評価します。フロー間のトリガー条件の変更は、既存のフローには影響しませんが、新しいフローに影響します。
- トリガーアクションの変更は、同じフローに適用されます。
- CF ポリシーの ID 範囲は定義されているが、サービススキーマが定義されていない場合、または EDNS に関連するトリガー条件が設定されていない場合、CF も EDNS も適用されません。
- Gx から CF ポリシー ID を受信しない場合、範囲チェックは実行されず、コンテンツフィルタリングはルールベースで定義されているとおりに機能します。

- 「security-profile」CLI コマンドがトリガーアクションで EDNS フォーマットの CLI に関連付けられていない場合、EDNS 送信パケットのデバイス ID は 32 ビットの CF ポリシー ID でのみ送信されます。
- A、AAAA、CNAME、NS、PTR、SRV、TXT、NULL 以外のタイプの DNS クエリは、EDNS に変換することはできません。
- インフロー間の Gx 経由の CF ポリシー ID の変更は、現在のフローには適用されません。現在のフローでは、フローの作成時に存在する CF ポリシー ID が引き続き挿入されます。

制限事項

この機能の制限は次のとおりです。

- この機能は、EDNS 応答パケットの再フォーマットはサポートしません。
- UPF では、EDNS0 クエリに IMSI MSISDN タグ値を含めることができるようにする必要があります。この機能は、EDNS0 パケットの暗号化された IMSI をサポートしません。また、この機能は現在、EDNS フィールドでの次の設定をサポートしません。

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

EDNS フォーマットとトリガーアクションの設定

DNS フィルタリングを有効にするには、次の構成を使用します。

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

range パラメータが 10 ～ 1000 に設定されている場合、コンテンツ フィルタリング ポリシー ID が 10 ～ 1000 に設定されているサブスクライバプロファイルは、標準コンテンツフィルタリング機能を使用します。コンテンツ フィルタリング ポリシー ID が 1000 より大きい、または 10 より小さいサブスクライバプロファイルは、EDNS0 機能をトリガーします。

DNS フィルタリングを無効にするには、次の構成を使用します。

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

DNS フィルタリングが無効になっている場合、標準コンテンツ フィルタリング ポリシーは、構成された内容または PCF から受信した内容に応じて再開されます。

アクティブ課金サービスでEDNSパケットアクションおよびフォーマットを設定するには、次の設定を使用します。

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

注：

- **external-content-filtering**：EDNS0 機能を有効にします。このフラグが True に設定され範囲基準が指定されている場合、EDNS0 機能は有効です。デフォルトでは、フラグは無効です。
- **app-proto = dns**：DNS 以外の通信の IP アドレスの再指定を回避します。この CLI が、multiline-or cli で有効な場合、すべての DNS 通信が、EDNS でエンコードされます。

次の構成により、EDNS パケットに挿入される EDNS フォーマットを定義するトリガーアクションが実行されます。

```
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
```

注：

- **trigger-action** *trigger_action_name*：トリガーアクションで flow-action CLI を構成できるようにします。
- **edns-format** *format_name*：EDNS が適用されている場合に EDNS フォーマットを使用します。
- **security-profile** *profile_name*：EDNS のセキュリティプロファイル設定を定義して、デバイス ID のマッピングを追加します。

（注） EDNS0 レコード機能のデバイス ID は、複数のセキュリティプロファイルをサポートしています。

- **flow action readdress server-list** *server_list_name* **[hierarchy] [round-robin] [discard-on-failure]**：EDNS を IP アドレス再指定に関連付けます。IP アドレス再指定を使用して、設定済みのサーバー IP 宛てのパケットをアドレス再指定します。このトリガーアクションの CLI は、サーバーリスト構成のみをサポートします。単一サーバーの IP やポート構成（charging-action など）はサポートしません。

次の構成を使用して、EDNS に CF ポリシー ID を挿入します。

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

32 MS ビットを設定するため、セキュリティプロファイルを含む静的な値が EDNS レベルで指定されます。

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

ペイロード長を指定する新しいタグを挿入するには、次の構成を使用します。

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

値の範囲：576 ～ 4096

設定例

以下に、EDNS パケットを設定するための設定例を示します。

```
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
```

モニタリングおよびトラブルシューティング

以下に、EDNS0 レコードにデバイス ID を挿入するための拡張コンテンツフィルタリングをサポートする show コマンドとその出力を示します。

show コマンドと出力

以下は、EDNS0 レコードへのデバイス ID の挿入に対応する拡張コンテンツフィルタリング機能をサポートするために変更された show コマンドとその出力です。

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

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

- **show user-plane-service statistics analyzer name dns**：出力が変更され、「EDNS Over UDP」および「EDNS Over TCP」の両方のセッションで「EDNS Response Received」 を含められるようになりました。
- **show subscribers user-plane-only full callid**：出力が変更され、サブスクライバごとのEDNS統計で次のパラメータを含められるようになりました。
  - DNS-to-EDNS アップリンクパケット数
  - DNS-to-EDNS アップリンクバイト数
  - 受信した EDNS レスポンス数
- **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
```

次の show コマンドを使用して、Trigger Action 統計を表示します。

- **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
```

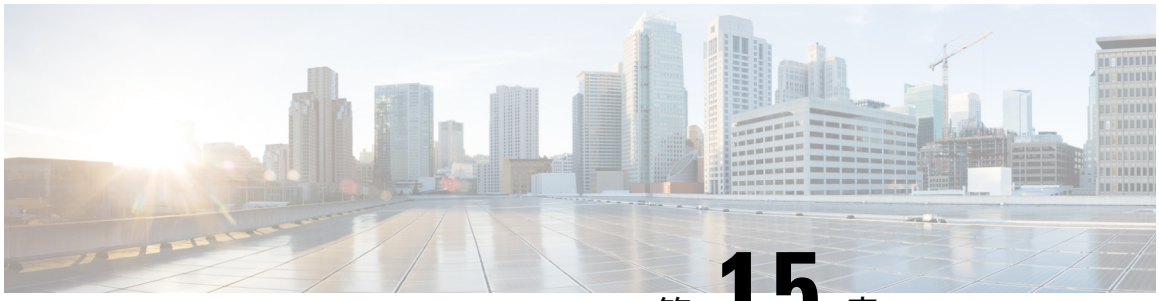
- **show user-plane-service trigger-action all**

```
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
```

バルク統計

EDNS0 レコード機能のデバイス ID をサポートするために、次のバルク統計が用意されています。

スキーマ：**ECS**	
統計	**説明**
ecs-dns-udp-edns-encode-succeed	UDP 経由で DNS から EDNS に変換されたパケットの数
ecs-dns-udp-edns-encode-failed	UDP 経由で DNS から EDNS への変換に失敗した数
ecs-dns-udp-edns-encode-response	UDP 経由で EDNS クエリに対して受信した応答の数
ecs-dns-tcp-edns-encode-succeed	TCP 経由で DNS から EDNS に変換されたパケットの数
ecs-dns-tcp-edns-encode-failed	TCP 経由で DNS から EDNS への変換に失敗した数
ecs-dns-tcp-edns-encode-response	TCP 経由で EDNS クエリに対して受信した応答の数



第 15 章

ダウンリンク データ通知

- 機能の概要と変更履歴 （211 ページ）
- 機能説明 （212 ページ）
- 機能の仕組み （212 ページ）
- リリース 10 非準拠 MME の DDN スロットリング （223 ページ）
- リリース 10 準拠 MME の DDN スロットリング （225 ページ）
- SAE-GW セッションのアイドルタイマー, on page 225
- S-GW セッションのアイドルタイムアウト （226 ページ）
- show コマンドの入力と出力 （227 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.02.0

機能説明

DDN Delay と DDN Throttling をサポートする Downlink Data Notification (DDN) メッセージおよび 5G-UPF で UE がアイドル状態の場合、SAEGW でのバッファリングが 5G-UPF でサポートされます。

機能の仕組み

この項では、この機能の仕組みを紹介します。

- バッファリングは SAEGW-U でサポートされています。
- Release Access Beare によって UE がアイドル状態に遷移すると、バッファリングのサポートが開始されます。
- アクティブ状態からアイドル状態への遷移：
  - SAEGW はバッファリング機能をサポートし、セッションの SAEGW-U でバッファリングをアクティブ化することを決定するため、UE が ECM-IDLE 状態に遷移すると、SAEGW-C は Sx セッション変更を介して SAEGW-U に通知します。
  - バッファリングが開始された後、最初のダウンリンクパケットがいずれかのベアラーに到着すると、SAEGW-U は SAEGW-C に通知します。 SAEGW-U は、特に指定されていない限り、Sx レポートメッセージを SAEGW-C に送信し、ダウンリンクパケットの受信先の S5/S8 ベアラーを識別します。
  - SAEGW-C は、レポートメッセージを受信すると、3GPP TS 23.401 [2] での定義に従って、DDN メッセージを MME に送信するかどうかを決定します。DDN 通知は、Sx 使用状況レポートとともに送信されます。
- アイドル状態からアクティブ状態への遷移：
  - UE が ECM-CONNECTED 状態に遷移すると、SAEGW-C は eNodeB/RNC/SGSN の F-TEIDu を使用して Sxa インターフェイスを介して SAEGW-U を更新します。バッファリングされたデータパケットがある場合は、SAEGW-U によって eNodeB/RNC/SGSN に転送されます。
- Apply Action が BUFFER で、SGW-U が回復した場合、SGW-U はダウンリンクデータパケットの到着時に Sx レポート（Report Type：DLDR）を開始します。
- SGW-U には、各 Sx レポート（Report Type：DLDR）が送信された後に開始するタイマーが実装されています。Apply Action が変更されていない場合、タイマーの期限が切れると、Sx Report（DLDR レポートタイプ）が再開されます。
- ベアラーの ARP は DDN メッセージに含まれます。

- マルチ PDN セッションでは、ある PDN に対して DDN が開始され、ベアラーの優先順位が高い別の PDN でデータが受信された場合、DDN は優先順位がより高い ARP 値で再度開始されます。

ダウンリンクデータ通知：遅延（DDN-D）のサポート

特定の条件下では、UE がサービス要求をトリガーすると、アップリンクおよびダウンリンクデータがトリガーされ、ベアラー変更要求（MBR）を受信する前に SGW-C で受信され、不要なダウンリンクパケット通知メッセージが送信されて、MME の負荷が増加します。

このような場合、MMEはこれらのイベントの発生レートをモニターします。レートがオペレータの設定値より大きくなり、MME の負荷がオペレータの設定値を超えた場合、MME はパラメータ D を使用して「Delay Downlink Packet Notification Request」を Serving Gateway に表示します。D は要求された遅延で、50 ミリ秒の倍数の整数、または 0 で指定します。S-GW では、ダウンリンクデータを受信してからダウンリンクデータ通知メッセージを送信するまでの間、この遅延が使用されます。

ダウンリンクデータ通知は、Collapsed コールと Pure-S コールの両方でサポートされています。

システムの分散型の性質により、特定の MME からのセッションは異なるセッションマネージャにオフロードされるため、セッションがオフロードされると、すべてのセッションマネージャに通知されます。また、この機能は、すべてのセッションマネージャから DEMUX マネージャにメッセージを送信できないように設計されています。

- DDN 遅延機能では、DDN 遅延タイマーは、セッション管理機能でサポートされます。
- 最初のデータパケットが到着すると、Sx/N4 Report メッセージが開始されますが、DDN メッセージは遅延タイマーの終了後にセッション管理機能から開始されます。
- DDN 遅延機能はピアレベルの機能であるため、DDN 遅延値の受信元であるピアのすべてのセッションに適用されます。
- 以前にピアから遅延値を受信していて、現在のメッセージに含まれていない場合、遅延値は 0 と見なされます。

DDN のセッションリカバリと ICSR がサポートされています。

5G SMF コール

ダウンリンクデータ通知：5G UE

UE が 5G コールモードでアイドル状態になると、SMF は FAR Apply Action が BUFFER 値に設定された Sx_Modify-Request を送信します。すべての QFI（デフォルト/専用）に対して、FAR Apply Action は BUFFER 値に設定されます。

サーバーからダウンリンクパケットを受信すると、UPF は、パケットルールの一致に従って、ルール ID（PDR ID）/QFI を含むダウンリンクデータ通知とともに Sx_Report_Request を送信し

ます。UPF は、すべての FAR でパケット制限が 5 に達するまで、パケットのバッファリングを継続します。

UE がアクティブな場合、Sx_Modify_Request は、FAR Apply Action が FWD（転送）および TEID（トンネルエンドポイント識別子）に設定された状態で UPF に到達します。UPF はパケットをバッファリングし、FIFO として UE に送信します。各パケットでは、ルール照合はデバッファリングプロセスの後に行われます。

DDN スロットリングのサポート

MME から SGW-C への DDN 要求が多すぎると、MME での処理が過負荷になる可能性があります。この負荷を軽減するために、MME は SGW-C に対して、所定の期間に送信される DDN メッセージを一定の割合で減らすよう動的に要求します。

DDN スロットリングの場合、S-GW は、所定の期間に一定の割合の DDN をドロップする必要があります。S-GW は、各セッションマネージャで確率的アルゴリズムを使用することで、この機能を実装します。

一方、DDN スロットリングの従来の実装では、各セッションマネージャが、低優先ベアラーの保留中の DDN リストを中央エンティティと共有する必要があります。中央エンティティは保留中の DDN の正味負荷を計算し、各セッションマネージャがドロップする必要がある DDN の数を決定します。この実装では、セッションマネージャでの DDN メッセージのバッファリングが必要になります。また、シャーシ内におけるソフトウェアサブシステムの分散処理の性質上、セッションマネージャと中央エンティティ（Boxer の場合は demuxmgr）間で定期的に大量のメッセージングが必要になります。

確率的アルゴリズムを実装すると、セッションマネージャでのバッファリングと、demuxmgr とのメッセージングの必要性がなくなります。セッションマネージャでの ARP 優先順位が低いページング負荷が増加すると、確率的アルゴリズムの精度が向上します。ページング負荷が低くても、指定されたスロットリング係数にかなり近い精度となります。

リリース 10 に準拠していない MME の場合、SGW_C には CLI を使用してスロットリングを有効にするオプションがあります。

低優先ベアラーの ARP しきい値は、S-GW サービス設定を使用して設定する必要があります。たとえば、設定された ARP 値が「9」の場合、ARP が 9 を超えるベアラーはすべて、低優先ベアラーと見なされます。DDN スロットリングは、この設定によって有効になります。SGW サービス設定を通じて DDN スロットリングが有効になっている場合、MME への各 DDN メッセージには ARP IE が含まれます。

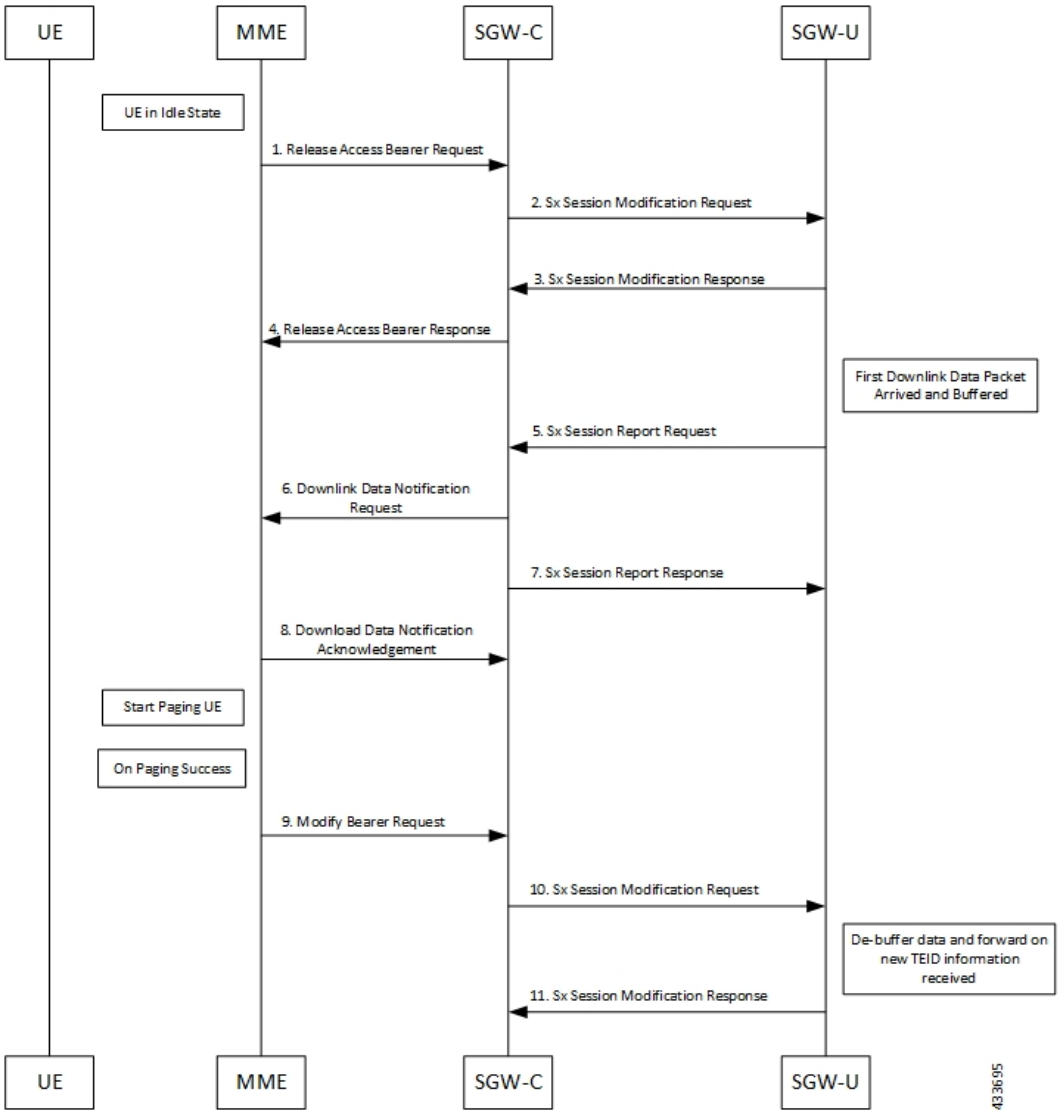
ユーザー接続タイマーのサポートなし

- 肯定的なダウンリンクデータ通知の確認応答後にベアラー変更要求を受信しない場合、タイマーが設定されます。
- タイマーは、DDN 確認応答を受信したときに SGW-C で開始されます。
- ベアラー変更要求の到着時に、SGW-C はこのタイマーを停止します。

- タイマーの期限が切れると、SGW-C はバッファリングされたパケットをドロップするように SGW-U に通知します。

DDN コールフロー

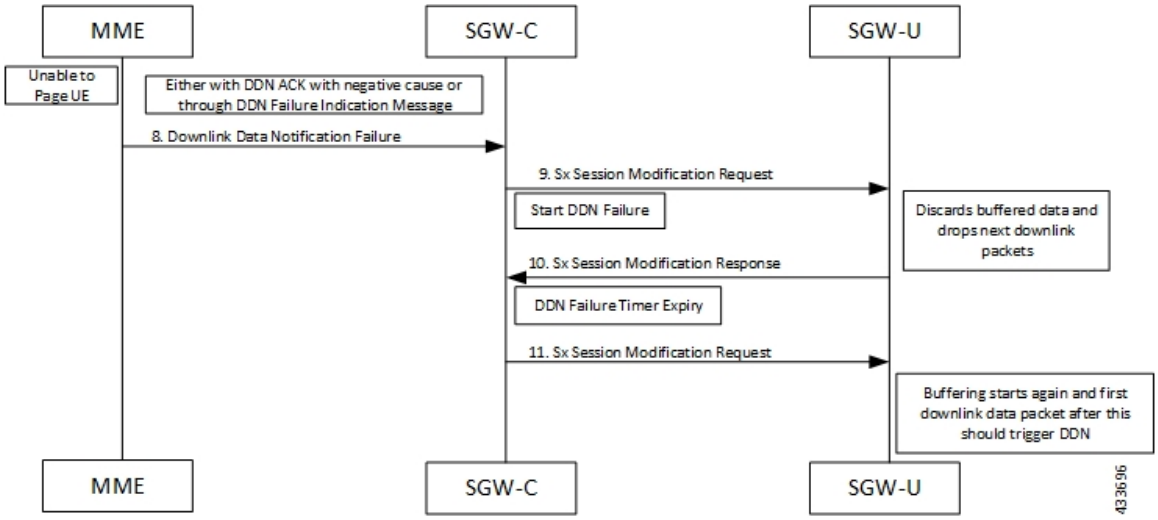
DDN の成功シナリオ



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。

3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME にアクセスベアラー解放応答を送信します。
5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（[Report Type] が「Downlink Data Report」）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. MME は、UE にページング要求を送信できる場合、ダウンリンクデータ通知確認応答メッセージで [Cause] を「Request Accepted」に設定して、SGW-C に送信します。
9. ページングが成功すると、SGW で S1-U 接続を設定する eNodeB TEID を使用して、MME が S-GW にベアラー変更要求を送信します。
10. SGW-C が、新しい TEID 情報に関する更新された FAR を含む Sx 変更要求を SGW-U に送信します。SGW-U は、バッファされたすべてのデータを eNodeB を介して UE に転送できるようになりました。
11. SGW-U が、SGW-C に Sx 変更応答を送信します。

DDN の失敗シナリオ



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。

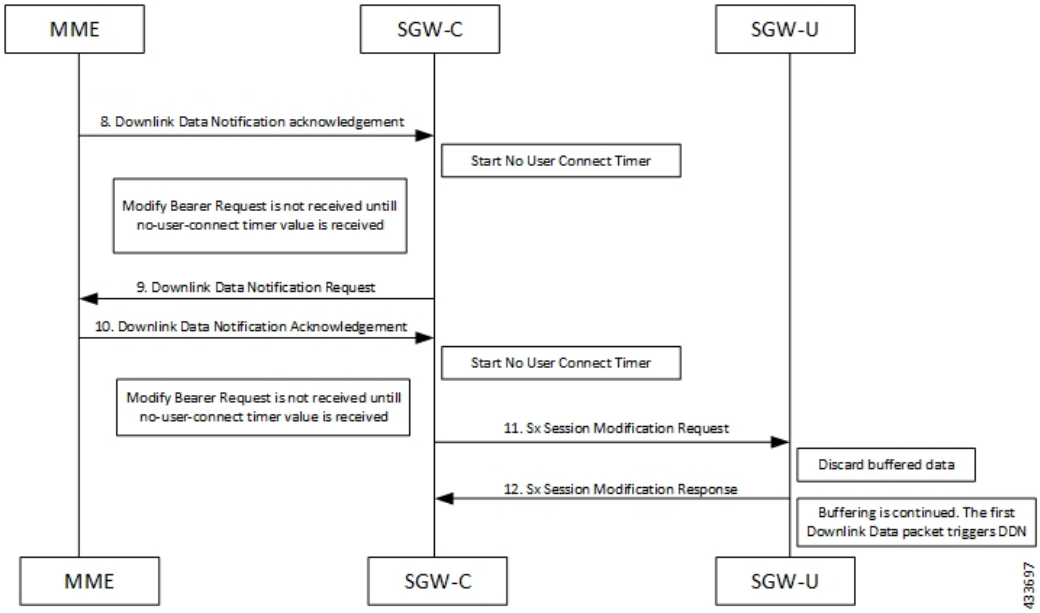
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME にアクセスベアラー解放応答を送信します。
5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx Report 要求（[Report Type] が「Downlink Data Report」）がトリガーされます。
6. Sx Report 要求メッセージを受信すると、SGW-C は、MME に対して Downlink Data Notification 要求メッセージを開始します。
7. SGW-C が、SGW-U 対して、Sx Report 応答メッセージを送信します。
8. MME が UE をページングできない場合、関連する原因でダウンリンクデータ通知要求を拒否できます。

   または

   MME がダウンリンクデータ通知要求を受け入れた場合、UE がページングに応答しなかったことを SGW-C に示すために、後でダウンリンクデータ通知の失敗通知を送信します。
9. SGW-C が DDN エラーを受信すると、次の DDN の送信をすぐに停止するために、SGW-C は、DDN エラータイマーを開始します。SGW-C は、DROBU フラグが立った Sx Modification 要求を送信し、バッファリングされたパケットと DROP としての Apply Action を破棄し、後続パケットとドロップします。
10. SGW-U が、SGW-C に Sx 変更応答を送信します。
11. DDN 失敗タイマーの期限が切れると、SGW-C はバッファリングを再開するために、Apply Action を BUFFER にして Sx 変更を開始します。

DDN の成功シナリオ （215 ページ） コールフローの手順 3 以降の手順が続きます。

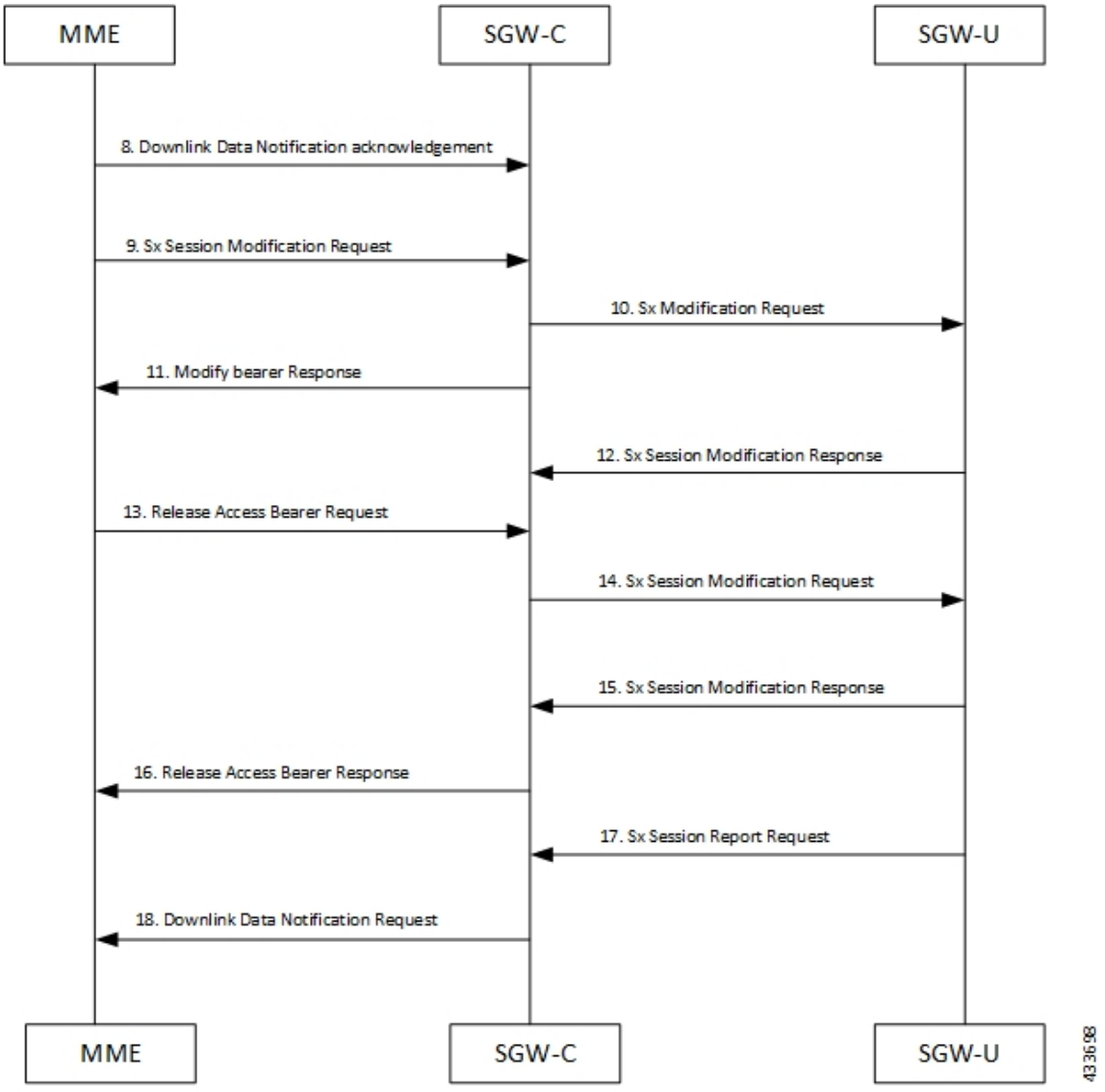
ユーザー接続タイマーのサポートなし



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。
2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME にアクセスベアラー解放応答を送信します。
5. SGW-U が受信する最初のダウンリンクデータにより、SGW-C に対する Sx レポート要求（[Report Type] が「Downlink Data Report」）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. ダウンリンクデータ通知確認応答が MME から受信されます。SGW-C が no-user-connect を開始します。
9. eNodeB TEID 情報を含むベアラー変更要求が受信されず、no-user-connect タイマーが期限切れになった場合、SGW-C はダウンリンク データ通知を再度送信します。
10. MME からダウンリンクデータ通知確認応答を受信します。SGW-C は、no-user-connect タイマーを再度開始します。

11. SGW-C はメッセージに DROBU フラグを付けて、SGW-U への Sx セッション変更要求を開始します。SGW-U はこのフラグを受信すると、バッファされたデータをドロップします。新しいデータはバッファリングされ、後続の最初のパケットは、ダウンリンクデータ通知メッセージを開始するための Sx レポートメッセージを開始します。
12. SGW-U が Sx 変更応答を送信します。

DDN 遅延タイマー



1. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C にアクセスベアラー解放要求を送信します。

2. アクセスベアラー解放要求を受信すると、SGW-C はすべての PDN への Sx 変更要求の Apply Action を BUFFER にして FAR を更新することで、同じ情報を SGW-U に通知します。
3. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
4. SGW-C が MME にアクセスベアラー解放応答を送信します。
5. SGW-Uが受信する最初のダウンリンクデータにより、SGW-Cに対するSxレポート要求（[Report Type] が「Downlink Data Report」）がトリガーされます。
6. Sx レポート要求メッセージを受信すると、SGW-C が MME へのダウンリンクデータ通知要求メッセージを開始します。
7. SGW-C が、SGW-U に向けて Sx レポート応答メッセージを送信します。
8. DDN遅延タイマー値に従い、MMEからダウンリンクデータ通知確認応答を受信します。この遅延タイマー値はこのピア用に保存されるため、その後、このピアに対するすべてのダウンリンクデータ通知は、この遅延の後に開始する必要があります。
9. ページングが成功すると、SGWでS1-U接続を設定するeNodeB TEIDを使用して、MMEが SGW にベアラー変更要求を送信します。
10. SGW-C が、新しい TEID 情報に関する更新された FAR を含む Sx 変更要求を SGW-U に送信します。 SGW-U は、バッファされたすべてのデータを eNodeB を介して UE に転送できるようになりました。
11. SGW-C が、ベアラー変更応答を MME に送信します。
12. SGW-U が、SGW-C に Sx 変更応答を送信します。
13. MME が、その UE に対するすべてのベアラーのダウンリンクリモート TEID を解放するために、SGW-C に Release Access Bearer 要求を送信します。
14. Release Access Bearer 要求の到着時に、SGW-C がすべての PDN の Sx 変更要求の Apply Action として BUFFER を使用して FAR を更新することで、同じ情報を SGW-U に通知します。
15. SGW-U が、対応する PDN に対して SGW-U でバッファリングを適用後、Sx 変更応答を送信します。
16. SGW-C が MME に Release Access Bearer 応答を送信します。
17. SGW-Uに到着した最初のダウンリンクデータにより、SGW-Cに対するSxレポート要求（レポートタイプはダウンリンクデータレポート）がトリガーされます。
18. Sx レポート要求メッセージの到着時に、SGW-C が DDN 遅延タイマーを開始します。DDN 遅延タイマーが期限切れになると、SGW-C が MME へのダウンリンクデータ通知メッセージを開始します。

Sx インターフェイス

Sx セッションレベルのレポート手順

アイドルモード UE の最初のダウンリンクデータの検出（SAEGW-U が実行）：

SAEGW-Uはダウンリンクパケットを受信するが、送信用のS1ベアラーを受信せず、バッファリングが SAEGW-U によって実行される場合、UE をページングするために、最初のダウンリンクデータの検出を SAEGW-C に報告します。

PFCP セッションレポート要求

PFCPセッションレポート要求は、PFCPセッションに関連する情報をコントロールプレーン機能に報告するために、ユーザープレーン機能によって Sxab インターフェイスを介して送信されます。

情報要素	P	条件/コメント	アプリケーション				IE タイプ
			Sxa	Sxb	Sxc	N4	
Report Type	M	この IE は、レポートのタイプを示します。	X	X	X	X	Report Type
Downlink Data Report	C	この IE は、レポートタイプが Downlink Data Report を示している場合に存在します。	X	-	-	X	Downlink Data Report

PFCP セッションレポート要求内の Downlink Data Report IE

Downlink Data Report のグループ化された IE は、次の表に示すようにエンコードされます。

オクテット 1 および 2		Downlink Data Report IE タイプ = 83（10 進数）

オクテット 3 および 4		長さ = n					
情報要素	P	条件/コメント	アプリケーション				IE タイプ
			Sxa	Sxb	Sxc	N4	
PDR ID	M	この IE は、UP 機能で受信されたダウンリンクデータパケットの PDR を識別します。 ダウンリンクデータパケットを受信した複数の PDR を表すために、このタイプの IE を複数含めることができます。	X	-	-	X	PDR ID

ユーザープレーン機能への DDN 障害に関する通知

コントロールプレーン機能はユーザープレーン機能に障害を通知します。これにより、バッファリングされたパケットがドロップされ、PFCP Sx 変更メッセージの DROBU フラグを介して DDN 関連フラグをリセットできます。

PFCPSMReq-Flags	C	DROBU（Drop Buffered Packets）：この PFCP セッションで現在バッファリングされているパケットをドロップするように UP 機能が要求された場合、CP 機能はこのフラグを設定します（注 1 を参照）。

制限事項

この機能には次の既知の制限事項があります。

- SAEGW バッファリングは、PDN セッションごとに 5 つのデータパケットに対して実行されます。
- DDN プロファイル設定はサポートされていません。
- フローアイドルタイムアウトまたはその他のケースが原因で削除されるバッファ データ（データパケットストリーム）のサポートはありません。

リリース 10 非準拠 MME の DDN スロットリング

リリース 10 以外の MME の DDN スロットリングを設定するには、次の設定を使用します。

```
configure
   context context_name
      sgw-service service_name
        ddn throttle arp-watermark arp_value [ rate-limit limit time-factor
 seconds throttle-factor percent increment-factor percent [ poll-interval
seconds ] throttle-time-sec seconds [ throttle-time-min minutes ] [
throttle-time-hour hour ] stab-time-sec seconds [ stab-time-min minutes ]
[ stab-time-hour hour ]
         no ddn throttle
         end
```

注：

- **rate-limit**：1 秒あたりに許可される DDN。
- **time-factor**：SGW がスロットリングを決定する秒単位の期間（有効な範囲：1 ～ 300 秒）。
- **arp-value**：1 ～ 15 の有効な ARP 値。設定された値よりも大きい ARP を持つパケットはすべて、スロットリング係数に従ってスロットリングされます。
- **throttling-factor**：DDN サージの検出時にドロップされる DDN のパーセンテージ（有効範囲：1 ～ 100）。
- **throttling-time-sec**：SGW で DDN がスロットリングされる秒単位の期間（有効な範囲：0 ～ 59 秒）。
- **throttling-time-min**：SGW で DDN がスロットリングされる分単位の時間（有効な範囲：0 ～ 59 分）。
- **throttling-time-hour**：SGW で DDN がスロットリングされる時間単位の期間（有効な範囲：0 ～ 310 時間）。
- **increment-factor**：既存のスロットリング係数では DDN の急増を抑制するには不十分な場合に、スロットリング係数を動的に増加させるパーセンテージ値。

- **poll-interval**：秒単位の時間（オプションの引数、デフォルト値：1 秒、ポーリング間隔 < time-factor）
- **stab-time-sec/min/hours**：安定化時間係数。DDN レートが正常に戻った場合に、スロットリング期間全体でスロットリングを適用する必要がない期間。

リリース 10 に準拠していない MME の DDN スロットリングは、SGW での既存のリリース 10 スロットリング実装を利用します。SGW サービスの設定メカニズムを提供することで、オペレータは DDN スロットリングを適用する際に MME からのフィードバックを必要としません。この機能の重要なポイントを以下に説明します。

1. CLI 設定は、MME/S4-SGSN ごとに適用されます。スロットリングパラメータは、MME/S4-SGSN ごとに個別に追跡されます。
2. CLI を使用してこの機能を設定すると、demuxmgr は送信された DDN の数について各 sessmgr をポーリングします。デフォルトでは、ポーリングは毎秒実行されます。この時間間隔は、poll-interval 時間を設定することで変更できます。ポーリング間隔を長くすると、シャーシ内の内部メッセージの数が少なくなります。ただし、DDN サージの検出には時間がかかります。
3. 時間係数を設定することで、オペレータは必要に応じて S-GW がスロットリングを適用する時間間隔を指定できます。実質的な DDN レートが時間係数の時間間隔で指定された制限内にある場合、DDN のサージがある程度許容されます。たとえば、time-factor = 10 秒、ddn rate = 1000、poll interval = 2 秒の場合について説明します。Demux は 2 秒ごとに各 sessmgr をポーリングします。許容される DDN レート制限は、1000*10 = 10 秒ごとに 10000 DDN です。たとえば、2 秒後に 4000 DDN が送信されたとします。この場合、10000 DDN のレート制限を 10 秒以内に超えるまで、S-GW はスロットリングを適用しません。これにより、DDN の断続的なバーストが可能になります。
4. DDN レート制限は CLI を使用して設定します。たとえば、DDN レート制限が 1000 で、ポーリング間隔が 1 秒、時間係数が 5 秒の場合、許容可能なレート制限は 5 秒間で 5000 DDN です。S-GW によって送信された DDN の数が 5 秒後に 5000 を超えた場合、demuxmgr はすべての sessmgr にスロットリングを開始するように要求します。
5. スロットリングされる DDN の割合は、スロットリング係数を使用して設定されます。
6. 既存のスロットリング係数では DDN の急増を抑制するには不十分な場合、オペレータは増分係数を指定してスロットリング係数を増やすことができます。たとえば、スロットリング係数 = 10%、DDN レート = 1000、増分係数 = 10% の場合について説明します。スロットリングが適用されると、S-GW は最大 10% の DDN をドロップします。ただし、DDN レートがさらに 1000 を超える場合、S-GW はスロットリング係数を 20% に増やします。それでも十分でない場合は、30% に増加します。スロットリング係数を増やした後、ドロップされた DDN の数が予想よりも多い場合、スロットリング係数は増分係数によって下げまれます。たとえば、このケースでスロットリング係数を 30% に増やした後、送信される DDN が 1 秒あたり 1000 未満になった場合（時間係数とポーリング間隔を考慮）、スロットリング係数は 20 に低下します。スロットリング係数低下の下限値は、設定された値（この場合は 10%）になります。

7. オペレータは、S-GW でスロットリングが適用される期間を設定できます。これは、日数の指定順序によっては大きな値になる場合があります（例：10 日または 240 時間）。オペレータは、 DDN レートが十分に制御されている場合に、安定化時間係数を設定することでスロットリングを停止できます。スロットリングを停止すると、DDNは不必要にドロップされません。たとえば、スロットリング時間 = 10 日、スタブ時間 = 8 時間の場合について説明します。S-GW が DDN スロットリングを開始した後、8 時間で送信された DDN + ドロップされた DDN が DDN レート * 8 時間未満の場合、スロットリングは停止されます。

リリース 10 準拠 MME の DDN スロットリング

DDN スロットリングは、ARP 値を指定することで、コール制御プロファイルを介して有効になります。たとえば、指定された ARP 値が 10 の場合、ARP 値が 10 ～ 15 であるベアラーはすべて優先順位が低いベアラーとして扱われ、スロットリング処理が行われます。S-GW サービス設定で ARP 値が指定されていない場合、スロットリングは有効になりません。また、DDN スロットリングがS-GWサービスを使用して設定されていない限り、MMEへのDDNメッセージに ARP IE は含まれません。MME がリリース 10 に準拠している場合、DDN 確認応答にスロットリング IE があるため、ユーザーが期間値を設定する必要はありません。準拠していない場合は、期間値を設定することで、S-GW でスロットリングを有効にできます。0 に設定されている場合、S-GW はスロットリングを繰り返し適用します。特定の期間のみスロットリングを有効にするには（リリース10非準拠のMME）、ユーザーが時間と分で値を設定する必要があります。設定時から、タイマーの期間が終了するまでスロットリングがS-GWで適用されます。たとえば、ユーザーが時間を 10、分を 30 と設定した場合、S-GW は次の 10 時間 30 分後にスロットリングを適用します。

再設定時に、すべてのパラメータが新しい値で設定されますが、ポーリング時間と時間係数を除き、次の再キャリブレーションからのみ適用されます。

リリース 10 MME の DDN スロットリングを設定するには、次の設定を使用します。

```
configure
  context context_name
    sgw-service service_name
      [ no ] ddn throttle arp-watermark arp_value
      end
```

注：

- **arp-value**：1 ～ 15 の有効な ARP 値。設定された値よりも大きい ARP を持つパケットはすべて、スロットリング係数に従ってスロットリングされます。

SAE-GW セッションのアイドルタイマー

アイドルタイマーは、SAE-GW で発生するアイドルセッションを識別して削除するためにサポートされています。

セッションが他のネットワークノードから削除されても、セッションがアイドル状態になる場合があります。技術的な不具合により、セッションがSAE-GWに残り、こうしたアイドルセッションによってリソースが保持される可能性があります。

アイドルタイマーを設定すると、設定された時間制限よりも長くアイドル状態のままになっているセッションが削除されるため、システムのキャパシティを効果的に使用できます。

Important この機能は現在、Pure-P および Collapsed Call に制限されています。

制限事項

アイドルタイマー機能は、冗長性イベントが発生した場合にアイドルタイマーの回復をサポートしていません。

SAE-GW セッションのアイドルタイマーの設定

アイドルタイマーは、APN レベルで設定できます。

SAE-GW セッションのアイドルタイマーを設定するには、次のコマンドを使用します。

```
configure
  context context_name
    apn apn_name
      timeout idle timeout_value
      no timeout idle
      default timeout idle
      end
```

- **no**：アイドルタイマー設定を無効にします。
- **default**：サブスクライバのタイムアウト設定のデフォルト値を設定します。デフォルトのアイドルタイムアウト値は 0 です。
- **idle** *timeout_value*：システムによりセッションが自動的に終了されるまでに、セッションがアイドル状態を維持できる時間の上限を秒単位で指定します。続けて 0 ～ 4294967295 までの秒数を指定する必要があります。「0」は、機能が無効であることを示します。

S-GW セッションのアイドルタイムアウト

この章では、S-GWセッションのアイドルタイムアウト処理機能について説明します。ASR5500プラットフォームでは、サブスクライバセッションはコールラインで表されます。S-GW 製品のコールラインは、S11/S4 の MME/S4-SGSN および S5/S8 の P-GW を介してピアに接続します。一部のシナリオでは、ピアセッションはそれぞれのピアによって削除されます。S-GW は削除メッセージを受信も除外もしないため、その結果、S-GW セッションはアイドル状態のままになります。このようなアイドル状態のセッションや古いセッションは、効率的にリソース

を消費して、キャパシティを減らすため、システム内の有効なコールラインにカウントされます。このような場合、S-GWは新しいサブスクライバセッションの取得をトリガーします。その結果、同じサブスクライバの古いセッションが削除されます。アイドルタイムアウト処理のサポートにより、このようなセッションの識別が可能になり、リソースを解放するために削除が開始されます。

次に、S-GW セッションのアイドルタイムアウト処理について説明します。

- サブスクライバのデータ トラフィック アクティビティがない場合、サブスクライバセッションはアイドル状態です。セッションマネージャは、コールラインの状態を追跡します。コールラインのデータトラフィックが記録されていない場合、そのようなセッションはアイドル状態に遷移します。
- アイドルタイムアウトと呼ばれる定義されたタイムフレームの間アイドル状態にあるセッションは、アイドルタイムアウト処理の対象と見なされます。アイドルタイムアウトセッションでは、S-GW はピアへのセッションの削除を開始します。
- アイドルタイムアウトは、ネットワーク要件に応じて秒単位で設定されます。タイムアウトの範囲は 1 ～ 4294967295 秒です。
- アイドルタイムアウトの設定は、S-GW サービスレベルで適用され、そのサービスによって処理される一連のサブスクライバのアイドル タイムアウト処理を有効にします。

セッション アイドル タイムアウトの設定

S-GW セッションのセッションアイドルタイマーは、S-GW サービスから設定できます。

S-GW のセッション アイドル タイムアウトを設定するには、次の設定を使用します。

```
configure
   context context_name
      sgw-service service_name
         [ no | default] timeout idle timeout_duration
         end
```

注：

- **timeout idle** *timeout_duration*：システムがセッションを自動的に終了する前に、セッションがアイドル状態を維持できる最大時間を秒単位で指定します。*timeout_duration* は 1 ～ 4294967295 の範囲の整数である必要があります。0 を指定すると、この機能が無効になります。デフォルトでは、この機能は S-GW サービスで無効になっています。

show コマンドの入力と出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show subscribers user-plane-only full all

このコマンドの出力には、この機能をサポートする次のフィールドが表示されます。

- buffered pkts
- buffered bytes
- buffer overflow drop pkts
- buffer overflow drop bytes

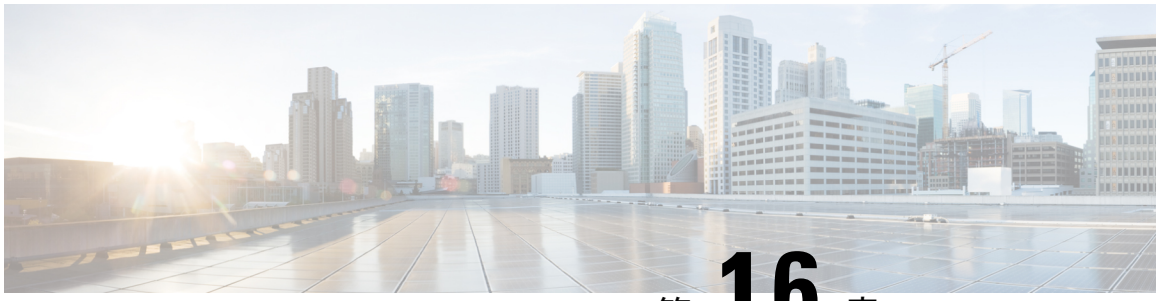
show subscribers user-plane-only full callid <call_id>

サブスクライバごとのバッファリングを確認するには、次の設定を使用します。

- DDN バッファ済みパケット
- DDN バッファ済みバイト
- DDN バッファ オーバーフロー ドロップ パケット
- DDN バッファ オーバーフロー ドロップ バイト

バッファリングされたパケットがバッファリング解除されると、状態はゼロに戻ります。

パケット制限が 5 に達するたびに、その他のパケットは、オーバーフロー ドロップとしてドロップされます。



第 16 章

Collapse コールの DSCP マーキング

- 機能の概要と変更履歴 （229 ページ）
- 機能説明 （230 ページ）
- 機能の仕組み （230 ページ）
- 構成 （234 ページ）
- モニタリングおよびトラブルシューティング （235 ページ）

機能の概要と変更履歴

表 *41* : 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

表 *42* : マニュアルの変更履歴

改訂の詳細	リリース
show subscribers user-plane-only full all および **show user-plane-service statistics qos-group sessmgr all** CLI コマンドの更新された出力を提供。	2022.04.0
初版	2021.02.0

機能説明

現在、QCI ベースの DSCP マーキングは Pure-S および Pure-P コールに適用されます。DSCP マーキングは、それぞれの S-GW サービスまたは P-GW サービスに関連付けられた QCI-QOS マッピングに基づいています。Collapse コールの場合、PGW サービスに関連付けられた QCI-QOS マッピングが適用されます。この機能は、アップリンクおよびダウンリンクトラフィックに関連付けられた S-GW および P-GW サービスに基づいて、Collapse コールに DSCP マーキングを適用するのに役立ちます。アップリンク通信には、論理 P-GW サービスに関連付けられた DSCP マーキングが適用されます。ダウンリンク通信には、論理 S-GW サービスに関連付けられた DSCP マーキングが適用されます。DSCP マーキングは、GTP-U ヘッダーおよび内部 IP の一部としてデータ通信の IP ヘッダーに存在します。CLI 設定でこの機能を有効または無効にするオプションがあります。この機能を有効にすると、新しい機能のみが適用され、有効にしない場合は既存の機能も動作します。デフォルトでは、この機能は無効になっているため、この機能にアップグレードしてもユーザーに影響はありません。

5G 通信の DSCP マーキング

SMF の QCI/QOS マッピング テーブルにより、パケットに適用される DSCP値が決まります。これは、PGW-CP と同様の構成です。DSCP 値は、コール確立中（Sx establishment 要求/Sx modification 要求）時に FAR の一部として送信されます。DSCP 値は、内部パケットと外部 GTPU パケットに適用されています。

4G Collapsed データパスコールに対する DSCP マーキング

Collapsed データパスコールの場合：

- Sxa レッグでは、DSCP マーキングが SGWC/Cn-SGWC から FAR で送信されます。
- N4 レッグでは、DSCP マーキングは SMF から FAR で送信されます。
- アップリンクパケットの場合、UPF は SMF 構成に従って DSCP マーキングを適用します。
- ダウンリンクパケットの場合、UPF は、GTPU ヘッダーの SGWC/Cn-SGWC 構成に従って DSCP マーキングを適用します。
- 内部パケットの場合、DSCP マーキングは SMF 構成に従います。

DSCP マーキングを送信する SMF の構成/ロジックは、PGW-C と同様です。 ECS 課金アクションの DSCP マーキングの場合、内部パケット DSCP マーキングの課金アクションの設定が優先されます。

機能の仕組み

以下に、Collapse コールの DSCP マーキングに関する手順を示します。

- Collapse コールの場合：
  - アクセス側では、SGW サービスに関連付けられている QCI-QOS マッピングテーブルが使用されます。
  - コア側では、PGW サービスに関連付けられた QCI-QOS マッピングテーブルが使用されます。
- 上記の条件は、機能が有効になると適用されます。有効でない場合は、PGW サービスに関連付けられている QCI-QOS マッピングテーブルが、両側に適用されます。
- APN に関連付けられた QCI-QOS マッピングテーブルは、P-GW サービス QCI-QOS マッピングテーブルよりも優先されます。
- APN プロファイルに関連付けられた QCI-QOS マッピングテーブルは、アクセス側の DSCP マーキングでは、SGW サービス QCI-QOS マッピングテーブルよりも優先されます。
- P-GW サービスのみに QCI-QOS マッピングテーブル構成がある場合、これらの DSCP マーキングは Collapse コールのアクセス側とコア側の両方に適用されます。
- S-GW サービスのみに QCI-QOS マッピングテーブル設定がある場合、これらの DSCP マーキングは Collapse コールのアクセス側に適用されます。
- 機能が有効か無効化を示す SAE-GW サービス内に新しい構成パラメータがあります。
- Pure-P から Collapse HO またはその逆の場合、トランスポート層マーキングは Sx Modify 要求の一部として FAR で更新されます。
- レイヤ 2 マーキングも、アクセス側およびコア側で選択された QCI-QOS マッピングテーブルに基づいて変更されます。
- DSCP マーキングは、セッション回復後に既存のベアラーに引き続き適用されます。
- DSCP マーキングは、スタンバイシャーシがアクティブモードに切り替わると、そのシャーシのベアラーで継続されます。

SessMgr SMF の変更

アップリンク/コアおよびダウンリンク/アクセスの DSCP マーキングは、sessmgr_sub_session_t → sessmgr_qci_tab_t 内にベアラーレベルで存在します。

ユーザーデータグラムの DSCP マーキングは、内部パケットの IP ヘッダーで更新されます。つまり、UE からインターネットに、またはその逆に送信されるパケットです。

カプセル化ヘッダーの DSCP マーキングは、GTP-U ヘッダー（外部ヘッダー）を持つ外部 IP レイヤの IP ヘッダーで更新されます。

DSCP マーキングは、次のように FAR IE 内で SMF から UPF に送信されます。

- トランスポート レベル マーキング：DSCP マーキングは、アクセス側のカプセル化ヘッダーと、コア側の Collapse コールのユーザーデータグラムで設定されます。

- トランスポート レベル マーキング オプション：2 つのオプションがあり、外部ヘッダーにのみ適用されます。
  - Copy-inner：内部パケットのマーキングを外部ヘッダーにコピーします。
  - Copy-outer：外部ヘッダーの DSCP マーキングをリレーします。

内部パケットマーキング：DSCP マーキングは、アクセス側のユーザーデータグラムで設定されます。コア側の場合、Collapse コールには適用されません。

Collapse コールを対象に、変更された DSCP マーキングを取得するロジック：

- アクセス/ダウンリンク側では、関連付けられた SGW サービスから、セッションの QCI および「qrp_pl」に基づいて DSCP マーキングをフェッチします。
- コア/アップリンク側では、関連付けられた PGW サービスから、セッションの QCI および「qrp_pl」に基づいて DSCP マーキングを取得します。
- アクセス/ダウンリンク側では、APN プロファイルに関連付けられた QCI-QOS-mapping マッピングテーブルが SGW Service QCI-QOS-mapping テーブルよりも優先されます。
- コア/アップリンク側では、APN 設定に関連付けられた QCI-QOS-mapping テーブルが PGW Service QCI-QOS-mapping テーブルよりも優先されます。
- SGW Service QCI-QOS-mapping マッピングテーブルが設定されていない場合、PGW Service QCI-QOS-mapping テーブルがアクセス側とコア側の両方に適用されます。
- PGW Service QCI-QOS-mapping テーブルが設定されていない場合、SGW Service QCI-QOS-mapping テーブルがアクセス側に適用され、コア側には DSCP マーキングは適用されません。
- DSCP マーキングは、SMF から UPF への Sx/N4 Establishment/Modification 要求の一部として送信される Create/Update FAR によって UPF で更新されます。
- Pure-P から Collapse への HO の場合、またはその逆の場合に、Update FAR IE の一部として Sx/N4 Modification 要求で TLM、IPM、および TLMO を更新します。
- Pure-P から Collapse への HO の場合、またはその逆の場合に、Update FAR IE の一部として Sx/N4 Modification 要求で Layer2 マーキングを更新します。

次の表に、Collapse コールのアクセス側およびコア側に適用される DSCP マーキングのさまざまな設定の組み合わせと結果を示します。

シリアル番号	機能の有効/無効	構成された **PGW Service QOS-QCI** テーブル（**Q1**）	構成された **SGW Service QOS-QCI** テーブル（**Q2**）	構成された **APN QOS-QCI** テーブル（**Q3**）	構成された **APN-Profile QOS-QCI** テーブル（**Q4**）	**Collapse** コールのアクセス/ダウンリンク **DSCP** マーキング	**Collapse** コールのコア/アップリンク **DSCP** マーキング
1	有効	はい	はい	はい	はい	Q4（APN プロファイル）	Q3（APN）

シリアル番号	機能の有効/無効	構成された PGW Service QOS-QCI テーブル（Q1）	構成された SGW Service QOS-QCI テーブル（Q2）	構成された APN QOS-QCI テーブル（Q3）	構成された APN-Profile QOS-QCI テーブル（Q4）	Collapse コールのアクセス/ダウンリンク DSCP マーキング	Collapse コールのコア/アップリンク DSCP マーキング
2	有効	はい	はい	はい	いいえ	Q2（SGW サービス）	Q3（APN）
3	有効	はい	はい	いいえ	はい	Q4（APN プロファイル）	Q1（PGW-service）
4	有効	はい	はい	いいえ	いいえ	Q2（SGW サービス）	Q1（PGW-service）
5	有効	はい	いいえ	はい	はい	Q4（APN プロファイル）	Q3（APN）
6	有効	はい	いいえ	はい	いいえ	Q3（APN）	Q3（APN）
7	有効	はい	いいえ	いいえ	はい	Q4（APN プロファイル）	Q1（PGW-service）
8	有効	はい	いいえ	いいえ	いいえ	Q1（PGW-service）	Q1（PGW-service）
9	有効	いいえ	はい	はい	はい	Q4（APN プロファイル）	Q3（APN）
10	有効	いいえ	はい	はい	いいえ	Q2（SGW サービス）	Q3（APN）
11	有効	いいえ	はい	いいえ	はい	Q4（APN プロファイル）	N/A（DSCP なし）
12	有効	いいえ	はい	いいえ	いいえ	Q2（SGW サービス）	N/A（DSCP なし）
13	有効	いいえ	いいえ	はい	はい	Q4（APN プロファイル）	Q3（APN）
14	有効	いいえ	いいえ	はい	いいえ	Q3（APN）	Q3（APN）
15	有効	いいえ	いいえ	いいえ	はい	Q4（APN プロファイル）	N/A（DSCP なし）
16	有効	いいえ	いいえ	いいえ	いいえ	N/A（DSCP なし）	N/A（DSCP なし）
17	無効	はい	はい	はい	はい	Q3（APN）	Q3（APN）
18	無効	はい	はい	はい	いいえ	Q3（APN）	Q3（APN）

シリアル番号	機能の有効/無効	構成された **PGW Service QOS-QCI** テーブル（**Q1**）	構成された **SGW Service QOS-QCI** テーブル（**Q2**）	構成された **APN QOS-QCI** テーブル（**Q3**）	構成された **APN-Profile QOS-QCI** テーブル（**Q4**）	**Collapse** コールのアクセス/ダウンリンク **DSCP** マーキング	**Collapse** コールのコア/アップリンク **DSCP** マーキング
19	無効	はい	はい	いいえ	はい	Q1（PGW-service）	Q1（PGW-service）
20	無効	はい	はい	いいえ	いいえ	Q1（PGW-service）	Q1（PGW-service）
21	無効	はい	いいえ	はい	はい	Q3（APN）	Q3（APN）
22	無効	はい	いいえ	はい	いいえ	Q3（APN）	Q3（APN）
23	無効	はい	いいえ	いいえ	はい	Q1（PGW-service）	Q1（PGW サービス）
24	無効	はい	いいえ	いいえ	いいえ	Q1（PGW-service）	Q1（PGW-service）
25	無効	いいえ	はい	はい	はい	Q3（APN）	Q3（APN）
26	無効	いいえ	はい	はい	いいえ	Q3（APN）	Q3（APN）
27	無効	いいえ	はい	いいえ	はい	N/A（DSCP なし）	N/A（DSCP なし）
28	無効	いいえ	はい	いいえ	いいえ	N/A（DSCP なし）	N/A（DSCP なし）
29	無効	いいえ	いいえ	はい	はい	Q3（APN）	Q3（APN）
30	無効	いいえ	いいえ	はい	いいえ	Q3（APN）	Q3（APN）
31	無効	いいえ	いいえ	いいえ	はい	N/A（DSCP なし）	N/A（DSCP なし）
32	無効	いいえ	いいえ	いいえ	いいえ	N/A（DSCP なし）	N/A（DSCP なし）

構成

SAEGW サービス内部で次のコマンドを構成して、この機能を有効または無効にします。

```
configure
  context egress
    saegw-service saegw_service_name
      downlink-dscp-per-call-type [ enabled | disabled ]
      end
```

（注） Collapsed コールの場合、この機能を有効にする場合は、ダウンリンクに S-GW service QCI-QOS mapping DSCP マーキングを使用します。デフォルトでは、downlink-DSCP-per-call-type は [Disabled] です。

モニタリングおよびトラブルシューティング

ここでは、Collapse コールの DSCP マーキングのモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドの出力

ここでは、Collapse コールの DSCP マーキングをサポートするために使用できる show CLI コマンドについて説明します。

show saegw-service all

この show コマンドにより、この機能が有効か無効かを確認できます。

```
Service name : SAEGW11
Service-Id : 47
Context : EPC1
Status : STARTED
sgw-service : SGW11
pgw-service : PGW11
sx-service : SX11C
User Plane Tunnel GTPU Service : SAEGW11SXU
Newcall policy : n/a
downlink-dscp-per-call-type : enabled
CUPS Enabled : Yes
Service name : SAEGW21
Service-Id : 25
Context : EPC2
Status : STARTED
sgw-service : SGW21
pgw-service : PGW21
sx-service : SX21C
User Plane Tunnel GTPU Service : SAEGW21SXU
Newcall policy : n/a
downlink-dscp-per-call-type : disabled
CUPS Enabled : Yes
```

show subscribers user-plane-only callid <call_id> far full all

このユーザープレーン CLI を使用して、アップリンク/ダウンリンク FAR のトランスポートレベルのマーキングオプションと内部パケットマーキングを検証します。

show subscribers user-plane-only full all

U/L および D/L の TOS マーク付きパケット数を表示するには、次のユーザープレーン CLI を使用します。

```
ToS marked Uplink Pkts: 0
ToS marked Downlink Pkts: 0
```

show user-plane-service statistics qos-group sessmgr all

このユーザープレーン CLI を使用して、QoS グループ Sessmgr インスタンスの U/L および D/L パケットの統計を表示します。

```
Uplink Packets Marked: 0
Downlink Packets Marked: 0
```



第 17 章

ダイナミックおよび静的 PCC ルール

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 237
- 機能説明, on page 238
- 定義済み PCC ルールをプロビジョニングする, on page 239
- ダイナミック PCC ルールのサポート, on page 240
- ポリシング （241 ページ）
- 帯域幅ポリシー構成の制限 （242 ページ）
- 静的ルールおよび事前定義済みルールのレート制限, on page 243
- ダイナミックルールのレート制限, on page 243
- 標準準拠, on page 245
- URR ID を構成する, on page 245
- しきい値の設定, on page 246

機能の概要と変更履歴

要約データ

Table 43: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 44: マニュアルの変更履歴

改訂の詳細	リリース
次に対するサポートが追加されました： • フローレベルのポリシング • 帯域幅ポリシーあたりの最大グループ数を増加する	2021.01.0
最初の導入。	2020.02.0

機能説明

ダイナミック PCC ルールは、HTTP インターフェイス経由で、PCF から PCEF にプロビジョニングされ、PCF で事前定義されり/静的であったり、または動的に生成されます。ダイナミック PCC ルールは、任意のタイミングでインストール、変更、および削除できます。

定義済み PCC ルールは、PCRF で構成され、PCF や PCEF は、任意のタイミングでアクティブ化または非アクティブ化できます。PCEF 内の静的 PCC ルールをグループ化すると、PCRF は HTTP 参照ポイントで一連の静的 PCC ルールを動的にアクティブ化できます。PCEF によってローカルにアクティブ化されるこれらの静的 PCC ルールは、PCF では明示的に認識されませんが、PCF は単に PCF からアクティブ化される静的 PCC ルールの識別子を認識します。

機能の仕組み

定義済み PCC ルールのサポート

Config URR ID は、静的ルールと事前定義ルールに適用されます。サブスクライバコールが発生すると、rulebase の静的ルールを通過します。バケツ ID をキーとして使用するサブスクライバプライマリ URR は、課金アクション構成があるさまざまなインターフェイス向けに対応する URR バケツを更新します。ダイナミックルールと事前定義済みルールの場合、PDR の URR ID リストは、ユーザープレーンで、URR バケツを作成します。

Cisco SMF と UPF が課金アクションでベンダーに依存しない方法で独立して動作できるようにするためのエコシステムの変更は、次のとおりです。

- UPF で構成可能な「Config URR」
- しきい値のローカル構成を有効にする UPF

定義済み PCC ルールをプロビジョニングする

事前設定された PCC ルールは、SMF（5GC の場合）で事前設定されます。定義済み PCC ルールは、PCF が任意のタイミングでアクティブ化または非アクティブ化できます。定義済み PCC ルールをグループ化すると、PCF は 動的に PCC ルール一式をアクティブ化できます。SMF は、次の方法で、UPF の PCF によってアクティブ化および事前定義された PCC ルールを適用できます。

- アクティブ化および事前定義された PCC ルールおよび対応する QoS および課金制御情報によってそれぞれ参照されるサービスデータフィルタまたはアプリケーション ID を決定します。
- サービスデータフロー、事前定義された PCC または ADC ルールが参照するアプリケーションを特定するために必要な PDR が無い場合は、作成します。
- サービスデータフローまたはアプリケーションレベルで QoS 適用に向けて必要な QER を作成します。
- 検出されたサービスデータフローまたはアプリケーション通信を転送するために QoS フローバインディングおよび QoS 制御の結果として、あるいは、事前定義された PCC ルールに含まれている場合に、リダイレクトまたは通信ステアリング制御を適用するために、新しい FAR を作成する必要がある場合は、必要な FAR を作成します。
- 事前定義された PCC ルールに含まれている場合、各 Monitoring Key、Charging Key、Charging Key と Service ID の組み合わせまたは、Charging Key、Sponso ID および Application Service Provider ID の組み合わせに対して必要な URR を作成します。

および、後で次の方法で：

- 作成した URR に新規作成された PDR を関連付けます。
- 既存の FAR または新しい FAR を新規作成された PDR に関連付けます。

必要に応じて、多くの PFCP セッションに共通の通信処理ポリシー（つまり、事前定義された QER、FAR、URR）をUPF で構成できます。SMF は、次のいずれかに Activate Predefined Rules IE を含めることで、これらの通信処理ポリシーをアクティブ化できます。

- PFCP Session Establishment 要求の Create PDR IE
- PFCP Session Modification 要求の Create PDR IE

アクティブ化および事前定義されたルールと関連付けられた PDR と一致する通信の場合、UPF は、ルールを適用します。たとえば、URR の場合、UPF は、使用状況レポートを生成し、それを SMF に送信し、SMF は、その使用状況レポートを処理します。

UPF の事前定義されたルールによってトリガーされるレポートで使用される URR ID も、SMF で事前設定されます。

ダイナミック PCC ルールのサポート

ダイナミック PCC ルールの場合、パケット転送制御プロトコル（PFPC）セッションごとに複数のフローがサポートされます。

- 5G QoS モデルでは、サブスクリプション関連および呼び出し関連の優先順位メカニズムに基づいて、特定のサービスの分類と差別化を行うことができます。これらのメカニズムは、優先順位が のQoS フローを呼び出す、変更、維持、リリースしたり、ネットワーク輻輳条件でのQoS特性に従ってQoS フローパケットを配信したりする機能を提供します。
- 5G QoS モデルは、QoS フローに基づいています。5G QoS モデルは、保証されたフロービットレートを必要とする QoS フロー（GBR QoS フロー）と、保証されたフロービットレートを必要としないQoS フロー（非 GBR QoS フロー）の両方をサポートします。
- QoS フローは、PPDU セッションにおける QoS 差別化の最小単位です。QoS フロー ID（QFI）は、5G システムで QoS フローを識別するために使用されます。PDU セッション内で同じ QFI を持つユーザープレーン通信は、同じ通信転送処理（スケジューリング、アドミッションしきい値）を受信します。
- 5GS 内では、デフォルトの QoS ルールに関連付けられた QoS フローを PDU セッションに対して確立する必要があり、PDUセッションのライフタイム全体にわたって確立されたままになります。この QoS フローは、非 GBR QoS フローである必要があります。
- QoS フローは、QoS パラメータおよび QoS 特性で指定されている QoS 要件に関連付けられます。QoS フローは、その QoS プロファイルに応じて「GBR」または「非 GBR」のいずれかになります。
  - 各 QoS フローの場合、QoS プロファイルには QoS パラメータが含まれます。
    - 5G QoS Identifier（5QI）
    - Allocation and Retention Priority（ARP）
  - 各 GBR QoS フローについてのみ、QoS プロファイルには QoS パラメータも含まれている必要があります。
    - 保証されているフロービットレート（GFBR）：UL と DL
    - 最大フロービットレート（MFBR）：UL と DL
  - GBR QoS フローのみの場合、QoS プロファイルには 1 つ以上の QoS パラメータも含まれる場合があります。
    - 通知の制御
    - 最大パケット損失レート：LD と DL

PDR の作成または変更中、UPF はフローでの QoS 適用に向けて QER を受信します。

QoS 適用ルール相関 ID は、複数の PFCP セッションコンテキストから QER を関連付けるために CP 機能によって割り当てられます。たとえば、PGW-U での APN-AMBR の適用は、同じ APN に対する UE のすべての PDN 接続の非 GBR ベアラーに対応するすべての PDR に関連付けられた異なる PFCP セッションの QER に、同じ QoS 適用ルール相関 ID を設定することで実現されます。複数の PFCP セッションの同じ QoS 適用ルール相関 ID に関連付けられている QES は、それらの各 PFCP セッションの同じ QER コンテンツを使用してプロビジョニングされます。QoS 適用ルール相関 ID は、UE が EPC にある場合に、APN-AMBR を適用する場合のみに使用され、N4 経由で CP 機能によって UP 機能に提供され、PDU セッションは、後の段階で EPC に移動する場合があります。

UPF は、5G PFCP セッション向けの QoS 適用ルール相関 ID を受信して、それを適用します。

ポリシング

ポリサー設定では、セッションマネージャからの入力を使用します。これらの入力は、PCF から AMBR として、またはフローレベルの QoS 情報から受信されます。セッションレベルの AMBR ポリシングでは、PCF から受信した値を常に許可します。ただし、フローレベルのポリシングがある場合は、それが優先され、AMBR ポリシングが順番に適用されます。つまり、ポリサーエンジンは階層型ポリシングを適用します。最初にフローレベル/ルールの帯域幅制限が適用され、次にセッションレベルの帯域幅制限が適用されます。



（注） RAR または CCA-U を介したセッション実行時の AMBR の変更が適用されます。

セッションマネージャから受信した入力値は、ポリサー設定およびポリサートークンバケットにプッシュされます。アップリンクまたはダウンリンクの各方向に対し、ポリサー設定とポリサートークンバケット用の新しいレコードが作成されます。

ポリサー設定はポリサーエンジンの参照先であり、ポリサートークンバケットは値の計算と復元に使用されます。

現在、ポリシングは、PCF から受信した AMBR およびダイナミックルールのルールレベルの QoS 情報に対してサポートされています。静的ルールおよび事前定義ルールの場合、帯域幅制限は帯域幅ポリシー設定によって実施されます。SMF の Active Charging Service Configuration モードの bandwidth-policy 構成で設定された拡張ビットレートは、RCM によって UPF に提供され、同じものが、UPF によってポリシングに適用されます。拡張ビットレートを使用した帯域幅ポリシーの設定例を次に示します。

```
configure
  active-charging service ACS
    bandwidth-policy BWP

      flow limit-for-bandwidth id 1 group-id 2

      flow limit-for-bandwidth id 2 group-id 3
      flow limit-for-bandwidth id 100 group-id 100


     group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
```

```
 discard
      group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000
violate-action discard
     group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
 lower-ip-precedence
      group-id 5 direction downlink peak-data-rate 300000 peak-burst-size 1200
violate-action lower-ip-precedence committed-data-rate 256000 committed-burst-size 1000
 exceed-action lower-ip-precedence
      group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
      group-id 100 direction uplink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
      exit
    charging-action catchall
      flow limit-for-bandwidth id 1
      exit
    rulebase cisco
      bandwidth default-policy BWP
      exit
    end
```

制限事項

このリリースでは、ポリシングに次の制限があります。

- **bandwidth-policy** の変更はサポートさません。
- トークンの補充などのその他機能（APN レベルと ACL レベルの両方）との通信は、サポートされていません。
- 現在、ポリサーベースの統計はサポートされていません。ネットワーク パフォーマンス モニタリング ツールを使用すると、帯域幅制限を確認できます。

帯域幅ポリシー構成の制限

ユーザーは、ダウンリンクとアップリンクの両方のパケットに対して、SMF と UPF の両方で帯域幅制限を構成できます。この構成は、帯域幅制限構成がすべての課金アクションで同じであっても、事前定義された PCC ルールのすべての課金アクションで行われます。

これらの設定を最適化するために、帯域幅IDを定義して、すべての帯域幅関連の構成を含め、課金アクションで帯域幅 ID を関連付ける必要があります。

帯域幅の値が変更されると、新しいサブスクライバは設定された帯域幅の値を使用し、既存のサブスクライバは古い値を使用し続けます。

帯域幅ポリシー構成の制限を次に示します。

- 帯域幅ポリシーの最大数：64
- 帯域幅ポリシーあたりのグループの最大数：1000
- 帯域幅ポリシーごとの帯域幅 ID の最大数：1000
- 帯域幅ポリシー全体のグループの最大数：10000

- 帯域幅ポリシー全体の帯域幅 ID の最大数：10000

静的ルールおよび事前定義済みルールのレート制限

静的ルールおよび事前定義ルールの場合、帯域幅制限は帯域幅ポリシー設定によって実施されます。帯域幅ポリシーは、Active Charging Service 構成モードの SMF および UPF で構成する必要があります。

次に、拡張ビット レートを使用した帯域幅ポリシーの構成例を示します。

```
config
   active-charging service ACS
      bandwidth-policy BWP
         flow limit-for-bandwidth id 1 group-id 2
         flow limit-for-bandwidth id 2 group-id 3
         flow limit-for-bandwidth id 100 group-id 100
         group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000
violate-action discard
         group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000
violate-action discard
         group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200
violate-action lower-ip-precedence
         group-id 5 direction downlink peak-data-rate 300000 peak-burst-size 1200
violate-action
         lower-ip-precedence committed-data-rate 256000 committed-burst-size 1000
exceed-action
         lower-ip-precedence
         group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
 4294967295 violate-action discard
         group-id 100 direction uplink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard
         exit
      charging-action catchall
         flow limit-for-bandwidth id 1
         exit
      rulebase cisco
         bandwidth default-policy BWP
         exit
         end
```

Note UPF は、帯域幅ポリシー構成の変更をサポートしません。

ダイナミックルールのレート制限

3GPP TS 29.244 に従い、以下の Information Element（IE）は、Session Establishment または Modification 要求の Create QER または Update QER の QoS 適用に向けて SMF から受信します。

- 最大ビットレート：この IE は、この PDR に一致するパケットに MBR 適用アクションが適用されている場合に存在します。存在する場合、この IE は、PDR に一致するパケット

に適用されるアップリンクやダウンリンクの最大ビットレートを示します。5GCの場合、この IE は次の値に設定できます。

- Session-AMBR：PDU セッションの GBR 以外の QoS フローのすべての PDR が参照する QER 向け。
- QoS フロー MBR：QoS フローのすべての PDR が参照する QER 向け。
- SDF MBR：SDF のすべての PDR が参照する QER 向け。

- Guaranteed Bitrate：この IE は、GBR がこの PDR と一致するパケットで認証されている場合に存在します。存在する場合、この IE は、承認されたアップリンクやダウンリンクの保証ビットレートを示します。この IE は、次の値に設定できます。
  - 集約 GBR：GBR ベアラーのすべての PDR が参照する QER 向け。
  - QoS フロー GBR：QoS フローのすべての PDR が参照する QER 向け。
  - SDF GBR：SDF のすべての PDR が参照する QER 向け。
- QoS flow identifier（QFI）：この IE は、UPF が、QoS フロー識別子を挿入した場合に存在します。
- Gate Status：この IE は、パケットが転送できるかどうか（ゲートが開いている）、またはアップリンクやダウンリンク方向で破棄されるかどうか（ゲートが閉じている）を示します。
- QER Correlation ID：この IE は、同じ APN への複数 UE の PDN 接続に対して APN-AMBR の適用を行うために、UP 機能で複数の PFCP セッションの QER を関連付ける必要がある場合に存在します。

Note 該当しませんが、UPF が 5G PFCP セッションの QoS Enforcement Rule Correlation ID を受信した場合は、それを適用します。

SMF は、SDF、QoS フロー、およびセッションを表す必要な PDR を作成し、次のようにそれぞれの QER を関連付けることにより、UPF で QoS 適用をプロビジョニングします。

- セッションレベル、SDF レベルで QoS 適用の QER を作成します。
- 同じ GBR QFI を持つ SDF の集約の QoS 適用のために QER を作成します。
- セッションレベルの QER を、セッションに定義されているすべての PDR に関連付けます。
- SDF またはアプリケーション QER を、SDF またはアプリケーションに関連付けられた PDR に関連付けます。
- SDF の集約の QER を、SDF または QER を共有するアプリケーションに関連付けられた PDR に関連付けます。

標準準拠

SMF と UPF 間の N4 インターフェイスは、3GPP TS 23.501 および 3GPP TS 23.502 で規定されています。

URR ID を構成する

Config URR ID は、デフォルトのベアラーにバインドされた静的ルールと事前定義済みルールに適用されます。サブスクライバコールが発生すると、Rulebase 内の静的ルールが通過されます。課金アクションで設定されたさまざまなインターフェイスに対応する URR バケツは、バケツ ID をキーとしてサブスクライバのプライマリ URR リストで更新されます。ダイナミックルールおよび専用ベアラーをバインドする事前定義されたルールの場合、PDR の URR ID リストは、UP の URR バケツの作成に使用されます。

現在、設定 URR ID は、SessCtrl で実行中のカウンタを使用して生成されます。

構成可能な Config URR ID を実現するには、次の手順を実行します。

- 課金アクション外の構成テンプレートで、「Rating Group」と「Service-id」との URR-ID マッピングが許可されます。
- Gy 用に別の Rating Group（RG）が設定されている場合、その RG が Gy バケツに適用されます。Gy に個別の RG が設定されていない場合は、すべてのインターフェイスに同じ「Content-ID」が適用されます。
- URR-ID マッピングでは「Service-id」はオプションです。
- URR-ID は一意です。これは、**show configuration error** CLI コマンド、個別の検証スクリプト、または構成時のチェックを通じて確実に実施する必要があります。
- UPF の場合、URR-ID 生成の値は構成から取得されます。UP は、PFD メッセージではなく、構成から Config URR-ID を受信します。PFD メカニズムは、SMF と UPF の間では使用されません。
- SMF は、URR-ID リストの構成をサポートしません。
- URR-ID は、rating group/content-id、service-id などを持つ静的ルールまたは事前定義ルールの UPF および SMF で個別に生成されます。

以下は、URR-ID プロファイルテンプレートの構成例です。

```
rg <x> si <y> urr-id <abc>
rg <x1> si <y1> urr-id <abc1>
rg <x> urr-id <abc2>
```

次の構成を使用して、Config URR ID を有効にします。

```
configure
   active-charging service service_name
      urr-list list_name
```

```
          rating-group group_number { service-identifier service_number |
urr-id id_range }
          end
```

注：

- **urr-list** *list_name*：Active Charging Service URR リストを構成します。*list_name* は、1 ～ 63 の英数字で指定する必要があります。
- **rating-group** *group_number* **:** 前払い課金で使用するレーティング ID を指定します。*group_number* は、1 ～ 2147483647 の整数で指定する必要があります。
- **service-identifier** *service_number* **:** サービスに付与する番号を指定します。
- **urr-id** *id_range* **:** レーティングやサービスグループの URR 識別子を指定します。 *id_range* は、1 ～ 134217727 の範囲で指定する必要があります。
- 値は動的に変更できます。ただし、新しいセッションに対してのみ有効になります。

しきい値の設定

GTPP グループの構成は、UPF でのしきい値の計算に必要です。

UPF は、APN 構成から使用可能な GTPP グループ名を使用します。APN 構成では、1 つの GTPP グループのみを関連付ける必要があります。

以下に設定サンプルを示します。

```
configure
  context context_name
    apn apn_name
      gtpp group group_name
      ip context-name name
      exit
    gtpp group group_name
      gtpp egcdr service-data-flow threshold interval interval
      gtpp egcdr service-data-flow threshold volume downlink bytes
      gtpp egcdr service-data-flow threshold volume uplink bytes
      gtpp egcdr service-data-flow threshold total bytes
      end
```

オフライン URR で上記の service-data-flow しきい値のいずれかがヒットした場合、UPF は SX_SESSION_REPORT_REQUEST をデータ量を報告する SMF に送信します。



第 18 章

ECS 正規表現

- 機能の概要と変更履歴 （247 ページ）
- 機能説明 （248 ページ）
- 機能の仕組み （248 ページ）
- 正規表現ルールの設定 （250 ページ）
- 設定例 （250 ページ）
- モニタリングおよびトラブルシューティング （250 ページ）

機能の概要と変更履歴

要約データ

表 *45 :* 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点：	N/A
関連資料	該当なし

更新履歴

表 *46 :* マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.2

機能説明

ECS 正規表現機能は、ユーザープレーン機能（UPF）での正規表現エンジンの実装をサポートします。さらに、この機能では、RCM 経由で正規表現ルールを構成できます。

UPF は、正規表現エンジンの再構築とルール照会の一環として、次のプロトコルをサポートします。

- HTTP
  - URL
  - URI
  - HOST
- WWW
  - URL
  - URI
- RTSP
  - URL
  - URI

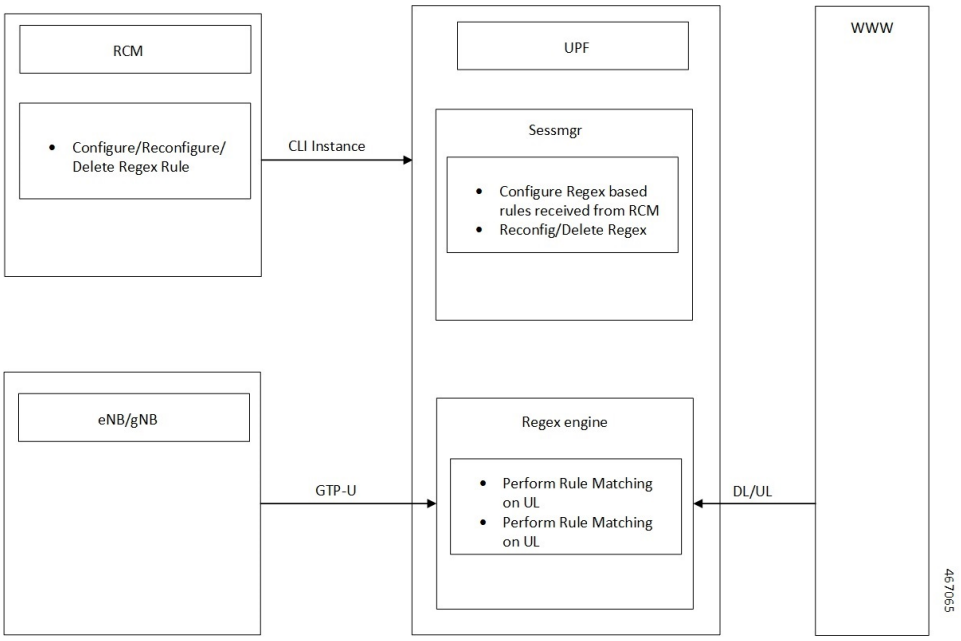
機能の仕組み

次の表に、正規表現ルールで使用できる特殊文字を示します。

表記法	説明
*	0 字以上の文字
+	+ の前のトークンを 0 回以上繰り返すインスタンス
?	0 または 1 文字
\character	エスケープ文字

表記法	説明
\?	疑問符に相当（\<ctrl-v>?）
\+	プラス記号に相当
*	アスタリスクに相当
\a	アラート（ASCII 7）
\b	バックスペース（ASCII 8）
\f	改ページ（ASCII 12）
\n	改行（ASCII 10）
\r	改行（ASCII 13）
\t	タブ（ASCII 9）
\v	垂直タブ（ASCII 11）
\0	Null（ASCII 0）
\\	バックスラッシュ
角カッコで囲まれた範囲 [0-9]	範囲内のいずれか 1 文字と一致する。
範囲の先頭の ^	範囲内に一致するものなし。他のすべての文字はそのものを表す。
.\x##	2 桁の 16 進表記で指定された任意の ASCII 文字。たとえば、\x5A は「Z」となる。

次の図は、RCM による正規表現ルールの構成を示しています。



正規表現ルールの設定

UPF CLI インスタンスを使用して RCM 経由で、または CLI 経由で UPF で直接正規表現ルールを構成します。

```
configure
   require rcm-configmgr
   end
```

設定例

次に、正規表現ルールを構成するための構成例を示します。

```
configure
   active-charging service <service_name>
      ruledef <ruledef_name>
         http url regex <regex_url>
         rtsp uri regex <regex_uri>
         www url regex <regex_url>
         end
```

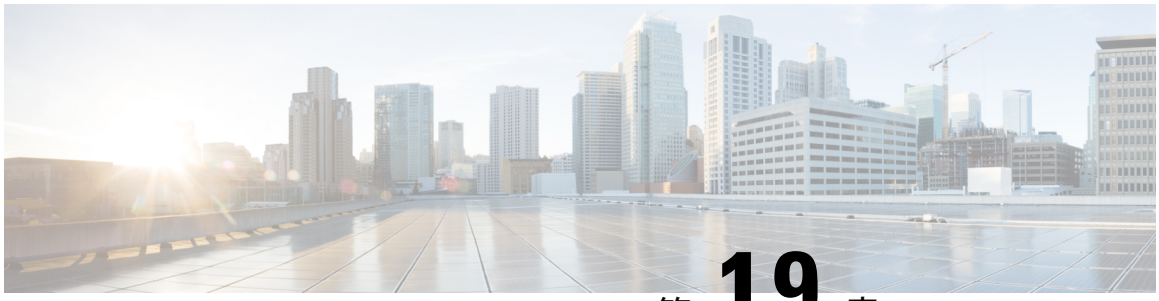
モニタリングおよびトラブルシューティング

この項では、この機能を監視して、障害対応を行うために使用可能な CLI コマンドについて説明します。

show コマンドと出力

この項では、UPF の ECS 正規表現機能をサポートするために使用可能な show コマンドの情報について説明します。

Show コマンド	説明
show user-plane-service regex status	このコマンドを使用すると、SessMgrインスタンスのエンジン状態を表示できます。
show user-plane-service regex statistics memory	このコマンドを使用すると SessMgr インスタンスのメモリ統計を表示できます。
show user-plane-service regex statistics memory summary	このコマンドを使用すると SessMgr の統合されたメモリ概要を表示できます。
show user-plane-service regex statistics ruledef	このコマンドを使用すると SessMgr の 正規表現 ruledef 統計を表示できます。
show user-plane-service regex statistics ruledef summary	このコマンドを使用すると SessMgr の統合 ruledef 統計の概要を表示できます。



第 19 章

GTP-U のサポート

- 機能の概要と変更履歴, on page 253
- 機能説明, on page 254
- 機能の仕組み, on page 255
- S5u/N3 インターフェイスでデュアル スタック サポートを有効にする （259 ページ）
- UDP チェックサムを無効にする （259 ページ）

機能の概要と変更履歴

要約データ

Table 47: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 48: マニュアルの変更履歴

改訂の詳細	リリース
このリリースでは、UDP チェックサムの最適化が追加されています。	2021.02.0

改訂の詳細	リリース
初版	2020.02.0

機能説明

Table 49: 機能の履歴

機能名	リリース情報	説明
S5uインターフェイスでのデュアルスタックのサポート	2024.02.0	UPFは、S5uインターフェイスのSGW-UとPGW-U間のIPv4およびIPv6接続を処理するためにデュアルスタックをサポートしています。 **[デフォルト設定（Default Setting）]**：有効 – 常時オン
S1-UおよびN3インターフェイスでのデュアル スタックのサポート	2024.01	UPFは、N3およびS1-Uインターフェイスで IPv4およびIPv6接続を処理するためのデュアルスタックをサポートしています。 **[デフォルト設定（Default Setting）]**：有効 – 常時オン

3GPPでは、5Gおよび4G NASの両方をサポート可能なUEがE-UTRANおよび5Gコアネットワークに接続するための規定を定めています。

EPSから5GSへのハンドオーバー中にデータ（G-PDUおよびEnd Markerパケット）を転送するために、SMFは次のタスクを実行します。

- E-RABごとに1つのPDRをプロビジョニングします（少なくとも1つのQoSフローのデータ転送をサポート）。
- 各PDRに1つのQERを作成して関連付け、QFIを含むGTP-U PDU Session Container拡張ヘッダーを挿入するようUPFに要求します。PDRには、E-RABにマッピングされたQoSフローの1つのQFI値に設定されたQFI IEが含まれます。

5GSとEPS間のハンドオーバー中のデータ転送は、次のようにサポートされます。「3GPP TS 38.300」を参照してください。

- 5Gから4Gへのハンドオーバーの場合、送信元NG-RANノードは、同じE-RABにマッピングされたQoSフローの1つのQFIを含む1つまたは複数のend-markerを送信し、PDUセッショントンネル経由でend-markerパケットをUPFに送信します。UPFはQFIを削除し、SGWへの適切なE-RABトンネルにマッピングします。

- 4G から 5G へのハンドオーバーの場合、送信元の eNB は、EPS ベアラートンネルで受信したエンドマーカーを SGW に転送します。その後、SGW はそれらを UPF に転送します。UPF は、その E-RAB にマッピングされた QoS フローの中で 1 つの QFI を end-marker に追加します。次に、UPF はそれらの end-marker をPDU セッションごとのトンネル内のターゲット NG-RAN ノードに送信します。

Note UPF は、S1-U、S5u、 および N3 GTP-U インターフェイスを介した IPv4 および IPv6 接続を処理するためのデュアルスタックをサポートします。

エラー表示と GTP-U パス障害

UPF 機能は、存在しない TEID が設定されている GTP-PDU を受信したときに、GTP-U ピアに関する Error Indication メッセージを送信者に通知します。この通知により、古いセッションやベアラーがなくなり、ネットワーク内の一貫性が維持されます。

SMF ノードと UPF ノード間の Error Indication と GTP-U Path Failure は、N4 インターフェイスでサポートされます。ネイバーノードの場合は、S1u/S5u インターフェイスでサポートされます。

本実装では、エラー表示と GTP-U パス障害についてローカルパージまたはシグナルピ アの動作バリエーションが考慮されています。

- Error Indication を受信すると、UPF は TEID および GTPU ピア情報を SMF に伝達して、GTPU ピアの削除または変更を確認します。
- 存在しない TEID が設定されている GTP-U パケットを受信すると、UPF は Error Indication を生成し、TEID および GTPU ピアエントリを使用して送信します。
- セッションやベアラーの削除は、SMF または UPF での Path Failure 検出に基づいて判断されます。
- GTP-U Path Failure は、UPF ノード間および UPF ノードと SMF ノード間で GTP-U echo メッセージを使用して検出されます。

機能の仕組み

コール フロー

MME と S-GW 経由の E-UTRAN での初期接続

E-UTRAN/EPS での初期接続は、3GPP TS 23.401、5.3.2.1 項で定義されている手順に従います。

次の図は、E-UTRAN/EPS での初期接続に関する 3GPP リファレンスから派生したコールフローを示しています。

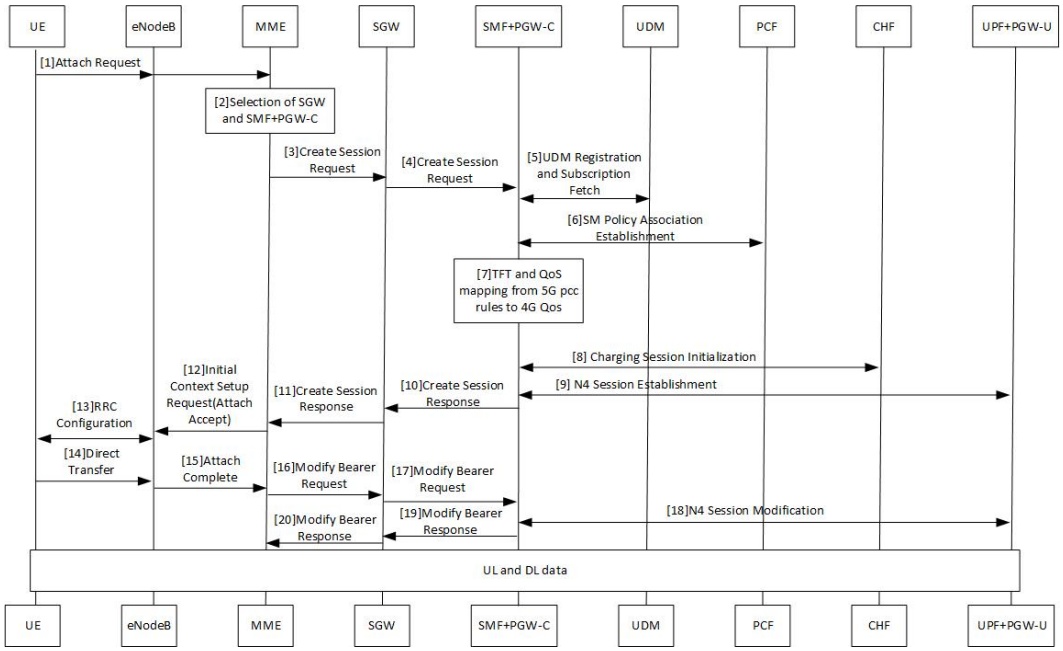


***Table 50: 5G* コア経由の *E-UTRAN* での初期接続コールフロー**

ステップ	説明
1	手順 9 では、SMF+PGW-C は UPF の選択を実行し、N4 Session Establishment 手順を実行します。このセッションは、SMF+PGW-C に接続されている 4G セッションため、各ベアラ-に対して、別の CN トンネルが作成され、QFI は、QER と PDR に送信されません。また相関 ID が存在する場合があります。
2	手順 18 では、SMF+PGW-C は、N4 Session Modification を実行して、UPF のデータパスで eNodeB TEID を更新します。

3GPP 仕様は、LTEから 5G NR、またはその逆への UE のモビリティを実現するメカニズムを提供します。このモビリティは、AMF と MME 間の N26 インターフェイスの有無にかかわらず、2 つの異なるアーキテクチャで実現されます。

N26 インターフェイスを使用する 5G から EPS へのハンドオーバー

N26インターフェイスを使用した5GからEPSへのハンドオーバーは、3GPP TS 23.502、4.11.1.2.1 項で定義されています。次の図は、N26インターフェイスの詳細なコールフローを示しています。

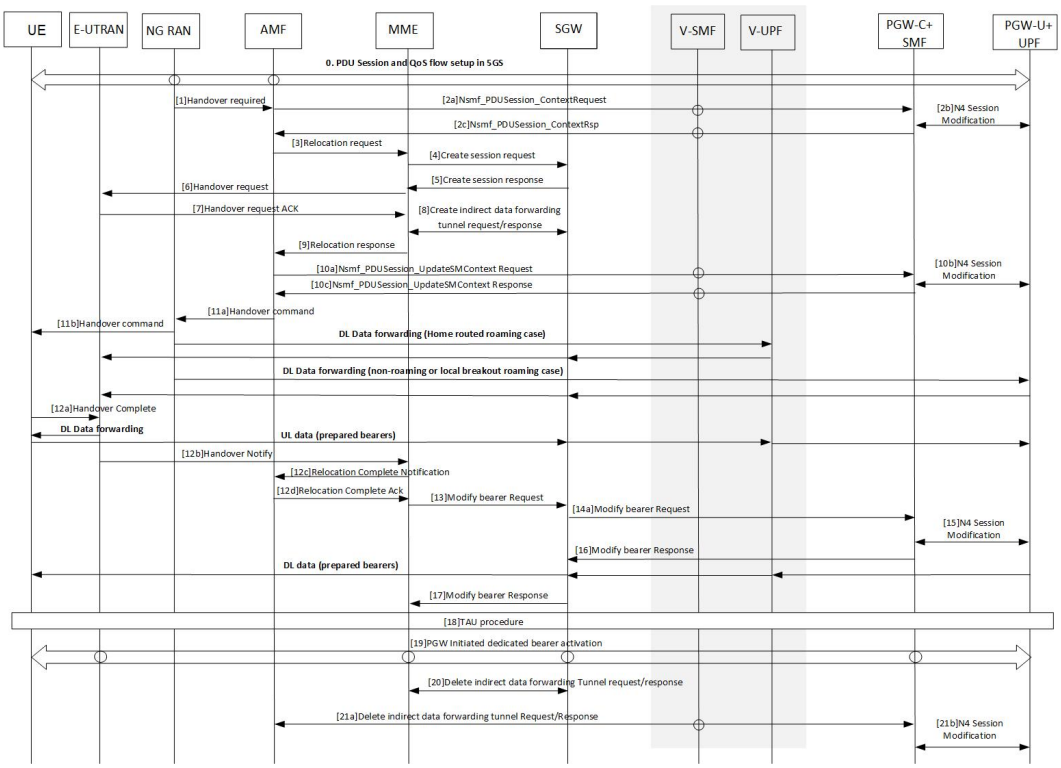


Table 51: N26 インターフェイスを使用する ***5G*** から ***EPS*** へのハンドオーバーのコールフロー

ステップ	説明
1	手順 2b では、SMF+PGW-C は N4 Session Modification を UPF に送信して、各 EPS ベアラーの CN トンネルを確立します。PCC から受信した 5G QoS および PCC ルールへのベアラー マッピングは、SMF にすでに存在している必要があります。SMF には、Bearer ID Allocation 手順から取得したベアラー ID も必要です。SMF + PGW-C は、N4 セッションの新しい PDR を作成し、4G システムのリクエストに応じて各ベアラー割り当てられる TEID を取得します。
2	手順 10b では、SMF + PGW-C は、N4 Modification 要求を UPF に送信して追加の PDR と FAR を作成し、NG RAN からの間接トンネル経由でリダイレクトされた DL データを受信し、それらを eNodeB に転送します。子の場合、アップリンク PDR は、NG RAN から転送された DL データと一致するために QFI が設定されている必要があり、データをeNodeB に転送する必要があるため、関連付けられた QER は QFI を持ちません。また、FAR は、受信したデータを QFI に基づいて適切なトンネルを介して eNodeB にリダイレクトします。
3	手順 11 では、データ転送の QoS フローに示されている QoS フローの場合、NG-RAN は、PDU セッションごとのデータ転送の CN トンネル情報に基づいて、UPF を介したデータ転送を開始します。次に、UPF は、5GS 内のデータ転送トンネルから受信したデータを EPS 内のデータ転送トンネルにマッピングし、サービング GW 経由でターゲット eNodeB にデータを送信します。

ステップ	説明
4	手順 15 では、SMF は N4 Modification 要求を UPF に送信し、E-UTRAN への DL データパスをアクティブにします。この時点で、間接トンネルと直接 DL パスの両方が eNodeB に対してアクティブになります。
5	手順 21 では、SMF は N4 Modification 要求を UPF に送信し、間接転送トンネルを削除します。

N26 インターフェイスを使用した、または N26 インターフェイスを使用しない EPS から 5G および 5G から EPS へのハンドオーバーに関連するその他のコールフローは、3GPP 23.502、4.11.1.2.1 項および 4.11.2 項で定義されています。

UP での Error Indication の処理

UPF で Error Indication を受信すると、TEID および GTP-U ピアアドレスを含むリモート F-TEID が記載されている Error Indication Report と一緒に PFCP Session Report 要求が開始されます。

- PGW-U の場合、Error Indication メッセージは、S5u 経由で送受信されます。
- SAEGW-U の場合、エラー通知メッセージは S1u を介して送受信されます。
- SGW-U の場合、エラー通知メッセージは S1u および S5u を介して送受信されます。

セッションまたはベアラーが存在しない TEID を使用してデータパケットを受信すると、UPF はピアに対して TEID および GTPU ピアアドレスを含む Error Indication を生成します。

UP での GTP-U パス障害のサポート

GTP-U Echo 要求は、UPF で設定された間隔に従って開始され、定期的に送信されます。GTP-U Echo 応答は、GTPU トンネル経由で SMF から受信した GTP-U Echo 要求に対して送信されます。

GTP-U Echo 要求に対する 応答を受信しない場合、UPF は設定された再送信タイムアウトと最大再試行回数に基づいて Echo 要求を再試行します。最大試行回数分の再試行を実行すると、UPF は、PFCP ノードを開始します。

レポート要求（ノード ID、ノードレポートタイプ、リモート GTP-U ピアを含むユーザープレーンパス障害レポート）。

UPF は、PFCP Node Report 応答と PFCP Session Deletion 要求を受信して、セッションを削除し、使用量レポートを含む削除リクエストへの応答を返します。

S5u/N3 インターフェイスでデュアル スタック サポートを有効にする

S5u/N3 インターフェイスでデュアルスタックを有効にするには、次の構成例を使用します。

```
context SAEGW
    interface pgw-gtpu loopback
      ip address 81.81.20.5 255.255.255.255
    exit

    gtpu-service pgw-gtpu
      no udp-checksum
      bind ipv4-address 81.81.21.x ipv6-address 2001:4888:81:81::21:5 bearer-type all
    exit

    user-plane-service user_plane_svc
      associate gtpu-service pgw-gtpu upf-ingress
      associate gtpu-service SxC cp-tunnel
      associate sx-service sx-svc
      associate fast-path service
      associate control-plane-group SAEGW
    exit
```

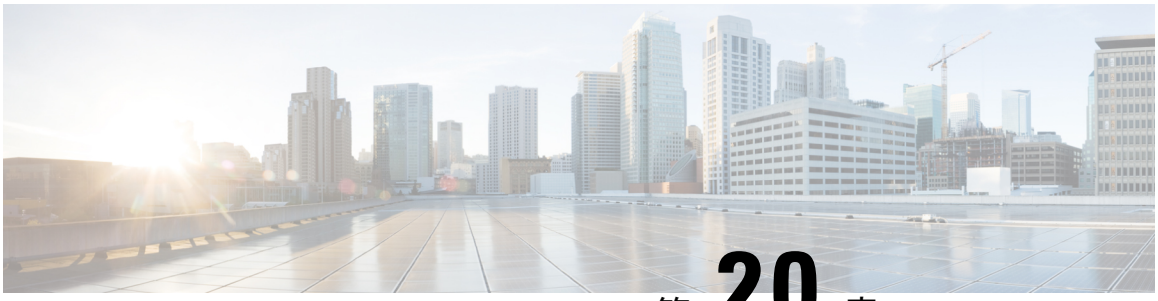
UDP チェックサムを無効にする

この機能は、GTP-U パケットの UDP ヘッダーの UDP チェックサムを無効にします。UDP チェックサムの値を 0 に設定します。

UDP チェックサムを無効にする

次の構成を使用して、GTP-U パケットの UDPヘッダーの UDP チェックサムを無効にします。

```
configure
   context context_name
      gtpu-service service_name
         no udp-checksum
         end
```



第 20 章

N4/Sx インターフェイスのハートビートサポート

- 機能の概要と変更履歴, on page 261
- 機能説明 （262 ページ）
- 機能の仕組み （262 ページ）
- N4/Sx インターフェイスのハートビートを構成する （263 ページ）
- モニタリングおよびトラブルシューティング （265 ページ）

機能の概要と変更履歴

要約データ

Table 52: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.01.0

機能説明

3GPP TS 29.244 に従って、N4/Sx インターフェイスを介したセッション管理機能（SMF）とユーザープレーン機能（UPF）間のノードレベルの Heartbeat 手順のサポートが追加されました。

Heartbeat 手順には、次の 2 つのメッセージが含まれます。

1. Heartbeat 要求
2. Heartbeat 応答

Heartbeat 要求

SMF または UPF は、ピアノードへのパスで Heartbeat 要求を送信して、ノードが動作しているかどうかを調べます。Heartbeat 要求メッセージは、Packet Forwarding Control Protocol（PFPC）制御アソシエーションが確立されている各ピアに送信されます。

PFCP 制御アソシエーションが確立されている各ピアの場合、SMF または UPF では、いつでも Heartbeat 要求を受信する準備が整っており、Heartbeat 応答で応答します。

Heartbeat 応答

このメッセージは、Heartbeat 要求の応答として送信されます。

機能の仕組み

SMF および UPF は、構成可能な期間後に Heartbeat メッセージを送信します。ピアが応答しない場合、メッセージは、再試行間隔で構成された回数だけ再試行され、対応するピアに関連付けられたコールに対して構成されたアクションが実行されます。

ノードの開始時刻を含む Recovery Time Stamp 情報要素（IE）は、Heartbeat 要求と Heartbeat 応答の両方でサポートされます。Heartbeat 要求には、独自の Recovery Time Stamp 値が含まれており、ピアに送信しますが、Heartbeat 応答にはピアのリカバリタイムスタンプ値が含まれます。

パス障害の検出

パス障害は次の条件で検出されます。

1. ハートビート障害：この状態は、ピアが送信されたハートビートに応答せず、リタイアした場合に発生します。
2. ハートビートのリカバリタイムスタンプの変更：この状態は、Heartbeat要求またはHeartbeat応答に以前受信した値よりも大きな新規値がある場合に発生します。
3. N4/Sxアソシエーションメッセージのリカバリタイムスタンプの変更：この状態は、N4/Sxアソシエーションメッセージを新しいリカバリタイムスタンプでピアから再受信した場合に発生します。

パスの障害の処理

受信した回復タイムスタンプ値が以前に受信した値より大きい場合、ピアの再起動が検出されます。タイムスタンプが以前に受信した値よりも小さい場合、その値は無視され、ピアの再起動は検出されません。

ピアの再起動が検出されると、ピアのパス障害を示すSNMPトラップが生成されます。また、パスの障害構成（「N4/Sx インターフェイスのハートビートを構成する （263 ページ）」を参照）に基づいて、そのピアに接続されているすべてのコールをクリアできます。

N4/Sx インターフェイスのハートビートを構成する

この項では、この機能をサポートするために使用可能な CLI コマンドについて説明します。

Sx インターフェイスのハートビートを有効にする

Sx サービス構成モードで次のコマンドを使用して、N4/Sx インターフェイスの Heartbeat パラメータを有効にします。

```
configure
   context context_name
      sx-service service_name
         [ default ] sx-protocol heartbeat { interval seconds |
max-retransmissions number | path-failure detection-policy {
control-recovery-timestamp-change | heartbeat-retry-failure |
heartbeat-recovery-timestamp-change } | retransmission-timeout seconds
}
         no sx-protocol heartbeat { interval | path-failure
detection-policy { control-recovery-timestamp-change |
heartbeat-retry-failure | heartbeat-recovery-timestamp-change }
         end
```

注：

- **default**：指定したパラメータに割り当てられているデフォルト値を設定または復元します。
- **no**：次のオプションを無効にします。

- **heartbeat**：N4/Sx Heartbeat パラメータを構成します。
- **interval** *seconds*：N4/Sx サービスに対して Heartbeat 間隔を秒単位で構成します。*seconds* は、1 ～ 3600 の整数で指定する必要があります。
- **max-retransmissions** *number*：N4/Sx Heartbeat 要求の最大再試行回数を構成します。0 ～ 15 の整数で指定する必要があります。デフォルト値は 4 です。
- **retransmission-timeout** *seconds*：N4/Sx サービスの Heartbeat 再送信タイムアウトを、1 ～ 20 の秒単位で設定します。デフォルトは 5 です。
- **path-failure**：パス障害が Heartbeat 要求タイムアウトによって発生した場合に使用するポリシーを指定します。

パス障害の検出ポリシーを構成する

Sx サービス構成モードで次のコマンドを使用して、パス障害に使用する検出ポリシーを指定します。

```
configure
  context context_name
    sx-service service_name
      [ default | no ] sx-protocol heartbeat path-failure
detection-policy { control-recovery-time-stamp-change |
heartbeat-retry-failure | heartbeat-recovery-
timestamp-change }
      end
```

注：

- **default**：指定したパラメータに割り当てられているデフォルト値を設定または復元します。
- **no**：次のオプションを無効にします。
- **detection-policy**：使用するポリシーを指定します。デフォルトのアクションは、Heartbeat 要求のタイムアウト時にクリーンアップを実行することです。
- **control-recovery-time-stamp-change**：Control 要求/応答メッセージのリカバリタイムスタンプが変更された際に、パス障害を検出します。
- **heartbeat-retry-failure**：Heartbeat メッセージの再試行がタイムアウトすると、パス障害が検出されます。
- **heartbeat-recovery-timestamp-change**：Heartbeat 要求/応答メッセージのリカバリタイムタイムスタンプが変更されると、パス障害が検出されます。

モニタリングおよびトラブルシューティング

ここでは、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドや出力

この項では、この機能のサポートにおける show コマンドまたはその出力について説明します。

show sx-service all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

- SX Heartbeat
  - インターバル
  - 再送タイムアウト
  - 最大再送数
- Sx パス障害の検出ポイント
  - ハートビート タイムアウト
  - Heartbeat Req/Rsp リカバリタイムスタンプの変更
  - 制御メッセージリカバリのタイムスタンプカウンタの変更

show sx-service statistics all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが表示されるようになりました。

- Heartbeat 要求
  - Total TX
  - Total RX
  - Initial TX
  - Initial RX
  - Retrans TX
- Heartbeat 応答
  - Total TX
  - Total RX

切断理由

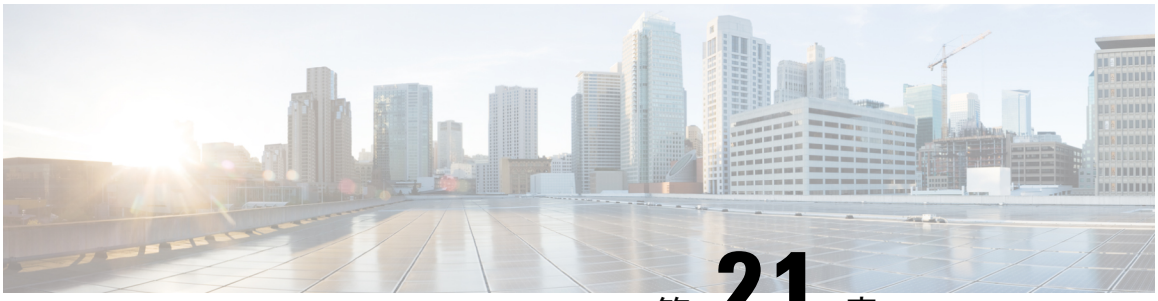
この機能のサポートとして、次の切断理由が追加されました。

- sx-path-failure：設定に基づいてリカバリタイムスタンプの変更またはハートビート障害が検出されると、この切断理由で通話がクリアされます。

SNMP トラップ

この機能をサポートするために、次の SNMP トラップが追加されました。

- SxPathFailure：このトラップは、ピアパス障害が検出されたときに生成されます。
- SxPathFailureClear：このトラップは、ピアのパスが復元されたときに生成されます。



第 21 章

アイドルモードのバッファリングとページング

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 267
- 機能説明, on page 268
- バッファリング アクション ルールのコールフロー, on page 269
- 最初の DL パケットのダウンリンクデータレポート, on page 269
- ページングポリシー差別化, on page 270

機能の概要と変更履歴

要約データ

Table 53: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 54: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

バッファリングアクションルール（BAR）は、ユーザープレーン機能（UPF）のバッファリング動作を制御する指示を提供します。BARは、パケット転送制御プロトコル（PFPC）セッションのすべての転送アクションルール（FAR）のバッファリング動作を制御します。この制御は、パケットをバッファリングしそれぞれの BAR に関連付けることを要求する Apply Action パラメータを PFCP セッションが設定している場合に適用されます。

機能の仕組み

ユーザープレーン機能が、ULまたはDLバッファリング制御（UDBC）機能のサポートを示している場合、SMF は BAR で buffering packet count IE を提供します。buffering packet count IE は、PFCP Session Establishment 手順または PFCP Session Modification 手順中に作成されます。SMF は、後続の PFCP Session Modification 要求、「および」または「または」PFCP Session Report 応答メッセージでこれを変更します。同じ BAR が PFCP セッションのすべての FAR に関連付けられ、PFCPセッション内のすべてのサービスデータフローがPFCPセッションのUPFで同じバッファを共有することを示します。PFCPセッションごとに1つのBARが作成されます。

UPF でのバッファリング アクション ルールをプロビジョニングする

SMF は、BAR で複数のバッファリングパラメータをプロビジョニングします。これは、さまざまな PFCP メッセージの Create BAR または Update BAR に含まれます。

現在、UPF は次の IE をサポートしています。

- 推奨される buffering packet count IE：UPF が、パケット数を示す UDBC 機能のサポートを示す場合。これには、SMF から新しい指示を受信するまで、SMF が UPF でのバッファリングを提案するアップリンクとダウンリンクの両方が含まれます。例：新しいクォータが付与された場合。
- DL buffering suggested packet count IE：この IE は、SMF が UPF でさらに多くの DL パケットをバッファリングすることを要求する場合、Session Report 応答メッセージで SMF からの Update BAR と一緒に受信されます。

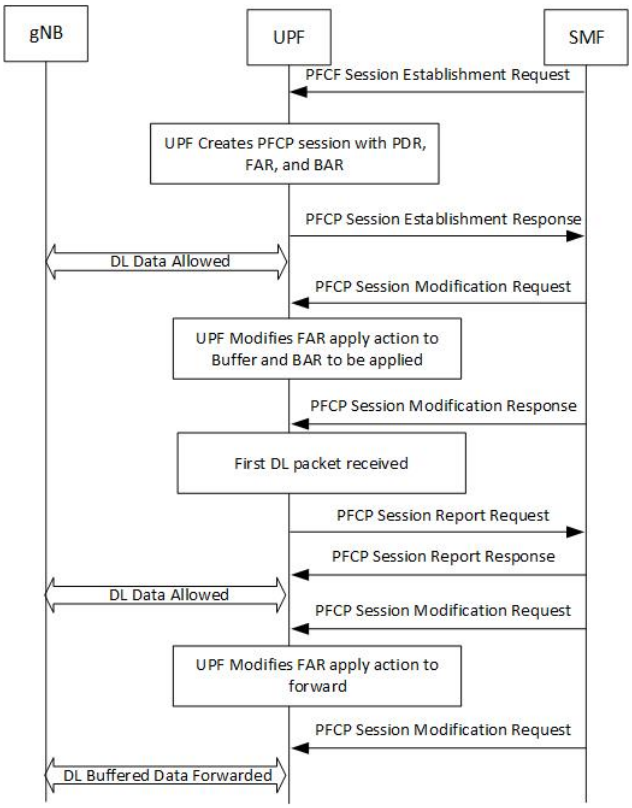
UPF は、DL buffering duration および DL buffering suggested packet count パラメータを適用せず、UPF でダウンリンクデータパケットの拡張バッファリングが終了した際に、（SMF からの明

確な要求がなしに）BAR からこれらのパラメータを削除します。UPF がSMF から新しい指示を受信した場合、UPF は、バッファリングを適用しません。バッファリングされたパケットは、パケット転送モデルに従ってドロップされるか転送されます。また、バッファリングされたパケットがすでに以前に処理されたことを考慮します。

バッファリング アクション ルールのコールフロー

この項では、UPF コールフローのバッファリング アクション ルールのプロビジョニングについて説明します。

Figure 12: バッファリング アクション ルール



最初の DL パケットのダウンリンクデータ レポート

DL パケットの到着をバッファリングして SMF に通知するように指示された場合、UPF は、指定された FAR の最初のダウンリンクパケットを受信すると、SMF に通知します。UPF は、ダウンダウンリンクパケットを受信したPDRを識別する Downlink Data Report IE を含む PFCP Session Report 要求を送信することによって、DL パケットの到着を通知します。

ページングポリシー差別化

UPF は、各 PDR と Downlink Data Notification をトリガーする各パケット向けの Paging Policy Differentiation をサポートします。UPD 機能は、Downlink Data Service Information IE の IP ペイロードで受信した ToS （IPv4）または TC（IPv6）情報の DSCP の値をコピーします。

各 PDR および Downlink Data Notification をトリガーする各パケットの場合、ダウンリンクデータパケットの QFI が使用可能な場合、QFI も Downlink Data Service Information IE で送信されます。

ページング ポリシー インジケータ（PPI）

UPF が、発信 PDU パケットでページング ポリシー インジケータを設定する必要がある場合、SMF は Create QER または Update QER で PPI 値を送信します。

PDU セッション ユーザー プレーン プロトコルのフレームフォーマット

Downlink PDU Session Information（PDU Type 0）：このフレームフォーマットは、インターフェイス経由のパケットの転送に関連付けられている一部の制御情報要素を NG-RAN が受信できるように定義されています。次の図は、各 DL PDU SESSION INFORMATION フレームを示しています。

Figure 13: DL PDU SESSION INFORMATION（PDU Type 0）フォーマット

Bits								Number of Octets
7	6	5	4	3	2	1	0	
PDU Type (=0)				Spare				1
PPP	RQI	QoS Flow Identifier						1
PPI				Spare				0 or 1
Padding								0-3

QoS フロー識別子（QFI）

説明：QoS Flow Identifier（QFI）パラメータは、転送されたパケットが属する QoS フローの QoS フロー識別子を示します。

値の範囲：値の範囲は、0 ～ 26-1 です。

フィールド長：6 ビット。

ページングポリシーの存在

説明：Paging Policy Presence (PPP) パラメータは、ページング ポリシー インジケータ（PPI）の存在を示します。

値の範囲：0 の値は、ページング ポリシー インジケータが存在しないことを示し、1 は、ページング ポリシー インジケータが存在することを示します。

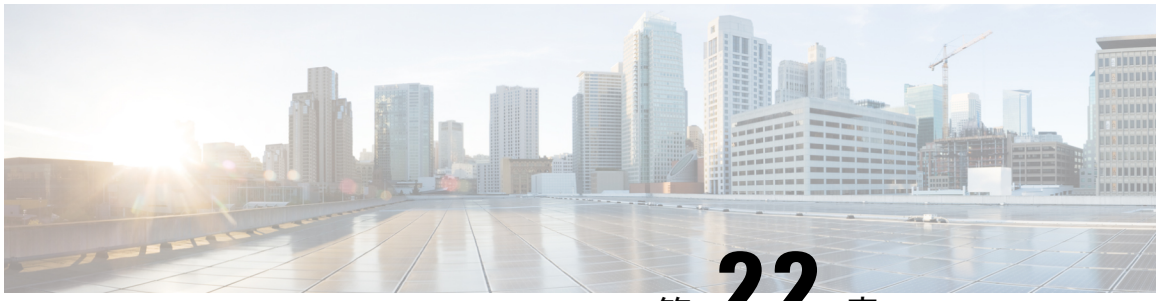
フィールド長：1 ビット。

ページング ポリシー インジケータ

説明：存在する場合、ページングポリシーインジケータ（PPI）がページングポリシーの差別化に使用されます（詳細については、「3GPP TS 23.501」を参照）。このフィールドは、IP タイプの PDU セッションに適用されます。

値の範囲：値の範囲は 0 ～ 23-1 です。

フィールド長：3 ビット。



第 22 章

間接転送トンネル

- マニュアルの変更履歴 （273 ページ）
- 機能説明 （273 ページ）
- 機能の仕組み （273 ページ）
- 間接転送トンネルの設定 （277 ページ）
- モニタリングおよびトラブルシューティング （278 ページ）

マニュアルの変更履歴

改訂の詳細	リリース
初版	2021.02.0

機能説明

UPF は、作成と削除のための Indirect Forwarding Tunnel（IDFT）手順をサポートします。これらの手順の対象は、専用ベアラーを使用した Pure-S コールおよび Collapsed コールです。この機能は、S-GW Relocation を使用した IDFT サポートに適用されます。

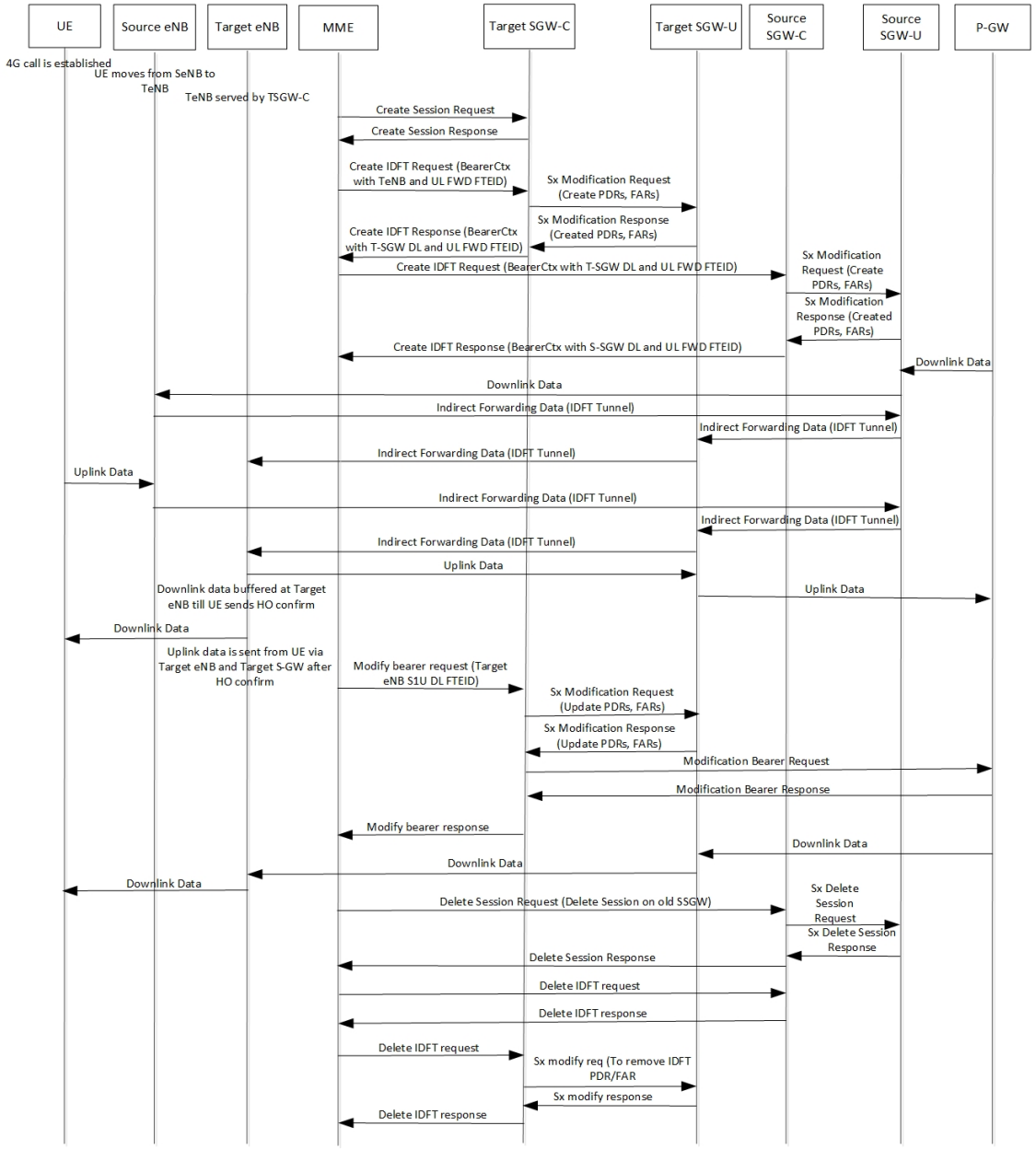
（注） UPF の IDFT は、CLI が制御する機能です。デフォルトでは、UPF の IDFT 機能は無効になっています。

機能の仕組み

通話フロー

次のコールフローは、S-GW 再配置を伴う IDFT のサポートを示しています。

図 *14 : S-GW* 再配置を伴う *IDFT* のサポート



上記のコールフローは、S-GW の再配置を行い、MME の変更を伴わない IDFT トンネルの確立と削除について説明しています。

IDFT トンネルが MME によって削除されない場合、S-GW は IDFT トンネルのローカル削除を開始します。

この機能は、Pure-S コールと Collapse コールの次のシナリオをサポートします。

- 同じ MME を使用した S-GW の再配置
- 同じ MME と異なる eNodeB を使用した S-GW の再配置

- 異なる MME を使用した S-GW の再配置
- S1 ベースの eNodeB ハンドオフ
- EUTRAN から UTRAN へのハンドオフ
- S-GW の再配置を伴う EUTRAN から UTRAN へのハンドオフ
- UTRAN から EUTRAN へのハンドオフ
- S-GW の再配置を伴う UTRAN から EUTRAN へのハンドオフ
- S-GW の変更および間接データ転送を伴うトラッキングエリア更新（TAU）
- IDFT アクティブ時の無線アクセスベアラー（RAB）
- IDFT のセットアップまたは削除中の Sx トランザクションのタイムアウト
- 保留中の Sx トランザクション（PCRF または OCS からのイベント）と IDFT 要求の受信
- IDFT アクティブ時のベアラー作成要求（CBR）
- IDFT アクティブ時のベアラー更新要求（UBR）
- IDFT アクティブ時のベアラー削除要求（DBR）
- IDFT アクティブ時の他の PDN でのベアラー変更要求（MBR）
- 送信元 MME パス障害
- ターゲット MME パス障害
- NTSR 有効時の MME パス障害
- eGTP-C S5 パス障害
- P-GW 再起動通知有効時の eGTP-C S5 パス障害
- Sx パス障害（クリーン IDFT およびコール）
- セッションの中止（clear sub all、local abort など）
- IDFT アクティブ時の他の PDN での CBR、UBR
- IDFT アクティブ時の他の PDN/ベアラーでの DBR
- ターゲット eNodeB の S1-u パス障害
- 送信元 eNodeB の S1-u パス障害
- 送信元 S-GW の S-GW パス障害
- ターゲット S-GW の S-GW パス障害
- IDFT アクティブ時のデフォルトベアラーでの S1-u エラー通知
- IDFT アクティブ時の専用ベアラーでの S1-u エラー通知

- ターゲット S-GW から送信元 S-GW ベアラーへの S1-u エラー通知
- ターゲット eNodeB からターゲット S-GW ベアラーへの S1-u エラー通知
- 障害後に IDFT トンネルを切断した際に End Marker を送信する
- SMF ICSR/SR が、IDFT のクリーンアップを発生させる場合、UPF は IDFT PDR/FAR もクリーンアップします。

IDFT による 5G から 4G へのハンドオーバー

3GPP TS 23.502 v15.5.1 に準拠し、UPF では IDFT を使用した 5G から 4G へのハンドオーバーがサポートされています。IDFT のコール/データパスフローの詳細については、3GPP 仕様書の「N26 インターフェイスを使用して 5GS から EPS にハンドオーバーする」項を参照してください。

この機能は、UPF では CLI で制御されません。

IDFT による 4G から 5G へのハンドオーバー

3GPP TS 23.502 v15.5.1 に準拠し、UPF では IDFT を使用した 4G から 5G へのハンドオーバーがサポートされています。コールフローの詳細については、3GPP 仕様書の「N26 インターフェイスを使用して EPS から 5GS にハンドオーバーする」（準備および実行フェーズ）項を参照してください。

この機能は、UPF では CLI で制御されません。

サポートされる機能

IDFT 機能は、次の機能をサポートしています。

- 複数のベアラーを使用した、Collapsed、Pure-S、Collapsed および Pure-S のマルチ PDN 複合コールの IDFT 作成要求。
- ダウンリンクおよびアップリンク IDFT ベアラーでのデータ転送。
- MME からの IDFT 削除要求。また、MME から IDFT 削除要求が送信されない場合、タイマーベースで、デフォルト値である 100 秒経過後に IDFT ベアラーを削除。
- 通常の PDN がダウンした場合の IDFT PDN の削除（MME/P-GW からのサブスクライバのクリア/削除を含む）。
- Pure-S および Collapsed PDN の Sx 障害処理の IDFT 作成。



重要 GTP-U アドレスのトランスポート機能は、eNodeB および S-GW 間で同じであると想定されます。

制限事項

IDFT 機能には、次の制限事項があります。

- その他の手順による IDFT PDN の確立時または削除時のメッセージのやり取りと競合はサポートされていません。
- IDFT PDN がアクティブな場合、非 IDFT PDN での S11/S5 および Sx パス障害処理はサポートされていません。
- IDFT 接続状態での部分的な専用ベアラーの削除はサポートされていません。

間接転送トンネルの設定

この項では、IDFT 機能のサポートで使用可能な CLI コマンドについて説明します。

間接転送トンネル機能の有効化

SMF で、次の CLI コマンドを使用して IDFT 機能を有効または無効にします。

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

注：

- **idft-support**：UFP で IDFT 機能を有効または無効にします。
- デフォルトでは、IDFT 機能は無効になっており、この CLI コマンドはランタイムの変更に適用できます。

間接転送トンネル機能の確認

show sgw-service name <service_name>

SMF では、CLI コマンドの出力が強化され、IDFT 機能が有効または無効かを表示できるようになりました。

- CUPS の IDFT 機能のサポート：有効/無効

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応のサポートに使用できるCLIコマンドに関する情報について説明します。

show コマンドの入力と出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show subscribers saegw-only full all

UPF で、このコマンドを使用して IDFT ローカルおよびリモート TEID データを表示します。次に、出力例を示します。

```
  Indirect Fwding   : Active
  DL fwd local  addr: 209.165.201.28          DL fwd remote   addr: 209.165.201.27
  DL fwd local  teid: [0x80028004]            DL fwd remote   teid: [0x2002d2e5]
  UL fwd local  addr: 209.165.201.28          UL fwd remote   addr: 209.165.201.27
  UL fwd local  teid: [0x8002a004]            UL fwd remote   teid: [0x20042bca]
```

show subscribers user-plane-only callid <call_id> pdr all

UPF で、このコマンドを使用すると、IDFT の PDR を表示できます。次に、出力例を示します。



重要 IDFT PDR には、送信元および接続先インターフェイスタイプとして ACCESS が設定されます。

```
+-----Source Interface:          (C) - Core            (A) - Access
|-----Type                       (P) - CP-function     (.) - Unknown
|
|+----Destination Interface:     (C) - Core            (A) - Access
||----Type                       (P) - CP-function     (.) - Unknown
||
||
||+---Rule-Type:                 (S) - Static          (P) - Predefined
|||---Type                       (D) - Dynamic         (.) - Unknown
|||
|||
vvv   PDR-ID    Associated FAR-ID    Associated URR-ID(s)    Associated QER-ID(s)
---   ------    -----------------    --------------------    --------------------
ACS   0x0001          0x8001              n/a                  0x80000001
CAS   0x0002          0x8002              n/a                  0x80000001
ACD   0x0003          0x0003           0x00000007              0x00000002
                                          n/a                  0x80000003
CAD   0x0004          0x0004           0x00000007              0x00000002
                                          n/a                  0x80000003
CAD   0x0005          0x0005           0x00000000              n/a
ACD   0x0006          0x0006           0x00000000              n/a
CAD   0x0007          0x0007           0x00000000              n/a
ACD   0x0008          0x0008           0x00000000              n/a
```

```
AAD   0x0009          0x0009          0x00000000              n/a
AAD   0x000A          0x000A          0x00000000              n/a
AAD   0x000B          0x000B          0x00000000              n/a
AAD   0x000C          0x000C          0x00000000              n/a

Total subscribers matching specified criteria: 1
```

同様に、**show subscribers user-plane-only callid** *call_id* **far all** CLI コマンドを使用すると、IDFT に対して作成された FAR を表示できます。

show subscribers user-plane-only full all



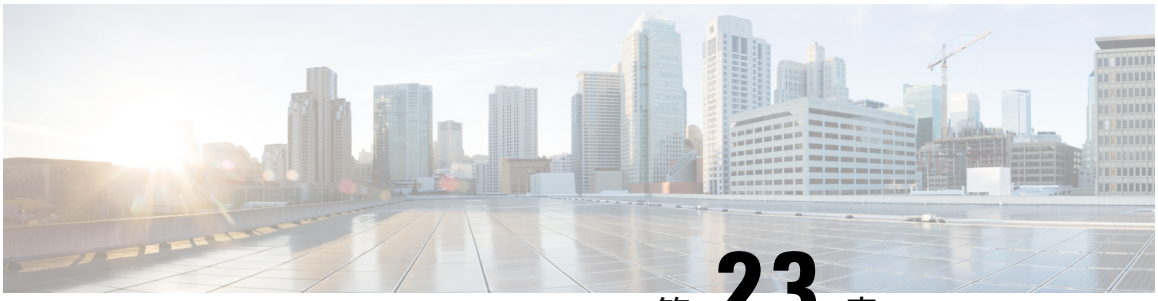
重要 IDFT PDR のデータ統計情報は、既存の PDR 統計情報と同じ方法でキャプチャされますが、制限付きです。DL および UL IDFT の統計情報は、Pkts-Down および Bytes-Down カテゴリで増分されます。

次にサンプル出力を示します。

```
Static & Predef Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------
catchall                      0          0          3       1368          3
  0          0/0              0/0

Dynamic Rule Match stats:
PDR Id    Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)    FP-Up(Pkts/Bytes)
-------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------    ------------------
0x0004        2       856          0           0          2              0
 0/0                 0/0
0x000b        2       856          0           0          2              0
 0/0                 0/0
0x000c        2       168          0           0          2              0
 0/0                 0/0
```

show subscribers user-plane-only full all



第 23 章

DHCP サーバー経由の IP 割り当て

表 *55 :* 機能の履歴

機能名	リリース情報	機能説明
プレフィックス制限のない DHCP ベースの IPv6 アドレス割り当て	2025.03.0	この機能により、UPF は、プレフィックスの制限なしに、外部 DHCP サーバーを介したサブスクライバ UE への IPv6 アドレス割り当てをサポートできます。 **導入されたコマンド**： **disable ipv6-validation**：この CLI は、IPv6 検証を無効にするように DHCP クライアントプロファイル構成モードで設定されます。 **コマンドの拡張**： **disable dhcpv6-client-unicast slot/port** *slot-port_number*：この CLI は、DHCP クライアントプロファイル構成モードで、ユニキャストオプションを無効にしてマルチキャストを有効にするように設定されます。 **デフォルト設定**無効：有効にするには構成が必要です。

機能名	リリース情報	機能説明
DHCP ベースの IP アドレス割り当て	2025.02.0	この機能により、ネットワークオペレータは、外部 DHCP サーバーを使用してサブスクライバ UE の IP アドレスを受信できます。 DHCP サーバーを使用して IP アドレスを割り当てることにより、複雑な 5Gネットワークを持つエンタープライズは、IP アドレスの割り当てを一元的に管理および制御できます。 **導入されたコマンド**： **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id*：この CLI は、DHCP サービス構成モードで構成され、UPF が DHCP サーバーを検出できるようにします。 **強化されたコマンド**： **dhcp ip skip-validation**：この CLI は、IPv4 アドレス検証をスキップするようにDHCP サービス構成モードで構成されます。 **デフォルト設定**無効：有効にするには構成が必要です。

5G ネットワークでは、SMF はローカル IPAM プールからのダイナミックな IP アドレスの割り当てを処理します。ただし、複雑な5Gエンタープライズ ネットワークでは、IPアドレスの割り当てと管理の一元化が必要です。

これを容易にするため、UPF では DHCP サーバーを使用してサブスクライバ UE に IP アドレスを割り当てることがサポートされています。これにより、ネットワーク オペレータは、複雑で大規模なエンタープライズ環境のニーズに合わせて、一元化された IP 管理を行うことができます。

- UPF が DHCP サーバー経由で UE IP を割り当てる方法 （282 ページ）
- DHCP ベースの IP 割り当てを有効にする （288 ページ）
- 制限事項 （293 ページ）

UPF が DHCP サーバー経由で UE IP を割り当てる方法

これらの段階では、外部 DHCP サーバー経由で UPF が UE IP アドレスを割り当てるプロセスを示しています。

1. **Session Establishment Request**： SMF が、UPF から UE IP アドレスを取得するように構成されている場合、SMF は、PFCP Session Establishment 要求メッセージの PDI IE の UE IP Address IE を UPD に送信します。

   このメッセージには、UE IP Address Pool Identity IE の Create PDR IE の VLAN ID が含まれており、次のメッセージビットの一方または両方が 1 に設定されています。

- **CHOOSE IPV4（CHV4）**： SMF は、割り当てに向けて IPv4 アドレスの UPF をリクエストします。
- **CHOOSE IPV6（CHV6）**：SMF は、割り当てに向けて IPv6 アドレスの UPF をリクエストします。

2. **DHCPサブネット選択**： UPF は、受信した VLAN ID を使用して、いくつかの条件に基づいて UE IP のサブネットを選択します。

   条件の詳細については、「DHCP サブネット選択の基準」に関するトピックを参照してください。

3. **DHCP 構成の検証**：UPF は、構成検証基準をチェックすることにより、DHCP サービスが構成され、実行されているかどうかを検証します。

   DHCP 構成の詳細については、「DHCP ベースの IP 割り当てを有効にする」項を参照してください。

   DHCP 構成検証に成功すると、UPF は、PFCP Establishment 要求を受け入れ、受信した VLAN ID を使用して指定のサブネットで DHCP サーバーに対して DHCP Discovery ハンドシェイクを開始します。基準に基づいた構成検証に失敗すると、UPF は、Establishment 要求を拒否します。

   構成検証の詳細については、「DHCP 構成検証の基準」項を参照してください。

4. **DORA または SARR ハンドシェイクプロセスの開始**：UPF は、IPv4 アドレスと IPv6 アドレスのそれぞれに対して、Discovery-Offer-Request-Acknowledge（DORA）または Solicit-Advertise-Request-Reply （SARR）ハンドシェイクを開始します。

   UPF は、DHCPv4 の場合は、**Discovery** メッセージをブロードキャストし、DHCPv6 の場合は、**Solicit** メッセージをサブネットにマルチキャストします。UPF はDHCPクライアントリレーとして機能し、受信した VLAN とともに 検出メッセージまたは要請メッセージを送信します。

（注）
- UPF は、宛て先ポート 67 で DHCP サーバーからユニキャストレスポンスを受信します。
- UPF は、VLAN のソースポート（68）および宛先ポート（67）で broadcast DHCPDISCOVER メッセージを送信すると、クライアントとして機能します。
- IPv6 プレフィックス割り当ての場合、UPF から DHCPv6 サーバーへのすべてのメッセージに、要求された 64 のプレフィックス長 の IA_PD オプションが含まれます。

5. **Offer または Advertise メッセージ**： IPv4 の場合、UPF は、DHCPv4 サーバーから、IPv4 アドレス、リース時間、およびサーバー識別子を含む **Offer** メッセージを受信します。

   IPv6 の場合、UPF は、DHCPv6 サーバーから、クライアント IPv6 アドレス、リース時間、およびサーバー識別子を含む、unicast **Advertise** メッセージを受信します。

6. **IPv4 および IPv6 検証**：UPF は、DHCP サーバーから受信した IP アドレスを検証します。検証プロセスは、要求された IP アドレスのタイプ（IPv4 または IPv6）によって異なります。

   - **IPv4 検証**： CLI **[no] skip-validation** が構成されている場合、UPF は、SMF に割り当てられた IPチャンクで受信した IPv4 アドレスを検証します。

     IPv4 検証が成功すると、UPF は要求メッセージを DHCP サーバーに送信します。IPv4 検証が失敗した場合、UPF は DHCPv4 サーバーに要求メッセージを送信せず、IPv4 アドレス割り当てプロセスは失敗します。

     IPv4v6 セッションの場合、IPv4 検証が失敗すると、UPF は、UE に割り当てられた IPv6 アドレスを使用して、コード **Partial Success** を含む Sx Session Establishment 応答を送信します。

   - **IPv6 検証**：CLI **enable ipv6-validation** が構成されている場合、UPF は、**要求**メッセージを DHCPv6 サーバーに送信します。DHCPv6 サーバーは、**Reply** メッセージを UPF に送信します。

     IPv6 の場合、プレフィックス検証は SARR ハンドシェイクで Reply メッセージを受信した後に行われます。

     IPv6 の検証に失敗した場合、UPF は DHCP v6 サーバーに DHCP DECLINE メッセージを送信して、UPF が DHCPv6 サーバーによって指定された IPv6 アドレスを使用しないことを示します。

     IPv4v6 セッションの場合、IPv6 検証が失敗すると、UPF は、UE に割り当てられた IPv4 アドレスを使用して、コード **Partial Success** を含む Sx Session Establishment 応答を送信します。

   IPv4 および IPv6 検証アドレスの基準とプロセスの詳細については、「DHCP サーバーと SMF からのIP アドレスの検証」項を参照してください。

7. **Renew と Rebind**：

   - **Renew 要求**：UPF は、割り当てられたリース時間が期限切れになると、リースの更新を試行します。この場合、UPF は割り当てられたリース時間の 50%（T1 しきい値）で DHCP サーバーに Renew 要求をユニキャストします。

     DHCP サーバーが Renew 要求に応答しない場合、UPF は最大再試行回数に達するまで Renew 要求を再試行します。

     サーバーが NAK（否定確認応答）で応答した場合は、リースを延長できないことを示しています。その後、UPF はコールを消去し、SMF に通知します。

     IPv6 アドレスの場合、Renew 要求は Reply パケットの T1 タイマー値になります。

   - **Rebind 要求**：最大再試行回数を超えても DHCP サーバーが Renew 要求に応答しない場合、割り当てられたリースが割り当てられたリース時間の 88%（T2 しきい値）に達すると、DHCP サーバーは Rebind 要求をブロードキャストします。

     DHCP サーバーが Rebind 要求に応答しない場合、UPF は再試行回数が上限に達するまで Rebind 要求を再試行します。最大再試行回数を超えても DHCP サーバーが応答せ

ず、割り当てられたリースの期限が切れた場合、コールは消去されます。UPF は、コールの削除について SMF に通知します。

サーバーが NAK に応答した場合は、リースを延長できないことを示しています。その後、UPF はコールを消去し、SMF に通知します。

IPv6 アドレスの場合、再バインドパケットは Reply パケットの T2 タイマー値になります。

T1 および T2 しきい値の値は設定可能です。

T1 および T2 しきい値の設定の詳細については、『*CLI*（コマンド ライン インターフェイス）リファレンス、モード *C - D*、*StarOS*』ガイドの「*DHCP Service Configuration Mode* コマンド」章を参照してください。

（注） Renew や Rebind のエラーを処理するには、EPFAR 構成が必須です。構成されていない場合、UPF は、ローカルパージを実行しますが、SMF と UPF 間で不一致が発生します。

8. **セッションの削除**：UPF はローカルにセッションを消去し、リース時間が期限切れになると、UPF が Session Report 要求でコールを削除したという通知を SMF に送信します。

   SMF は、N4 インターフェイス経由で PCRF Session Deletion 要求を UPF に送信します。UPF は、SMF から PFCP Session Deletion 要求メッセージを受信すると、DHCP サーバーに対して fire-and-forget DHCP release 要求を開始します。

DHCP サブネット選択基準

UPF は、次の条件に従って IPv4 サブネットを選択するために、UE IP Address Pool Identity IE を VLAN ID として解釈します。

N4 Session Establishment に以下が含まれている場合...	また **Create PDR IE** に以下が含まれている場合...	結果...
CHOOSE IPV4 ビットのみ	単一の UE IP Address Pool Identity IE	UPF は、IPv4 IP アドレス割り当てのサブネットを識別する VLAN として解釈されます。
CHOOSE IPV4 ビットのみ	1 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。
CHOOSE IPV6 ビットのみ	単一の UE IP Address Pool Identity IE	UPF は、IPv6 IP アドレス割り当てのサブネットを識別する VLAN として解釈されます。
CHOOSE IPV6 ビットのみ	1 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。

N4 Session Establishment に以下が含まれている場合...	また Create PDR IE に以下が含まれている場合...	結果...
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	単一の UE IP Address Pool Identity IE	UPF が、「原因コード：必須 IE が正しくない」の Session Establishment 要求を拒否します。
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	2 つの UE IP Address Pool Identity IE	UPF は、最初と 2 番目の UE IP Address Pool Identity IE を VLAN として解釈し、IPv4 と IPv6 IP アドレス割り当てのサブネットをそれぞれ識別します。
CHOSE IPV4 ビットと CHOSE IPV6 ビットの両方。	2 つ以上の UE IP Address Pool Identity IE	UPF は、UE IP Address Pool Identity IE の追加の発生を無視します。

DHCP 構成の検証基準

DORA または SARR プロセスを開始する前に、UPF は次の検証を実行します。

- CHOSE IPV4 ビットと CHOSE IPV6 ビットのいずれかまたは両方が設定されている場合、IPv4 と IPv6 の両方の DHCP 設定は存在しません。それ以外の場合、UPF は、原因コード**「必須 IE が間違っています」**を SMF に送信します。
- CHOOSE IPV4 および CHOOSE IPV6 ビットのいずれかまたは両方が設定されているか、IPv4 アドレスまたは IPv6 アドレスが存在しない場合は、ローカル APN レベル構成である **ip address alloc-method dhcp-proxy** および **ipv6 address alloc-method dhcpv6-proxy** が、DHCPv4 と DHCPv6 それぞれに存在するはずです。それ以外の場合、UPF は原因コード**「IP 割り当てエラー」**を UPF に送信します。
- 受信した VLAN ID は、UPF の構成で IPv4 と IPv6 のいずれかまたは両方に存在するはずです。

  受信した VLAN ID が UPF 構成に存在しない場合、UPF は原因コード**「RESourCES がありません」**を SMF に送信します。
- DHCP サーバーの検出が無効で、DHCP サーバーの IP アドレスが構成されていないが、DHCPv4 サービスが実行されている場合、UPF は、原因コード**「RESources がありません」**を SMF に送信します。
- ユニキャストが有効で、DHCP サーバーの IP アドレスも構成されていないが、DHCPv6 サービスが実行されている場合、UPF は原因コード**「リソースがありません」**を SMF に送信します。
- スロット/ポートが存在し、設定内の IPv4 または IPv6 の正しいインターフェイスにリンクされている必要があります。それ以外の場合、UPF は原因コード**「IP 割り当てエラー」**を SMF に送信します。

- CHOSE IPV4 ビットと CHOSE IPV6 ビットのいずれかまたは両方が設定されている場合、v4 と v6 の DHCP 設定が有効である必要があります。DHCPv4 および DHCPv6 サービスを開始する必要があります。それ以外の場合、コールは拒否され、UPF は原因コード**「IP 割り当てエラー」**を UPF に送信します。

IPv4 および IPv6 アドレスの検証

UPF は、DORA または SARR プロセス中に SMF によって割り当てられたチャンクと、DHCP サーバーから受信した IPv4 または IPv6 アドレスを比較します。

DORA プロセス中の IPv4 検証

次の段階は、DORA ハンドシェイクプロセス中の IPv4 検証プロセスを示しています。

1. UE/CPE は DHCP Discover メッセージを UPF に送信します。
2. UPF は、クライアント IPv6 アドレス、リース時間、およびサーバー識別子と一緒に DHCPv4 サーバーから DHCP Offer メッセージを受信します。

   UPF は、受信した最初の Offer メッセージを受け入れ、別の DHCPv4 サーバーからの後続のすべての Offer メッセージを無視します。
3. UPF は、SMF から送信された IP プールチャンクで受信した IP アドレスを検証します。

IP 検証が...	結果
成功した場合	UPF は、DHCP 要求メッセージを DHCPv4 サーバーに送信し、DHCPv4 サーバーから DHCP 確認応答メッセージを受信します。
失敗した場合	UPF は、Offer メッセージを破棄し、DHCP 要求メッセージを DHCPv4 サーバーに送信しません。その後、UPF はセッションを拒否します。

4. UPF は DHCP サーバーから確認応答メッセージを受信します。UPF は、Offer と確認応答メッセージで受信した IP が同一であるかどうかを検証します。UPF は、リース検証、chadr 検証、サーバー識別子検証などの他の検証も実行します。

   Offer メッセージと確認応答メッセージで受信した IP 値が同じ場合、UPF は IP 検証が成功したと見なします。この場合、UPF は UE IP を SMF に転送します。

   Offer メッセージと確認応答メッセージで受信した IP アドレスが一致しない場合、UPF は IP 検証プロセスが失敗したと見なします。この場合、UPF は DHCP decline メッセージを DHCPv4 サーバーに送信し、セッションを削除します。

   IP アドレス検証を除き、オファーパケットと確認応答パケットの値に不一致がある場合、UPF は DHCP release メッセージを DHCPv4 サーバーに送信します。

SARR プロセス中の IPv6 検証

IPv6 セッションの場合、**enable ipv6-validation** が構成されていると、UPF は、SARR プロセス後に IPv6 検証を実行します。これらの段階は、IPv6 検証プロセスを示しています。

1. UPF は、Solicit メッセージを DHCPv6 サーバーに送信します。
2. UPF は、DHCPv6 サーバーから Advertise メッセージを受信します。
3. UPF は、要求メッセージを DHCPv6 サーバーに送信します。
4. UPF は、DHCPv6 サーバーから Reply メッセージを受信します。
5. UPF は、SMF から送信された IPv6 プールチャンクで受信した IPv6 アドレスを検証します。

IP 検証が...	結果
成功した場合	UPF は、受信した IPv6 アドレスを使用して正常な Establishment 応答を送信します。
失敗した場合	UPF は、DHCPv6 サーバーによって指定された IPv6 を UPF が使用しないことを示す DHCP DECLINE メッセージを DHCPv6 サーバーに送信します。 Establishment 要求は、IPv6 専用 PDN セッションを拒否します。Establishment 要求は、IPv4v6 PDN セッションに対する部分成功の原因コードで受け入れられます。

DHCP ベースの IP 割り当てを有効にする

UPF で DHCP ベースのIP 割り当てを有効にするために必要な手順は次のとおりです。



重要 DHCP機能を有効にする際には、最初にスタンバイ UPF でDHCP サービスを有効にしてから、アクティブな UPF で DHCP サービスを有効にすることを常にお勧めします。機能の CLI を変更した後、変更した設定を起動設定に保存して機能を有効にします。

既存のDNNに対してこの機能を有効にすると、進行中の通話でサービスの中断が発生します。新しい DNN に対してこの機能を有効にすると、新しい通話には常に DHCP サーバーからの IP 割り当てが設定されるため、サービスの中断は発生しません。

手順

ステップ 1 DHCP サービスを開始します。

ステップ 2 DHCP サーバーの検出を有効にするようにスロット/ポートを設定します。

DHCPv4 または DHCPv6 サービスを開始する

N4 Establishment には、CHV4 ビットまたは CHV6 メッセージビットと、SMF が IP アドレスを必要とすることを示す UE IP Address Pool Identity IE が含まれます。DHCP サーバーを介した IP 割り当てを有効にするには、UPF は DHCP サービスが有効になっていることを確認する必要があります。

したがって、UPF は、ローカルの APN レベルの設定を使用して、DHCP サーバーを使用した IP アドレス割り当てを実行します。

このタスクにより、DHCP プロキシベースの IP 割り当てを有効にするように APN を構成できます。

手順

ステップ 1 コマンド **context** *context_name* を使用して、コンテキストのインスタンスを作成します。

例：

```
[local]UPF(config)# context ingress
[ingress]UPF(config-ctx)#
```

ステップ 2 コマンド **apn** *apn_name* を使用して、APN 構成モードでインスタンスを作成します。

例：

```
[local]UPF(config)# context ingress
[ingress]UPF(config-ctx)# apn intershat
[ingress]UPF(config-apn)#
```

（注） DHCPv4 では、DHCP コンテキスト名が、APN で構成されていない場合、構成された IP コンテキスト名が、DHCP コンテキストとして使用されます。

ステップ 3 コマンド **ip address alloc-method dhcp-proxy** または **ipv6 address alloc-method dhcpv6-proxy** を使用して、IPv4 および IPv6 用にそれぞれ、DHCP プロキシとして IP アドレス割り当てを定義します。

例：

```
[ingress]UPF(config-apn)# ip address alloc-method dhcp-proxy
[ingress]UPF(config-apn)# ipv6 address alloc-method dhcpv6-proxy
[ingress]UPF(config-apn)#
```

（注） DHCPv4 では、DHCP サービス名が、APN で構成されていない場合、構成された IP コンテキスト名からの DHCP サービスまたは DHCP コンテキストが使用されます。

ステップ 4 コマンド **dhcp service-name** *dhcp_service_name* **| { dhcpv6 service-name** *dhcpv6_service_name* **server-profile** *dhcpv6_server_prof* **client-profile dhcpv6-client-prof }** を使用して、IPv4 または IPv6 に使用する DHCP サーバーを指定します。

例：

```
[ingress]UPF(config-apn)# dhcp service-name dhcp_service
[ingress]UPF(config-apn)# dhcpv6 service-name dhcpv6-service server-profile
dhcpv6-server-prof client-profile dhcpv6-clientprof
[ingress]UPF(config-apn)# exit
```

ステップ 5 コマンド **bind address** *dhcp/dhcpv6_ip_address* を使用してコンテキスト構成モードで、UPF インターフェイスをバインドします。現在の構成モードを保存して、終了します。

例：

```
[ingress]UPF(config-ctx)# bind address 209.165.201.1
[ingress]UPF(config-ctx)# bind address 2001:DB8::1
[ingress]UPF(config-ctx)# exit
```

この構成は、DHCP サービスを開始し、アドレス割り当てメソッドを DHCP プロキシとして定義します。

次のタスク

スロット/ポートを構成して、DHCP サーバーにブロードキャストメッセージを送信します。詳細については、「スロット/ポートを構成して DHCP セールスフォースの検出を有効にする」項を参照してください。

スロット/ポートを構成して DHCP サーバーの検出を有効にする

このタスクは、DHCP サーバーにブロードキャストメッセージを送信するように UPF のスロットまたはポートを構成するのに役立ちます。

（注） スロット/ポートが構成されている場合、UPF はブロードキャストメッセージを送信します。ただし、スロット/ポートが構成されていない場合は、DHCP サーバーの IP アドレスを設定する必要があります。この場合、UPF はユニキャストパケットを送信します。

始める前に

DHCPサーバーの検出を有効にするようにスロットを構成する前に、IPv4のDHCPサービスを有効にする必要があります。詳細については、項を参照してください。

手順

ステップ 1 コマンド **context** *context_name* を使用して、コンテキスト構成モードに入り、インスタンスを作成します。

例：

```
[local]UPF(config)# context ISP
[egress]UPF(config-ctx)#
```

ステップ 2 UPF が DHCP または DHCPv6 サーバーに接続する際に経由するスロット/ポートを構成します。

a) **DHCPv4の場合**：コマンド **dhcp-service** *dhcp_service_name* **dhcp server enable-discover slot/port** *slot_port_number* **dhcp-node-id** *node_id* を使用して、コンテキスト構成モードでスロット/ポートを構成します。

例：

```
[egress]UPF(config-ctx)# dhcp-service dhcp_service
[egress]UPF(config-dhcp-service)# dhcp server enable-discover slot/port 1/10
dhcp-node-id 5
[egress]UPF(config-dhcp-service)# dhcp client-identifier { msisdn | imsi }
[egress]UPF(config-ctx)#
```

（注）
- SMF が IPv4 と IPv6 の両方のコールに同じ VLAN ID を送信する場合、IPv4 と IPv6 のスロットとポートの構成は両方のコールで同じである必要があります。
- VLAN 構成は、すべての UPF ノードで同じである必要があります。

b) **DHCPv6 の場合**：コンテキスト構成モードで、CLI **dhcp-server-profile** *dhcpv6_server_prof* **{ enable | disable } dhcpv6-server-unicast** を使用して、DHCPv6 サーバーの [サーバーユニキャスト（server unicast）] オプションを有効または無効にします。また、CLI **dhcp-client-profile** *dhcpv6-client-prof* **{ enable | disable } dhcpv6-client-unicast slot/port***slot_port_number* を使用して、特定のスリットやポートの DHCPv6 の [クライアントユニキャスト（client unicast）] オプションを有効または無効にします。

例：

```
[egress]UPF(config-ctx)# dhcp-server-profile dhcpv6-server-prof
[egress]UPF(config-dhcp-server-profile)# enable dhcpv6-server-unicast
[egress]UPF(config-dhcp-server-profile)# exit
[egress]UPF(config-ctx)# dhcp-client-profile dhcpv6-client-prof
[egress]UPF(config-dhcp-client-profile)# disable dhcpv6-client-unicast slot/port 1/11
[egress]UPF(config-dhcp-client-profile)# exit
[egress]UPF(config-ctx)#
```



重要 CLI **disable dhcpv6-client-unicast** を使用するには、「Unicast Address Support for DHCPv6 Messages」ライセンスが必要です。

CLI **slot/port** *slot_port_number* を使用するには、UPF ライセンスが必要です。

ライセンスの詳細については、シスコのアカウント担当者にお問い合わせください。

ステップ 3 受信した IPv4 アドレスと IPv6 アドレスのいずれかまたは両方の IP 検証を無効または有効にします。

a) **IPv4 の場合**：コマンド **[no] dhcp ip skip-validation** を使用して、DHCP サーバーから受信した IPv4 アドレスの検証をスキップします。これは任意のコマンドです。

例：

```
[egress]UPF(config-dhcp-service)# dhcp ip skip-validation
[egress]UPF(config-dhcp-service)#
```

b) **IPv6 の場合**：コマンド **disable ipv6-validation** を使用して、DHCP サーバーから受信した IPv6 アドレスの IP 検証プロセスを無効にします。

例：

```
[egress]UPF(config-dhcp-client-profile)# disable ipv6-validation
[egress]UPF(config-dhcp-client-profile)# exit
[egress]UPF(config-ctx)#
```

ステップ 4 コマンド **dhcp lease-expiration-policy { auto-renew | disconnect }** を使用して、IP アドレスのリースが期限切れになった場合の必要なアクションを構成します。

例：

```
[egress]UPF(config-dhcp-service)# dhcp lease-expiration-policy auto-renew
```

ステップ 5 IPv4 または IPv6 の DHCP サービスの状態を確認します。

a) **IPv4 の場合**：CLI **show dhcp-service all** を使用して、すべての IPv4 DHCP サービスの状態を確認します。

例：

```
[local]UPF# show dhcp-service all

Service name:                  dhcp_service
  Context:                       ISP
  Bind:                          Done
  Local IP Address:                 100.100.103.20
  Next Hop Address:                 None
  DHCP Subnet mask used:            host mask
      MPLS-label:                   None

  Service Status:                   Started
  Retransmission Timeout:           3000 (milli-secs)
  Max Retransmissions:              5
  Lease Time:                       600 (secs)
  Minimum Lease Duration:           600 (secs)
  Maximum Lease Duration:           86400 (secs)
  DHCP Dead Time:                   120 (secs)
  DHCP Dead consecutive Failure:    5
  DHCP T1 Threshold Timer:          50
```

```
DHCP T2 Threshold Timer:          88
DHCP Client Identifier:           Use MSISDN
DHCP Server Discovery:         Enabled
    Slot/Port:  1/10
    Node Id:    5
DHCP Algorithm:                   First Server
DHCP Servers configured:          None
DHCP server port: 67
DHCP server rapid-commit:         disabled
DHCP client rapid-commit:         disabled
DHCP server check msg size:       disabled
DHCP relay agent option:          disabled
DHCP chaddr validation:           enabled
DHCP IP address validation:    enabled
```

b) コマンド **show dhcpv6-client-profile { all | name }** *client-profile-name* を使用して、IPv6 サービスの状態を検証します。

例：

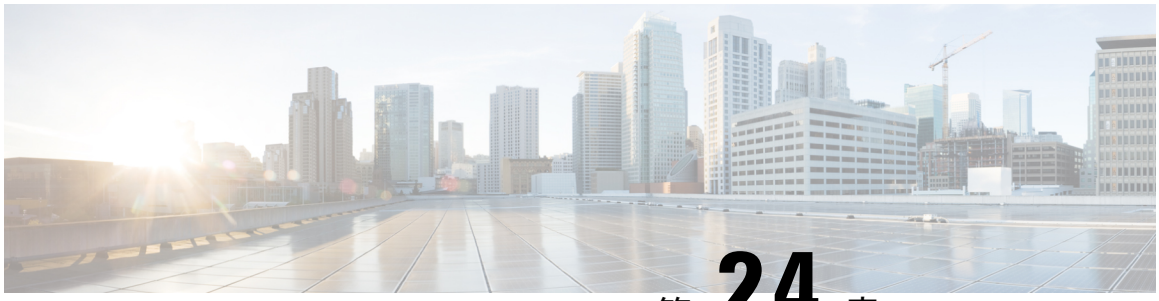
```
[local]UPF# show dhcpv6-client-profile name dhcpv6-client-prof
Client Profile name: dhcpv6-client-prof
Context: ISP
Rapid-commit-dhcpv4: disabled
Rapid-commit-dhcpv6: disabled
Dhcp_msg_spray: disabled
Dns_address: enabled
Netbios_address: disabled
Sip_server_address: enabled
Client_Unicast_to_Server: disabled
IPV6 Validation: disabled
Slot/Port: 1/11
Client identifier: MSISDN
User Class Option: NONE
```

このタスクにより、スロットまたはポート番号を使用して DHCPv4 および DHCPv6 サーバーの検出が可能になります。

制限事項

APN が DHCP サービスにリンクされ、DHCP サービスが APN にリンクされたコンテキストとは異なるコンテキストで定義されている場合、DORA プロセスは発生しません。

異なるコンテキスト間で複数の APN があるデプロイメントでは、各コンテキスト内で個別の DHCP サービスを設定する必要があります。



第 24 章

IPv6 向け IPsec サポート

- 機能の概要と変更履歴, on page 295
- IPsec AH および ESP （296 ページ）
- IPSec の転送およびトンネルモード （296 ページ）
- IPSec 用語 （297 ページ）
- モニタリングおよびトラブルシューティング （300 ページ）

機能の概要と変更履歴

要約データ

Table 56: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 57: マニュアルの変更履歴

改訂の詳細	リリース
初版	2021.04.0

機能説明

IPSec は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピアセキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセスコントロール、およびデータソース認証を提供します。

IPsec AH および ESP

Authentication Heade（AH）とEncapsulating Security Payload（ESP）は、IPSec で使用される 2 つの主要なワイヤレベルプロトコルです。IPSec接続を介して流れるデータを認証（AH）し、暗号化して認証（ESP）します。

- AH は、IP トラフィックの認証に使用されるもので、暗号化には使用されません。認証は、IPパケットのほぼすべてのフィールド（TTLやヘッダーチェックサムなど、転送中に変更される可能性があるフィールドを除く）に対する暗号化ハッシュベースのメッセージ認証コードを計算することによって実行されます。計算されたメッセージ認証コードは、新たに追加される AH ヘッダーに格納され、相手側に送信されます。AH ヘッダーは、元の IP ヘッダーとペイロードの間に挿入されます。
- ESP は暗号化と、オプションとして認証を提供します。ESP には、暗号化とオプションである認証をサポートするヘッダーフィールドとトレーラフィールドが含まれます。IPペイロードの暗号化は転送モードでサポートされ、パケット全体の暗号化はトンネルモードでサポートされます。認証は、ESP ヘッダーと暗号化されたデータが対象となります。

IPSec の転送およびトンネルモード

トランスポートモードではIPペイロードがカプセル化されるため、2つのエンドポイント間にセキュアな接続が提供されます。トンネルモードは、IP パケット全体をカプセル化して、2 つのゲートウェイ間で仮想セキュアホップを提供します。

トンネルモードでは、IPパケット全体が別の内部にカプセル化されて、接続先に配信される、より一般的な VPN 機能が形成されます。完全な IP ヘッダーとペイロードがカプセル化されます。

（注） IPSec 経由の UPF:UPF ICSR は、トンネルモードでのみ機能します。トランスポートモードは、サポートされていません。

IPSec 用語

暗号アクセス制御リスト

アクセス制御リストでは、特定の条件を満たすサブスクライバ データ パケットを処理するためのルール（通常は権限）を定義します。ただし、暗号ACL では、IPSec トンネル経由でルーティングされるサブスクライバ データ パケットに対応するために必要な条件を定義します。

インターフェイス、コンテキスト、または 1 つ以上のサブスクライバに適用される他の ACL とは異なり、暗号 ACL はクリプトマップと照合されます。また、暗号 ACL には 1 つのルールのみが含まれますが、他の ACL タイプは複数のルールで構成できます。

ルーティングの前に、システムは各サブスクライバデータ パケットのプロパティを調べます。パケットのプロパティが暗号ACL で指定された条件と一致する場合に、システムは暗号化マップで指定された IPSec ポリシーを開始します。

トランスフォームセット

トランスフォームセットは、IPSec セキュリティ アソシエーション（SA）を定義するために使用されます。IPSec SA では、パケットを保護するために使用する IPSec プロトコルを指定します。

トランスフォームセットは、IPSec 確立のフェーズ 2 で使用されます。このフェーズでは、システムとピア セキュリティ ゲートウェイが、パケットを保護するためのルールを含む 1 つ以上のトランスフォームセット（IPSec SA）をネゴシエートします。このネゴシエーションにより、両方のピアがパケットを適切に保護および処理できるようになります。

ISAKMP ポリシー

Internet Security Association Key Management Protocol（ISAKMP）ポリシーを使用すると、インターネット キー エクスチェンジ（IKE）SA を定義できます。IKE SA は、システムとピア セキュリティ ゲートウェイ間の共有セキュリティパラメータ（使用する暗号化パラメータ、リモートピアの認証方法など）を指定します。

IPSec 確立のフェーズ 1 では、システムとピア セキュリティ ゲートウェイが IKE SA をネゴシエートします。これらの SA は、IPSec SA ネゴシエーションプロセスを含むピア間の後続の通信を保護するために使用されます。

クリプト マップ

Crypto Map は、サブスクライバ データ パケットに IPSec を実装する方法を決定するトンネルポリシーを定義します。

5G-UPF では、各種 Crypto Map がサポートされています。その内容は次のとおりです。

- 手動クリプトマップ
- IKEv2 クリプトマップ
- ダイナミッククリプトマップ

暗号テンプレート

暗号テンプレートは、IKEv2 IPSec ポリシーを設定します。これには、暗号化および認証アルゴリズムのほとんどの IPSec パラメータと IKEv2 ダイナミックパラメータが含まれます。セキュリティ ゲートウェイ サービスは、暗号化テンプレートが設定されていなければ機能しません。

サービスごとに設定できる暗号テンプレートは 1 つのみです。

サポートされるアルゴリズム

5G-UPF の IPSec は、RFC 5996 で指定されている次の表のプロトコルをサポートします。

プロトコル	タイプ	サポートされるオプション（**VPP** あり）
インターネットキー	IKEv2 暗号化	
Exchange バージョン 2	IKEv2 疑似ランダム関数	PRF-HMAC-SHA1、PRF-HMAC-MD5、AES-XCBC-PRF-128
	IKEv2 整合性	HMAC-SHA1-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192 HMAC-SHA2-512-256、HMAC-MD5-96、AES-XCBC-96
	IKEv2 Diffie-Hellman グループ	グループ 1（768 ビット）、グループ 2（1024 ビット）、グループ 5（1536 ビット）、グループ 14（2048 ビット）

プロトコル	タイプ	サポートされるオプション（VPP あり）
IP Security	IPSec カプセル化セキュリティペイロード暗号化	NULL、DES-CBC、3DES-CBC、AES-CBC-192、AES-CBC-128、AES-CBC-256、AES-128-GCM-128、AES-128-GCM-64、AES-128-GCM- 96、AES-192-GCM、AES-256-GCM-128、AES-256-GCM-64、AES-256-GCM-96
	拡張シーケンス番号	0 またはオフの値がサポートされます（ESN 自体はサポートされません）。
	IPSec の完全性	NULL、HMAC-SHA1-96、HMAC-MD5-96、HMAC-SHA2-256-128、HMAC-SHA2-384-192、HMAC-SHA2-512-256 **重要** HMAC-SHA2-384-192 および HMAC-SHA2-512-256 は、ハードウェアに暗号化ハードウェアがない場合、VPC-DI および VPC-SI プラットフォームではサポートされません。

制限事項と制約事項

この機能には次の既知の制限事項と制約事項があります。

- この機能は、アプリケーション ToS の変更をサポートしていません。
- SA で、パケットの順番が変更された場合、アンチリプレイメカニズムにより、受信側でパケットが破棄される場合があります。
- この構成は許可されていない種、IPv4 通信は、IPv6 トンネルを通過できません。ただし、IPv4 および IPv6 通信にはそれぞれ IPv4 および IPv6 トンネルが必要です。

設定例

設定例

```
context ipsec-s
ipv6 access-list foo6
permit ip host 2002::1 host 2001::1
#exit
ipsec transform-set B-foo6
#exit
ikev2-ikesa transform-set ikesa-foo6
#exit
crypto map foo6 ikev2-ipv6
match address foo6
authentication local pre-shared-key encrypted key <encrypted_key>
authentication remote pre-shared-key encrypted key <encrypted_key>
ikev2-ikesa max-retransmission 3
```

```
ikev2-ikesa retransmission-timeout 15000
ikev2-ikesa transform-set list ikesa-foo6
ikev2-ikesa rekey
payload foo6-sa0 match ipv6
ipsec transform-set list B-foo6
rekey keepalive
#exit
peer fd4d:5643:2886:6e::7c:1
ikev2-ikesa policy error-notification
#exit
interface ike
ipv6 address fd4d:5643:2886:6e:6b::1/64
crypto-map foo6
#exit
interface loop1 loopback
ipv6 address 2002::1/128
#exit
subscriber default
exit
aaa group default
#exit
ipv6 route 2001::1/128 next-hop fd4d:5643:2886:6e::7c:1 interface ike
#exit
#exit
end
```

モニタリングおよびトラブルシューティング

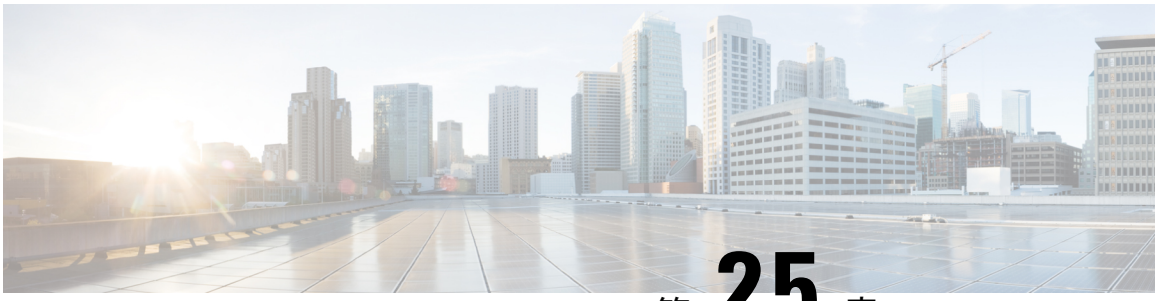
この項では、IPv6 機能の IPSec サポートの監視や障害対応に使用できる CLI コマンドについて説明します。

Show コマンド

ここでは、この機能をサポートする show コマンドとその出力について説明します。

- **show crypto map**
- **show crypto map tag** *map_name*： このコマンドを使用して、マップの状態を確認します。
- **show crypto map summary**
- **show crypto ikev2-ikesa security-associations**
- **show crypto ikev2-ikesa security-associations tag** *map_name*
- **show crypto ikev2-ikesa security association summary**： このコマンドを使用して、IKEv2 SA が開始されているかどうかを確認します。
- **show crypto ipsec security associations**:このコマンドを使用して、IPsec SA が安定しているかどうかを確認します。
- **show crypto ipsec security-associations tag** *map_name*
- **show crypto ipsec security-associations peer** *Peer IP Address*
- **show crypto ipsec security-associations summary**

- **show crypto statistics**
- **clear crypto ike-all**：指定の基準に基づいてマップの IKEv1 SA/IKEv2 SA をクリアします。
- **clear crypto managers**：暗号マネージャをクリアします。
- **clear crypto statistics**：このコンテキストの暗号統計をクリアします。
- **clear crypto ikev2 { local-gateway | peer | tag }**
- **clear crypto security-associations { all | counters | local-gateway | peer | tag }**



第 25 章

IPv6 プレフィックス委任

- IPv6 プレフィックス委任 （304 ページ）
- ライセンス （305 ページ）
- IPv6 プレフィックス委任のガイドラインと制限事項 （305 ページ）
- IPv6 プレフィックスの委任 （305 ページ）
- プレフィックス委任向けに DHCP サーバー名を構成する （307 ページ）
- IPv6 プレフィックス委任を検証する （308 ページ）

IPv6 プレフィックス委任

表 *58 :* 機能の履歴

機能名	リリース情報	説明
要求側の UE または CPE への IPv6 プレフィックス委任のサポート	2024.04.0	UPF は、要求元ユーザー機器（UE）または顧客宅内機器（CPE）への IPv6 Prefix Delegation をサポートします。 この機能により、IPv6 プレフィックスの効率的かつ動的な割り当てが保証され、ネットワーク内のデバイスのシームレスな接続とアドレス管理が容易になります。 この機能を使用するには、有効なライセンスが必要です。詳細については、シスコのアカウント担当者にお問い合わせください。 **導入されたコマンド**：この機能を有効にするには、APN 構成モードで既存の CLI **ipv6 address alloc-method no-dynamic allow-prefix-delegation pd-alloc-method no-dynamic** を設定する必要があります。さらに、DHCP サービスも APN 構成に関連付ける必要があります。 **デフォルト設定**：無効：有効にするには設定が必要。

IPv6プレフィックス委任機能を使用すると、ユーザー機器（UE）または顧客宅内機器（CPE）が IPv6 プレフィックスを取得し、それを使用して IPv6 アドレスをネットワーク内のデバイスに割り当てることができます。

UPF は IP プールをローカルで管理しないため、UPF は SMF に依存してプレフィックスの割り当てを行います。UPF では、IPv6プレフィックス委任機能がDNN（APN）レベルで制御され、正しいネットワークコンテキストが適用されるようにします。

ライセンス

IPv6 プレフィックス委任機能には、Radius 1K ライセンスによる DHCPv6 PD プレフィックスおよび IPv6 インターフェイス ID が必要です。詳細については、シスコのアカウント担当者にお問い合わせください。

IPv6 プレフィックス委任のガイドラインと制限事項

IPv6 プレフィックス委任機能の機能には、次の前提条件があります。

- UE または CPE のパケットデータユニット（PDU）セッションが正常に確立され、UE が IPv6 Prefix Delegation 要求を開始する前に、IPv6 アドレスが割り当てられている必要があります。
- IPv6 Prefix Delegation のサポートは、SMF にあります。

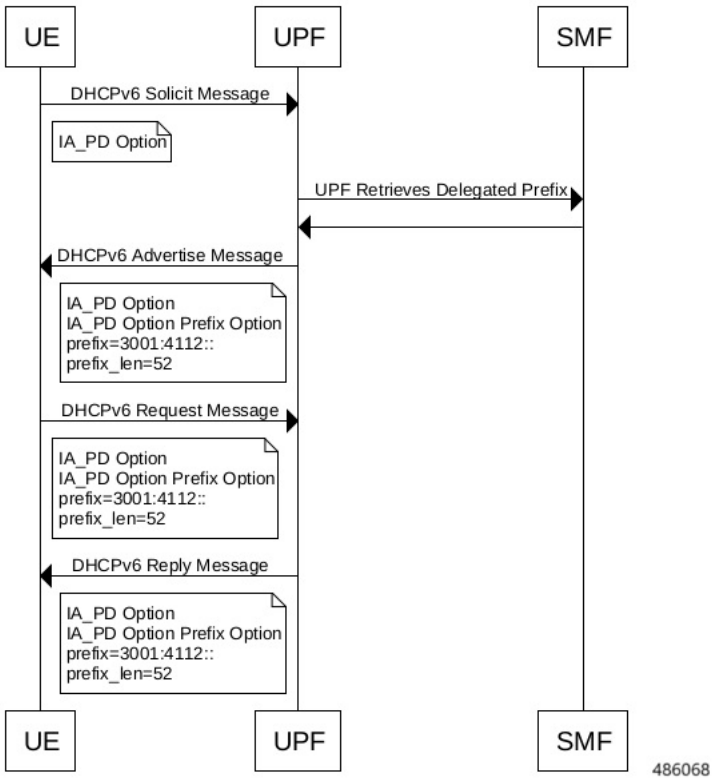
制限事項は次のとおりです。

- 委任されたプレフィックスは、UE からの DHCPv6 Solicit メッセージで受信したプレフィックス長が、SMF のプレフィックス長と一致する場合にのみ、割り当てられます。Solicit メッセージで送信された Preferred Prefix に関する UE 要求は考慮されません。
- DHCPv6 ベースのプレフィックスに対するプレフィックス除外オプション（RFC 6603）は、サポートされていません。
- 高速コミットオプションはサポートされていません。
- IPv6 プレフィックス委任機能は、SxA での IP 送信元違反機能とインターワーキングしません。UE の背後にあるデバイスからのアップリンクパケットは、SxA でドロップされます。
- UPF は、Solicit、Request、Release などの再送信された UE initiated DHCPv6 メッセージの解析はサポートしていません。
- それぞれのタイマーが無限に設定されているため、UPF は、DHCPv6 Renew および Rebind 手順をサポートしません。
- UPF は、機能が有効な状態の稼働中の Downgrade をサポートしません。MOP に従って、IPv6 プレフィックス委任セッションを SMP と UPF からクリアし、UPF をダウングレードする前に、関連する SMF 構成と IP チャンクを削除する必要があります。

IPv6 プレフィックスの委任

この項では、IPv6 プレフィックス委任のコールフローと各段階について説明します。

図 *15 : IPv6* プレフィックスの委任



次の段階では、委任されたプレフィックスの割り当てと管理に向けたSMF（セッション管理機能）と UPF（ユーザープレーン機能）間の相互作用について説明します。

1. UE/CPE は DHCPv6 要請メッセージを UPF に送信します。UE/CPE では、inIA_PD プレフィックスオプションにプレフィックス長を含めることができます。
2. UPF は、UE の PDN セッションが確立されたときに作成された GTPU トンネル上の N3 または S1U/S5U インターフェイスを介して要求されたメッセージを受信します。UPF は IP プールをローカルで管理しないため、UPF はプロキシ DHCP サーバとして機能し、SMF からプレフィックスを受信します。SMF は、DNN 構成に従って委任されたプレフィックスを提供します。構成されたプレフィックス長の値とは異なるプレフィックス長で DHCP 請求を受信した場合、SMF は要求を拒否します。プレフィックス長が受信されない場合、SMF は構成されたプレフィックス長に従って割り当てます
3. UPF は、IA_PD オプションに委任されたプレフィックスを含む DHCP アドバタイズ メッセージを使用して、DHCPv6 要請メッセージに応答を送信します。

   SMF は、ローカル IPAM プールから委任されたプレフィックスを割り当てます。

（注） UPF は、UE/CPEにが要求したプレフィックスの割り当てに失敗すると、状態コード：NoPrefixAvail の IA_PD オプションを含む DHCPv6 Advertise メッセージで DHCPv6 Solicit に応答します。

IPv6 プレフィックスのリリース

UPF は、UE/CPE から受信した DHCPv6 Release メッセージの応答として、DHCPv6 Reply を送信し、UPF でプレフィックスアドレスの解除を確認します。

プレフィックス委任向けに DHCP サーバー名を構成する

プレフィックス委任に対して server-mode で DHCP サービスを有効にするには、次の手順を実行します。

手順

ステップ 1 コンテキスト構成モードを開始します。

ステップ 2 **dhcpv6 service-name** *dhcp_service_name* コマンドを入力して、プレフィックス委任に対して DHCP サービスと 有効な *interface IP | loopback* アドレスが設定された **bind address** を有効にします。DHCP サービスの bind-address は、コンテキストで設定されているループバック インターフェイスに割り当てられた IP です。

例：

```
config
context ingress
        dhcpv6-service dhcp_service_name
             bind address {valid interface IP | loopback address }
      exit
```

ステップ 3 Enter the **apn** *apn_name* コマンドを入力して、UPF ノードに関連付けられている APN 名を指定します。

例：

```
config
context ingress
dhcpv6-service dhcp_service_name
             bind address {valid interface IP | loopback address }
      exit
      apn intershat
          ipv6 address alloc-method no-dynamic allow-prefix-delegation pd-alloc-method no-dynamic
      dhcpv6-service dhcp_service_name
exit

exit
```

ステップ 4 **ipv6 address alloc-method no-dynamic allow-prefix-delegation pd-alloc-method no-dynamic** コマンドを入力して、DHCPv6 prefix-delegation を許可するように APN を構成します。

例：

```
config
context ingress
dhcpv6-service dhcp_service_name
            bind address {valid interface IP | loopback address }
      exit
      apn intershat
          ipv6 address alloc-method no-dynamic allow-prefix-delegation pd-alloc-method no-dynamic
        dhcpv6-service dhcp_service_name
      exit

exit
```

ステップ 5 **exit** コマンドを入力して現在の構成モードを終了します。

IPv6 プレフィックス委任を検証する

この項では、IPv6 プレフィックス委任機能の show コマンドとその出力について説明します。

show subscribers user-plane-only full all callid

show subscribers user-plane-only full all callid *call-id* の 出力には、サブスクライバに委任されたプレフィックスが含まれます。

```
…
NAT Policy NAT64: n/a
Converged Session: No    Converged Peer Callid:      n/a
Visited Call: No
Prefix Delegation:
  IPv6 Delegated Prefix: 3001::/48 Sent to UE: Yes
  Preferred Lifetime: 0xFFFFFFFF
  Valid Lifetime: 0xFFFFFFFF
Subscriber Parameters:
IMSI: 404019011037182
IMEI: 1122334455667788
 …
```

（注） UE が IPv6 プレフィックスを要求しない場合、show コマンドは **Sent to UE: No** 値を表示します。

IPv6 プレフィックス委任が UPF で構成されていないか、サポートされておらず、SMF からプレフィックスを受信しない場合、次の出力詳細が表示されます。

```
NAT Policy NAT64: n/a
Converged Session: No    Converged Peer Callid:      n/a
Visited Call: No
Prefix Delegation:
  IPv6 Delegated Prefix Not Received
```

```
Subscriber Parameters:
IMSI: 404019011037182
IMEI: 1122334455667788 …
```

（注） UE が DHCPv6 Release 経由でプレフィックスをリリースする場合、show コマンドは上記の出力を表示します。

show dhcpv6 statistics

APN が、ローカルプールから Delegated Prefix を受信するように構成されている場合、セッション統計が、**show dhcpv6 statistics** の CLI コマンド出力に表示され、次の出力が表示されます。

```
DHCPv6 Session Stats:

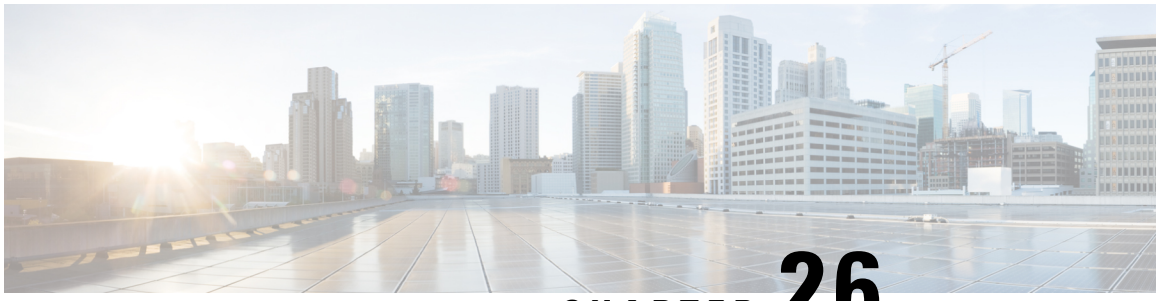
  Total Current:                    0
     DHCP Proxy:                    0
     DHCP Server:                   0
     DHCP PD:                       0
     Radius/SMF PD:                 0
     Local PD :                     0

  Total Setup:                      0
     DHCP Proxy:                    0
     DHCP Server:                   0
     DHCP PD:                       0
     Radius/SMF PD:                 0
     Local PD :                     0

  Total Released:                   0
     DHCP Proxy:                    0
     DHCP Server:                   0
     DHCP PD:                       0
     Radius/SMF PD:                 0
     Local PD :                     0

  Session Release Reasons:(dhcp-proxy)
     Admin Releases:                        0   Bearer Call Terminated:             0
     Lease Exp Policy:                      0   No Address Available:               0
     IP Address mismatch:                   0   Unspecified Failure:                0
     Not on link status:                    0   Other Reasons:                      0

  Session Release Reasons:(dhcp-prefix-delegation)
     PDNs Released:                         0   Lease Exp Policy:                   0
     UE Initiated Release:                  0   Other Reasons:                      0
```



CHAPTER 26

LTE：Wi-Fi のシームレスハンドオーバー

- 機能の概要と変更履歴 （311 ページ）
- 機能説明 （311 ページ）
- 機能の仕組み （312 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.02.0

機能説明

進行中のデータセッションを継続する必要がある UE の場合、LTE と Wi-Fi（S2b）間のシームレスなハンドオーバーは、5G UPF アーキテクチャでサポートされています。

LTE から Wi-Fi へのハンドオーバーが開始され、セッション作成応答（CSR）が Wi-Fi トンネルで送信されるとすぐに、ベアラー削除要求（DBR）が LTE トンネルを介して送信されます。この際、ePDG での IPSec トンネル確立の遅延により、パケット損失が発生します。パケット損失の問題に対処するために、設定されたハンドオーバータイマーの期限が切れたときにのみ、ベアラー削除要求が LTE トンネルで送信されます。LTE トンネルがアクティブな場合、アップリンクとダウンリンクのデータは LTE トンネルで交換されます。ハンドオーバーが完了すると、アップリンクとダウンリンクのデータが Wi-Fi トンネルで交換されます。これにより、パケット損失を防げます。Wi-Fi から LTE へのハンドオーバー中に、ベアラー変更要求が HI=1 で受信されると、仕様に従って Wi-Fi から LTE へのトンネル切り替えが開始されます。

この機能には次の利点があります。

- LTE から Wi-Fi（S2bGTP）へのハンドオーバー中のパケット損失を最小限に抑え、ハンドオーバーをシームレスにします（つまり、メイクビフォアブレーク）。
- P-GW で両方のトンネルが確立されている場合、LTE 手順は LTE トンネルを介して正常に処理されます。
- P-GW で両方のトンネルが確立されている場合、Wi-Fi 手順は Wi-Fi トンネルを介して正常に処理されます。



重要

- LTE から Wi-Fi または Wi-Fi から LTE へのハンドオーバーでは、シームレスなハンドオーバーを実行するために、新しいアクセストラフィックタイプにトンネル識別子が割り当てられます。

機能の仕組み

EPC から非 3GPP への信頼できない Wi-Fi ハンドオーバー コール フロー

このセクションでは、EPC から非 3GPP の信頼できない Wi-Fi ハンドオーバー コール フローについて説明します。

図 *16 : EPC* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フロー

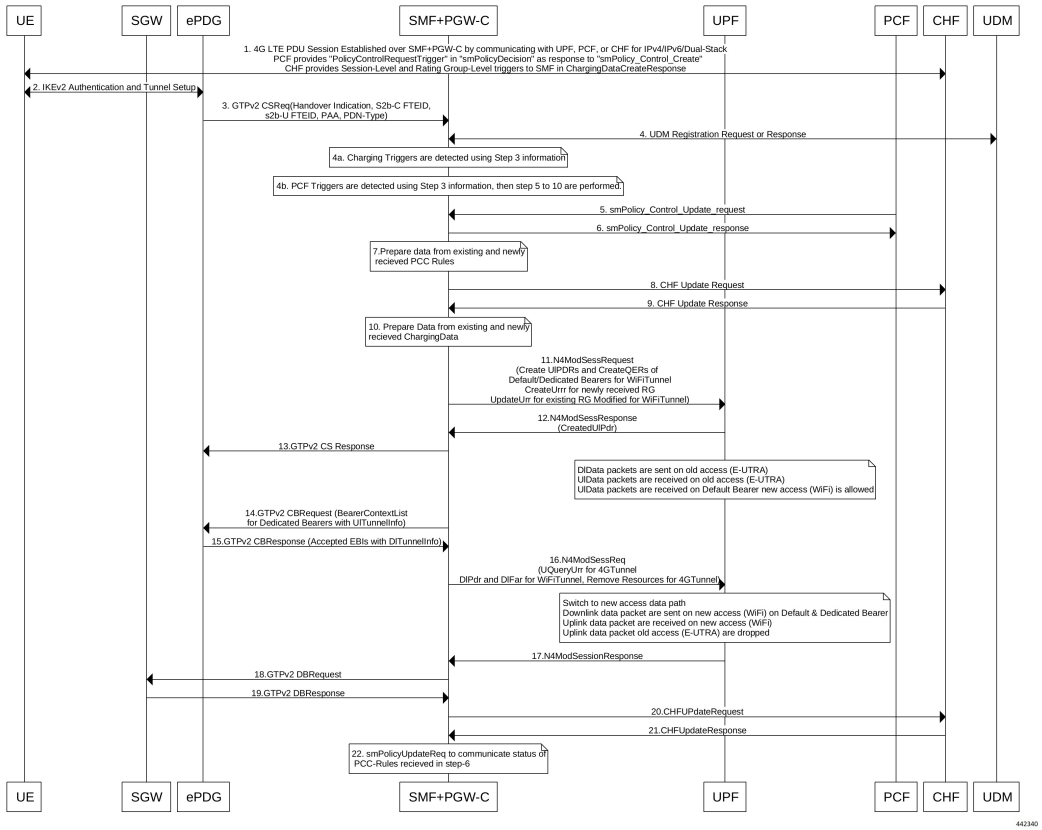


表 *59 : EPC* から非 *3GPP* への信頼できない *Wi-Fi* ハンドオーバー コール フローの説明

ステップ	説明
1	UE は 3GPP アクセス ネットワークに接続されています。 SMF + PGW-C は、IPv4、IPv6、またはデュアルスタックの UPF、PCF、および CHF と通信して、4G LTE PDU セッションを確立します。PCF は、SM ポリシー制御の作成に応答して、SM ポリシーの決定であるポリシー制御要求トリガーを送信します。CHF は、課金データ作成の応答で、SMF に対しセッション レベルまたは料金設定グループレベルのトリガーを提供します。
2	UE は信頼できない非 3GPP アクセスに接続され、ePDG 選択プロセスで ePDG が選択されます。次に、UE は、*3GPP TS 23.402*（セクション *8.6.2.1*）で定義されているハンドオーバー接続手順を開始します。UE と ePDG の間に IKE トンネルが確立され、UE が AAA サーバとの SWm インターフェイスを介して認証された後、UE は IKE 認証（IKE_AUTH）を開始します。IKE_AUTH には、EPC および P-CSCF と DNS のオプションで以前に割り当てられた IPv4 または IPv6 アドレスの構成パラメータが含まれます。

ステップ	説明
3	ePDG は、Create Session 要求を P-GW に送信します。この要求には、詳細が含まれています。 • IMSI • APN • ハンドオーバー インジケータ • RAT タイプ • コントロール プレーンの ePDG TEID • ユーザー プレーンの ePDG アドレス • ユーザー プレーンの ePDG TEID • EPS ベアラー ID • ユーザーの現在地 RAT タイプは、非 3GPP アクセス テクノロジー タイプを示します。UE が IP アドレスの保持をサポートし、ポート アナライザ アダプタ（PAA）に含まれている場合、ePDG はセッション作成要求で引き継ぎの通知を構成し、PDN ゲートウェイが UE に割り当てられた同じ IP アドレスまたはプレフィックスを再割り当てできるようにします。 この IP アドレスまたはプレフィックスは、UE が 3GPP IP アクセスに接続され、PCF でポリシー変更手順を開始するときに割り当てられます。
4a	SMF は、UDM を使用して PGW-C FQDN を更新することにより、UDM 登録を実行します。 EPC とのセッション確立中に UDM 登録は行われません。
4b	SMF は、EPC セッションの確立中に受信した課金トリガーに対してステップ 3 で利用可能な情報を使用して、課金トリガーを検出します。
4c	SMF は、EPC セッション確立中に PCF との通信で受信した要求ポリシー制御トリガーに対してステップ 3 で利用可能な情報を使用して PCF トリガーを検出します。
5	ステップ 4b で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。
6	PCF は、新しいまたは更新された PCC ルールを含み、SM ポリシー制御更新応答を送信します。更新応答には、SM ポリシー決定に関する情報が含まれています。
7	ステップ 6 で受信した情報と EPC セッションの既存のポリシー データに基づいて、SMF は新しいまたは更新された PCC ルールの情報を準備します。

ステップ	説明
8	クォータ情報を必要とする新しい料金設定グループを含む新しいPCCルールをステップ 6 で受信した場合、SMF は CHF に課金情報の更新要求を送信します。SMF には、PDU セッション情報の新しいアクセス パラメータも含まれます。
9	CHF は、ステップ 8 で要求された料金設定グループのクォータ情報を含むマルチユニット情報とともに課金更新応答を SMF に送信します。CHF は、EPC セッションの既存の料金設定グループの新しいクォータ情報を送信することもできます。
10	SMF は、CHF から課金更新応答として受信した情報を処理します。
11	SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求には、アップリンク PDR の作成、QER の作成、受信した新しい料金設定グループ クォータ情報の URR の作成、および変更されたクォータ情報の URR の更新に関する詳細が含まれています。
12	UPF は、N4 セッション変更応答として作成された PDR 内にある UL トンネル情報を SMF に送信します。
13	SMF は GTPv2 セッション作成応答を S-GW に送信します。このレスポンスでは、承認されたまたは部分的に承認されたリクエスト、P-GW S2b F-TEID、PAA、APN-AMBR、ベアラーコンテキスト作成、課金ゲートウェイアドレス、APCO に関する詳細を示します。
14	SMF は、S-GW に GTPv2 ベアラー作成要求を送信します。この要求には、作成されるエンドユーザーへの DL トンネル情報を含むベアラー コンテキスト リストに関する情報が含まれています。
15	S-GW は SMF に GTPv2 ベアラー作成応答を送信します。応答には、承認された要求または部分的に承認された要求の詳細と、ベアラー コンテキストが含まれます。
16	SMF はベアラー応答の作成を処理し、確立されたベアラーの DL トンネル情報と失敗した EBI リスト（ある場合）を取得します。SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求では、各ベアラーの DL トンネル情報、RAT 変更情報を使用して DL PDR および DL FAR を作成し、4G トンネルのリソースを削除します。SMF は、受信した失敗した EBI リストまたは失敗した QFI リストの Wi-Fi トンネルの N4 リソースも削除します。
17	UPF は、N4 セッション変更応答として使用状況レポートを SMF に送信します。
18	SMF + PGW-C は、S-GW に GTPv2 DB 要求を送信します。この要求には、EBI または EBI のリストが含まれます。
19	S-GW は SMF + PGW-C に GTPv2 DB 応答を送信します。
20	SMF は、課金更新要求を CHF に送信します。この要求には、ステップ 8 で受信した新しいアクセスパラメータと使用状況レポートの詳細を含む複数使用状況レポートを含む PDU セッション情報が含まれています。

ステップ	説明
21	CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、既存の料金設定グループの新しいクォータ情報が含まれている場合があります。
22	SMF は、SM ポリシー制御の更新要求を UPF に送信します。このリクエストには、ベアラー応答の作成の一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。 PCF は、SM ポリシー制御更新応答として SM ポリシー決定を送信します。 SMF は SM ポリシー決定を処理し、*3GPP 23.502* セクション *4.3.3.2* で定義されている PCF Initiation Modify 手順として処理します。

非3GPP信頼できないWi-FiからEPCへのハンドオーバー コール フロー

このセクションでは、非 3GPP の信頼できない Wi-Fi から EPC ハンドオーバー コール フローへのについて説明します。

図 *17* : 非 *3GPP* 信頼できない *Wi-Fi* から *EPC* へのハンドオーバー コール フロー

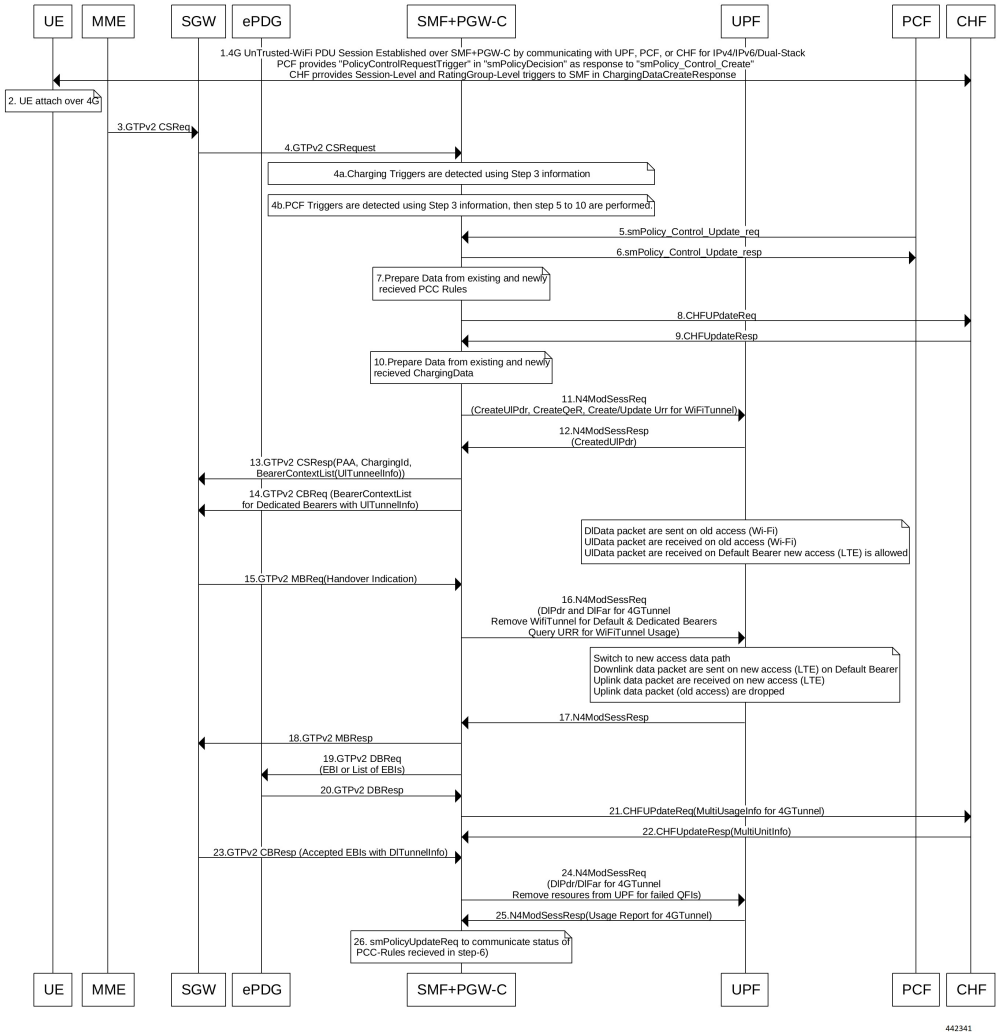


表 *60* : 非 *3GPP* 信頼できない *Wi-Fi* から *EPC* へのハンドオーバーコール フローの説明

ステップ	説明
1	信頼できない非 3GPP アクセスを介して UE と ePDG 間で 1 つ以上の PDU セッションが確立されます。UE の 5G NAS 機能により、ePDG は PGW + SMF を組み合わせて選択します。UE が PDU セッション ID を PGW+SMF に送信します。

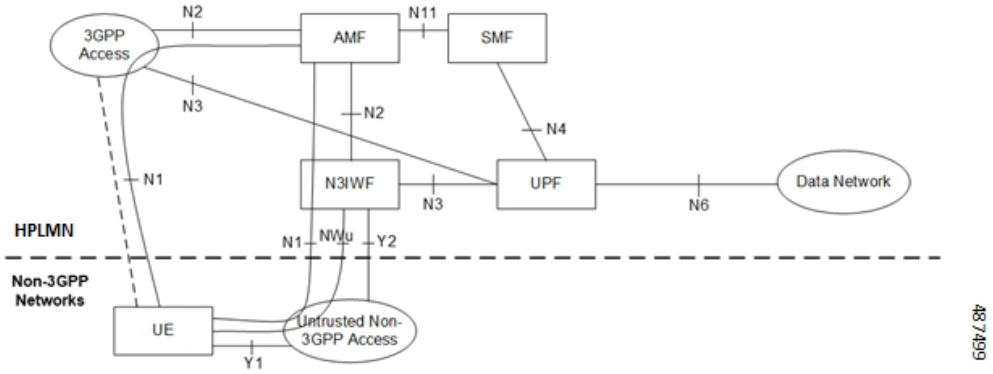
ステップ	説明
2	UE は E-UTRAN アクセスを検出し、現在使用されている非 3GPP アクセス システムから E-UTRAN にセッションを引き継ぎます。3GPP アクセスシステムの UE 検出の詳細については、「*3GPP TS 23.401*」、4.8 項を参照してください。 UE はハンドオーバー接続要求タイプのアタッチ要求を MME に送信します。E-UTRAN は、*3GPP TS 23.401* で定義されているように、UE から受信したメッセージを MME にルーティングします。UE には、送信元の非 3GPP アクセスの PDN 接続に対応する APN の 1 つが含まれます。APN は、*3GPP TS 23.401* で定義されているように提供されます。
3	MME と HSS が認証を実行します。次に、位置情報の更新手順とサブスクライバデータの取得によって APN 情報を受信します。 MME は、*3GPP TS 23.401* で定義されているように APN、SGW、および PDN ゲートウェイを選択します。MME がセッション作成要求メッセージを SGW に送信します。この要求には、IMSI、MME コンテキスト ID、PDN-GW アドレス、「ハンドオーバー」要求タイプのハンドオーバー指示、および APN に関する情報が含まれます。
4	SGW は、*3GPP TS 23.401* で説明されているように、Create Session Request（ハンドオーバー通知）メッセージを HPLMN の PDN-GW に送信します。MME はセッション要求作成メッセージにハンドオーバー指示情報を含めるため、SGW は GTPv2 セッション要求メッセージを PDN GW に送信します。このメッセージには、IMSI の詳細、APN、ハンドオーバーの表示、RAT タイプ、ユーザー プレーンの S5-C TEID、S5-U TEID、EBI、およびユーザー ロケーション情報に関する詳細が含まれます。RAT タイプは、3GPP IP アクセス E-UTRAN テクノロジー タイプを示します。UE が IP アドレスの保存をサポートしており、PAA に含まれている場合、SGW はセッション作成要求でハンドオーバー通知を構成します。この構成では、PDN GW は、UE が 3GPP IP アクセスに接続している間に UE に割り当てられていたのと同じ IP アドレスまたはプレフィックスを再割り当てします。この構成では、SGW は PCF に対してポリシー変更手順を開始します。 ハンドオーバー通知に含まれているため、PDN GW は、この時点で非 3GPP IP アクセスから 3GPP アクセス システムにトンネルを切り替えることはありません。 登録は Wi-Fi セッションの確立中に行われるため、SMF は UDM 登録を実行しません。
4a	SMF は、EPC セッションの確立中に受信した課金トリガに対してステップ 3 で利用可能な情報を使用して、課金トリガを検出します。
4b	SMF は、EPC セッション確立中に PCF との通信で受信した要求ポリシー制御トリガに対してステップ 3 で利用可能な情報を使用して PCF トリガを検出します。
5	ステップ 4b で受信した検出されたアーム化されたポリシー制御トリガに基づいて、SMF は、ステップ 3 で検出されたアクセス パラメータを使用して PCF に SM ポリシー制御更新要求を送信します。

ステップ	説明
6	PCF は、新規または更新された PCC ルールを含めることによって、SM ポリシーの決定である SM ポリシー制御更新応答を送信します。
7	ステップ 6 で受信した情報と EPC セッションの既存のポリシー データに基づいて、SMF は新しいまたは更新された PCC ルールの情報を準備します。
8	SMF はステップ 6 で新しい PCC ルールを受信した場合、課金更新要求を、クォータ情報を持つ新しい料金設定グループとともに CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報が含まれています。
9	CHF は、SMF に課金更新応答としてマルチユニット情報を送信します。マルチユニット情報には、料金設定グループの新しいクォータ情報と、EPC セッションの既存の料金設定グループ（存在する場合）が含まれます。
10	SMF は、CHF が送信した受信済みの課金更新応答の課金データを準備します。
11	SMF は、N4 セッション変更要求を UPF に送信します。この要求には、UL および DL PDR の作成、QER の作成、受信した新しい料金設定グループ クォータ情報の URR の作成、変更されたクォータ情報の更新された URR、および FAR の作成に関する詳細が含まれています。
12	UPF は、SMF への N4 セッション変更応答として、作成された PDR 内の UL トンネル情報を送信します。
13	SMF は GTPv2 セッション作成応答を S-GW に送信します。このレスポンスでは、承認されたまたは部分的に承認されたリクエスト、P-GW S2b F-TEID、PAA、APN-AMBR、ベアラーコンテキスト作成、課金ゲートウェイアドレス、APCO に関する詳細を示します。
14	SGW は、Wi-Fi トンネルから 4G トンネルへのデータ パス切り替えについて、ハンドオーバー通知を含む変更ベアラー要求を PGW に送信します。
15	PGW は N4 セッション変更要求を送信して、Wi-Fi トンネルを削除し、ステップ 4 の 4G トンネルの GTPv2 セッション要求の作成で受信した DL トンネル情報を設定します。
16	UPF が SMF に N4 セッション変更応答を送信します。
17	SMF は、ベアラー コンテキスト リストを含む GTPv2 セッション作成要求を SGW に送信します。このリストには、エンドユーザー向けの DL トンネル情報が含まれています。
18	SGW は GTPv2 セッション作成応答を SMF に送信します。この応答には、承認された要求または部分的に承認された要求の詳細と、ベアラー コンテキストが含まれます。
19	ePDG は GTPv2 ベアラー要求の作成を送信します（DL トンネル情報を持つ EBI を SMF に

ステップ	説明
20	SMF はベアラー応答の作成を処理し、確立されたベアラーの DL トンネル情報と失敗した EBI リスト（ある場合）を取得します。SMF は、Wi-Fi トンネルのために、N4 セッション変更要求を UPF に送信します。この要求は、DL トンネル情報、RAT 変更情報を使用して DL FAR を更新し、4G トンネルのリソースを削除することです。SMF は、受信した失敗した EBI リストまたは失敗した QFI リストの Wi-Fi トンネルの N4 リソースも削除します。
21	UPF は、使用状況レポートを含む N4 セッション変更応答を SMF に送信します。
22	SMF は、課金更新要求を CHF に送信します。この要求には、新しいアクセス パラメータを含む PDU セッション情報と、ステップ 8 で受信した使用状況レポートで構成される複数使用状況レポートが含まれています。
23	CHF は、既存の料金設定グループのクォータ情報を含むマルチユニット情報とともに、課金更新応答を SMF に送信します。
24	SMF + PGW-C は、EBI または EBI リストを含めることで、SGW への GTPv2 DB 要求を開始します。
25	SGW は、SMF + PGW-C に対して GTPv2 DB 応答を送信します。
26	SMF は、SM ポリシー制御の更新要求を UPF に送信します。このリクエストには、ベアラー応答の作成の一部として AMF から受信した失敗した QFI リストの新しいアクセス パラメータとルール レポートが含まれています。 PCF は、SM ポリシー制御更新応答として SM ポリシー決定を送信します。 SMF は SM ポリシー決定を処理し、3GPP 23.502 セクション 4.3.3.2 で定義されている PCF 開始変更手順として処理します。

非 3GPP インターワーキング機能

3GPP リリース 15 以降、非 3GPP インターワーキング機能（N3IWF）は、5G コアとの統合のために信頼できない Wi-Fi（802.11）を適応させることにより、コアネットワークへの非 3GPP アクセスを容易にします。UPF の N3IWF は、信頼できる 3GPP RAN と、パブリックホットスポットやプライベートルータなどの信頼できない Wi-Fi アクセス ポイントの両方からの通信をシームレスに管理します。WPA2 などのリンクレイヤーセキュリティとは独立した、セキュアなエンドツーエンド通信を保証します。UPF は、両方のアクセスタイプからの通信をアンカーし、ネットワーク間で信頼性の高いの高いスケーラブルな接続を可能にします。



N3IWF の接続とハンドオーバーの手順については、「非 3GPP アクセス向け N3IWF」を参照してください。UPF では、この機能は ePDG と同じですが、コールが N3IWF コンポーネントからの場合、UPF は NRTAI 値が設定されている ULI を受信します。この NRTAI 値は、ULI の既存の PFCP_IE_SUB_PARAMS IE に入力されます。UPF は、この NRTAI 値を EDR にダンプします。

ICSR とセッションのリカバリ

- セッション管理機能では、移行中、最新の状態が、安定した状態であると認識され、ハンドオーバーが LTE から Wi-Fi（S2BGTP）またはその逆で完了すると、完全なチェックポイントがトリガーされます。これは、セッションリカバリと ICSR に適用されます。ユーザープレーンには、受信したすべてのメッセージに個別のセッションリカバリと ICSR チェックポインティングがあります。
- ハンドオーバーが失敗した場合、つまり SMF と UPF が同期されない場合、SMF セッションは直近のアクセス時の状態で復旧し、UPF は新たな移行状態で復旧します。この動作は、UPF 障害発生時に適用されます。

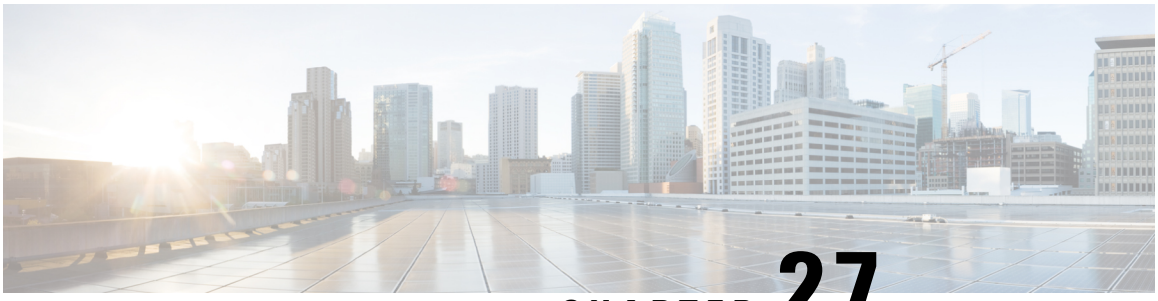
制限事項

LTE - Wi-Fi 間のシームレスハンドオーバー機能では、LTE から eHRPD および Wi-Fi から eHRPD へのハンドオーバーとハンドバックはサポートされません。

標準準拠

LTE - Wi-Fi シームレスハンドオーバー機能は、次の標準規格に準拠しています。

- 3GPP TS 23.214
- 3GPP TS 29.244
- 3GPP TS 23.401
- 3GPP TS 23.402



CHAPTER 27

モニタ サブスクライバ

- 機能の概要と変更履歴, on page 323
- 機能説明 （324 ページ）
- 機能の仕組み （325 ページ）
- UPF での MonSub の 16 進ダンプモジュールの設定 （342 ページ）
- モニタリングおよびトラブルシューティング （343 ページ）

機能の概要と変更履歴

要約データ

Table 61: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
SMF からのサブスクライバ トレーシングシングのサポートが追加されました。	2023.02.0

改訂の詳細	リリース
このリリースでは、MonSub CLI、サブスクライバトレーシングシング制限、パケット処理スループット、PCAP の成功、およびエラーコード通知に関連する拡張機能がこの機能に追加されています。このリリースでは CP および UP セッションマネージャ機能も追加されています。	21.22.x
最初の導入。	21.16.1

機能説明

サブスクライバモニター（MonSub）機能を使用すると、ユーザーと制御通信を含むサブスクライバ関連の情報と、デバッグに役立つ課金イベントや内部イベントなどのイベントをトレースできます。デフォルトでは、この情報は、セッション管理機能（SMF）コンソールに表示されます。ここでは、ユーザーは、MonSub tracing CLI コマンドを実行でき、UPF で、Packet Capture (PCAP) ファイルをキャプチャできます。

ユーザー通信は、パケットがアプリケーションを横断する際に、slowpath で、またはパケットがアプリケーションを横断する必要はないが fastpath 処理（VPP）にオフロードされる際に、fastpath で伝送されます。fastpath オフロード（VPP）が SAEGW に導入されるまでは、slowpath モードがデフォルトモードでした。

サブスクライバモニターには、次の機能があります。

- UPF の PCAP ファイルの fastpath からユーザー通信を継続的にキャプチャします。
- UPF は、制御パケットとデータパケットの両方をキャプチャします。
- 制御イベント通信とその他の関連情報は、UPF 内の個別の PCAP ファイルにキャプチャされます。
- 新しいオプション、UP PCAP trace [W - UP PCAP Trace (ON)] が、MonSub CLI の SMF と UPF に導入されました。slow-path および fast-path PCAP は、このオプションがオンの場合にのみ生成されます。
- UPF ごとに最大 4 つの MonSub セッションを有効にできます。
- デフォルトでは、UPF は次の MonSub オプションをサポートしています。
  - PFCP データ（オプション 49）
  - CSSデータ（オプション34）
  - L3 データ（オプション 19）
  - GTPU（オプション 26）
  - EDR（オプション 77）
  - コール切断後のサブスクライバ概要

- CSS データは、FLOW IDLE TIMEOUT によるフロー終了を追加でキャプチャするようになりました。

この機能に関連する重要な定義の一部を以下に示します。

- **シャーシトラフィック量**：シャーシのパケットスループットの合計量。
- **モニター対象トラフィック量**：すべての MonSub セッションにおける、MonSub を介したすべてのサブスクライバの合計スループットのモニタリング。
- **PCAP 成功** ：PCAP ファイルでの MonSub traffic capture 要求と成功したキャプチャの割合。

PCAP の成功

PCAP の成功は次の要因によって決まります。

- PCAP の成功レベルは、モニター対象のトラフィック量、VPP 使用率、MonSub のモニター優先順位、バックグラウンドディスク I/O など、いくつかの要因によって決まります。
- 一般に、PCAP の成功率は次の場合に高くなります。
  - VPP 使用率が低く、MonSub のモニター優先順位がベストエフォートを超えている場合。
  - モニター対象のトラフィック量がシャーシのトラフィック量の 10% 未満である場合。

  例：VPP が 80% の使用率で実行され、約 10 Gbps のシャーシ通信量を処理している場合、モニター対象の通信量が 1 Gbps 以下であれば、PCAP 成功率が高くなると考えられます。

機能の仕組み

サブスクライバのモニター機能については、次項で詳しく説明します。

SMF と UPF の相互作用

UPF は、CLI 構成を使用したサブスクライバのモニタリングをサポートし、UE ごとにサブスクライバの監視を可能にします。ただし、ネットワークに複数の UPF がある場合、ユーザーは、すべての UPF で UE のサブスクライバの監視を有効にするか、UE が接続して、それを処理している UPF を特定してから、その UPF でサブスクライバの監視を有効にする必要があります。

この機能により、SMF の構成に基づいて UPF のサブスクライバを監視できるため、キャプチャが失われるリスクがなくなります。

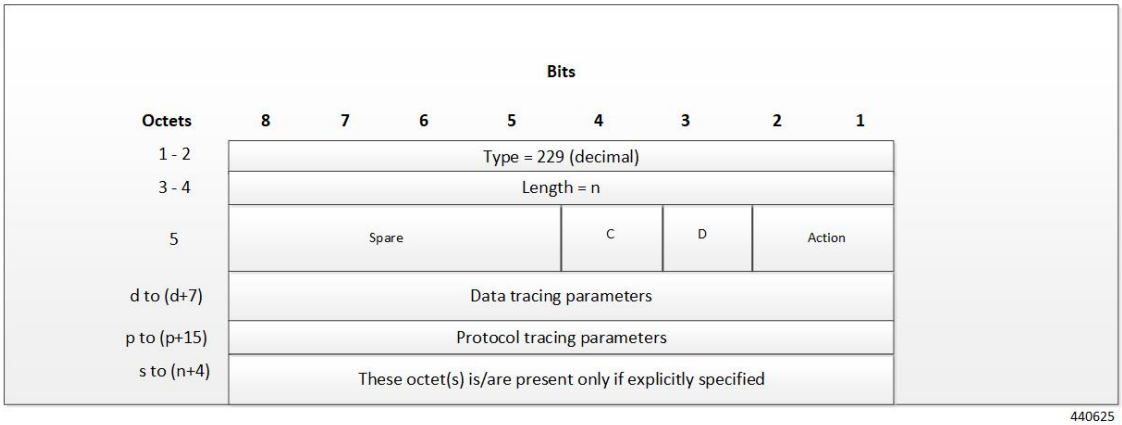
SMF からのサブスクライバ トレーシングシング

SMF からのサブスクライバ トレーシングシング用の MON SUB IE

SMF は、独自のMON SUB IE を UPF に送信して、特定の IMSI のサブスクライバ トレーシング セッションを開始または停止します。MON SUB IE は、private Information Element（IE）であり、選択したトレースオプションが U-Plane の参加を必要とする場合にのみ含めることができます。

PFCP_IE_MONITOR_SUBSCRIBER_INFO

図 *18 :* サブスクライバトレース



アクション：サブスクライバトレースを STOP / START でモニターします。STOP = 1、START = 2。

（注） D=1 の場合、D＝DATA イベントトレーシングは、オンです。8 オクテット（d ～ d＋7）には、D = 1 の場合にのみ存在する必要があるDATA イベントトレーシング（fastpath）情報が含まれます。

C=1 の場合、C = CONTROL イベントトレーシングは、オンです。

データトレーシング（fastpath）情報（8 オクテット）：これには、パケットキャプチャ、パケットキャプチャサイズ、MEH ヘッダーなどの data filter パラメータが含まれます。

- **オクテット 1** :
  - ビット 1：VPP の有効化/無効化
  - ビット 2：FCAP：パケットキャプチャ
  - ビット 3：MEH あり
  - ビット 4 ～ 6：優先順位
- **オクテット 2 ～ 3**：パケットサイズ

• **オクテット 4 ～ 8**：将来の使用のために予約済み。現在、すべて 0 に設定されています。

プロトコルトレーシング情報（16 オクテット/128 ビット）：16 オクテット p-to-(p+15)には、プロトコルトレーシング情報が含まれます。これは、コントロールフラグ（C）またはデータフラグ（D）のいずれかが有効な場合のみ存在します。各ビットは、モニターする一意のプロトコルを表します。たとえば、49 番目のビットが 1 の場合、PFCP イベントトレースシングは、オンです。コントロールイベントフラグは、Protocol Tracing *Rulematch Events*（オプション *34*）、*L3 Data*（オプション *19*）、*GTPU*（オプション *26*）、*EDR*（オプション *77*） および *Subscriber Summary After Call Disconnect* を制御します。

SMF からのサブスクライバ トレーシングシングを有効化する

SMF は、次の 2 つのいずれかの状況で MON SUB IE を送信します。

1. Session Establishment 要求（新しいセッションの場合）、または
2. Session Modification 要求（進行中のセッションの場合）

SMF でのサブスクライバ トレーシングの有効化は、新しい CLI を使用して行われます。詳細については、「SMF モニターサブスクライバの構成」を参照してください。

（注） セッショントレーシングの有効化は、PFCP メッセージにピギーバックされません。セッショントレーシングは、SMF からの個別の Sx Modification 要求経由で UPF で有効になります。

SMF からのサブスクライバ トレーシングシングを無効化する

SMF からのサブスクライバ トレーシングを無効にするには、Action が STOP に設定されている MON SUB IE が Session Modification 要求で送信されます。

PCAP の生成

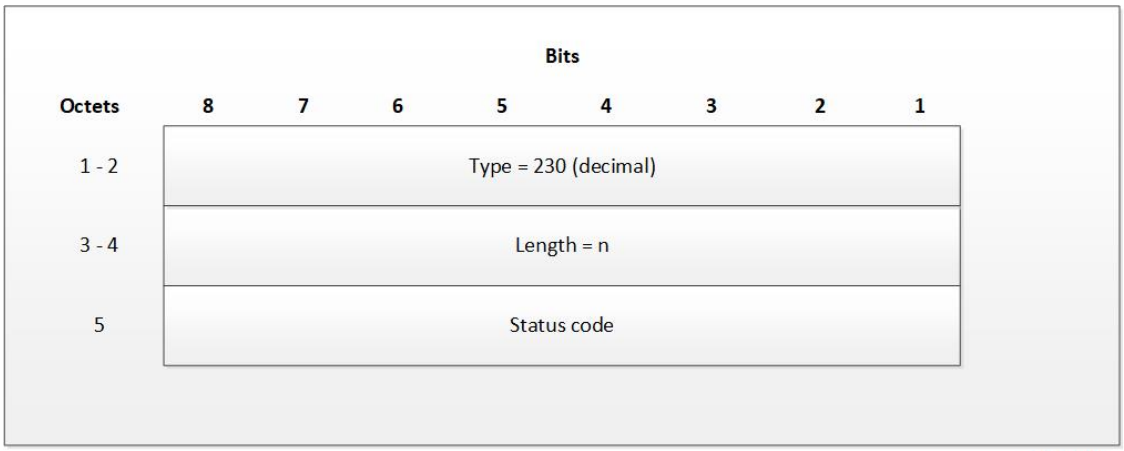
UPF は、次の 3 つの状況で slowpath および fastpath PCAP を生成します。

1. N4 インターフェイス経由で SMF からサブスクライバ トレーシングが停止した場合。
2. サブスクライバセッションが正常に削除された場合。
3. サブスクライバセッションが UPF でローカルに消去された場合。

サブスクライバ トレース ステータス レポート IE（プライベート IE）

Subscriber Trace Status Report IE は、SMF から受信したすべての monsub START 要求に対応して送信されます。

図 *19 :* サブスクライバ トレース ステータス レポート



ステータスコードは、UP でのサブスクライバトレースの受け入れまたは拒否を表します。ステータスコード = 0 は、成功を意味します。1 ～ 255 の値で、特定のエラーコードや通知を一意に指定します。エラーコードのリストと通知は、開発後に定義されます。

表 *62 :* エラーコードと通知テーブル

ステータス コード	ステータスの説明
MONSUB_SM_SUCCESS（0）	
MONSUB_SM_ERROR_FAILURE（1）	MonSub：一般的な障害状態を受信しました。
MONSUB_SM_ERROR_UNSUPPORTED（2）	MonSub：サポートされていない障害です。
MONSUB_SM_ERROR_SESSION_EXIST_NONE（3）	MonSub：セッションが見つかりません。);
MONSUB_SM_ERROR_SESSION_LIMIT_EXCEED（4）	MonSub：最大接続数に達しました。
MONSUB_SM_ERROR_SESSION_INVALID_PARAM（5）	MonSub：接続メッセージが失敗しました。
MONSUB_SM_ERROR_SESSION_ALLOC_FAIL（6）	MonSub：NPU で MonSub セッションを割り当てられませんでした。
MONSUB_SM_ERROR_CONFIG_INVALID_PARAM（7）	MonSub：設定メッセージが失敗しました。
MONSUB_SM_ERROR_MONITOR_LIMIT_EXCEED（8）	MonSub：最大ストリーム制限に達しました。

ステータス コード	ステータスの説明
MONSUB_SM_ERROR_MONITOR_INVALID_PARAM（9）	MonSub：モニターメッセージが失敗しました。
MONSUB_SM_ERROR_MAX（10）	MonSub：最大エラー。
MONSUB_COPROCDATA_CORRUPTED（11）	MonSub：ファイル処理プロセスが失敗しました。
MONSUB_MAX_TRACING_SESSIONS_REACHED（12）	MonSub：トレーシングセッションの最大数に達しました。
MONSUB_STOP_RECVD_WAIT_POLL_TIMEOUT（13）	MonSub：STOP 通知が成功しました。次のトレースを開始するには、ポーリングタイムアウトの設定時間まで待機してください。
MONSUB_FILECOPY_SOURCE_DIR_NOT_EXIST（14）	MonSub：ソースディレクトリが存在しません。
MONSUB_FILECOPY_DEST_DIR_NOT_EXIST（15）	MonSub：接続先ディレクトリが存在しません。
MONSUB_FILECOPY_SOURCE_DIR_OPEN_FAILURE（16）	MonSub：ソースディレクトリを開けません。
MONSUB_FILECOPY_DEST_DIR_OPEN_FAILURE（17）	MonSub：接続先ディレクトリを開けません。
MONSUB_FILECOPY_SOURCE_OPEN_FAILED（18）	MonSub：ソースファイルを開けません。
MONSUB_FILECOPY_DESTINATION_OPEN_FAILED（19）	MonSub：接続先ファイルを開けません。
MONSUB_FILECOPY_DONE_FILE_DELETION_FAILED（20）	MonSub：ソースパスの .done ファイルを削除できません。
MONSUB_FILECOPY_PCAP_FILE_DELETION_FAILED（21）	MonSub：接続先パスの .pcap ファイルを削除できません。
MONSUB_RESPONSE_NPUMGR_MONSUB_SESS_FAILED（23）	MonSub：NPUMGR へのセッション通知中に Messenger にエラーが発生しました。
MONSUB_RESPONSE_NPUMGR_MONSUB_CFG_FAILED（24）	MonSub-Config を NPUMGR にプッシュします。
MONSUB_RESPONSE_NPUMGR_MONSUB_MONITOR_FAILED（25）	NPUMGR への MonSub-Monitor 通知。

ステータス コード	ステータスの説明
MONSUB_RESPONSE_COPROC_FAILED（27）	MonSub：ファイル処理プロセスが失敗しました。
MONSUB_RESPONSE_FILE_TRANSFER_SUCCESS（28）	MonSub：ファイル転送が成功しました。
MONSUB_RESPONSE_FILE_TRANSFER_FAILED（29）	MonSub：ファイル転送が失敗しました。
MONSUB_ADMINISTRATIVE_DISCONNECT（30）	MonSub：管理上の接続解除。
MONSUB_FILECOPY_DESTINATION_DISK_FULL（31）	MonSub：宛先パスにスペースがありません。
MONSUB_FILECOPY_COPROC_ABRUPTLY_KILLED（32）	MonSub：File copy co-proc が突然終了しました。
MONSUB_LOGGING_COPROC_ABRUPTLY_KILLED（33）	MonSub：Logging co-proc が突然終了しました。
MONSUB_SM_DISCONNECT（34）	
MONSUB_FILECOPY_STATUS_MAX（35）	
その他	プロトコルモニタートレースの追加中に内部エラーが発生しました。中止しています…

fastpath および slowpath パケットキャプチャ

MonSub でのパケットキャプチャは、Slowpath と Fastpath で行われます。

Slowpath

- Slowpath PCAP は、slowpath（アプリケーション）を通過するパケットをキャプチャします。

  オプション PFCP(49)、GTPU(26)、L3(19)、および CSS(34) が有効になっている場合、MonSub が有効になっている時点から N4 メッセージ/データパケットが表示されます。

- アップリンクデータパケットは、受信 GTPU、ルールマッチ、発信 L3 として表示されます。

- ダウンリンクデータパケットは、受信 L3、ルールマッチ、発信 L3 として表示されます。

Fastpath

- Fastpath PCAP は、fastpath を通過するパケットをキャプチャします。

- 純粋な Fastpath パケットの場合、アップリンクデータパケットは受信 GTPU、発信 L3 として表示されます。
- ダウンリンクデータパケットは、受信 L3、発信 GTPU として表示されます。
- Slowpath パケットは、両方向に UPF を出力しながら、Fastpath PCAP にも表示されます。

UPF SessMgr の機能

この機能をサポートするためにUPFセッションマネージャで行われた変更は次のとおりです。

- MonSub トレースを有効または無効にするためのサービスを CLI に提供します。
- NPUMgr を制御して、MonSub セッションを接続/開始/停止/追加/削除します。
- CLIからの指示に基づいて、パケットサイズや優先順位などを変更するために（NPUMGR経由で）パノプティコンを構成します。
- 生成された pcap ファイルのストレージを管理するには、「hex dump module」構成を読み取ります。
- ファイルをコピーできない場合、またはセッションマネージャ MonSub インスタンス化に問題がある場合は、SNMP アラームを生成します。
- 制御パケットまたは slowpath パケットを個別の slowpath PCAP としてキャプチャします。
- この機能は、UPF インスタンスに対して最大 4 つのモニター サブスクライバ トレーシング セッションをサポートします。NPUMgr はトレース制限を適用します。
- ハードディスクに空き領域がない場合、またはハードディスクがない場合、MonSub トレースセッションは終了します。
- フローアイドルタイムアウトによるフロー終了も、オプション 34 のCSS データでキャプチャされます。
- N4/Sx Establishment 要求/応答もキャプチャされます。

マルチ PDN マルチトレース

マルチ PDN コールの場合、Multi-trace=OFF で MonSub を開始すると、その MonSub セッションの一部として 1 つの PDN のみがトレースされます。新しい PDN が開始されると、既存の PDN トレースが停止し、新しい PDN トレースが開始します。これを行うには、まず新しい PDN トレースを開始してから、既存の PDN トレースを停止します。よって、新しい PSN およびセッションマネージャのサブセッション ID が割り当てられます。

マルチ PDN コールの場合、Multi-trace=ON で MonSub を開始すると、新しい fastpath トレースセッション（つまり、MonSubセッション）の一部として新しいPDNがトレースされるため、4 つの PDN をトレースすると、最大トレースセッションに到達したことが MonSub CLI に示されます。各 PDN のトレースは、個別の MonSub セッションとして実行されます。

MonSub 統計

fastpath PCAP キャプチャの品質に関する統計をパブリッシュするための新しいメカニズムが MonSub CLI に追加されました。新しいメカニズムは、5 秒ごとにスロットリングされたバッファフル MEH 指示をセッションマネージャで受信するたびに統計を公開します。この機能は、MonSub セッションに対応する fastpath PCAP に対して最大 4 つのバッファをサポートします。この機能はデフォルトでは統計を公開しないため、UPF でデバッグ CLI を使用して有効にする必要があります。

- **debug uplane monsub-stats disabled**
- **debug uplane monsub-stats enabled**

統計情報には、次の情報が含まれます。

```
Packet accepted: 14250000          Packet rejected: 62297
Congestion Short Term: 0                    Congestion Longer Term: 0
Throttled: 0                                PCAP File Transfer Rate: 9.91 mbps
```

PCAP ファイルの転送速度は、copy Co-Proc が RAM-FS から HD-RAID に PCAP を書き込む速度です。

X-Header

この機能は、slowpath PCAP における X-Header のキャプチャをサポートします。UPF がアップリンクパケットの X-Header を挿入すると、UPF は入口と出口のインターフェイスでパケットをキャプチャします。したがって、N6 に送信される出口パケットには、挿入済みの X-header が含まれます。

UPF がダウンリンクパケットの X-Header を挿入すると、UPF は入口と出口のインターフェイスでパケットをキャプチャします。したがって、N3 に送信される出口パケットには、挿入済みの X-header が含まれます。

UPF におけるサブスクライバのモニターの設定手順

プロトコルモニターは、現在処理中の特定のサブスクライバセッションの情報を表示するために使用できます。モニター対象のプロトコルの数と進行中のセッション数に応じて、大量のデータが生成されます。生成されたすべての情報をキャプチャするには、端末クライアントでロギングを有効にすることを強くお勧めします。

MonSub は、UPF コンソールから開始することもできます。特定の IMSI のモニタリングは、SMF および UP コンソールのいずれからも有効にしないでください。

特定のサブスクライバセッションのプロトコルモニタリングツールを起動して設定するには、この項の手順に従います。

手順

ステップ 1 **monitor subscriber** CLI コマンドを入力して、Exec モードから monitor subscriber コマンドを呼び出します。

```
[local]host_name# monitor subscriber { callid | imei | imsi | ipaddr | ipv6addr |
msid | msisdn | next-call | pcf | peer-fa | peer-lac | sgsn-address | type |
username | smgr-instance }
```

現在使用可能なすべてのプロトコル（それぞれに割り当てられた番号を持つ）が一覧表示された出力が表示されます。適切なキーワードを入力して、モニターが使用するメソッドを指定します。

ステップ 2 適切なキーワードを入力して、モニターが使用するメソッドを指定します。

その他のオプションを選択したり、選択したキーワードに適切な情報を入力したりします。

ステップ 3 その他のオプションを選択したり、選択したキーワードに適切な情報を入力したりします。

モニターの起動時に、指定された基準に一致するセッションが処理されなかった場合は、使用可能なモニタリングオプションの画面が表示されます。

ステップ 4 モニターによって表示される情報の量を設定します。オプションを有効または無効にするには、そのオプションに関連付けられている文字または 2 桁の数字（C、D、E、11、12 など）を入力します。冗長性を向上または低下させるには、プラス（+）またはマイナス（-）キーを使用します。

各オプションの右側には、[ON (enabled)] または [OFF (disabled)] の現在の状態が表示されます。

マルチコールトレースを実行するためのオプション **Y** は、GGSN での使用に対してのみサポートされています。

```
WARNING!!! You have selected options that can DISRUPT USER SERVICE
Existing CALLS MAY BE DROPPED and/or new CALLS MAY FAIL!!!
(Under heavy call load, some debugging output may not be displayed)
Proceed? - Select (Y)es or (N)o
```

ステップ 5 必要に応じてステップ 6 を繰り返して、複数のプロトコルを有効または無効にします。

ステップ 6 **[Enter]** キーを押して画面を更新し、モニタリングを開始します。

モニターは、無効になるまでアクティブのままになります。プロトコルモニターを終了してプロンプトに戻るには、**q** を押します。

Monsub CLI オプション

モニターサブスクライバ CLI：新しいオプション

以下のオプションとそのデフォルト値が、既存の **monitor subscriber** コマンドに追加されます。

UPF Monitor Subscriber CLI

オプションは次のとおりです。

- **W - UP PCAP Trace (ON)**：このパラメータは、slowpath と fastpath に対して PCAP トレースを作成し、CUPS のみに適用できます。
- **U - Mon Display (ON)**：slowpath PCAP ファイルで、統計、ECS からの課金情報などのプロトコル以外のイベントもキャプチャされ、U-PLANE モニタコンソールで表示されます。
- **V - PCAP Hexdump (ON)**：このフラグを ON に設定すると、U-PLANE 上でプロトコルパケットをキャプチャし、hexdump 形式のテキストファイルに保存できます。

（注） 現在、CUPS で、fastpath および slowpath PCAP ファイルをキャプチャするには、UP PCAP トレースフラグを ON に設定する必要があります。

モニターサブスクライバ CLI：新しいオプション

以下のオプションとそのデフォルト値が、既存の **monitor subscriber** コマンドに追加されます。

- **F - Packet Capture (Full Pkt)**：fastpath からすべてのパケットをキャプチャします。

  オペレータはこのオプションを使用して、完全なパケットキャプチャと部分的なパケットキャプチャを選択できます。**F** を入力すると、パケットキャプチャタイプを完全なキャプチャまたは部分的なキャプチャに変更できます。部分的なパケットキャプチャでは、1 ～ 16384 バイトのパケットサイズを入力できます。たとえば、20 と入力すると、fastpath パケットの最初の 20 バイトだけがキャプチャされ、残りのパケットはドロップされます。

（注） PCAP ファイルを開くと、概要ビューにはパケットのフルレングスが表示されますが、詳細ビューには切り捨てられたパケットのみが表示されます。

- **/ - Priority (0)**：値は「0（ベストエフォート）」～「7（保証）」の範囲です。
  - 0：ベストエフォート
  - 1：低
  - 2：低～中
  - 3：中
  - 4：中～高
  - 5：高
  - 6：クリティカル
  - 7：保証



注意　デフォルト値を変更しないことを強く推奨します。システム パフォーマンスに悪影響を及ぼす可能性があります。

- **N - MEH Header (OFF)**：このオプションが設定されている場合、IP パケットから MEH ヘッダーが削除されます。

Monitor Subscriber セッションの表示

進行中の MonSub セッションを表示する新しい CLI を以下に示します。

CLI **show monitor subscriber fastpath session all** は、UPF からトリガーできます。

- **SessId**：UPF セッションマネージャの MonSub セッションのローカルセッション ID です。
- **CallID**：Userplane のコール ID。
- **PSN**：これはパノプティコンのシーケンス番号です。1 つの UP には、0 ～ 3 の範囲の PSN を持つ最大 4 つの MonSub fastpath トレースセッションがあります。
- **Start time**：MonSub トレースセッションの開始時刻。
- **Interface Type**：開始された MonSub fastpath トレースセッションのコールタイプ（Sxa、Sxb、Sxab）を識別します。

Monitor Subscriber セッションの解除

進行中の MonSub セッションを切断する新しい CLI を以下に示します。UPF から CLI をトリガーできます。

monitor subscriber fastpath disconnect sessmgr-instance <UP SMGR Instance ID> session-id <Local Monitor subscriber Session ID at SMGR instance level>

MonSub セッションの切断に成功すると、次のメッセージがコンソールに表示されます。

セッションが正常に切断されました

MonSub セッションの切断に失敗すると、次のメッセージがコンソールに表示されます。

モニタ　サブスクライバセッションが存在しません



（注）　モニター切断 CLI を実行できるのは、セキュリティ管理者だけです。

モニターサブスクライバのコンテキスト、CDRMOD、および16進ダンプのインタラクション

16進ダンプモジュールは、オペレータがファイル名とポーリングタイマーを設定するためのプロビジョニングを提供するように設定する必要があります。16進ダンプモジュールは、CDRMOD機能の一部である EDR、UDR などのモジュールの 1 つです。ECS コンテキストなどの非ローカルコンテキストで16進ダンプを設定します。ローカルコンテキストでは16進ダンプモジュールはサポートされていません。

16 進ダンプモジュールとその設定の詳細については、「UPF での MonSub の 16 進ダンプモジュールの設定」の項を参照してください。

PCAP ファイル名の表記法

ここでは、PCAP ファイルの命名規則について説明します。



（注） PCAP ファイルの命名では、**monitor-subscriber-file-name** および **rotation** オプションのみを使用します。

slowpath ファイル名の規則

slowpath ファイル名は次のフォーマットになります。

```
curr_slowpath_{SMGR Mon Sub Session
Id}_{monsub_file_name_option_val}_{Timestamp}_{RotationCount}.pcap
```

、または

```
slowpath_{SMGR Mon Sub Session
Id}_{monsub_file_name_option_val}_{Timestamp}_{RotationCount}.pcap
```

プレフィックス「curr_」が付いているファイルは、現在書き込み中で、まだ閉じられていないファイルです。ファイルをローテーションする場合（ファイル ローテーション パラメータに応じて）、プレフィックス「curr_」が付いていないファイルがハードディスクにコピーされます。

SMGR MonSub Session Id：これは、この PCAP を作成した Uplane SMGR インスタンス ID で作成された MonSub セッションのセッション ID です。この ID は SMGR インスタンスに対してローカルであるため、同じ ID でキャプチャされた slowpath PCAP が 2 つ存在する可能性があります。

ファイルをハードディスクにコピーする場合、monsub_file_name_option_val は次のように置き換えられます。

- **monitor-subscriber-file-name** が「imsi」に設定されている場合は IMSI 値
- **monitor-subscriber-file-name** が「call-id」に設定されている場合はコール ID 値
- **monitor-subscriber-file-name** が「username」に設定されている場合はユーザー名の値

タイムスタンプのフォーマットは「MMDDYYYYHHMMSS」です。

- MM：月、DD：日、YYYY：年
- HH：時間、MM：分、SS：秒

RotationCountは9桁の値で、古いファイルがローテーションされ、新しいファイルが生成されるたびに 1 増加します。

最初のファイルは00000000、2番目のファイルは00000001というように増えていきます。

slowpathファイルのローテーションは、**hexdump-module file**設定の次のオプションによって規定されます。

rotation { num-records *number* **| time** *seconds*| **volume** *bytes* **}**

- **num-records**：[num-records] はパケット数を指定します。パケット数がこの数を超えると、新しいファイルが生成され、ファイル名の [RotationCount] が 1 増加します。[number] の範囲は 100 ～ 10240 で、デフォルト値は 1024 です。
- **time**：[time] は新しいファイルが生成され、ファイル名の [RotationCount] が 1 増加するまでの待機時間を秒単位で指定します。[seconds] は 30 ～ 86400 までの整数である必要があります。デフォルト値は 3600 です。
- **volume**：[volume] はバイト数を指定します。バイト数がこの数を超えると、ファイル名の [RotationCount] が 1 増加します。[bytes] は 51200 ～ 62914560 までの整数である必要があります。デフォルト値は 102400 です。

（注） ローテーション中の**tarriff-time**パラメータは、PCAPファイルのキャプチャには適していないため、無視されます。

以下に、slowpath PCAP ファイルのファイル命名規則の例を示します。

- [imsi] オプションが設定されていて、IMSI が「112233445566778」である場合、slowpath ファイルは次のように命名されます。

```
slowpath_S0_112233445566778_07152019050907_000000000.pcap
```

- [call_id] オプションが設定されていて、コール ID が「01317b22」である場合、slowpath ファイルは次のように命名されます。

```
slowpath_S0_01317b22_07152019050907_000000000.pcap
```

（注） **tarrif-time** パラメータは、PCAP ファイルキャプチャには適用されません。

fastpath ファイル名の規則

fastpath ファイル名は次のフォーマットになります。

```
vpp_{S}_{B}_{encap}_{monsub_file_name_option}_{Timestamp}_{FileCount}.pcap
```

- S は、「S1」、「S2」、「S3」、「S4」のいずれかに置き換えられます。
- B は、Panopticon によって生成されたバンドルに応じて、「B0」、「B1」、「B2」、「B3」のいずれかに置き換えられます。
- monsub_file_name_option は次のように置き換えられます。
  - **monitor-subscriber-file-name** が「imsi」に設定されている場合は IMSI 値
  - **monitor-subscriber-file-name** が「call-id」に設定されている場合はコール ID 値
  - **monitor-subscriber-file-name** が「username」に設定されている場合はユーザー名の値

タイムスタンプのフォーマットは「MMDDYYYYHHMMSS」です。

- MM：月、DD：日、YYYY：年
- HH：時間、MM：分、SS：秒

RotationCount は 9 桁の値で、古いファイルがローテーションされ、新しいファイルが生成されるたびに 1 増加します。

最初のファイルは 00000000、2 番目のファイルは 00000001 というように増えていきます。

fastpath の [FileCount] は、slowpathの [RotationCount] パラメータと同じではないため、fastpath ファイルの命名時には [hexdump-module file Rotation] パラメータは無視されます。

この機能のフェーズ 1 では、fastpath で生成されたファイル名は「vpp_S1_B0_ip.pcap」または「vpp_S1_B1_ip.pcap」などであり、不揮発性ストレージにコピーされるときに次のように名前が変更されます。

- `vpp_S1_B0_ip_01317b22_07152019050907_000000000.pcap`
- `vpp_S1_B1_ip_01317b22_07152019050908_000000001.pcap`
- `vpp_S1_B0_ip_01317b22_07152019050908_000000002.pcap`

MonSub フェーズ 3 では、PCAP「バンドル」は、イーサネットカプセル化を使用する単一の PCAP ファイルに置き換えられます。

フェーズ 3 では、各 fastpath セッションファイルは「vpp_S0_B0_eth.pcap」というイーサネット PCAP ファイルにキャプチャされ、不揮発性ストレージにコピーされるときに次のように名前が変更されます。

```
vpp_S0_B0_eth_01317b22_07152019050907_000000000.pcap
```

[call_id] オプションが設定されていて、コール ID が「12345678ef」である場合：

- `slowpath_S0_12345678ef _07152019050907_000000000.pcap`

- vpp_S1_B0_eth_12345678ef _07152019050907_000000000.pcap

[username] オプションが設定されていて、ユーザー名が「9890098900」である場合：

- slowpath_S0_07152019050907_000000000_9890098900.pcap
- vpp_S1_B0_eth_07152019050907_000000000_9890098900.pcap

PCAP ファイルの場所

fastpath PCAP ファイルは、セッションマネージャがサブスクライバセッションを所有しているのと同じカードおよび CPU コンプレックス内の /records/pcap ディレクトリに書き込まれます。

/records ディレクトリは「tmpfs」ファイルシステムにマッピングされ、このファイルシステムは RAM にマッピングされます。この状態で、ファイルには「.pending」の拡張子が付けられます。次に例を示します。

```
-rw-rw-r-- 1 root root 268599296 Sep 23 14:04 vpp_S1_B0_eth.pending
```

（注） この段階のファイルサイズは、永続ストレージに書き込まれるときの実際のファイルサイズではありません。

fastpath トレースメカニズムによってファイルが書き込まれると、「.pcap」ファイルに変換され、次のように名前が変更されます。「.done」の拡張子で終わるファイルもあります。

```
-rw-rw-r--    1 root     root       8689188 Oct 16 22:06 vpp_S0_B0_eth.pcap
```

PCAP ファイルが fastpath トレースメカニズムによって書き込まれた後、Co-Proc 機能によってファイルがインスタンス化され、ハードディスクまたは永続ストレージにコピーされます。

前述の fastpath のファイル格納プロセスは、slowpath にも当てはまります。

すべてのケースでターゲットファイルの場所は /hd_raid/records/hexdump になります。ただし、16 進ダンプモジュールの設定では **use-harddisk** が有効になっており、**hexdump file** では **directory** オプションはカスタム値になります。たとえば、**directory** オプションの値が「abc」に設定されている場合、PCAP ファイルのターゲットの場所は /hd_raid/records/hexdump/abc/ になります。

この機能を実装すると、事前定義した場所が PCAP ファイルに設定されます。

- **use-harddisk** および **hexdump module** の設定を使用して問題が発生した場合に、/records/pcap ディレクトリにデータが入力されないようにするため。
- /hd_raid/records/hexdump ディレクトリを定期的にクリーンアップするため。

外部ロケーションへのファイル転送

ファイルがハードディスクにコピーされたら、**hexdump-module** コンフィギュレーションの **hexdump** コマンドで **transfer-mode** オプションを使用すると、外部サーバーにコピーできます。

transfer-mode 以外にも、**hexdump** では他の関連オプションを外部へのファイル転送に使用できます。オペレータはこれらのコマンドを使用して、fastpath 処理中のストレージ不足を回避できます。

制限事項

モニターサブスクライバ機能の一部の既知の制限は次のとおりです。

- この機能は、SR/ICSR をサポートしません。
- UPF ごとに最大 4 つの mon サブセッションを有効にできます。
- 特定の IMSI のモニタリングは、SMF および UP コンソールのいずれからも有効にしないでください。
- コンボコールは、2 つの PDN（同じ IMSI を持つが一意のコール ID を持つ SXA および N4 レッグ）のモニタリングが関与するため、2 つの mon サブセッションで構成されます。
- 受信アップリンクパケット（GTPU を使用）は、このフェーズでは VPP イングレスではキャプチャされません。
- 終了直後にトレースを再開すると、`/records/pcap` ディレクトリ内の fastpath ファイルが上書きされる可能性があります。したがって、数秒後にセッションを再開します。
- MonSub トレースが停止すると、切断プロセスに数秒かかることがあるため、数秒待つことをお勧めします。MonSub トレースを切り替えて開始する前に、最大 5 秒（秒単位の 16 進ダンプのポーリングタイマー値）かかります。そうでない場合、オペレータ側で一時的に、MAX TRACING SESSIONS REACHED と表示されることがあります。
- Monitor Subscriber fastpath sessions show CLI は、停止しているセッションを表示しません。そのため、一時的に最大セッション数に達したことにより、新しい MonSub セッションが拒否される期間が発生します。ただし、show CLI で表示されるセッションは少なくなります。したがって、しばらく待機してから、新しい MonSub トレースセッションを開始することを推奨します。
- fastpath 設定オプションの変更は、**UP Pcap トレース**が [OFF] に設定されている場合にのみ可能です。
- マルチ PDN で MT=ON になっている場合、MT=OFF になると、MAX TRACING REACHED が原因で新しい PDN トレースは開始されず、他のすべてのトレースが停止します。これは、最初の新しい PDN トレースが開始されてから MT=OFF になり、以前の PDN がすべて停止されたためです。
- 異なる CLI から同じ UE MonSub セッションを起動しないでください。

- slowpath PCAP では、GTP-U ヘッダーを追加する機能が fastpath で利用可能であるため、エグレス DL パケットには GTP-U ヘッダーが表示されません。そのため、イングレスパケットに HTTP X-Header などのパケット変更が適用されない限り、イングレス DL パケットとエグレス DL パケットには重複したパケットが表示されます。
- C オプションと D オプションを切り替えても、UPF の PCAP キャプチャには影響しません。
- マルチ PDN の場合、fastpath ファイル名にはコール ID は使用されません。定義上、マルチ PDN のケースには複数のコール ID があり、IMSI などの上位レベルの構成がファイルの命名に適しているためです。
- このドキュメントで明示的に言及されている名前付きオプションのみが、*hexdump-module file* ファイルの構成でサポートされます。
- fastpath でトレースできるストリームの数は 5,000 に制限されています。ストリームは、TCP または UDP フローとして定義されます。これには、送信元 IP アドレス、宛先 IP アドレス、ソースポート、および宛先ポート、TCP または UDP などのトランスポートプロトコルが含まれます。
- fastpath パケットは外部サーバーにストリーミングできないため、これらは、ハードディスクに格納され、手動または **transfer-mode** オプションのいずれかで転送されます。
- fastpath および slowpath PCAP ファイルをキャプチャするには、UP PCAP トレースを [ON] に設定する必要があります。
- MonSub CLI オプション <SPACE> [Pause] は、コンソールイベントを一時停止するだけです。このオプションは、他のトレースイベント（slowpath PCAP、fastpath PCAP、および 16進ダンプ形式のテキストファイルのプロトコルパケットトレース）には影響しません。
- UP トレース PCAP ファイルには、競合状態が原因で、最初の PFCP Sx 要求/応答は含まれていません。
- ICMP パケットと TCP および UDP ストリームの最初のパケットは、slowpath と fastpath の両方を通過します。GTPU（オプション 26）およびユーザー L3（オプション 19）のデフォルト値は [OFF] に設定されているため、それらのパケットは slowpath キャプチャでキャプチャされません。オプション 26 が [ON] に設定されている場合、それらのパケットは slowpath PCAP キャプチャでキャプチャされます。オプション 19 は slowpath PCAP キャプチャには影響しません。
- fastpath および slowpath PCAP ファイルをキャプチャするには、データイベントフラグを [ON] に設定する必要があります。
- MoSub トレースは、UP 時の **Next-SAEGW Call** オプションではサポートされていません。
- MonSub トレースは、Pure-S コールタイプの **Next call by APN** オプションではサポートされていません。
- デフォルト値の poll-timer を使用した ASR 5500 セットアップでは、既知の問題が原因ですべてのパケットがキャプチャされない可能性があります。多数のパケットが拒否されないようにするには、poll-timer 値を可能な限り低い値（10 ミリ秒）に変更します。

- コンテキストの置換が発生した場合（同じサブスクライバが切断されずに再接続した場合）、新しいコールの slowpath キャプチャは古い slowpath ファイルに残ります。

UPF での MonSub の 16 進ダンプモジュールの設定

MonSub ポールタイマーの設定

この設定を使用して、PCAP ファイルキャプチャチェックの頻度を設定します。

```
configure
  context context_name
    hexdump-module
      hexdump monitor-subscriber-poll-timeout poll_timer_value
      end
```

注：

- **hexdump monitor-subscriber-poll-timeout** ：このオプションは、揮発性ストレージ内の新たにキャプチャされたPCAPファイルを、永続ストレージにコピーする前に実行する必要があるチェックの頻度を指定します。
- *poll_timer_value*：ポーリングタイマー値をミリ秒単位で指定します。10 ミリ秒～ 60 秒までの整数で指定する必要があります。デフォルト：30 秒。

（注） このタイマーに 5 秒未満の値は設定しないでください。

- このオプションは、fastpath 機能を備えた製品（PGW、ASR-5500 上の SAEGW、および VPC-SI）で MonSub が有効になっている場合にのみ適用されます。

MonSub ファイル名の設定

次の設定を使用して、IMSI、コール ID、またはユーザー名を含む PCAP ファイルのファイル名を指定します。

```
configure
  context context_name
    hexdump-module
      file rotation { num-records number | tariff-time minute minutes
hour hours | time seconds| volume bytes | monitor-subscriber-file-name {
imsi | username | call-id }
      end
```

注：

- **monitor-subscriber-file-name { imsi | username | call-id }**：このオプションは、キャプチャされた PCAP ファイルの名前に IMSI、コール ID、またはユーザー名を含むかどうかを指定します。このオプションは、fastpath 機能を備えた製品（PGW、ASR 5500 上の SAEGW、および VPC-SI）で、かつサブスクライバのモニター機能が有効になっている場合にのみ適用されます。デフォルトは IMSI です。
- **rotation { num-records** *number* **| tariff-time minute** *minutes* **hour** *hours* **| time** *seconds* **| volume** *bytes* **}**：16 進ダンプファイルを閉じて新しいファイルを作成するタイミングを指定します。
  - **num-records** *number*：16 進ダンプファイルに追加する必要があるレコードの最大数を指定します。ファイル内のレコード数がこの値に達すると、ファイルが完成します。

    number は 100 ～ 10240 の整数である必要があります。デフォルト：1024
  - **tariff-time minute** *minutes* **hour** *hours*：現在の 16 進ダンプファイルを閉じて、タリフ時間（時分単位）に基づいて新しいファイルを作成します。

    minutes は 0 ～ 59 までの整数である必要があります。

    hours は 0 ～ 23 までの整数である必要があります。
  - **time** *seconds*：現在の 16 進ダンプファイルを閉じて新しいファイルを作成するまでの待機時間（秒単位）を指定します。

    seconds は 30 ～ 86400 の整数である必要があります。デフォルト：3600

重要 ローテンション時間は 30 秒に設定します。

  - **volume** *bytes*：16 進ダンプファイルを閉じて、新しいファイルを作成するまでのファイルの最大サイズを指定します（バイト単位）。

    bytes は 51200 ～ 62914560 の整数である必要があります。compression キーワードが gzip に設定されている場合、設定が大きいほど圧縮率が向上する場合があることに注意してください。デフォルト：102400

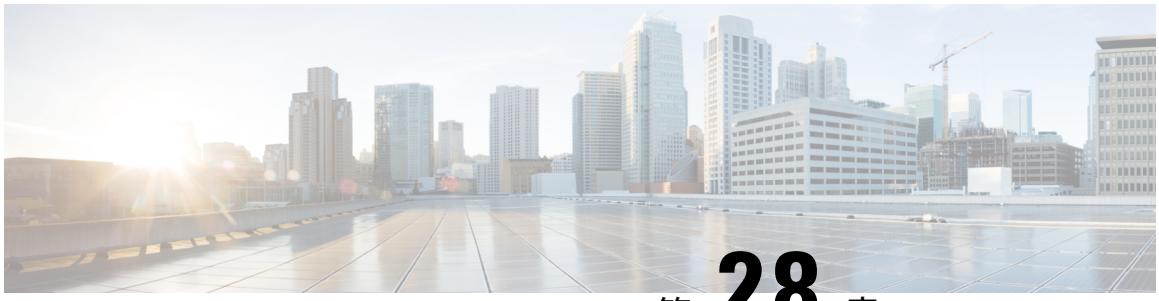
モニタリングおよびトラブルシューティング

この項では、モニターサブスクライバ機能のモニタリングと障害対応について説明します。

SNMP トラップ

モニターサブスクライバ機能をサポートするために、次の SNMP トラップが追加されました。

- **MonSubProcessInitFailure**：このトラップは、MonSub ハンドラプロセスが特定のプロセスやサービスで失敗した場合にトリガーされます。



第 28 章

UPF での MPLS のサポート

- 機能の概要と変更履歴 （345 ページ）
- 機能説明 （346 ページ）
- 機能の仕組み （347 ページ）
- モニタリングおよびトラブルシューティング （355 ページ）

機能の概要と変更履歴

要約データ

表 *63 :* 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
N9 インターフェイス経由の MPLS サポートが追加されました。	2023.02.0
N6 インターフェイスを介した MPLS のサポートが追加されました。	2023.01.0

改訂の詳細	リリース
最初の導入。	2022.04.0

機能説明

マルチプロトコルラベルスイッチング（MPLS）は、IPアドレスを使用する代わりにラベルを使用してパケットをルーティングするプロトコルです。UPFは、データプレーンフォワーダとして VPP を使用して MPLS 通信を切り替えるために MPLS をサポートしています。

ASR 5500 では、NP4c ネットワークプロセッサが、MPLS 通信を生成および処理します。VPC-DI では、IFTask は MPLS 通信を生成および処理します。

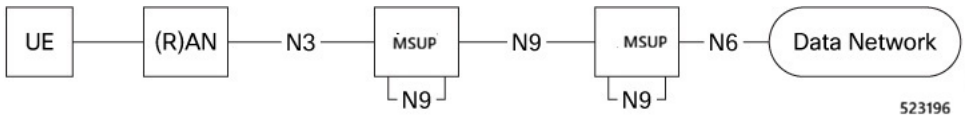
VPC-SI は、データプレーンフォワーダとして VPP を使用します。VPP は、MPLS ラベルを使用してサブスクライバ通信のカプセル化とカプセル化解除を行います。VPPは、個別のグラフノードとして MPLS スタックを含む複数のデータプレーン機能をサポートします。この機能は、さまざまな顧客 VRF を区別して、アドレッシングモデルと要件が異なる企業 APN をサポートします。

UPF は、VPP を使用した 5G デプロイメントの次のインターフェイスで MPLS カプセル化をサポートします。

- N6：N6 は、UPF とデータネットワーク（DN）間のインターフェイスです。
- N9：N9 インターフェイスは、2つの UPF を接続します。これは、中間 I-UPF（Visited）と UPF セッションアンカー（Home）の間のインターフェイスです。

次の図は、UPF での MPLS カプセル化に使用されるさまざまなインターフェイスを示しています。

図 *20 : MPLS* インターフェイス



UPF は、MPLS の次の機能をサポートしています。

- VPP MPLS スタックを使用して、MPLS ラベル付きパケットを送信します。
- VPP MPLS スタックを使用して、受信ラベル付き MPLS パケットを処理します。
- Label Distribution Protocol（LDP; ラベル配布プロトコル）として MP-BGP のみを使用します。
- VPPCTL CLI コマンドは、デバッグおよび Boxer の構成値との比較のために、VPP で FTN、FIB および ILM テーブルを表示します。

機能の仕組み

この項では、UPF での MPLS 機能の仕組みについて概説します。

VPP フォワーダーは、MPLS パケット処理とその MPLS スタックに関するすべての既存の機能をサポートします。VPP MPLS スタックは、適切な FTN（FEC から NHLFE）、Forwarding Information Base（FIB; 転送情報ベース）テーブル、および受信ラベルマップ（ILM）テーブルを使用して構成されます。エグレスは、正しい MPLS ヘッダーを使用して、MPLS パケットを生成します。また、これは、受信 MPLS パケットを処理し、受信ラベルに基づいて適切な VRF テーブルにきりかえます。

また、VPC-SI は RFC 4659（*BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*）で説明されているとおり、VPNv6 をサポートします。

N9 インターフェイスを使用して UPF をデプロイする

5G コア UPF は、N9 インターフェイス経由で 2 つの UPF を順番にデプロイできます。N9 インターフェイスは、中間 I-UPF と UPF セッションアンカー間の 2 つの UPF を接続します。ネットワーク全体で安定した IP アンカーを使用して完全なモビリティを提供するには、オペレータネットワークの構成に応じて、2 つの UPF が接続されます。

UPF 間のアップストリーム通信とダウンストリーム通信は、いずれも GTP-U パケットの形式です。N9 インターフェイス経由で MPLS をサポートするために、2 つの UPF の間に存在する L3 ルータは、BGP ルートとラベルを UPF にアドバタイズできます。

アップストリーム方向では、I-UPF は gNodeB から GTP-U パケットを受信し、接続先（アンカー）UPF に基づいて GTP-U ヘッダーの内容を変更します。IP ヘッダーのルックアップに基づいて MPLS カプセル化が行われ、GTP-U パケットがカプセル化されます。挿入する必要がある MPLS ラベルは、UPF 間の中間 L3 デバイスから BGP 経由で受信されます。アンカー UPF では、MPLS ヘッダーのカプセル化が解除され、IP パケットとして PDN に送信されます。

ダウンストリーム方向では、PDN から受信した IP パケットが GTP-U ヘッダーによってカプセル化された後、アンカー UPF で MPLS カプセル化が行われます。その後、この MPLS ヘッダーが I-UPF でカプセル化解除され、対応する GTP-U パケットが gNodeB に送信されます。

次のシナリオでは、UPF は N9 インターフェイスを VRF に移動し、VPNv4 または VPNv6 AF BGP ネイバーシップを確立します。

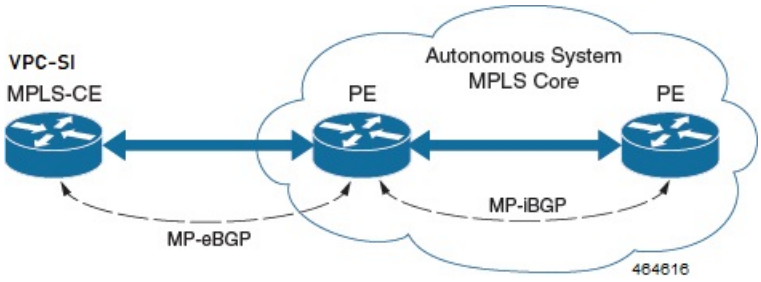
- N3 および N9 インターフェイスが同じ物理インターフェイスを共有している場合。
- N3 と N9 インターフェイスが分離されている場合。

PE に接続された MPLS-CE

VPC-SI は、プロバイダーエッジ（PE）ラベルエッジルータ（LER）に接続されている MPLS-CE（カスタマーエッジ）ネットワーク要素として機能し、その結果、RFC 4364 に従い MPLS コアに接続されます。

次の図は、MPLS-CE から PE への接続を示しています。

図 *21 : VPC-SI MPLS-CE* から *PE*



MPLS-CE は、独自の自律システム（AS）内の PE ルータのように機能します。MPLS-CE では、Virtual Routing and Forwarding（VRF）ルートが維持され、MP-eBGP（マルチプロトコル外部 BGP）セッションを介して、VPN ルート情報が PE と交換されます。

PE も VRF を使用して設定され、MP-iBGP（マルチプロトコル内部 BGP）接続を介して AS 内の他の PE と VPN ルートを交換し、MP-eBGP 接続を介して MPLS-CE を交換します。

EBGP 接続を使用すると、PE は、IBGP ピアから学習したルート内のネクストホップ IP アドレスとラベルを変更してから、MPLS-CE にアドバタイズできます。MPLS-CE は、ルートをアドバタイズして学習するために MP-eBGP だけを使用します。直接接続 EBGP ピアリングのため、Label Distribution Protocol（LDP）および Resource Reservation Protocol（RSVP）は必要ありません。MPLS-CE は、PE との間で（MP-eBGP 接続を介して学習された）単一のラベルをプッシュまたはポップします。

設定例

MPLS N6 構成

次に、UPF で N6 インターフェイスを使用して基本的な MPLS 機能を構成する例を示します。

```
context egress
    ip vrf MPN00001
      ip maximum-routes 100
    #exit
mpls bgp forwarding
router bgp 64455
      neighbor 172.31.35.29 remote-as 65200
      neighbor 172.31.35.29 timers keepalive-interval 60 holdtime-interval 300
      neighbor 172.31.35.29 update-source 172.31.35.4
      neighbor 172.31.35.29 fall-over bfd
      neighbor 172.31.35.29 srp-activated-soft-clear
       address-family ipv4
        redistribute connected
        redistribute static
      #exit
      address-family vpnv4
        neighbor 172.31.35.29 activate
        neighbor 172.31.35.29 send-community extended
      #exit
      address-family vpnv6
        neighbor 172.31.35.29 activate
        neighbor 172.31.35.29 send-community extended
```

```
    #exit
    address-family ipv6
      redistribute connected
      redistribute static
    #exit
     ip vrf MPN00001
      route-distinguisher 64455 11100001
      route-target both 64455 11100001
    #exit
    address-family ipv4 vrf MPN00001
      redistribute connected
    #exit
    address-family ipv6 vrf MPN00001
      redistribute connected
    #exit
  interface N6-11
    ip address 172.31.35.4 255.255.255.224
    ip mtu 1504
    bfd interval 999 min_rx 999 multiplier 3
 #exit
  interface N6-12
    ip address 172.31.35.35 255.255.255.224
    ip mtu 1504
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface loop_MPN00001 loopback
    ip vrf forwarding MPN00001
    ip address 2.2.4.2 255.255.255.255
  #exit
```

MPLS N9 構成

次に、UPF で N9 インターフェイスを使用して MPLS 機能を構成する例を示します。

```
context SAEGW
   ip vrf mpls-vrf-1
   #exit
   ip vrf mpls-vrf-2
   #exit
   mpls bgp forwarding
      bfd-protocol
      #exit
   ip prefix-list name up seq 15 permit 50.50.41.4/32
   ip prefix-list name up seq 20 permit 50.50.41.5/32
   ip prefix-list name up seq 25 permit 50.50.41.6/32
   ip prefix-list name up seq 40 permit 50.50.41.7/32
   ip prefix-list name n9-up1 seq 50 permit 60.60.41.5/32
   ip prefix-list name n9-up1 seq 55 permit 60.60.41.6/32
   route-map up_routes1 permit 10
      match ip address prefix-list n9-up1
      #exit
   route-map up_routes permit 10
      match ip address prefix-list up
      #exit
   ip vrf mpls-vrf-1
   route-distinguisher 61601 11100001
   route-target export 61601 11100001
   route-target import 61606 11100001
   route-target import 65200 11100001
   #exit
   address-family ipv4 vrf mpls-vrf-1
      redistribute connected
      redistribute static
      #exit
```

```
address-family ipv6 vrf mpls-vrf-1
   redistribute connected
   redistribute static
   #exit
ip vrf mpls-vrf-2
route-distinguisher 61601 11100002
route-target export 61601 11100002
route-target import 61606 11100002
route-target import 65200 11100002
#exit
address-family ipv4 vrf mpls-vrf-2
   redistribute connected
   redistribute static
   #exit
address-family ipv6 vrf mpls-vrf-2
   redistribute connected
   redistribute static
   #exit
 #exit
interface gn-mpls-n9-ingress
   ip address 172.31.40.5 255.255.255.224
   ip mtu 1504
   bfd interval 999 min_rx 999 multiplier 3
   #exit
interface n9-ingress-hupf loopback
   ip vrf forwarding mpls-vrf-1
   ip address 60.60.41.5 255.255.255.255
   #exit
user-plane-service user_plane_svc
   associate gtpu-service pgw-gtpu upf-ingress
   associate gtpu-service n9-ingress upf-ingress interface-type n9
   associate gtpu-service sgw-gtpu-ingress-phazr sgw-ingress
   associate gtpu-service sgw-gtpu-egress sgw-egress
   associate gtpu-service SxC cp-tunnel
   associate sx-service sx-svc
   associate fast-path service
   associate control-plane-group SAEGW
   associate userplane-load-control-profile LCP
   associate userplane-overload-control-profile OLCP
   #exit
```

VPN 関連 CLI コマンド

UPF では、VPN 関連の機能といくつかの CLI コマンドモードをサポートしています。次の表は、VPN 関連の機能の設定とモニタリングに関連するコマンドを示しています。

表 *64 : VPN* 関連の設定コマンド

CLI モード	コマンド	説明
BGP アドレスファミリ（IPv4/IPv6）構成モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGP アドレスファミリ（IPv4/IPv6）構成モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータ（ネイバー）にコミュニティ属性を送信します。

CLI モード	コマンド	説明
BGP アドレスファミリ（IPv4/IPv6）構成モード	**redistribute connected**	別のプロトコルからBGPへのルートをBGPネイバーとして再配布します。
BGPアドレスファミリ（VPNv4）構成モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGPアドレスファミリ（VPNv4）構成モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータに拡張コミュニティ属性を送信します。VPNでは、ルート識別子とルートターゲットはBGP拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つBGPルートをネイバーに送信します。
BGPアドレスファミリ（VRF）構成モード	**neighbor** *ip_address* **activate**	ピアルータとのルーティング情報の交換を有効にします。
BGPアドレスファミリ（VRF）構成モード	**neighbor** *ip_address* **send community { both | extended | standard }**	ピアルータに拡張コミュニティ属性を送信します。VPNでは、ルート識別子とルートターゲットはBGP拡張コミュニティでエンコードされます。このコマンドは、拡張コミュニティを持つBGPルートをネイバーに送信します。
BGPアドレスファミリ（VRF）構成モード	**redistribute connected**	別のプロトコルからBGPへのルートをBGPネイバーとして再配布します。
BGP 構成モード	**address-family { ipv4 vrf** *vrf_name* **| vpnv4 }**	IPv4 VRFのルーティング情報の交換を有効にします。アドレスファミリごとに異なるモードがあります。
BGP 構成モード	**address-family { ipv6 vrf** *vrf_name* **| vpnv6 }**	BGP で VPNv6 アドレスファミリと IPv6 VRF ルーティングを設定します。
BGP 構成モード	**ip vrf** *vrf_name*	BGP に VRF を追加し、VRF 構成モードにスイッチして、VRF の BGP 属性を設定できるようにします。

CLI モード	コマンド	説明
BGP IP VRF 構成モード	**route-distinguisher {** *as_value* **|** *ip_address* **}** *rd_value*	VRF の ルート識別子（RD）を割り当てます。RD 値は、VRF ごとにルータ上の一意の値にする必要があります。
BGP IP VRF 構成モード	**route-target { both | import | export } {** *as_value* **|** *ip_address* **}** *rd_value*	インポートおよびエクスポートのルートターゲット拡張コミュニティのリストを VRF に追加します。
コンテキスト構成モード	**ip pool** *pool_name addr_range* **vrf** *vrf_name* **[mpls-label input** *inlabel1* **output** *outlabel1 outlabel2* **]**	指定された VRF にプールを設定します。Next-Hop パラメータを使用して、このコマンドを指定します。*inlabel1* は、MPLS ラベルでこのプールに指定されたインバウンド通信を識別します。*outlabel1* および *outlabel2* は、このプールからサブスクライバに送信されるパケットに追加する MPLS ラベルを指定します。
コンテキスト構成モード	**ip vrf** *vrf_name*	VRF を作成し、VRF-ID を割り当てます。VRF がルータに作成されます。
コンテキスト構成モード	**ipv6 pool** *pool_name* **vrf** *vrf_name*	プールを VRF に関連付けます。 **注**：デフォルトでは、設定された ipv6 プールはグローバル ルーティング ドメインに関連付けられます。
コンテキスト構成モード	**mpls bgp forwarding**	MPLS のボーダー ゲートウェイ プロトコル（BGP）転送をグローバルに有効化します。

CLI モード	コマンド	説明
コンテキスト構成モード	**mpls exp** *value*	3 ビット MPLS EXP ヘッダーのゼロ値を使用して、デフォルトの動作をベストエフォートとして設定します。この値は、コンテキスト内のすべての VRF に適用されます。デフォルトの動作では、DSCP から EXP への明示的な設定がない場合に、モバイルサブスクライバのトラフィックの DSCP 値が EXP ヘッダーにコピーされます (**mpls map-dscp-exp dscp** *n* **exp** *m*コマンドを使用)。 **mpls exp** はデフォルトの動作を無効にし、EXP 値を設定された値に設定します。
コンテキスト構成モード	**mpls ip**	通常ルーティングされるパスに沿って IPv4 パケットの MPLS 転送がグローバルに行われるようにします。
コンテキスト構成モード	**radius change-authorize-nas-ip** *ip_address* **{ encrypted | key }** *value* **port** *port_num* **mpls input** *inlabel* **output** *outlabel1 outlabel2*	指定された MPLS ラベルを使用するように COA 通信を設定します。*inlabel* はインバウンド COA 通信を識別します。*outlabel1* および *outlabel2* は、COA 応答に追加する MPLS ラベルを指定します。 *outlabel1* は内部出力ラベル、 *outlabel2* は外部出力ラベルです。
イーサネットインターフェイス構成モード	**mpls ip**	このインターフェイスで IP パケットのダイナミック MPLS 転送を有効にします。
Exec モード	**clear ip bgp peer**	BGP セッションをクリアします。

表 *65 : VPN* 関連のモニタリングコマンド

CLI モード	コマンド	説明
Exec モードの show コマンド	**show ip bgp neighbors**	BGP ネイバーに関する情報を表示します。

CLI モード	コマンド	説明
Exec モードの show コマンド	**show ip bgp vpnv4 { all | route-distinguisher | vrf }**	すべての VPNv4 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	**show ip bgp vpnv6**	VPNv6 ルーティングテーブルの内容を表示します。
Exec モードの show コマンド	**show ip bgp vpnv6 { all | route-distinguisher | vrf }**	すべての VPNv6 ルーティングデータ、VRF またはルート識別子のルーティングデータを表示します。
Exec モードの show コマンド	**show ip fib table-id** *table_id*	FIB テーブルに関する情報を表示します。
Exec モードの show コマンド	**show ip pool**	設定された VRF を含むプールの詳細を表示します。
Exec モードの show コマンド	**show mpls cross-connect**	MPLS 相互接続情報を表示します。MPLS トンネルは、インターフェイスとラベルスイッチドパス（LSP）間で相互接続します。LSP は、MPLS トンネル経由で同じタイプの 2 つの遠隔インターフェイス回線を接続します。
Exec モードの show コマンド	**show mpls fib table** *table_id*	Forwarding Information Base（FIB; 転送情報ベース）テーブル情報を表示します。
Exec モードの show コマンド	**show mpls ftn [vrf** *vrf_name* **]**	MPLS FEC-to-NHLFE（FTN）テーブルの情報を表示します。
Exec モードの show コマンド	**show mpls ftn [vrf** *vrf_name* **]**	指定された VRF の MPLS FTN テーブルの内容を表示します。
Exec モードの show コマンド	**show mpls ilm [all | label** *label_value* **]**	MPLS の着信ラベルマップ（ILM）テーブルの情報を表示します。
Exec モードの show コマンド	**show mpls nexthop-label-forwarding-entry**	MPLS のネクストホップラベル転送エントリ（NHLFE）テーブルの情報を表示します。

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できるCLIコマンドに関する情報について説明します。

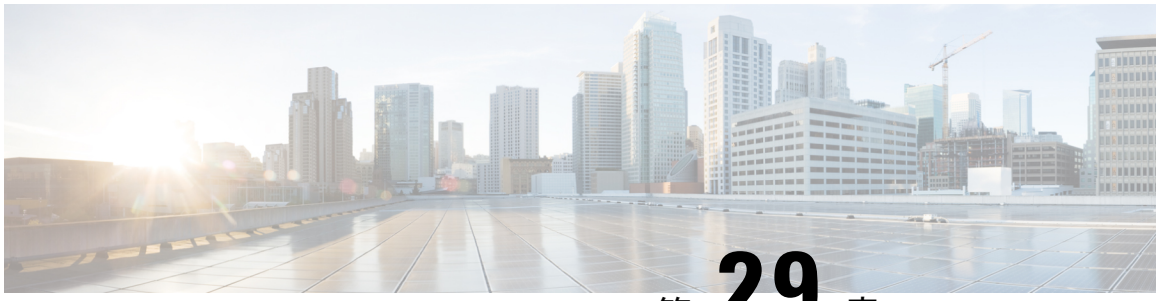
show コマンドと出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show mpls ftn vpp

このコマンドの出力には、VPPデータプレーンフォワーダで設定されているVPPデータプレーン値を表示する [vpp] フィールドが含まれます。このコマンドはデバッグ目的で使用します。

- vpp
  - all-vrf
  - summary
  - vrf



第 29 章

複数の cnSGW のサポート

- 機能の概要と変更履歴, on page 357
- 機能説明 （358 ページ）
- 機能の仕組み （358 ページ）
- 複数の SMF/cnSGWs を構成する （359 ページ）
- モニタリングおよびトラブルシューティング （359 ページ）

機能の概要と変更履歴

要約データ

Table 66: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

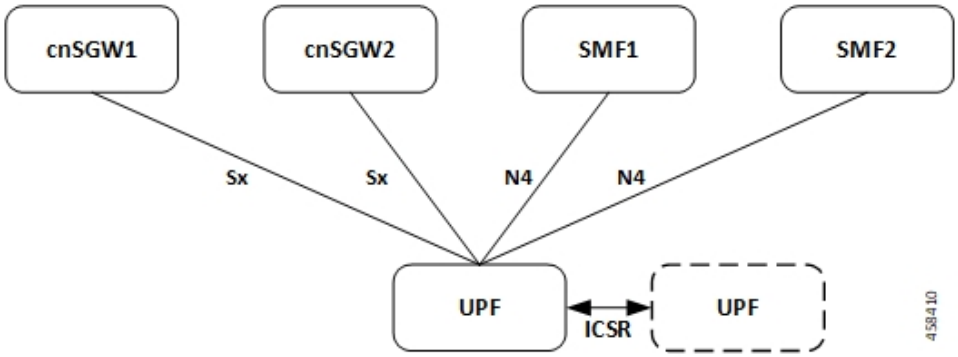
改訂の詳細	リリース
最初の導入。	2021.02.0

機能説明

複数 SMF/cnSGW サポート機能により、1 つの UPF で、cnSGW およびそれぞれに対応する SMF と複数の N4/Sx インターフェイスを確立できます。複数の SMF と cnSGW の組み合わせを 1 つの UPF に統合することで、リソースを適切に使用できます。

アーキテクチャ

次の図は、複数の cnSGWs/SMF のアーキテクチャを示しています。



他の機能との関係性

複数の cnSGW サポート機能は、複数の *N4/Sx* インターフェイス機能に関連しています。

機能の仕組み

複数の cnSGW 機能の内容は、次のとおりです。

- 単一の UPF には、SMF/cnSGW との複数の N4/Sx インターフェイスのアソシエーションがあります。
- 個々の SMF ごとの UPF での構成のスライシングはありません。
- 累積的に、最大 4 つのピア（cnSGW/SMF または必要に応じた個々の cnSGW/SMF の組み合わせ）が 1 つの UPF に接続されます。
- 個々の N4/Sx アソシエーションのリリースは、影響を受ける SMF ピアのセッションを消去します。
- UPF 冗長性はシームレスに機能します。
- UPF とペアになっているすべての cnSGW は、単一のユーザープレーンサービスに関連付けられます。

複数の SMF/cnSGWs を構成する

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

UPF での複数の SMF/cnSGW を構成する

次の CLI コマンドを使用して、コントロールプレーングループ構成モードで、複数のピアノ―度を追加して、UPF に複数の SMF/cnSGWs を構成します。

```
configure
  user-plane-service service_name
    associate control-plane-group group_name
  control-plane-group group_name
    peer-node-id ipv4-address ipv4_address interface n4
    peer-node-id ipv4-address ipv4_address interface n4
    peer-node-id ipv4-address ipv4_address
    peer-node-id ipv4-address ipv4_address
    end
```

モニタリングおよびトラブルシューティング

この項では、複数 cnSGW 機能のモニタリングと障害対応について説明します。

show コマンドと出力

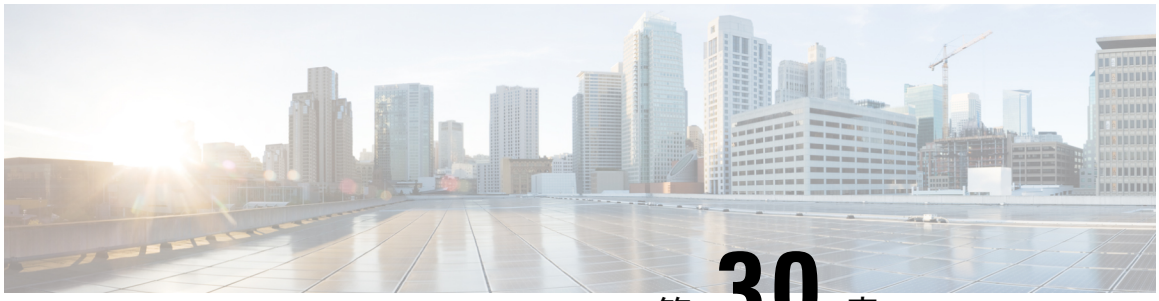
この項では、この機能をサポートするために使用可能な show コマンドについて説明します。

show subscribers user-plane-only full all

この CLI コマンドの出力は、対応するコントロール プレーン アドレスを表示するように拡張されています。

show sx peers

この CLI コマンドの出力は、ピア ID とそれに対応するセッションの数を表示するように拡張されています。



第 30 章

複数の N4/Sx インターフェイス

- 機能の概要と変更履歴, on page 361
- 機能説明 （362 ページ）
- 機能の仕組み （363 ページ）
- 複数の N4/Sx インターフェイスを構成する （363 ページ）
- モニタリングおよびトラブルシューティング （364 ページ）

機能の概要と変更履歴

要約データ

Table 67: 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
UPF は、次の機能をサポートしています。: • 任意の数のコントロールプレーン NF を持つ複数の N4/Sx インターフェイス • 18 の Nx/Sx ピアノードの最大構成	2023.04.0
最初の導入。	2021.01.0

機能説明

表 *68 :* 機能の履歴

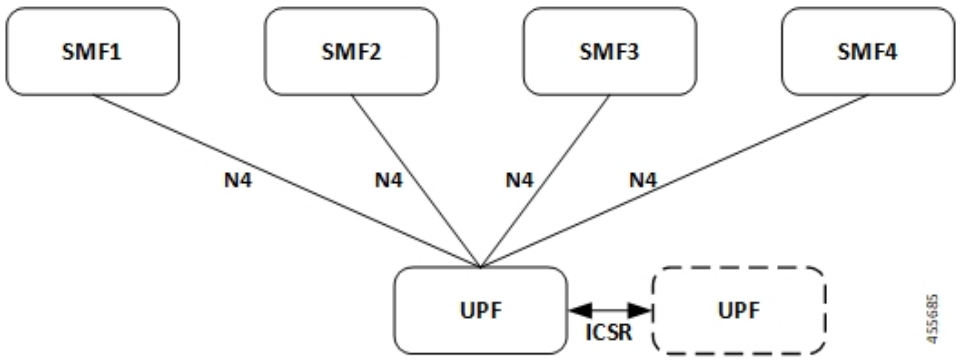
機能名	リリース情報	説明
複数の N4/Sx インターフェイスのサポート	2023.04	単一の UPF で、任意の数のコントロール プレーン ネットワーク機能（SMF、cnSGWc、SAEGW-C、PGW-C、SGW-C など）を持つ複数の N4 または Sx インターフェイスを確立できます。このリリースでは、サポートされる N4/Sx ピアノードの最大数が 16 ノードから 18 ノードに増加しました。

複数の N4/Sx インターフェイス機能により、単一の UPF で任意の数のコントロールプレーン NF に対して複数の N4 または Sx インターフェイスを確立できます。コントロールプレーン NF には、SMF、SAEGW-C、PGW-C、SGW-C、および cnSGWc が含まれます。

複数のコントロールプレーンノードを単一の UPF と統合することで、リソースの使用率が最適化されます。UPF は、コントロール プレーン グループごとに 18 の N4 または Sx ピアノードの最大構成をサポートします。

アーキテクチャ

次の図は、単一の UPF を持つ複数の N4 インターフェイスのアーキテクチャを示しています。



機能の仕組み

複数の N4/Sx 機能の機能は次のとおりです。

- UPF の ECS/ACS 構成は、すべての個別のコントロールプレーン固有の構成の集まりです。

  例：

  SMF1 には、rulebase *RB1* があり、*RB2* がない

  SMF2 には、rulebase *RB2* があり、*RB1* がない

  UPF には、*RB1* と *RB2* からのセッションに対応するために、*RB1* と *RB2* の両方の rulebase があります。

- 個々の SMF ごとの UPF での構成のスライシングはありません。
- 最大 4 つの SMF ピアが単一の UPF に接続されます。
- 複数の SMF からの重複 IP プールは、VRF ID に基づいて分離されます。
- 個々の N4 アソシエーションの解除は、影響を受ける SMF ピアのセッションを消去します。
- UPF 冗長性はシームレスに機能します。
- 異なる SMF 構成と競合中は、構成された CLI のシーケンスでインストールされ、UPF では解決されません。

複数の N4/Sx インターフェイスを構成する

ここでは、この機能をサポートするために使用可能な CLI コマンドについて説明します。

複数のピアノードを構成する

UPF で複数のピアノードを設定するには、次の構成例を使用します。

```
configure
  user-plane-service service_name
    associate control-plane-group group_name
  control-plane-group group_name
    peer-node-id ipv4-address ipv4_address interface n4
    peer-node-id ipv4-address ipv4_address interface n4
    peer-node-id ipv4-address ipv4_address
    . . .
    . . .
    . . .
    end
```

注：

- **peer-node-id ipv4-address** *ipv4_address*：ピアノードの IPv4 アドレスを指定します。
- **interface n4**：N4 インターフェイスを特定します。
- コントロール プレーン グループごとに最大 18 のピアノードを設定できます。

  上限である 18 のピアノードを超えると、次のエラー メッセージが表示されます。

  エラー：コントロール プレーン グループ ノードの最大数制限を超えました。

モニタリングおよびトラブルシューティング

この項では、複数 N4/Sx インターフェイス機能のモニタリングと障害対応について説明します。

show コマンドと出力

この項では、この機能をサポートするために使用可能な show コマンドについて説明します。

show ip chunks

この CLI コマンドの出力は、Gi コンテキストの複数の SMF から UPF にプッシュされた IP プールを表示するように拡張されています。

show ipv6 chunks

この CLI コマンドの出力は、Gi コンテキストの複数の SMF から UPF にプッシュされた IPv6 プールを表示するように拡張されています。

show subscribers user-plane-only full all

この CLI コマンドの出力は、対応するコントロール プレーン アドレスを表示するように拡張されています。

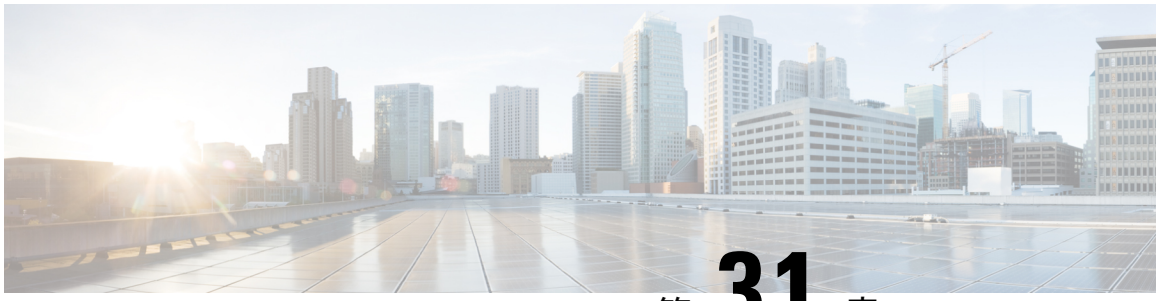
show sx peers

この CLI コマンドの出力は、ピア ID とそれに対応するセッションの数を表示するように拡張されています。

show user-plane-service statistics peer-address <address>

この CLI コマンドの出力は、SMF のピアごとの統計を表示するように拡張されています。

show user-plane-service statistics peer-address <address>



第 31 章

ネクストホップ転送サポート

- 更新履歴 （367 ページ）
- 機能説明 （367 ページ）
- 機能の仕組み （367 ページ）
- ネクストホップ転送サポートを構成する （374 ページ）
- ネクストホップ転送を使用した VLAN セグメンテーション （378 ページ）
- モニタリングおよびトラブルシューティング （383 ページ）

更新履歴

表 *69*：マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.0

機能説明

ネクストホップ転送は、パケットと隣接するルータまたはデバイスに転送するプロセスです。ネクストホップルータは、接続先パス内のパケットに次に最も近い IP または 最適な IP です。

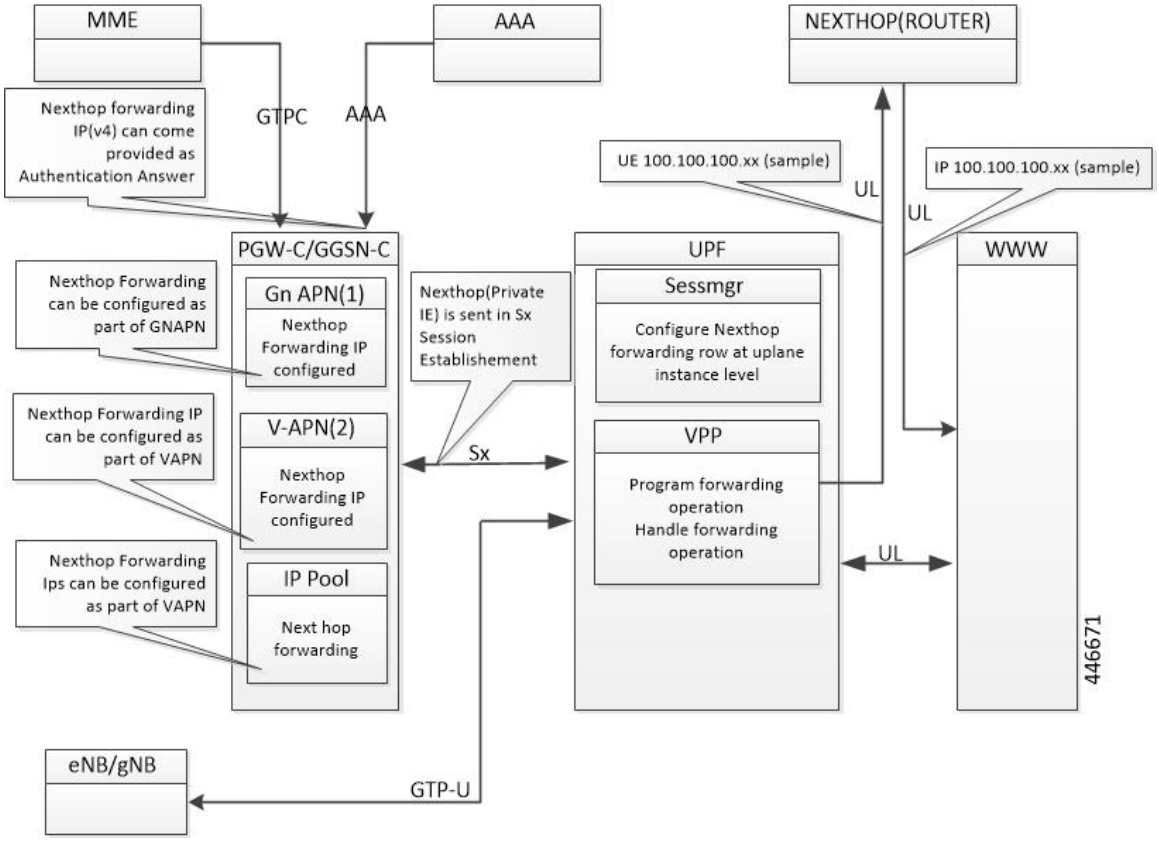
アップリンク方向では、UE と GI IP が異なるサブネットにある可能性があります。UPF のルーティングパスは、それに応じてアップリンクパケットを転送できるように定義されます。

機能の仕組み

アーキテクチャ

次の図は、ネクストホップ転送機能の概要を示しています。

図 *22 :* ネクストホップ転送



DNN プロファイルまたは IPAM プロファイルの SMF でネクストホップ IP アドレスを構成できます。PDU Establishment 中、SMF は、PFCP Session Establishment 要求の NEXT HOP IP private IE の N4 インターフェイス経由で IPv4/IPv6 アドレスをリレーします。

Charging-Action を使用して、UPF でネクストホップ IP アドレスを構成することもできます。

（注） ネクストホップアドレスが SMF と UPF の両方の Charging-Action によって提供されている場合、UPF Charging-Action ネクストホップアドレスが優先されます。

設定の優先順位

シリアル番号	設定	優先度
1.	UPF（課金アクション）	1
2.	DNN プロファイル	2
3.	IP プール	3

構成の使用例

ケース	IP タイプ	DNN	IPプール	UPF（課金アクション）	ネクストホップ IP の選択
DNN でのみ指定されるネクストホップ	IPv4	209.165.201.18	未設定	未設定	ネクストホップアドレスは、DNN: IPv4: 209.165.201.18 IPv6: 8001::10 から選択されます。
	IPv6	8001::10	未設定		
IP プールでのみ指定されるネクストホップ	IPv4	未設定	209.165.201.19	未設定	ネクストホップアドレスは、IP Pool: IPv4: 209.165.201.19 IPv6: 8001::10 から選択されます。
	IPv6	未設定	8001::10		
DNN および IP プールで設定された IPv4 および IPv6	IPv4	209.165.201.18	209.165.201.19	未設定	ネクストホップアドレスは、DNN: IPv4: 209.165.201.18 IPv6: 9001::3 から選択されます。
	IPv6	9001::3	8001::10		
DNN で構成された IPv6 および IP プールの IPv4	IPv4	未設定	209.165.201.19	未設定	ネクストホップ IPv4 は、IP pool: 209.165.201.19 から選択されます。 DNN : 8001::10 から選択されたネクストホップ IPv6
	IPv6	8001::10	未設定		
DNN で構成された IPv6、IP プールの IPv4、UPF Charging Action の IPv4	IPv4	209.165.201.18	209.165.201.19	209.165201.20	ネクストホップアドレスは、UPF (CA): 209.165.201.20 から選択されます
	IPv6	8001::10	未設定	未設定	
DNN で構成された IPv6、IP プールの IPv4、UPF Charging Action の IPv6	IPv4	209.165.201.18	209.165.201.19	未設定	ネクストホップアドレスは、UPF(CA) : 9001::10 から選択されます
	IPv6	8001::10	未設定	9001::10	

インターフェイス

次の Private IEs が Sx/N4 Session Establishment メッセージに導入されます。

238	PFCP_IE_NEXTHOP	PFCP_IE_NEXTHOP							Sx/N4 Session Establishment 要求	Private IE：UPF：ネクストホップ転送サポート：IPv4 /IPv6 アドレス
		ビット								
		オクテット	7	6	5	4	3	2	1	
		1 ～ 2	タイプ = 238（10 進数）							
		3 ～ 4	長さ = n							
		5 ～ 10	PFCP_IE_NEXTHOP_ID							
		11 ～ 14	PFCP_IE_NEXTHOP_IP							

<table>
<tr><td rowspan="9">2
3
9</td><td rowspan="9">PFCP
_IE_
NEXTHOP
_ID</td><td colspan="8">PFCP_IE_NEXTHOP_ID</td><td>1 に送信します。Sx Session Establishment 要求の Create FAR IE 内</td><td rowspan="9">Private IE：UPF：ネクストホップ転送サポート：IPv4 /IPv6 アドレス</td><td rowspan="9"></td></tr>
<tr><td colspan="8">ビット</td><td>2 に送信します。Sx/N4 Session Establishment 要求の PFCP_IE_NEXTHOP IE 内</td></tr>
<tr><td>オクテット</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td rowspan="6">Sx/N4 Session Establishment 要求の PFCP_IE_NEXTHOP</td></tr>
<tr><td>1 ～ 2</td><td colspan="7">タイプ = 239（10 進数）</td></tr>
<tr><td>3 ～ 4</td><td colspan="7">長さ = 5</td></tr>
<tr><td>5 ～ 10</td><td colspan="7"></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="7"></td></tr>
</table>

240	PFCP_IE_NEXTHOP_IP	PFCP_IE_NEXTHOP_IP								Sx/N4 Session Establishment 要求の PFCP_IE_NEXTHOP	Private IE：UPF：ネクストホップ転送サポート：IPv4/IPv6 アドレス
		ビット									
		オクテット	7	6	5	4	3	2	1		
		1 ～ 2	タイプ = 240（10 進数）								
		3 ～ 4	長さ = n								
		5	予備					V4	V6		
		m ～ m+3	IPv4 アドレス								
		p ～ p+15	IPv6 アドレス								

次に、SMF が、ネクストホップ IP を UPF にリレーする SX_SESSION_ESTABLISHMENT_REQUEST の出力例を示します。

```
CREATE FAR:
  Type: 3
  Value:
   FAR ID:
     Type: 108
     Value: 0x80000002
   APPLY ACTION:
     Type: 44
     Value:
       DROP: 0
       FORW: 1
       BUFF: 0
       NOCP: 0
       DUPL: 0
   FORWARDING PARAMETERS:
     Type: 4
     Value:
       DESTINATION INTERFACE:
         Type: 42
         Value: CORE (1)
       PDN INSTANCE:
          Type: 22
          Value: intershat
          INNER PACKET MARKING:
            Type: 220
            TOS/TRAFFIC CLASS: 0xB8 0xFC
    NextHop ID:
       Value: 0x0001
```

```
CREATE TRAFFIC ENDPOINT:
    Type: 127  Length: 20
    Value:
    Traffic Endpoint ID:
        Type: 131  Length: 1
        Value: 0x0004
        Hex: 0083 0001 04
        Local F-TEID:
            Type: 21  Length: 1
            Value:
                CH: 1
                IPv4: 0
                IPv6: 0
                CHID: 0
            Hex: 0015 0001 04
        Bearer Info:
            Type: 225  Length: 6
            QCI: 5
            ARP: 84
            Charging ID: 5592407
            Hex: 00E1 0006 0554 0055 5557
    Hex: 007F 0014 0083 0001 0400 1500 0104 00E1
                 0006 0554 0055 5557
 NEXT HOP IP:
     Type: 237  Length: 14
     Value:
     NextHop ID:
         Type: 238  Length: 1
         Value: 0x0001
         Hex: 00EE 0001 01
     IP ADDR:
         Type: 239  Length: 5
         Value:
             IPv4: 1
             IPv6: 0
             IPv4: 209.165.202.150
             IPv6:
             Hex: 00EF 0005 020F 0F0F 0F
     Hex: 00ED 000E 00EE 0001 0100 EF00 0502 0F0F
          0F0F
```

制限事項

この機能には次の既知の制限事項があります。

- AAA を介したネクストホップ転送の構成はサポートされていません。
- RADIUS および Diameter（PCF からのリダイレクト情報）インターフェイス経由で送信されるネクストホップアドレスは、認定されていません。
- DNN プロファイルと IPAM でネクストホップ転送を構成すると、ネクストホップは Sx Establishment でのみ表示され、Sx Session Modification 要求の Create FAR IE では表示されません。

ネクストホップ転送サポートを構成する

課金アクションを使用してネクストホップ転送を構成する

UPFで、次のCLIコマンドを使用して、課金アクションを使用してネクストホップ転送を構成します。

```
configure
  active-charging service service_name
    charging-action charging_action_name
      nexthop-forwarding-address ipv4_address/ipv6_address
```

注：

- **charging-action***charge_action_name*：課金アクションの名前を指定します。*charge_action_name*は、1～63文字の英数字の文字列である必要があります。また、句読点を含めることができます。各家禽アクションには一意の名前が必要です。
- **nexthop-forwarding-address***ipv4v6_address* | *ipv4_address* | *ipv6_address* ：このAPNのネクストホップ転送アドレスを構成します。

DNNプロファイル経由でネクストホップ転送を構成する

SMFで、次のCLIコマンドを使用して、DNNプロファイル経由でネクストホップ転送を構成します。

```
configure
  profile dnn intershat
       nexthop-forwarding-address { ipv4 ipv4_address| ipv6  ipv6_address
}
       end
```

注：

- **nexthop-forwarding-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**：ネクストホップ転送アドレスを構成します。
  - *ipv4_address*：IPv4アドレスを構成します。
  - *ipv6_address*：IPv4アドレスを構成します（コロン区切りの16進数表記をサポート）。

IPv4アドレスのIPAMプロファイルによるIPプールでのネクストホップ転送の構成

SMFで、次のCLIコマンドを使用して、IPv4アドレスのIPAMプロファイル経由でIPプールにネクストホップ転送を構成します。

```
configure
  ipam
    instance instance_id
      address-pool pool_name
        ipv4
        address-ranges
          address-range start_ipv4_address end_ipv4_address
nexthop-forwarding-address nexthop_forwarding_address
          prefix-range prefix_value length  prefix_length
nexthop-forwarding-address nexthop_forwarding_address
          split-size per-cache number_of_addresses
          split-size per-dp number_of_addresses
          commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv4**：プールの IPv4 モードを開始します。
- **address-ranges**：IPv4 アドレス範囲の開始アドレスを指定します。ネクスト ホップ転送アドレスを使用して IPv4 アドレス範囲とプレフィックス範囲のアドレスを入力します。
  - **address-range** *start_ipv4_address end_ipv4_address* **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスで IPv4 アドレス範囲の開始アドレスと終了アドレスを指定します。
  - **prefix-range** *prefix_value* **length** *prefix_length*：IPv4 アドレス内のプレフィックス値と長さを指定します。
  - **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスを指定します。
- **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で指定します。IPAM サーバーは、この構成を使用します。 *number_of_addresses* は 、2 ～ 262144 の範囲の整数である必要があります。
- **split-size-per-dp** *number_of_addresses*：データ プレーンに割り当てるチャンクあたりの IPv4 アドレスの数を指定します。2 の累乗で を指定します。IPAM キャッシュは、この構成を使用します。

  number_of_addresses は 、2 ～ 262144 の範囲の整数である必要があります。

IPv6 アドレスの IPAM プロファイル経由で IP プールのネクストホップ転送を構成する

IPv6 プールおよびアドレス範囲のネクスト ホップ構成で IPv6 アドレスを構成するには、次の構成例を使用します。

```
configure
  ipam
    instance instance_id
      address-pool pool_name
        ipv6
        address-ranges
          address-range start_ipv6_address end_ipv6_address
nexthop-forwarding-address nexthop_forwarding_address
          prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
            split-size per-cache number_of_addresses
            split-size per-dp number_of_addresses
            exit
            prefix-range prefix_value length prefix_length
nexthop-forwarding-address nexthop_forwarding_address
          commit
```

注：

- **address-pool** *pool_name*：アドレス プールの名前を指定します。 *pool_name* は 文字列である必要があります。
- **ipv6**：プールの IPv6 モードを開始します。
- **address-ranges**：ネクストホップ転送アドレスを使用して、IPv6アドレス範囲とプレフィックス範囲のアドレスを指定します。

（注） IANA IPv6 構成は BNG により使用されます。

  - **address-range** *start_ipv6_address end_ipv6_address* ：IPv6 アドレス範囲の開始アドレスと終了アドレスを指定します。
  - **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクストホップ転送アドレスを指定します。
  - **prefix-range** *prefix_value* **length** *prefix_length*：IPv6アドレス内のプレフィックス値と長さを指定します。
  - **nexthop-forwarding-address** *nexthop_forwarding_address*：ネクスト ホップ転送アドレスを指定します。

- **prefix-ranges** ：IPv6 アドレスのプレフィックス範囲を指定します。

（注） SMF は、IAPD IPv6 構成のみをサポートしています。

  - **split-size per-cache** *number_of_addresses*：IPAM キャッシュを割り当てるチャンクあたりの IPv6 アドレスの数を指定します。

- **split-size-per-dp** *number_of_addresses*：データプレーン割り当て向けにチャンクごとのIPv6アドレスの数を指定します。
- **prefix-range** *prefix_value* **length** *prefix_lengthnexthop_forwardng_address* **nexthop-forwarding-address** ：ネクストホップ転送アドレスでIPv6アドレス内のプレフィックス値と長さを指定します。

設定例

次に、IPv4アドレスのIPAMプロファイル経由でIPプールでネクストホップ転送を構成する構成例を示します。

```
config
   ipam
      instance 1
         address-pool p1
                  ipv4
                     split-size per-cache 1024
                     split-size per-dp 256
                     end
```

次に、IPv6アドレスのIPAMプロファイル経由でIPプールでネクストホップ転送を構成する構成例を示します。

```
ipam
 instance 1
  address-pool ISE-Pool1
   vrf-name ISP
   tags
    dnn cisco_vlan400.com
   exit
   ipv6
    address-ranges
      address-range 1000::1 1000::ffff nexthop-forwarding-address :9001::3
      prefix-range 2607:fc20:1010:: length 98 nexthop-forwarding-address :9001::3
    prefix-ranges
       split-size
           per-cache 32768
           per-dp    32768
       exit
       prefix-range 2607:fc20:1010:: length 44 nexthop-forwarding-address :9001::3
   exit
  exit
```

ネクストホップ転送を使用した VLAN セグメンテーション

表 *70 :* 機能の履歴

機能名	リリース情報	説明
ネクストホップ転送を使用した通信の VLAN セグメンテーション	2024.01	UPF では、ネクストホップ転送を使用して VLAN セグメンテーションを行うことができます。UPF は、接続先 IP にパケットを送信するのではなく、接続先ホップ IP が最も到達可能な場所から VLAN にパケットを送信します。 **デフォルト設定**：無効 - 有効にするには構成が必要です。

機能説明

UPF は、仮想 LAN（VLAN）を使用した企業通信のセグメント化をサポートしています。VLAN は、1 つの物理 LAN セグメントをさらに小さな仮想ネットワークに分割し、ポートのグループ同士を、物理的に異なるセグメント上にあるかのように分離できるようにします。VLAN セグメンテーションでは、異なるクラスに属する UE は、通信分離のために異なる VLAN に割り当てられます。

VLAN セグメンテーションは、次の 2 つのメソッドを使用して実現できます。

1. Next Hop Forwarding
2. 仮想ルーティングおよび転送

ネクストホップ転送を使用する VLAN セグメンテーションでは、IP プールが VLAN タグにマッピングされます。このマッピングは、SMF で行われます。IP プールは、N6 インターフェイスのネクストホップ転送アドレスに関連付けられます。このアドレスは、コントロールセンターで構成されている、IP プールに関連付けられた VLAN 経由で到達可能です。

（注） この機能は、1 ラックユニットと 3 ラックユニットの両方のアーキテクチャでサポートされ、N6 インターフェイスで最大 16 の VLAN をサポートできます。

機能の仕組み

ネクストホップ転送を使用して VLAN セグメンテーションを実現するには、次のプロセスに従います。

- SMF は、ネクストホップ転送アドレスが設定されている N4 Session Establishment 要求を UPF に送信します。
- UPF は、ネクストホップ転送アドレスをセッションに関連付けます。このアソシエーションにより、UPF のセッション管理レイヤは、そのセッションに属するアップリンクパケットのネクストホップ転送を実行するように VPP をプログラムします。
- UPF のセッションマネージャは、適切なネクストホップ IP でのネクストホップ転送操作を行う VPP Fastpath コンジットでアップリンクストリームを作成します。したがって、UPF は、パケットを転送するために実際の IP 接続先ルートを調べません。代わりに、UE の IP アドレスをネクストホップ IP と関連付け、ネクストホップ IP が到達可能な VLAN のアップリンクパケットを転送します。

ネクストホップ転送を使用して VLAN セグメンテーションを有効にする

ネクストホップ転送を使用して UPF で VLAN セグメンテーションを構成するには、次の構成を使用します。

```
config
  port ethernet slot/port
    no shutdown
    vlan vlan_tag_ID
    no shutdown
    bind interface interface_name context_name
    end
    context context_name
      { ip | ipv6 } address address subnetmask [ secondary ]
      end
```

注：

- **port ethernet** *slot*/*port*：VLAN タグが含まれるイーサネットポートまたはスロット。
- **no shutdown**：指定した VLAN で通信を有効または無効にします。
- **vlan** *vlan_tag_ID*：VLAN 構成モードに入ります。
- **no shutdown**：現在の VLAN で通信を有効または無効にします。
- **bind interface** *interface_name context_name*：VLAN サービスをサポートするために、仮想インターフェイスとコンテキストをバインドします。
- **context** *context_name*：インターフェイスを作成するコンテキストを構成します。

- **{ ip | ipv6 } address** *address subnetmask* **[secondary]** ：IP プールと構成した VLAN をマッピングします。 **[secondary]** キーワードは、複数の IP アドレスをインターフェイスに割り当てます。

設定例

UPF でネクストホップ転送を使用して VLAN セグメンテーションを有効にするには、次の構成例を使用します。

```
config
     port ethernet 1/10
       no shutdown
       vlan 400
         no shutdown
         bind interface N6_interface1 ISP
       #exit
       vlan 401
         no shutdown
         bind interface N6_interface2 ISP
       #exit

context ISP
 interface N6_interface1
      ip address 209.165.200.225 209.165.200.254
      ip address 209.165.201.1 209.165.200.254 secondary
      ipv6 address 2001:DB8::1/32 secondary

interface N6_interface2
      ip address 209.165.202.129 209.165.200.254
      ip address 209.165.201.30 209.165.200.254 secondary
      ipv6 address 2001:DB8:1::1/32 secondary
```

UPF でネットワーク到達可能性サーバーを構成する

パケットをネクストホップ IP に転送するには、UPF が送信元ベースのルーティングを実行し、ネクストホップに ARP リクエストを送信してネクストホップ IP の MAC アドレスも学習する必要があります。

ネットワーク到達可能性を設定すると、UPF は ping パケットを接続先に送信してネットワークデバイスをテストできます。

IPv4 アドレスの UPF のネットワーク到達可能性または障害をテストおよび検出するには、次の構成を使用します。

```
config
   context context_name
  nw-reachability server server_name  [ remote-addr  ip_addr  ]  [ local-addr
 ip_addr  ]
```

注：

- **nw-reachability server** *server_name* **[remote-addr** *ip_addr* **] [local-addr** *ip_addr* **]** ：この CLI は、reachability-detect サーバーを追加または削除します。**[local-addr** *ip_addr* は、パ

ケットが送信される送信元 IP を指定し、I**[remote-addr** *p_addr* は、接続先 IP を指定して、ping パケットを送信し、ネットワーク障害や到達可能性を検出します。

（注） UPF は、コンテキストごとの VPN ネットワーク到達可能性構成において、VPN ごとに最大 2000 の IPv4 プールおよび 256 の IPv6 プールをサポートします。

IPv6 アドレスの UPF のネットワーク到達可能性または障害をテストおよび検出するには、次の構成を使用します。

```
config
   context context_name
      ip access-list acl_name
      { deny | permit } [ log ] any
      exit
  nw-reachability server server_name [ remote-addr ip_addr ] [ local-addr
 ip_addr ]
   end if_name
   interface if_name
      ipv6 address ipv6_address ipv6_mask
         bfd interval interval_value min_rx rx_value multiplier multiplier_value
         exit
      port ethernet slot/port
         no shutdown
         vlan vlan_tag_ID
         no shutdown
         bind interface interface_name context_name
         end
```

注：

- **ip access-list** *acl_name*：**ip access-list** は、サブスクライバ通信の種類を指定し、方向（アップリンク、ダウンリンクまたは両方）通信をリダイレクトします。**ip access-list** は、サブスクライバ認証が実行されるコンテキストで指定する必要があります。
- **{ deny | permit } [log] any**：一致した場合に対応するパケットを破棄または許可するルールを示します。**[log]** は、ログに記録されるフィルタと一致するすべてのパッケージを示します。

  any は、送信元および/または接続先に関係なく、すべてのパケットがフィルタに一致することを示します。
- **interface** *if_name*：BFD を有効にするインターフェイスを指定します。
- **ipv6 address** *ipv6_address ipv6_mask*：静的ルートの構成に向けて IPv6 ドレスを指定します。
- **bfd interval** *interval_value* **min_rx** *rx_value* **multiplier** *multiplier_value*：**bfd interval** *interval_value* は、制御パケットの送信間隔を、50 ～ 10000 の整数値（ミリ秒）で指定します。**min_rx** *rx_value* は、制御パケットの最小受信間隔を、50 ～ 10000 の整数値（ミリ秒）で指定しま

す。**multiplier** *multiplier_value* は、ホールドダウン時間の計算に使用する値を、3 ～ 50 の整数値で指定します。

設定例

次に、ネクストホップ IP の MAC アドレスを学習するためのネットワーク到達可能性の構成例を示します。

```
(config-ctx)# nw-reachability server test remote-addr 209.165.200.225 local-addr
209.165.202.129
```

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

モニタリングのサポート

この項では、機能レベルのモニタリングのサポート情報について説明します。

show ip arp vpp

この show コマンドは、ネクストホップ IP アドレスに関連付けられた正しい MAC アドレスを表示します。

```
# show ip arp vpp
Wednesday November 22 13:03:40 EST 2023
    Time        IP      Flags     Ethernet              Interface
slot/port
3460.6250  10.1.105.254  D   00:fd:22:53:01:81  VirtualFunctionEthernet0/6/0.1105   1/10
3446.2276  10.2.105.254  D   00:fd:22:52:ff:5f  VirtualFunctionEthernet0/7/0.2105   1/11
```

show configuration context

構成された ALC リストを確認するには、次の show コマンドを使用します。

```
[ISP]Hertz-UPF-A# show configuration context  ISP
  context ISP
    ip access-list ecs-v4.acl
      permit any
    #exit
    nw-reachability server NHFWDVlan1 remote-addr 192.11.55.100 local-addr 192.11.55.51
   nw-reachability server NHFWDVlan1_ipv6 remote-addr 2001:4888:192:1155::100 local-addr
 2001:4888:192:1155::51
    #exit
  interface isp-1155
      ip address 192.11.55.51 255.255.255.0
      ipv6 address 2001:4888:192:1155::51/64 secondary
      bfd interval 50 min_rx 50 multiplier 3

  port ethernet 1/10
    no shutdown
    vlan 1155
      no shutdown
      bind interface isp-1155 ISP
    #exit
```

show nw-reachability server

この show コマンドは、両方のネクストホップ IP（remote-addr）の到達可能性状態を表示します。ネクストホップ IP が到達可能な場合は、**[アップ（Up）]** と表示されます。

```
[ISP]upf01#  show nw-reachability server all
 Server               remote-addr             local-addr              Vrf           state
 ---------------     ---------------    --------------- ---------------- ---------------

 vlan2645             10.28.45.1              10.28.45.2              n/a             Up
 vlan2646             10.28.46.1              10.28.46.2              n/a             Up
NHFWDVlan1_ipv6  2001:4888:192:1155::100 2001:4888:192:1155::51      n/a             Up

Total Network Reachability Servers: 3 Up: 3
```

show ipv6 interface summary

この show コマンドは、IPv6 設定を使用した VLAN 設定のインターフェイスの概要を表示します。

```
[ISP]Hertz-UPF-A# show ipv6 interface summary
Interface Name               Address/Mask               Port               Status
====================    ========================    ==================    ============
   =========
isp                      2001:4888:192:1153::51/64      1/10 vlan 1153          UP
    [sec]
isp-1155                 2001:4888:192:1155::51/64      1/10 vlan 1155          UP
    [sec]
```

モニタリングおよびトラブルシューティング

ここでは、機能のモニタリングと障害対応に使用できる CLI コマンドについて説明します。

show コマンドと出力

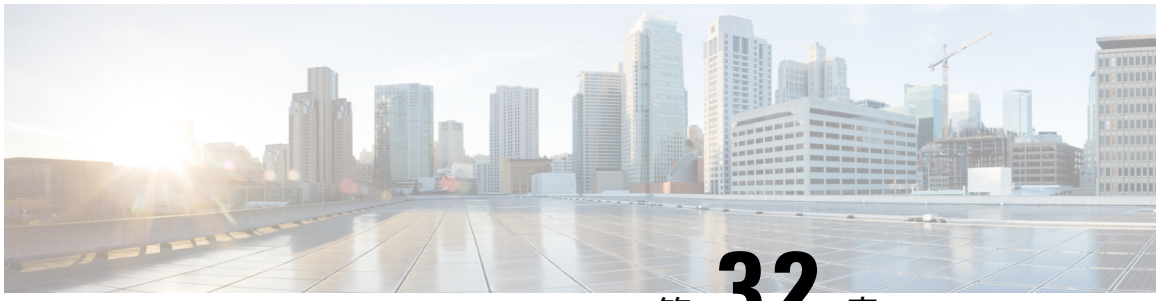
ここでは、この機能をサポートする show コマンドとその出力について説明します。

show subscriber user-plane-only full all

この show コマンドの出力範囲が拡張され、この機能をサポートするために導入された次のフィールドが含まれるようになりました。

- **Next Hop Ip Address**：構成されたネクストホップ IP アドレスを表示します。

（注） **Next Hop Ip Address** フィールドは、ネクストホップ IP アドレスが SMF からリレーされる場合にのみ表示されます。ネクストホップ IP アドレスが Charging-Action を使用して UPF でのみ構成されている場合、このフィールドは表示されません。



第 32 章

N:M 冗長化および冗長化構成マネージャ

- 機能の概要と変更履歴, on page 385
- 機能説明 （386 ページ）

機能の概要と変更履歴

要約データ

Table 71: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G RCM* 構成およびアドミニストレーション ガイド

更新履歴

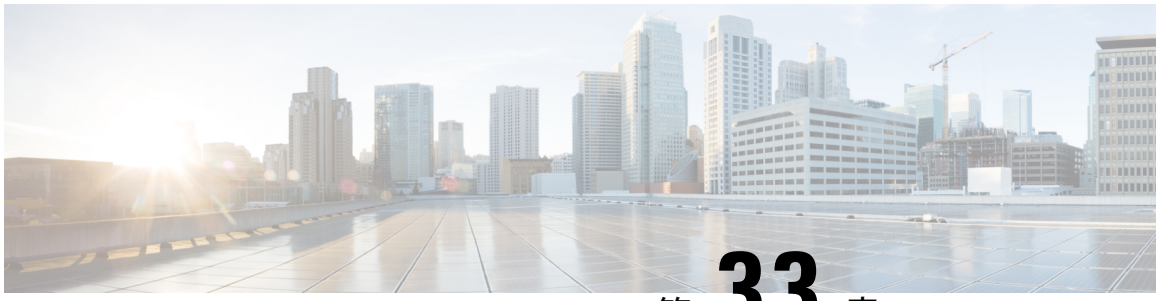
Table 72: マニュアルの変更履歴

改訂の詳細	リリース
SSH IP のインストールの延期がサポートされました。	2021.02.2
Network Services Orchestrator（NSO）経由で RCM を構成するサポートが追加されました。	2021.02.0
最初の導入。	2021.01.0

機能説明

Redundancy Configuration Manager（RCM）は、シスコ独自のノード/ネットワーク機能（NF）で、StarOS ベースの UP/UPF の冗長化を提供します。RCM は、UP/UPF の N:M 冗長化を提供します。このでの「N」は、クティブな UP/UPF の数で 10 未満であり、「M」は冗長化グループ内の スタンバイ UP/UPF の数です。

詳細については、『Redundancy Configuration Manager - 構成およびアドミニストレーション ガイド』を参照してください。



第 33 章

PDU セッション情報の N3 転送

- 機能の概要と変更履歴, on page 387
- 機能説明, on page 387

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

PDU セッション情報の N3 転送には、N3 インターフェイスの gNodeB に対する GTP-U カプセル化の実行中に QoS Field Identifier (QFI) IE の挿入と、gNodeB からパケットを受信した際に GTP-U カプセル化解除の実行中に、GTP-U 拡張ヘッダーの削除が含まれます。

QFI IE は、特定の QoSセッションに関する通信を検出します。これは、gNodeB と UPF 間で制御情報を送信するために使用されます。

機能の仕組み

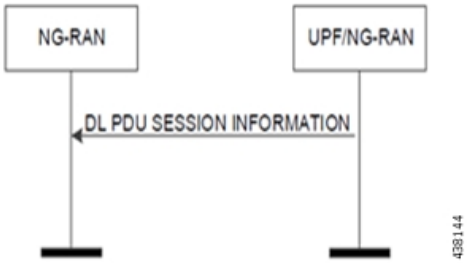
この項では、アップリンクおよびダウンリンクパケットの gNodeB と UPF 間での PDU session Information 手順について説明します。

ダウンリンクデータパケットの PDU セッション情報の転送

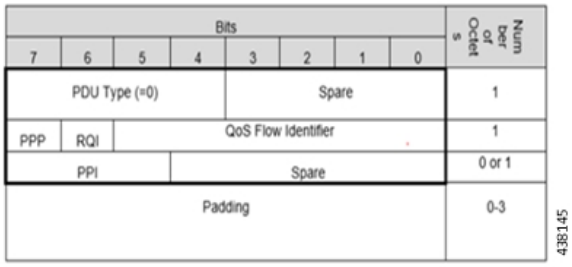
ダウンリンクデータパケットに関する PDU セッション情報の転送には、UPF/NG-RAN から NG-RAN への PDU セッション関連の制御情報要素の転送が含まれます。

この転送手順を使用する PDUセッションユーザープレーンインスタンスは、単一の PDUセッションに関連付けられます。この手順は、その特定のPDUセッションのパケットを関連するインターフェイス インスタンス間で転送する必要があるたびに呼び出されます。

DL PDU SESSION INFORMATION フレームには、転送されたパケットに関連付けられた QoS フロー識別子（QFI）フィールドが含まれます。NG-RAN は、受信した QFI を使用して、受信したパケットに関連付けられている QoS フローと QoS プロファイルを決定します。



次のフレームには、それぞれの DL PDU SESSION INFORMATION が表示されます。



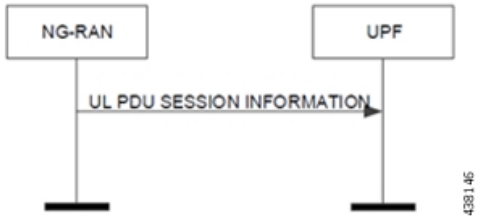
注：現在の実装では、DL PDU SESSION INFORMATION フレームの Reflective QoS Indicator（RQI）および Paging Policy Presence（PPP）はサポートされていません。

アップリンクデータパケットの PDU セッション情報の転送

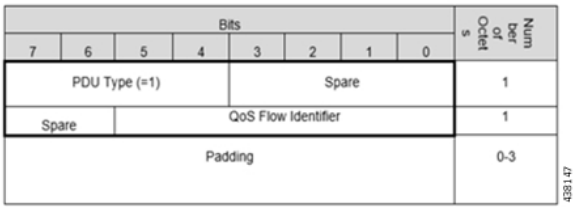
アップリンクデータパケットに関する PDU セッション情報の転送には、NG-RAN から UPF への PDU セッション関連の制御情報要素の転送が含まれます。

転送手順を使用する UL PDU ユーザープレーンは、単一の PDU セッションに関連付けられます。この手順は、その特定のPDU セッションのパケットを関連するインターフェイス インスタンス間で転送する必要があるたびに呼び出されます。

UL PDU SESSION INFORMATION フレームには、転送されたパケットに関連付けられた QoS フロー識別子（QFI）フィールドが含まれます。



次のフレームには、それぞれの UL PDU SESSION INFORMATION が表示されます。



PDU Session Information Frame IE

次の表では、PDU セッション情報フレームに存在する情報要素について説明します。

情報要素	説明
PDU Type	PDU Type は、PDU セッション UP フレームの構造を示します。このフィールドには、識別する PDU Type の値が設定されます。「0」は PDU タイプ 0 を示します。PDU Type は、フレームの最初のオクテットのビット 4 ～ 7 です。 **値の範囲**：{0= DL PDU SESSION INFORMATION, 1=UL PDU SESSION INFORMATION, 2-15=reserved for future PDU type extensions} **フィールド長**：4 ビット
スペア	スペアフィールドは送信者によって「0」に設定され、受信者が解釈するべきものではありません。このフィールドは、以降のバージョン用に予約されます。 **値の範囲**：(0 ~ 2n-1) **フィールド長**：n ビット

情報要素	説明
QoS Flow Identifier	この IE が存在する場合、このパラメータは、転送されたパケットが属するQoS フローの QoS Flow Identifier を示します。 **値の範囲**：{0 to 2^6-1} **フィールド長**：6 ビット
パディング	PDU セッション ユーザー プレーン プロトコル PDU 長（パディングと将来の拡張を含む）が、(n*4–2) オクテットになるように、パディングはフレームの最後に含まれます。ここで n は正の整数です。 **フィールド長**：0 ～ 3 オクテット。

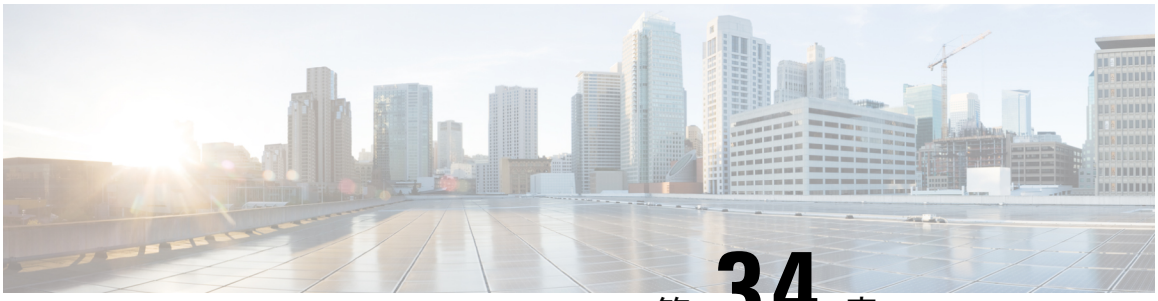
標準準拠

この機能は、3GPP TS 38.415 V15.2.0（NG-RAN; PDU Session User Plane Protocol）の標準規格に準拠しています。

制限事項

このリリースにおけるこの機能の制限事項は次のとおりです。

- Reflective QoS Indicator（RQI）は、このリリースではサポートされていません。



第 34 章

3GPP仕様とのN4インターフェイスの準拠

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 391
- 機能説明, on page 392

機能の概要と変更履歴

要約データ

Table 73: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効、常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 74: マニュアルの変更履歴

改訂の詳細	リリース
Outer Header Removal IE にサポートが追加されました。	2021.04.0
このリリースでは、PFCP ライブラリがアップグレードされ、Outer Header IE の最新バージョンがサポートされます。	2020.02.5

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

3GPP TS 29.244 に準拠して、ユーザープレーン機能（UPF）は次の IE をサポートします。

- Averaging Window
- Paging Policy Indicator（PPI）
- Outer Header Creation
- Outer Header Removal

Averaging Window

Averaging window IE には、GBR と MBR が計算される期間が含まれます。これは、UPF のデフォルト pre-configured 値をオーバーライドする必要がある場合に、Create QER または Update QER parent IE と共に、SMF から UPF に送信されます。

IE のエンコードとデコードには、次のフォーマットが使用されます。

	ビット							
Octets	8	7	6	5	4	3	2	1
1 ～ 2	タイプ = 157（10 進数）							
3 ～ 4	長さ = n							
5 ～ 8	Averaging Window							
9 ～ (n+4)	これらのオクテットは、明示的に指定されている場合にのみ存在します。							

注意：値は、ミリ秒で設定されているはずです。

Paging Policy Indicator

UPF が発信パケットでページング ポリシー インジケータを設定する必要がある場合、SMF は Create QER または Update QER で PPI 値を送信します。

Network Triggered Service 要求および UPF バッファリング ダウンリンク データ パケットの場合、UPF は、ダウンリンクデータパケットの IP ヘッダーからの Tos（IPv4）/TC（IPv6）値の DSCP を含めます。また、Data Notification メッセージの対応する QoS フローの指示を SMF に送信します。PPD が適用される場合、SMF は UPF から受信した DSCP に基づいてページング ポリシー インジケータ（PPI）を決定します。

Network Triggered Service 要求と SMF バッファリング ダウンリンク データ パケットの場合、PPD が適用されると、SMF は、受信したダウンリンク データ パケットの IP ヘッダーからの Tos（IPv4）/TC（IPv6）値の DSCP に基づいて PPI を判断し、受信したダウンリンク データ パケットの QFI の対応する QoS フローを特定します。

IE のエンコードとデコードには、次のフォーマットが使用されます。

	ビット							
Octets	8	7	6	5	4	3	2	1
1 ～ 2	タイプ = 158（10 進数）							
3 ～ 4	長さ = n							
5	Spare					PPI 値		
6 ～ (n+4)	これらのオクテットは、明示的に指定されている場合にのみ存在します。							

注：PPI は、0 ～ 7 の 3 ビット値としてエンコードする必要があります。

Outer Header Creation

3GPP TS 29.244 v16.4.0 に従い、[Outer Header Creation Description] フィールドが存在する場合、次の表に指定されているとおりにエンコードされます。これはビットマスクの形式になり、各ビットは発信パケットに作成される外部ヘッダーを示します。スペアビットは、受信側では無視されます。

オクテット/ビット	発信パケットで作成された外部ヘッダー
5/1	GTP-U/UDP/IPv4
5/2	GTP-U/UDP/IPv6
5/3	UDP/IPv4
5/4	UDP/IPv6
5/5	IPv4
5/6	IPv6
5/7	C-TAG
5/8	S-TAG
6/1	N19 Indication
6/2	N6 Indication
6/3	TCP/IPv4
6/4	TCP/IPv6

注：

- 現在、UP/UPF は、Outer Header Creation Description の値をサポートしていません。

- IPv4
- IPv6
- C-TAG
- S-TAG
- N19 Indication
- N6 Indication

- 6 番目のオクテットの 3 番目と 4 番目のビット（つまり、6/3 と 6/4）は、LI over TCP に使用されるスペアビット（つまり、3GPP TS）です。
- Outer Header Creation IE が、GTP-U/UDP/IPv4 および GTP-U/UDP/IPv6 の両方が設定されている [Outer Header Creation description] フィールドとともに受信した場合、26 バイトの Outer Header Creation IE 長が検証されます。長さが、26 バイトではない場合、Offending IE: OUTER_HDR_CREATION 原因コードが設定された PFCP_CAUSE_MANDATORY_IE_INCORRECT で Sx メッセージを受信します。



重要 SMF/CP が、Outer Header Creation の古いバージョンを使用している場合、クラッシュを含む未定義の動作が発生する場合があります。

Outer Header Removal

Outer Header Removal 機能は、アップリンク GTP-U パケットから GPRS Tunneling Protocol User Plane（GTP-U）ヘッダーを削除するために使用されます。

以下のフォーマットが、Outer Header Removal Information Element（IE）のエンコードに使用されます。

	ビット							
Octets	8	7	6	5	4	3	2	1
1 ～ 2	タイプ = 95（10 進数）							
3 ～ 4	長さ = n							
5	Outer Header Removal Description							
6	GTP-U Extension Header Deletion							
7 ～（n + 4）	これらのオクテットは、明示的に指定されている場合にのみ存在します。							

3GPP TS 29.244 に従い、[Outer Header Removal Description] フィールドが存在する場合、次の表に指定されているとおりにエンコードされます。

表 *75 : Outer Header Removal Description*

受信パケットから削除される外部ヘッダー	値（10 進数）
GTP-U/UDP/IPv4（注 1、2 を参照）、	0
GTP-U/UDP/IPv6（注 1、2 を参照）	1
UDP/IPv4（注 3、6 を参照）	2
UDP/IPv6（注 3、6 を参照）	3
IPv4（注 6 を参照）	4
IPv6（注 6 を参照）	5
GTP-U/UDP/IP（注 4 を参照）	**6**
VLAN S-TAG（注 5 を参照）	7
S-TAG および C-TAG（注 5 を参照）	8
未使用。送信されません。受信した場合、値「1」として解釈されます。	9 ～ 255

注：

- SGW-U/I-UPF は、GTP-U 拡張ヘッダーを保存します。これらのヘッダーは、[GTP-U Extension Header Deletion] フィールドによって削除が要求されていないパケットに転送されます。
- SGW-U/I-UPF は、転送する必要がある GTP-U シグナリングメッセージの GTP-U メッセージタイプを保存します。たとえば、End Marker メッセージです。
- この値は、非 IP PDN 接続に対して PGW-U が受信する DL パケットに適用されます。これらの接続では、UDP/IP のカプセル化に基づく SGi トンネリングを使用します。
- CP 機能は、この値を使用して、IPバージョン（IPv4 または IPv6）に関係なく GTP-U/UDP/IP ヘッダーを削除するように UP 機能に指示します。
- この値は、イーサネット PDU セッションの N6 を介した UPF によって受信される DL パケットに適用されます。
- この値は、明示的な N6 通信ルーティング情報が SMF に提供されている場合、N6 経由で UPF（PDU セッションアンカー）が受信する DL パケットに適用されます。
- Created PDR IE または Traffic Endpoint IE のローカル F-TEID には、ローカルの GTP-U エンドポイントが入力されます。このエンドポイントは、Created PDR IE で受信した Outer Header Removal に関係なく、設定に基づいて割り当てられます。たとえば、GTP-U サービス設定が IPv4 アドレスと IPv6 アドレスの両方をサポートしている場合、これらのアドレスの両方が割り当てられ、Created PDR IE および Traffic Endpoint IE でアドバタイズされます。

ローカル F-TEID 割り当てプロセスに加えて、ユーザープレーンは、次のシナリオで、Created PDR IE および Traffic Endpoint IE 経由で コントロールプレーンに F-TEID をアドバタイズします。

- Create PDR IE で受信した Outer Header Removal も、Created PDR IR または Traffic Endpoint IE の入力時に考慮されます。
- Outer Header Removal を GTP-U、UDP、または IP として受信した場合、ローカル GTP-U エンドポイントは割り当て済みとしてアドバタイズされます。つまり、IPv4 アドレスと IPv6 アドレスの両方が GTP-U サービスで構成されている場合、これらの両方がアドレスが割り当てられ、アドバタイズされます。IPv4 または IPv6 アドレスが構成されている場合、必要なアドレスのみが割り当てられ、Created PDR IR または Traffic Endpoint IE でアドバタイズされます。
- Outer Header Removal が GTP-U、UDP、または IPv4 として受信される場合、これらの両方のアドレスが設定されていても、IPv6 アドレスのみがアドバタイズされます。
- Outer Header Removal が GTP-U、UDP、または IPv6 として受信される場合、これらの両方のアドレスが設定されていても、IPv6 アドレスのみがアドバタイズされます。

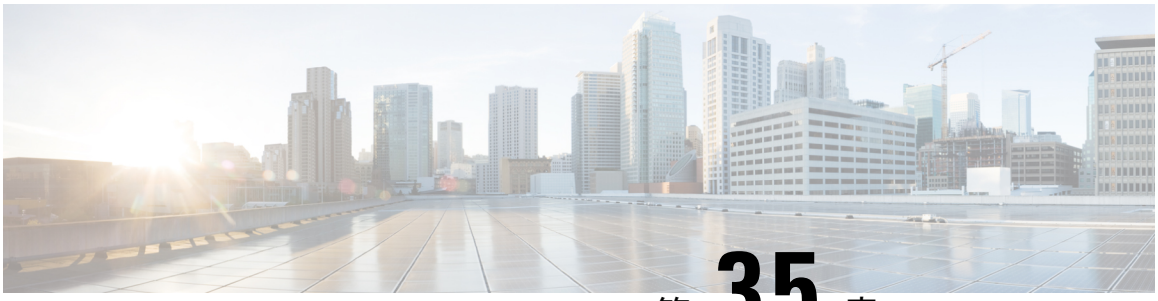
ソフトウェア要件

ソフトウェア要件は次のとおりです。

- この機能を使用して、N4 インターフェイスでワイルドカード トンネル タイプ「GTP-U/UDP/IP-6」を識別、エンコード、およびデコードするには、UPF サポートが必要です。
- IPv4 および IPv6 アドレスが Outer Header Creation（OHC）の一部として受信された場合、IPv6 エンドポイントに優先順位が付くため、IPv6 Outer Header Removal（OHR）エンドポイントは UPF によって保持されます。
- N4 インターフェイスの GTP-U/UDP/ IP-6 は、Sx Establishment または Sx Modification 要求メッセージ経由で受信できます。UPF は、両方のケースでタイプ 6 をサポートする必要があります。
- ハンドオフシナリオでは、OHR 値が 6 に設定されているすべての PDR に対して、ダウンリンク FAR に対応する PDR に適切な OHC IE が受信されるまで、アップリンクパケットがバッファリングされます。
- アップリンクパケットは、UPF で適切な OHR タイプが設定された後にのみ転送されます。

制限事項

- アップリンク PDR に対して 6 のOuter Header Removal 値を受信した場合、UPF はアップリンクPDRに対して IPv6 Outer Header Removal IE のみを維持します。UPF は、ダウンリンク FAR 用に適切な Outer Header Creation IE を受信するまで、それを保持します。
- この機能は、N4 インターフェイスにのみ適用されます。



第 35 章

N4 インターフェイスの構成

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 397
- 機能説明, on page 398
- N4 および Sx インターフェイスにおける圧縮の統一性 （398 ページ）
- N4 インターフェイスを構成する, on page 399

機能の概要と変更履歴

要約データ

Table 76: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効（無効にするには構成が必要）
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 77: マニュアルの変更履歴

改訂の詳細	リリース
新しい IE は、3GPP TS 29.244 のコンプライアンスに順守して、UPF でサポートされます。	2021.01.0
最初の導入。	2020.02.0

機能説明

この章では、N4インターフェイスとなるピアノードを識別する構成情報と、Sx サービスでN4パラメータを変更する構成について説明します。

N4 および Sx インターフェイスにおける圧縮の統一性

この機能により、PFCP Association Setup 手順中にピアレベルのハンドシェイクメカニズムが導入されます。これにより、UPF とコントロールプレーン（CP）は圧縮機能をネゴシエートし、UPF がピアごとに圧縮されたメッセージまたは圧縮されていないメッセージを送信できるようにします。

ユーザープレーン機能（UPF）がコンバージドコア（cnSGW/SMF）と従来ののコントロールおよびユーザープレーン分離（CUPS）コアの間で共有されるデプロイメントでは、UPF で Sx 圧縮が有効になっていると、コールの拒否が発生する場合があります。これは、コンバージドコアノードが現在、圧縮された PFCP メッセージをサポートしていないためです。

仕組み

この機能は、PFCP Association Setup 手順での Information Element（IE）の交換に依存しています。

1. UPF 機能：UPF は、Association Setup 要求でオペレータが構成可能な UPF capability IE（3GPP TS 29.244 で定義されているタイプ 359）を送信します。
2. CP 機能：CP（SMF/cnSGW）は、Association Setup 応答で独自のオペレータが構成可能な CP capability IE（タイプ 32769、エンタープライズ ID 9）で応答します。
3. 機能ロジック：
   - CP が「0」を報告した場合、UPF はそのピアに圧縮されていないメッセージを送信します。
   - CP が「1」を報告するか、IE が存在しない（後方互換性）場合、ローカル CLI により CPF が圧縮メッセージを送信できるように構成されていれば、UPF は圧縮メッセージを送信します。

ピアごとの圧縮ロジック

UPF は、次のロジックに基づいて発信 PFCP メッセージを圧縮するかどうかを決定します。

ローカル CLI 構成	ピア機能（IE 32769）	UPF 圧縮
無効化	未送信/0/1	無効化
未設定	未送信/1	有効
未設定	0	無効
有効	未送信/1	有効
有効済み	0	無効

構成

UPF で Sxプロトコル圧縮を有効または無効にするには、次の CLI コマンドを使用します。

```
configure
          context <context_name>
            sx-service <service_name>
              [no] sx-protocol compression
               end
```

（注） `sx-protocol compression` CLI は、発信メッセ圧縮のみを制御します。圧縮フラグ（IE 359/IE 32769）は、圧縮されたメッセージを受信するノードの機能を示します。ランタイムの構成変更は、Association Update を必要とせずにすぐに有効になります。

検証

特定のピアに対して交換された圧縮機能を確認するには、次のコマンドを使用します。

```
show sx peers full address <peer-ip>
```

サンプル出力：

```
Peer IP      : 21.21.21.101
Sx Service Id: 1
Group Name   : default
...
Compression  : Enabled
```

N4 インターフェイスを構成する

この項では、次の構成について説明します。

- N4 インターフェイスを識別する
- Sx サービスでの N4 タイプと N4 パラメータの変更を追加する

N4 インターフェイスを識別する

次の構成を使用して、ピアノードが、N4 インターフェイスタイプであるかどうかを識別します。

```
configure
   control-plane-group group_name
      peer-node-id [ ipv4-address ipv4_address | ipv6-address ipv6_address
] interface n4
      end
```

注：

- **n4 interface** CLI コマンドを有効にするには、UPF ライセンスに依存する UPF で **require upf** CLI コマンドが必要です。
- **[ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **]** ：

  ipv4-address *ipv4_address*：ピアノードの IPv4 アドレスを指定します。

  ipv6-address *ipv6_address*：ピアノードの IPv6 アドレスを指定します。
- **interface n4**：N4 インターフェイスを特定します。

Sx サービスの N4-type パラメータの変更

Sx サービスで N4 タイプのパラメータを変更するには、次の構成を使用します。

```
configure
   context context_name
      sx-service service_name
         n4 [ max-retransmissions max_retransmission_value |
retransmission-timeout-ms timeout_value ]
         end
```

注：

- **n4**：N4 パラメータへの変更を許可します。
- **[max-retransmissions***max_retransmission_value* **| retransmission-timeout-ms** *timeout_value***]**：

  max-retransmissions *max_retransmission_value* Sx コントロールパケットの最大再試行数を構成します。*max_retransmission_value* は、0 ～ 15 の整数で指定する必要があります。デフォルト値は 4 です。

  retransmission-timeout-ms：Sx のコントロールパケット再送信タイムアウトをミリ秒単位で構成します。*timeout_value* は、1000 ～ 20000 ミリ秒の整数で指定する必要があります。タイムアウト値は、たとえば、1000、1100、1200 などの 100 単位で設定する必要があります。デフォルト値は 5000 ミリ秒です。

統計情報

この項では、この機能をサポートする show コマンドとその出力について説明します。

show control-plane-group

このコマンドの出力には、この機能の次のフィールドが表示されます。

- インターフェイスタイプ：このフィールドは、ピアインターフェイスが N4 であるかどうかを示します。N4 以外のインターフェイスの場合は表示されません。

show sx-service all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- N4
  - N4 再送信タイムアウト
  - N4 最大要求再送信

show subscribers user-plane-only all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- インターフェイス
  - N4

show user-plane-service statistics all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- N4 インターフェイスタイプの PDN
  - アクティブ
  - 設定
  - リリース日

show subscribers user-plane-only seid number pdr all

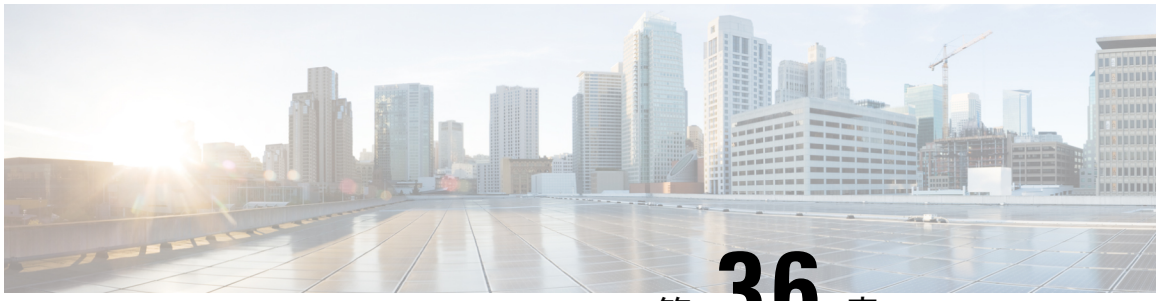
このコマンドの出力には、この機能の次のフィールドが表示されます。

- Associated-QFI

show subscribers user-plane-only callid number pdr full all

このコマンドの出力には、この機能の次のフィールドが表示されます。

- QoS Flow Identifier



第 36 章

IPSec 経由の N4/Sx

- 機能の概要と変更履歴 （403 ページ）
- 機能説明 （404 ページ）
- 推奨タイマー （406 ページ）
- 設定例 （413 ページ）
- モニタリングおよびトラブルシューティング （415 ページ）

機能の概要と変更履歴

要約データ

表 *78* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.04.0

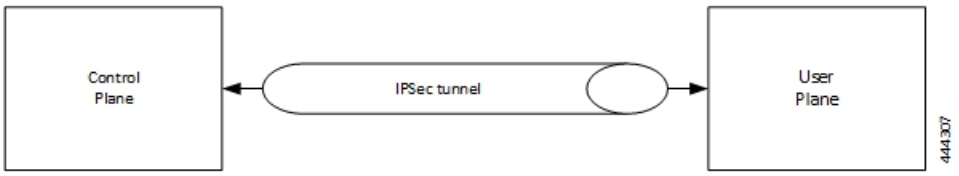
機能説明

Internet Protocol Security（IPSec）は、IP ネットワーク全体でセキュアなプライベート通信を提供するために相互にデータをやり取りする一連のプロトコルです。これらのプロトコルにより、システムはピア セキュリティ ゲートウェイとセキュアなトンネルを確立して維持できます。IPSec は、IP データグラムに機密性、データの完全性、アクセス制御、およびデータソース認証を提供します。

Cisco Cloud Native 5G では、セッション管理機能（SMF）とユーザープレーン機能（UPF）の両方でトンネルモードで IPSec 機能を使用できます。IPSec 暗号マップは、それぞれのノードの適切なインターフェイスで関連付けられます。IPSec トンネルは、各 SMF または UPF のペア間に明示的に作成されます。この機能は、IPv4 および IPv6 トンネリングモードをサポートします。N4/Sx サービスの構成に変更はありません。

IPSec トンネルモードは、IP パケット全体をカプセル化して、2 つのゲートウェイ間で仮想セキュアホップを提供します。これは、VPN のような機能を形成し、IP パケット全体を別のパケット内にカプセル化して接続先に配信します。完全な IP ヘッダーとペイロードがカプセル化されます。

図 *23 : IPSec* トンネル経由の *N4/Sx*



VPP を実行している UPF NF で IPSec 経由の N4/Sx が有効になっている場合、IPSec 経由の N4/Sx 機能を機能させるには、「VPP パラメータ」で次のパラメータを使用する必要があります。

VPP_DPDK_DATA_SIZE=5120

VPP パラメータは CD-ROM の **staros-para.cfg** ファイルに保存されます。この構成は、起動時に UPF によって読み取られ、VPP に適用されます。

（注） このパラメータは、VPP バージョン 19.08 までサポートされます。このパラメータにより、約 800 MB のメモリオーバーヘッドが発生します。この機能を使用する前に、この条件を考慮する必要があります。UPF の RAM が少ない場合、機能が正常に動作するように追加の 1 GB の RAM メモリを VM に割り当てる必要があります。

IPSec のサポートに関する詳細については、StarOS の「*IPSec* リファレンス」を参照してください。

IKEv2 キープアライブメッセージ（デッドピア検出）

N4/Sxインターフェイス向けIPSecは、IPSecトンネルの両端から発信される、Dead Peer Detection（DPD; デッドピア検出）とも呼ばれるIKEv2キープアライブメッセージをサポートします。RFC 3706に従い、DPDはピア間の通信とトンネルの可用性を検証するために必要なメッセージングを簡素化するために使用されます。

IPSec DPDは、任意構成です。無効になっている場合、IPSecノードは、DPD要求を開始しません。ただし、ノードはそのDPD構成に関係なく、常にピアノードが開始するDPD Availabilityメッセージに応答します。

次の方法を使用して、IPSec経由のN4/Sx機能が設定されている場合のキープアライブ間隔値を計算できます。

```
((max-retransmissions + 1) * retransmission-timeout-ms) * 2
```

キープアライブ間隔値は、DPDがトリガされるまでIPSecトンネルが稼働状態を維持する時間を指定します。

例：

次に、N4/Sx サービスでの **show configuration context** *context-name* **verbose** CLI コマンドの出力例を示します。

```
sx-service sx
   instance-type userplane
   bind ipv4-address 192.168.1.1 ipv6-address bbbb:abcd::11
   sxa max-retransmissions 4
   sxa retransmission-timeout-ms 5000
```

ここでは、**max-retransmissions** の値は 4、**retransmission-timeout-ms** は 5000 です。したがって、キープアライブ間隔の値は 50 になります。

((max-retransmissions + 1) * retransmission-timeout-ms) * 2 = キープアライブ間隔

((4+1) * 5000) * 2 = 50

IKESA キー再生成

UPF は、IKESA キー再生成とIPSecキー再生成の両方をサポートします。

IKESA キー再生成の場合は、**lifetime** *interval* CLI を **ikev2-ikesa transform-set** *transform-set* で設定する必要があります。**crypto map** 構成で、**ikev2-ikesa rekey** を構成する必要もあります。次に、構成例を示します。

```
ikev2-ikesa transform-set ikesa-foo
   encryption aes-cbc-256
   group 14
   hmac sha2-256-128
   lifetime 28800
   prf sha2-256
...
...
...
crypto map foo0 ikev2-ipv4
   match address foo0
   authentication local pre-shared-key encrypted key secret_key
   authentication remote pre-shared-key encrypted key secret_key
   ikev2-ikesa max-retransmission 3
```

```
ikev2-ikesa retransmission-timeout 15000
ikev2-ikesa transform-set list ikesa-foo
ikev2-ikesa rekey
keepalive interval 50
control-dont-fragment clear-bit
payload foo-sa0 match ipv4
   ipsec transform-set list A-foo
   lifetime 600
   rekey keepalive
#exit
peer 172.19.222.2
ikev2-ikesa policy error-notification
```

推奨タイマー

次の表に、IPSec、N4/Sx、およびSRPに関連するCLIコマンドの推奨タイマー値を示します。

IPSec	**SMF**	**UPF**
ikev2-ikesa max-retransmission	*3*	*3*
ikev2-ikesa retransmission-timeout	*1000*	*1000*
keepalive	**interval** *4* **timeout** *1* **num-retry** *4*	**interval** *5* **timeout** *2* **num-retry** *4*
N4/Sx	**SMF**	**UPF**
sx-protocol heartbeat interval	*10*	*10*
sx-protocol heartbeat retransmission-timeout	*5*	*5*
sx-protocol heartbeat max-retransmissions	*4*	*4*
sxa max-retransmissions	*4*	*4*
sxa retransmission-timeout-ms	*5000*	*5000*
sxb max-retransmissions	*4*	*4*
sxb retransmission-timeout-ms	*5000*	*5000*
sxab max-retransmissions	*4*	*4*
sxab retransmission-timeout-ms	*5000*	*5000*
sx-protocol association reattempt-timeout	*60*	*60*
SRP	**SMF**	**UPF**
hello-interval	*3*	*3*
dead-interval	*15*	*15*

推奨設定

以下に、N4/Sx および SRP over IPSec に関連する推奨構成と制限事項を示します。

- SMF と UPF 間のマルチホップ BFD タイマーは、7 秒に設定する必要があります（データ UPF の場合）。
- シングルホップ BFD は、すべてのコンテキスト（SMF GW/課金情報および UP Gn/Gi）で有効にする必要があります。
- シャーシ間マルチホップ BFD は、SMF-SMF ICSR および UPF-UPF ICSR（IMS UPF）に対して有効にする必要があります。
- SRP-IPSec ACL は、IP プロトコルではなく TCP プロトコル用に設定する必要があります。
- N4/Sx-IPSec ACL は、IP プロトコルではなく UDP プロトコル向けに設定する必要があります。

SMF の構成例

マルチホップ BFD 設定 VPC-DI

次に、7 秒タイマーを使用したマルチホップ BFD の設定例を示します。

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 350 min_rx 350 multiplier 20
    #exit
```

マルチホップ BFD 設定 VPC-SI

次に、タイマーが 3 秒のマルチホップ BFD 設定の例を示します。

```
bfd-protocol
      bfd multihop-peer 209.165.200.226 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.227 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.225 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.230 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.228 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 209.165.200.229 interval 150 min_rx 150 multiplier 20
    #exit
```

BGP の設定

以下に、推奨タイマーを使用した BGP の設定例を示します。

```
router bgp 1111
      router-id 209.165.200.225
      maximum-paths ebgp 15
      neighbor 209.165.200.250 remote-as 1000
      neighbor 209.165.200.250 ebgp-multihop
      neighbor 209.165.200.250 update-source 209.165.200.225
      neighbor 1111:2222::101 remote-as 1000
      neighbor 1111:2222::101 ebgp-multihop
```

```
      neighbor 1111:2222::101 update-source 1111:2222::1
      bgp graceful-restart restart-time 120
      bgp graceful-restart stalepath-time 300
      timers bgp keepalive-interval 30 holdtime-interval 90 min-peer-holdtime-interval
0 server-sock-open-delay-period 10
      address-family ipv4
        redistribute connected
      #exit
      address-family ipv6
        neighbor 1111:2222::101 activate
        redistribute connected
      #exit
    #exit
```

シングルホップ BFD 設定

タイマーが 3 秒のシングルホップ BFD の設定例を以下に示します。

```
interface bgp-sw1-2161-10
      ip address 209.165.200.233 209.165.200.255
      ipv6 address 1111:222::9/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-11
      ip address 209.165.200.234 209.165.200.255
      ipv6 address 1111:222::10/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-12
      ip address 209.165.200.235 209.165.200.255
      ipv6 address 1111:222::11/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-3
      ip address 209.165.200.226 209.165.200.255
      ipv6 address 1111:222::2/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-4
      ip address 209.165.200.227 209.165.200.255
      ipv6 address 1111:222::3/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-5
      ip address 209.165.200.228 209.165.200.255
      ipv6 address 1111:222::4/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-6
      ip address 209.165.200.229 209.165.200.255
      ipv6 address 1111:222::5/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-7
      ip address 209.165.200.230 209.165.200.255
      ipv6 address 1111:222::6/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-8
      ip address 209.165.200.231 209.165.200.255
      ipv6 address 1111:222::7/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-9
```

```
      ip address 209.165.200.232 209.165.200.255
      ipv6 address 1111:222::8/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
```

マルチホップ BFD 設定のスタティックルート

次に、スタティック ルート マルチホップ BFD 設定の例を示します。

```
ip route static multihop bfd UP-5 209.165.200.240 209.165.200.245
    ip route static multihop bfd UP-6 209.165.200.240 209.165.200.246
    ip route static multihop bfd UP-9 209.165.200.240 209.165.200.247
    ip route static multihop bfd UP-10 209.165.200.240 209.165.200.248
    ip route static multihop bfd UP-7 209.165.200.240 209.165.200.249
    ip route static multihop bfd UP-8 209.165.200.240 209.165.200.250
```

シングルホップ BFD 設定用のスタティックルート

次に、スタティックルートのシングルホップ BFD 設定の例を示します。

```
ip route static bfd bgp-sw1-2161-3 209.165.200.230
    ip route static bfd bgp-sw1-2161-4 209.165.200.230
    ip route static bfd bgp-sw1-2161-5 209.165.200.230
    ip route static bfd bgp-sw1-2161-6 209.165.200.230
    ip route static bfd bgp-sw1-2161-7 209.165.200.230
    ip route static bfd bgp-sw1-2161-8 209.165.200.230
    ip route static bfd bgp-sw1-2161-9 209.165.200.230
    ip route static bfd bgp-sw1-2161-10 209.165.200.230
    ip route static bfd bgp-sw1-2161-11 209.165.200.230
    ip route static bfd bgp-sw1-2161-12 209.165.200.230
```

IPSec ACL の設定

以下に、SMF での IPSec ACL の構成例を示します。

```
ip access-list UP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec トランスフォームセットの設定

SMF での IPSec トランスフォームセットの設定例を以下に示します。

```
ikev2-ikesa transform-set ikesa-UP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256

    ipsec transform-set A-UP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14
```

IPSec クリプトマップの設定

SMF での IPSec 暗号化マップの設定例を以下に示します。

```
crypto map UP-1 ikev2-ipv4
      match address UP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
```

```
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-UP-1
      ikev2-ikesa rekey
      keepalive interval 4 timeout 1 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-UP-1
        lifetime 300
        rekey keepalive
      #exit
      peer 209.165.200.224
      ikev2-ikesa policy error-notification
    #exit
```

N4/Sx の構成

以下は、SMF での N4/Sx 構成例です。

```
sx-service SX-1
      instance-type controlplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
      sx-protocol supported-features load-control
      sx-protocol supported-features overload-control
    exit
end
```

ルータの設定例

インターフェイスのスタティックルート

次に、インターフェイスのスタティックルートの設定例を示します。

```
ip route 209.165.200.224/27 Vlan1111 209.165.200.225
ip route 209.165.200.224/27 Vlan1111 209.165.200.226
ip route 209.165.200.224/27 Vlan1111 209.165.200.227
ip route 209.165.200.224/27 Vlan1111 209.165.200.228
ip route 209.165.200.224/27 Vlan1111 209.165.200.229
ip route 209.165.200.224/27 Vlan1111 209.165.200.230
ip route 209.165.200.224/27 Vlan1111 209.165.200.231
ip route 209.165.200.224/27 Vlan1111 209.165.200.232
ip route 209.165.200.224/27 Vlan1111 209.165.200.233
ip route 209.165.200.224/27 Vlan1111 209.165.200.234
```

シングルホップ BFD のスタティックルート

次に、シングルホップ BFD のスタティックルートの設定例を示します。

```
ip route static bfd Vlan1111 209.165.200.225
ip route static bfd Vlan1111 209.165.200.226
ip route static bfd Vlan1111 209.165.200.227
```

```
ip route static bfd Vlan1111 209.165.200.228
ip route static bfd Vlan1111 209.165.200.229
ip route static bfd Vlan1111 209.165.200.230
ip route static bfd Vlan1111 209.165.200.231
ip route static bfd Vlan1111 209.165.200.232
ip route static bfd Vlan1111 209.165.200.233
ip route static bfd Vlan1111 209.165.200.234
```

シングルホップ BFD のインターフェイス

シングルホップ BFD のインターフェイスの設定例を以下に示します。

```
interface Vlan1111
  no shutdown
  bandwidth 10000000
  bfd interval 999 min_rx 999 multiplier 3
  no bfd echo
  ip address 209.165.200.224/27
  ipv6 address 1111:222::1/112
```

BGP の設定

以下に、推奨タイマーを使用した BGP の設定例を示します。

```
router bgp 1000
  router-id 209.165.200.226
  timers bgp 30 90
  timers bestpath-limit 300
  timers prefix-peer-timeout 30
  timers prefix-peer-wait 90
  graceful-restart
  graceful-restart restart-time 120
  graceful-restart stalepath-time 300
```

UPF の構成例

IPSec ACL の設定

UPF での IPSec ACL の構成例を以下に示します。

```
ip access-list CP-1
      permit udp host 209.165.200.225 host 209.165.200.226
    #exit
```

IPSec トランスフォームセットの設定

以下に、UP での IPSec Transform Set の構成例を示します。

```
ipsec transform-set A-CP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14

    ikev2-ikesa transform-set ikesa-CP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256
```

IPSec クリプトマップの設定

UPF での IPSec 暗号マップの構成例を以下に示します。

```
crypto map CP-1 ikev2-ipv4
      match address CP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-CP-1
      ikev2-ikesa rekey
      keepalive interval 5 timeout 2 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-CP-1
      #exit
      peer 209.165.200.230
      ikev2-ikesa policy error-notification
    #exit
```

N4/Sx の構成

以下は、UPF における N4/Sx の構成例です。

```
sx-service SX-1
      instance-type userplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
    exit
```

SRP の設定例

IPSec ACL の設定

次に、SRP の IPSec ACL 設定の例を示します。

```
ip access-list SRP
      permit tcp host 209.165.200.227 host 209.165.200.228
    #exit
```

SRP の設定

SRP の設定例を以下に示します。

```
configure
  context srp
    bfd-protocol
      bfd multihop-peer 209.165.200.225 interval 999 min_rx 999 multiplier 3
    #exit
configure
  context srp
```

```
    service-redundancy-protocol
      chassis-mode primary
      hello-interval 3
      dead-interval 15
      monitor bfd context srp 209.165.200.226 chassis-to-chassis
      monitor bgp context gi-pgw 209.165.200.245
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 209.165.200.245
      monitor bgp context saegw 3333:888::2
      peer-ip-address 209.165.200.227
      bind address 209.165.200.228
    #exit
    ip route static multihop bfd srp 209.165.200.229 209.165.200.245
    ip route 209.165.201.1 209.165.202.129 209.165.200.230 SRP-Physical-2102
    ip route 209.165.201.2 209.165.202.130 209.165.200.231 SRP-Physical-2102
    ip route 209.165.201.3 209.165.202.131 209.165.200.232 SRP-Physical-2102
    ip igmp profile default
    #exit
  #exit
end
```

設定例

次の構成例では、N4/Sx および IPSec インターフェイスの IP アドレスは次のように定義されています。

```
SMF N4/Sx - 192.0.2.1
UPF N4/Sx - 192.0.2.7
SMF IPSec - 198.51.100.1
UPF IPSec - 198.51.100.2
```

（注）

- このリリースでの UPF の推奨タイマー値は次のとおりです。

  ```
  sx-protocol heartbeat retransmission-timeout 20
  sx-protocol heartbeat max-retransmissions 3
  ```

- このリリースでの SMF の推奨タイマー値は次のとおりです。

  ```
  sx-protocol heartbeat retransmission-timeout 20
  sx-protocol heartbeat max-retransmissions 5
  ```

コントロール プレーン

IPSecの設定

```
config
  context EPC-CP
    ip access-list foo0
      permit ip host 192.0.2.1 host 192.0.2.7
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
```

```
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 300
        rekey keepalive
      #exit
      peer 198.51.100.2
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface CP_IPSEC loopback
      ip address 198.51.100.1 255.255.255.0
   crypto-map foo0
    #exit
end
```

N4/Sx の構成

```
   sx-service SX-1
      instance-type controlplane
      bind ipv4-address 192.0.2.1
      sx-protocol heartbeat retransmission-timeout 20
      sx-protocol heartbeat max-retransmissions 5
   exit
```

ユーザープレーン

IPSecの設定

```
config
  context EPC-UP
    ip access-list foo0
      permit ip host 192.0.2.7 host 192.0.2.1
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
```

```
      #exit
      peer 198.51.100.1
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface UP_IPSEC  loopback
      ip address 198.51.100.2 255.255.255.0
   crypto-map foo0
    #exit
end
```

N4/Sx の構成

```
   sx-service SX-1
      instance-type userplane
      bind ipv4-address 192.0.2.7 ipv6-address dddd:51:31:1:209::
      sxa max-retransmissions 12
      sxb max-retransmissions 12
      sxab max-retransmissions 12
      sx-protocol heartbeat interval 30
      sx-protocol heartbeat retransmission-timeout 20
      sx-protocol heartbeat max-retransmissions 3
    exit
```

SMF プロトコル Pod で IPSec トンネル CLI を検証し、SMF で *ipsec.yaml* ファイルを検証するには、SMI StrongSwan 構成例に関する「インターフェイスサポート」>「*N4* インターフェイス」章を参照してください。

最新の strongSwan 構成については、『*Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』を参照してください。

モニタリングおよびトラブルシューティング

この項では、SMF と UPF の両方の IPSec 経由の N4/Sx 機能に対する show コマンドの CLI コマンド出力例を示します。

show crypto ikev2-ikesa security-associations summary

```
I - Initiator
  R - Responder
Mgr                                                                    Lifetime
ID  VPN Local IPSec GW:Port   Remote IPSec GW:Port  State             /Remaining
=== === ==================== ==================== ================ ===========
54  2   192.168.170.55 :500   192.168.196.55 :500   AUTH_COMPLETE(I) 86400/16448

1 IKEv2 Security Association found in this context.
```

show crypto ipsec security-associations summary

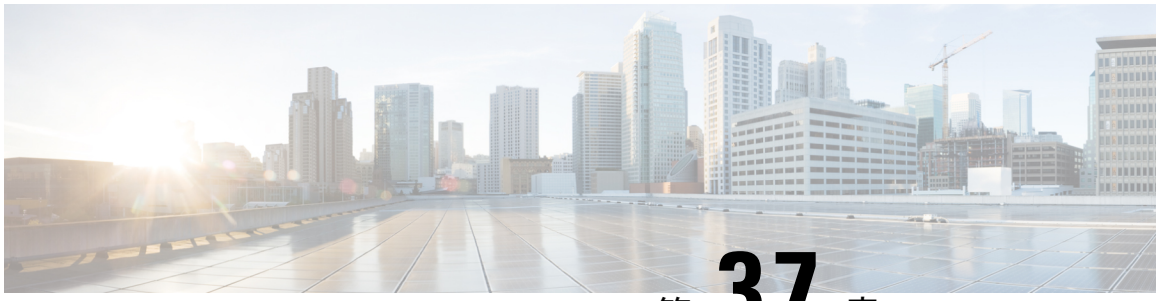
```
+------ SA state:           (E) - Established
      |                         (P) - Partially Established
      |                         (N) - No SAs
      |
      |+----- Rekey/Keepalive:    (D) - Rekey Disabled
      ||                          (E) - Rekey Enabled/No Keepalive
      ||                          (K) - Rekey Enabled/Keepalive
      ||
```

```
      ||+---- Crypto Type:        (D) - Dynamic Map
      |||                         (I) - IKEv1 Map
      |||                         (J) - IKEv2 Map
      |||                         (M) - Manual Map
      |||                         (C) - CSCF Map
      |||
      |||
      VVV           Map Name                                                  Rekeys En
Pkts    De Pkts
===== === ========================================================================== ======
========== ==========
1     EDJ foo0                                                                 0      3496
       3496

1 Crypto Map Found.
1 Crypto Map Established.
```

SMF プロトコル Pod で IPSec トンネル CLI を検証し、SMF で *ipsec.yaml* ファイルを検証するには、SMI StrongSwan 構成例に関する「インターフェイスサポート」>「*N4* インターフェイス」章を参照してください。

最新の strongSwan 構成については、『*Ultra Cloud Core* サブスクライバ マイクロサービス インフラストラクチャ操作ガイド』を参照してください。



第 37 章

N4 Session Management、Node Level、および Reporting 手順

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 417
- 機能説明, on page 418
- 機能の仕組み, on page 419
- N4 Session/Node-level Reporting 手順を構成する, on page 431
- グレースフル セッション終了の拡張された PFCP 関連付けのリリース手順 （434 ページ）

機能の概要と変更履歴

要約データ

Table 79: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
N4インターフェイス経由のSx EstablishmentまたはModificationメッセージで受信したPFCP IEを表示するために**show user-plane-service statistics all**コマンドが強化されました。	2023.01 2021.02.2
このリリースでは、PDN Update手順が導入されています。	2021.02.0
最初の導入。	2020.02.0

機能説明

N4 Session Management、Node Level、および Reporting 手順

N4 Node-level 手順

ユーザープレーン機能（UPF）のN4 Node-level手順には、次のプロセスが含まれます。

- N4 Association Setup手順：セッション管理機能（SMF）とUPF間のN4アソシエーションを設定するために使用される手順。
- N4 Association Update手順：SMFとUPF間の既存のN4アソシエーションを変更するために使用される手順。
- N4 Association Release手順：SMFとUPF間のN4アソシエーションを終了するために使用される手順。
- N4 Heartbeat手順：Heartbeat要求と応答を送受信するために使用される手順。
- N4 Reporting手順：GTP-uパスの障害に対するEcho要求と応答の報告に使用される手順。

N4 Session Management

N4 session management手順は、UPFの機能を制御するために使用されます。SMFは、3GPP TS 23.501、5.8.2節で説明されている、UPFのN4セッションコンテキストを作成、更新、および削除できます。

N4 Session Managementでは、次の手順が実行されます。

- N4 Session Establishment
- N4 Session Modification
- N4 Session Deletion

注：SMFは、上記のすべての手順を開始します。

N4 Session/Node-level Reporting 手順

UPF と gNB 間のデータパスが停止するたびに、検出され、修正措置のために SMF に報告されます。検出して SMF に報告するメカニズムは、3GPP の仕様で明確に定義されています。レポートは、GTP-u トンネルレベルまたは GTP-u エンドポイントレベルごとに行われます。

関係

次の機能は、N4 Session Management、node level、および reporting 手順をサポートします。

End Marker サポート

UPF は、目的の無線アクセスネットワーク（RAN）で再順序付け機能をサポートするために End Marker パケットを送信します。UPF は、再順序付け機能に必要な End Marker パケットを構築します。

UPF 経由で End Marker パケットを構築する

ハンドオーバー手順の時点で、UPF ノードで構成される UE のPDU セッションは、PDU セッションアンカーおよび中間の UPF 終端 N3 参照ポイントとして機能します。SMF は、NG RAN の新しい AN トンネル情報を含む N4 Session Modification 要求メッセージを送信し、N3 パスに切り替える UPF を指定します。さらに、SMF は、古い N3 ユーザープレーンパスで End Marker パケットを送信する UPF も指定します。

UPF が指示を受信すると、End Marker が作成され、古いパスの最後の PDU を送信した後、送信元 NG RAN に向けて各 N3 GTP-U トンネルに送信されます。

UEs IPv4、IPv6 および IPv4v6 サポート

UPF は、UE の IPv4、IPv6、および IPv4v6 セッションをサポートします。

IPv6 セッションの N4 Session Establishment および Modification 手順は、IPv4 セッションと同じです。セッションが確立されると、SMF は、通信に使用する IPv6 プレフィックスを通知する Router Advertisement（RA）メッセージを UE に送信します。必要に応じて、SMF から IPv6 パラメータを迅速に取得するために、UE は IPv6 Router Solicitation（RS）を開始することもできます。

IPv4v6 セッションの N4 Session Establishment および Modification 手順は、2 つの UE IP アドレス（1 つは IPv4 用、もう 1 つは IPv6 用）の割り当てを除いて、IPv4 または IPv6 セッションと似ています。SMF は、セッションの確立後に通信に使用される IPv6 プレフィックスを通知する Router Advertisement メッセージを UE に送信します。必要に応じて、UE は IPv6 Router Solicitation を開始して、SMF から IPv6 パラメータを迅速に受信することもできます。

機能の仕組み

この項では、N4 Node-Level、Session Management、Reporting 手順、および関連するコールフローについて説明します。

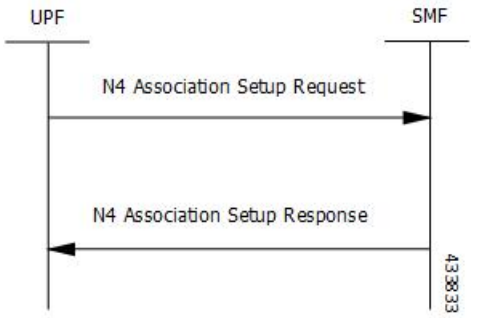
N4 Node-level 手順コールフロー

N4 Association Setup 手順のコールフロー

N4 Association Setup 手順では、SMF と UPF の間に N4 アソシエーションを作成し、SMF が UPF リソースを使用して N4 セッションを確立できるようにします。N4 Association Setup 手順には、次の手順が含まれます。

1. UPF は、N4 Association Setup 要求を SMF に送信することにより、手順を開始します。
2. SMF は、UPF から要求を受信した後、N4 Association Setup 応答を送信します。

次のコールフローでは、UPF が開始する N4 Association Setup 手順について説明します。



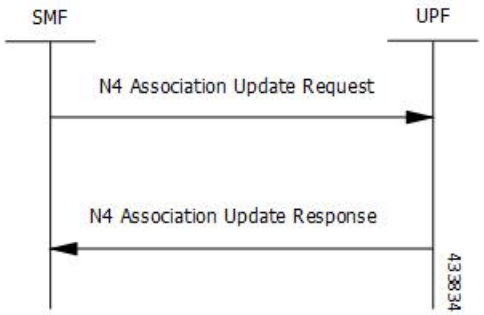
UPF は、次の PFCP Association Setup 要求を送信します。

- ノード ID（UPF）。
- UPF でサポートされているオプション機能。UPF は、F-TEID の割り当てとリリース、End Marker の送信などをサポートしています。

N4 Association Update 手順のコールフロー

N4 Association Update 手順では、SMF と UPF 間の既存の N4 アソシエーションを変更します。これは、UPF または SMF が開始し、サポートされている機能または使用可能な UPF リソースを更新できます。

次のコールフローは、SMF が開始する N4 Association Update 手順を示しています。



次のコールフローは、UPF が開始する N4 Association Update 手順を示しています。



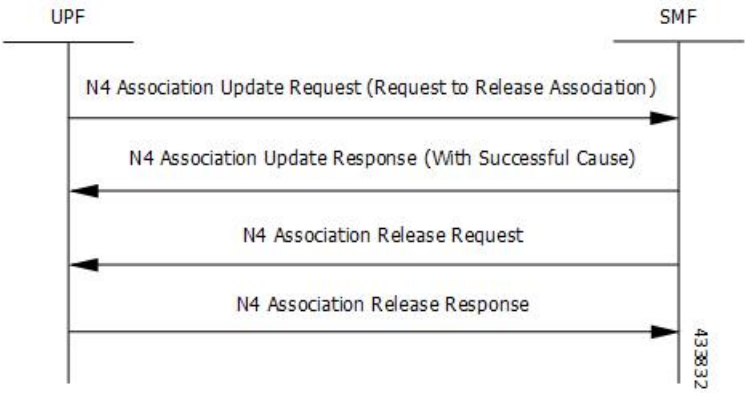
N4 Association Release 手順のコールフロー

N4 Association Release 手順は、SMF と UPF 間の N4 アソシエーションを終了します。SMF または UPF のいずれかによって開始できます。UPF は、PFCP Association Update 要求を送信して PFCP アソシエーションを解放するよう SMF に要求します。その後、SMF は、PFCP Association Update 要求を開始して PFCP アソシエーションを解放します。

次のコールフローは、SMF が開始する N4 Association Release 手順を示しています。



次のコールフローは、UPF が開始する N4 Association Release 手順を示しています。



N4 Heartbeat 手順

PFCP Heartbeat 手順には、次のメッセージが含まれます。

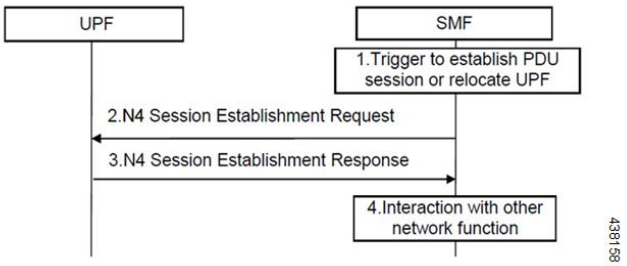
- Heartbeat 要求
- Heartbeat 応答

N4 Session Management 手順のコールフロー

次の項では、N4 Session Management 手順について説明します。

N4 Session Establishment コールフロー

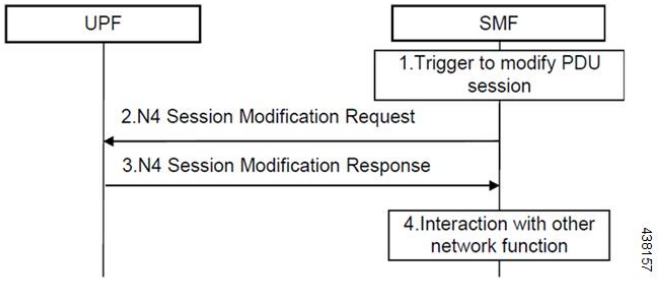
N4 Session Establishment は、UPF で PDU セッションの最初の N4 セッションコンテキストを作成するために使用されます。SMF は、新しい N4 セッション ID を割り当て、UPF に提供します。N4 セッション ID は両方のエンティティによって保存され、対話中に N4 セッションコンテキストを識別するために使用されます。SMF は、UE の N4 セッション ID と PDU セッションとの関係も保存します。



ステップ	説明
1	SMF は、新しい PDU セッションを確立するか、確立された PDU セッションの UPF を変更するトリガーを受信します。
2	SMF は、UPF がどのように動作する必要があるかを定義する構造化された制御情報を含む UPF に N4 Session Establishment 要求メッセージを送信します。
3	UPF は、受信した制御情報に応じて SMF に提供する必要がある情報を含む N4 Session Establishment 応答メッセージで応答します。
4	SMF は、この手順をトリガーしたネットワーク機能と通信します。例：AMF または PCF。

N4 Session Modification コールフロー

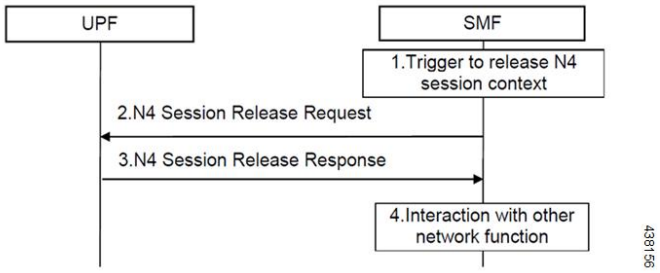
N4 Session Modification は、UPF で既存の PDU セッションの N4 セッションコンテキストを更新するために使用されます。 PDUセッション関連のパラメータを変更する必要があるたびに、SMF と UPF の間で実行されます。



ステップ	説明
1	SMF は、既存の PDU セッションを変更するトリガーを受信します。
2	SMF は、N4 Session Modification 要求メッセージを UPF に送信します。このメッセージには、UPF の動作方法を定義する構造化制御情報の更新が含まれます。
3	UPF は、N4 セッション ID によって変更される N4 セッションコンテキストを識別し、SMF から送信されるパラメータのリストに従って、この N4 セッションコンテキストのパラメータを更新します。UPF は、N4 Session Modification 応答メッセージで応答します。これには、受信した制御情報に応じて UPF が SMF に提供する必要がある情報が含まれています。
4	SMF は、この手順をトリガーするネットワークエンティティとやり取りします。例：AMF または PCF。

N4 Session Delete コールフロー

N4 Session Delete は、UPF での既存の PDU セッションの N4 セッションコンテキストを削除するために使用します。



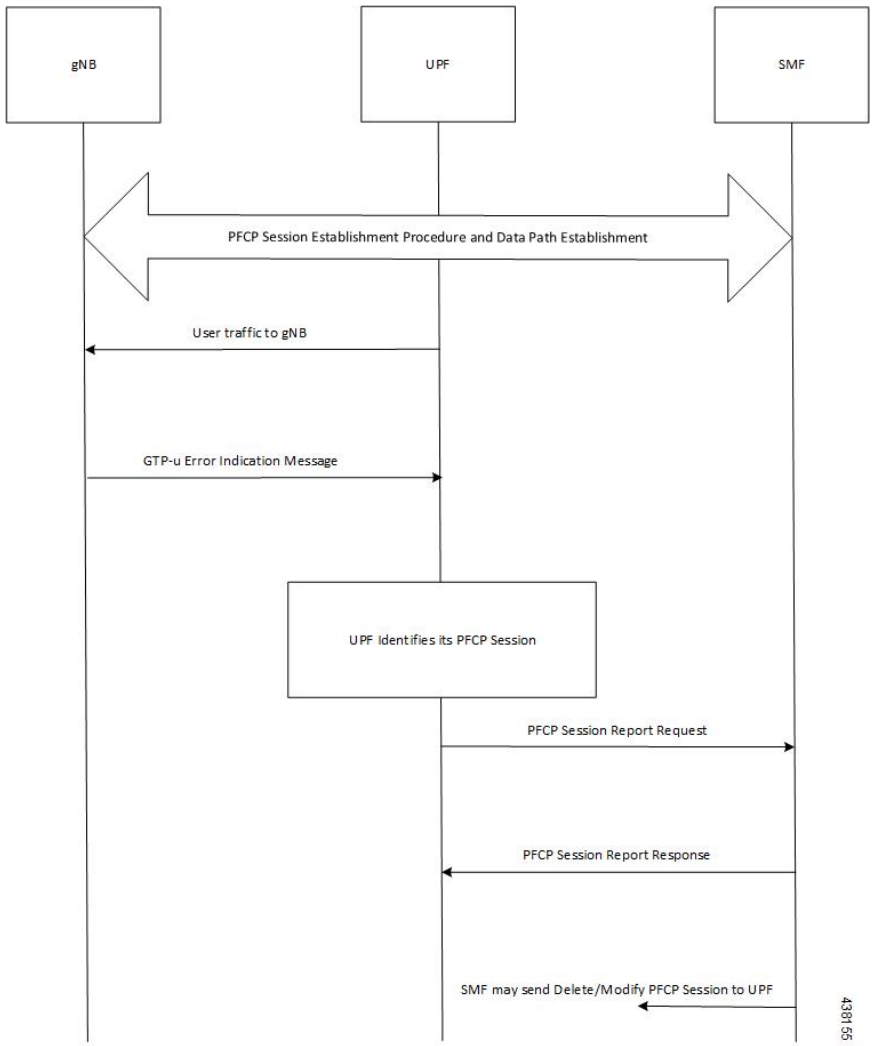
ステップ	説明
1	SMF は、PDU セッションの N4 セッションコンテキストを削除するためのトリガーを受信します。
2	SMF は、N4 session delete 要求を UPF に送信します。

ステップ	説明
3	UPF は、N4 Session ID が削除する N4 セッションコンテキストを特定し、セッションコンテキスト全体を削除します。UPF は、UPF が SMF に提供すべき情報を含む N4 session delete 応答メッセージで応答します。
4	SMF は、この手順をトリガーするネットワークエンティティとやり取りします。例：AMF または PCF。

N4 Session/Node-level Reporting 手順コールフロー

GTP-u Error Indication コールフローによるセッションレベルのレポート

UPF は、gNB から GTP-u Error Indication を受信すると、PFCP セッションを検出し、Error Indication Report IE とともにセッションする SMF ハンドリングに PFCP Session Report 要求を送信します。Error Indication IE には、GTP-u ピアアドレスと GTP-u Error Indication IE から受信した TEID を含むリモート F-TEID IE も含まれます。

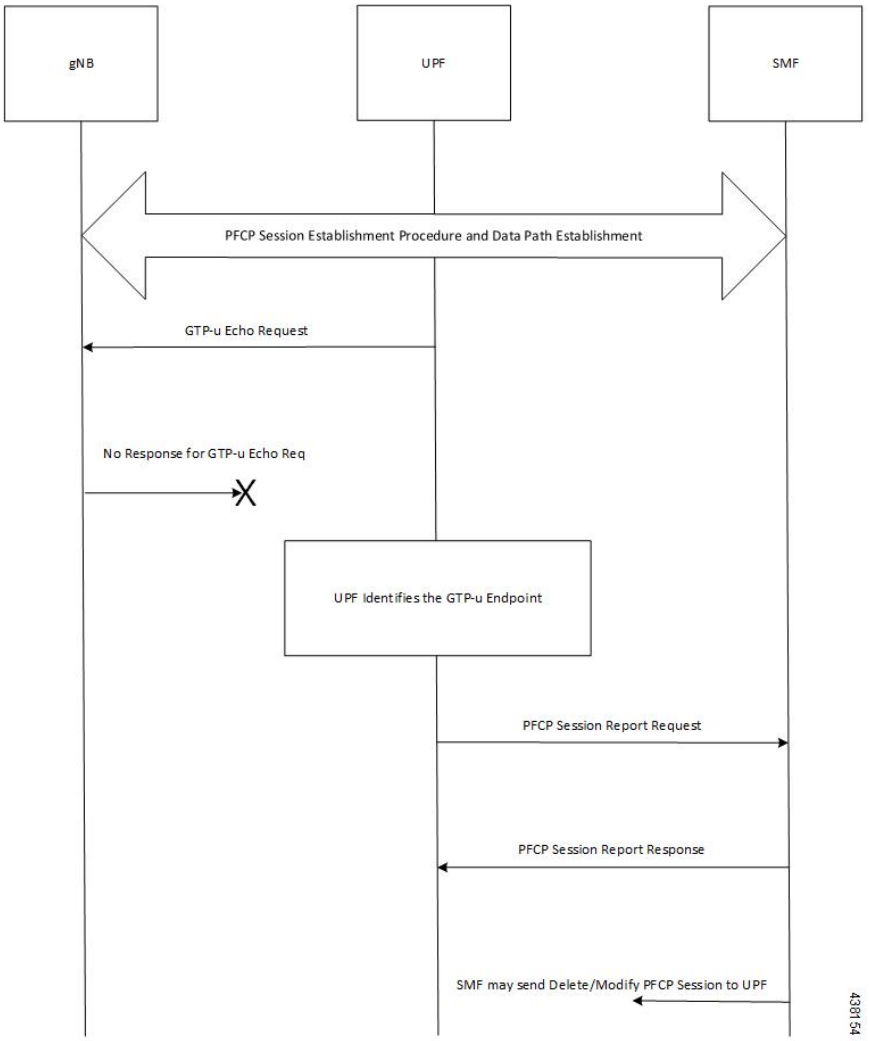


ステップ	説明
1	PFCP セッションが確立され、データ通信の実行が開始されます。
2	gNB は、何らかの理由で TEID の詳細をローカルでクリアすると、不明な TEID の UPF に GTP-u Error Indication を送信します。
3	Error Indication を受信すると、UPF は PFCP セッションを識別し、PFCP Session Report 要求を SMF に送信します。
4	Session Report 要求には、Error Indication を受信した TEID とリモートIP アドレスが含まれます。

GTP-u パス障害コールフローによる Node-level Reporting 手順

UPF は、GTP-u エンドポイントの GTP-u Echo 手順を有効にし、応答がないことが原因でデータ パス障害を特定すると、PFCP Node Report 要求を SMF に送信します。PFCP Node Report 要求のノードレポートタイプは、SMF に送信されるときにユーザープレーンパス障害レポートに

設定されます。Node Report 手順には、PFCP セッションに固有ではないため、Remote GTP-u Peer IE（User Plane Path Failure IE の子 IE）のピア IP アドレスのみが含まれます。



ステップ	説明
1	PFCP セッションが確立され、GTP-u Echo 手順が設定されると、UPF は、少なくとも 1 つの GTP-u トンネルを持つ各ピアに対して GTP-u Echo 要求を開始します。
2	指定された回数の再試行後に GTP-u Echo 応答を受信しない場合、UPF は PFCP Node Report 要求を SMF に送信します。
3	GTP-u トンネル固有の障害ではないため、ピア IP アドレスのみがノードレポート要求で送信されます。
4	メッセージを受信すると、SMF は、その gNB のすべての PFCP セッションの削除および変更要求を UPF に送信します。

PDN Update 手順：eNodeB F-TEIDu

機能説明

S-GW または SAEGW の場合、N4/Sx Modification 要求を開始する手順は、次に対して実装されます。

- eNodeB F-TEIDu Update
- eNodeB リリースへの Release Access Bearer（RAB）要求

機能の仕組み

PDN Update 手順には、eNodeB F-TEIDu Update/Release に関する次のイベントが含まれます。

- eNodeB F-TEIDu Update の場合：
  1. SGW-C は、MME から eNodeB F-TEIDu Update に対して Modify Bearer 要求を受信すると、N4/Sx Session Modification 要求を SGW-U に送信します。
  2. eNodeB F-TEIDu Update の N4/Sx Modification 要求には、「転送」の Apply Action が設定された Update FAR と Update Forwarding Parameters IE の一環である Outer Header Creation で更新された eNodeB IPv4/IPv6 アドレスが含まれます。
- eNodeB F-TEIDu Release の場合：
  1. SGW-C は、MME からの RAB 要求を受信すると N4/Sx Modification 要求を SGW-U に送信します。
  2. RAB は UE レベルのメッセージです。UE に複数の PDN 接続がある場合、N4/Sx Modification 要求が、各 PDN 接続に個別に送信されます。
  3. SGW-C は、宛先インターフェイスを ACCESS として、Update FAR を使用して Sx セッションに関する Sx Session Modification 要求を SGW-U に送信します。Update FAR には、FAR ID と Apply Action「Drop」が含まれます。宛先インターフェイスが CORE の FAR は更新されません。

標準準拠

PDN 更新手順は、次の標準規格に準拠しています。

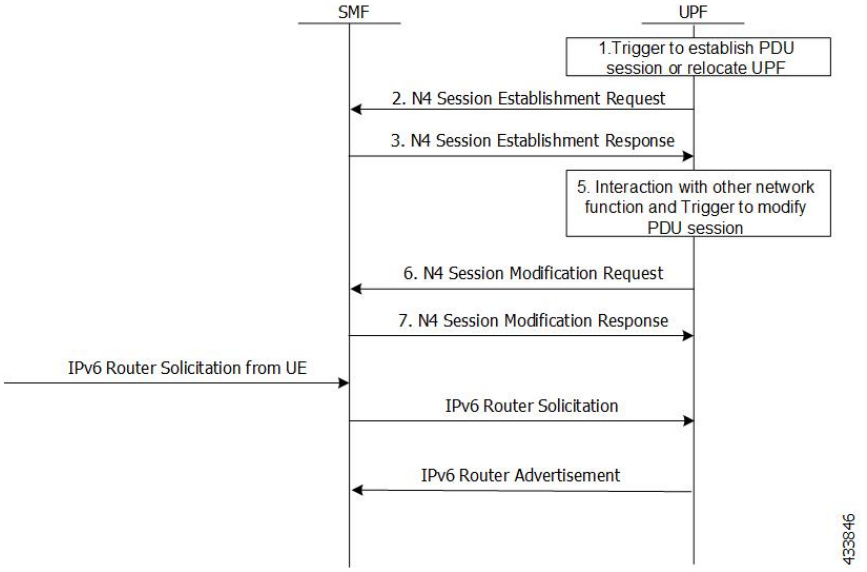
- 3GPP TS 23.401：「General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access」。
- 3GPP TS 29.274「3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3」
- 3GPP TS 29.244：「Interface between the Control Plane and the User Plane of EPC」。
- 3GPP TS 23.214：「Architecture enhancements for control and user plane separation of EPC nodes; Stage 2」。

• 3GPP TS 23.714：「Study on control and user plane separation of EPC nodes」。

UEs IPv4、IPv6 および IPv4v6 サポートコールフロー

IPv6 コールフローの N4 Session Establishment と Modification 手順

次のコールフローは、IPv6 の N4 Session Establishment と Modification 手順の概要を示しています。

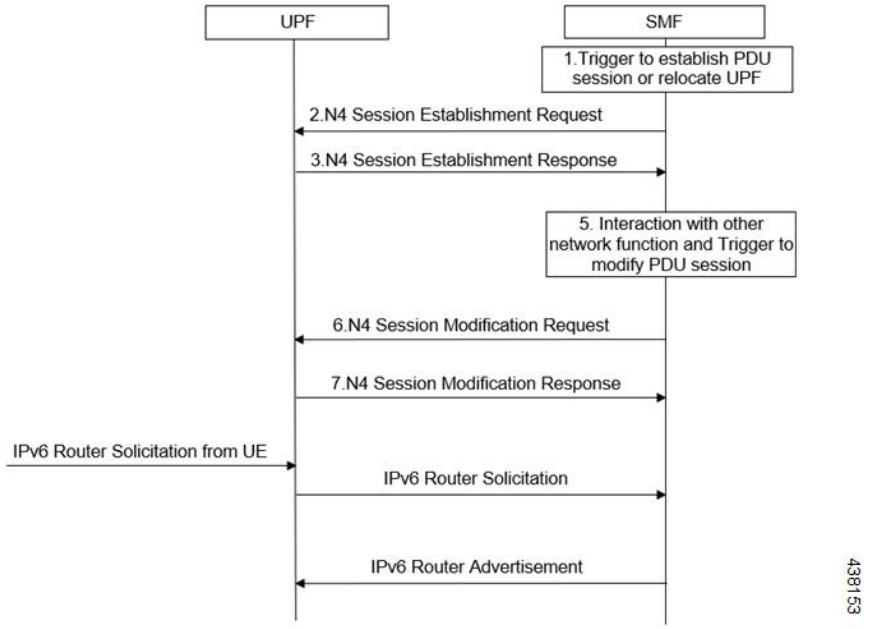


ステップ	説明
1	SMF は、新しい PDU セッションを確立するか、または確立された PDU セッションの UPF を変更するトリガーを受信します。
2	SMF は N4 Session Establishment 要求メッセージを UPF に送信します。UPF では Create PDR IE には IPv6 UE アドレスが含まれ、SDF フィルタには PDR を選択する IPv6 フィルタがあります。
3	UPF は、N4 Session Establishment 応答メッセージで応答します。これには、受信した制御情報に応じて UPF が SMF に提供する必要がある情報が含まれています。
4	SMF はネットワーク機能とやり取りし、PDU セッションを変更するためのトリガーを発生させます。
5	SMF は、N4 Session Modification 要求メッセージを UPF に送信します。これには、UPF がどのように動作する必要があるかを定義する構造化された制御情報が含まれます。

ステップ	説明
6	UPF は、N4 セッション ID が変更する N4 セッションコンテキストを定義します。次に、UPF は、SMF から送信されたパラメータのリストに従って、この N4 セッションコンテキストのパラメータを更新します。UPF は、N4 Session Modification 応答メッセージで応答します。これには、受信した制御情報に応じて UPF が SMF に提供する必要がある情報が含まれています。
7	IPv6 セッションでは、ルータ要請（RS）およびルータアドバタイズメント（RA）という追加の手順が必要です。セッションが確立されると、UE はネットワークに RS メッセージを送信してリンク層アドレスを取得します。UPF は、このメッセージを SMF に転送します。SMF は、UE の IPv6 アドレスを構成するために必要なパラメータを含む RA メッセージを送信します。
8	UPF と SMF 間の RS および RA は GTP-U でカプセル化され、SMF は Session Establishment と Modification 手順中に PDR の追加のペアを送信します。このペアでは、GTP-U トンネリング用の GTP-U トンネル ID が交換されます。
9	SMF から送信される追加の PDR のペアは次のとおりです： • 1 つの PDR には、アクセスとしての送信元インターフェイスと、UE から SMF に IPv6 RS を転送するための CP 機能としての接続先インターフェイスがあります。SDF フィルタが存在するため、UPF は UE から IPv6 RS に対してこの PDR を選択できます。 • 例：Permit in 58 from any tp ff01::2 any • 別の PDR には、CP 機能としての送信元インターフェイス、アクセスとしても接続先インターフェイスがあり、これは、SMF から UE に IPv6 RA を転送します。SDF フィルタが存在するのは、UPF が SMF からすべての IPv6 RA に対してこの PDR を選択できるようにするためです。 • 例：Permit out 58 from any to ff01::2 any
10	RS および RA 手順を完了すると、UE は PDN に IPv6 を送信します。

IPv4v6 コールフローの N4 Session Establishment と Modification 手順

次のコールフローは、IPv4v6 の N4 Session Establishment と Modification 手順の概要を示しています。



IPv4v6 Session Establishment と Modification 手順は、次の手順を除き、IPv6 Session Establishment と Modification 手順に似ています。

ステップ	説明
1	Session Establishment 要求では、IPv4 と IPv6 の両方の UE アドレスを含む PDR IE が作成されます。SDF フィルタには、PDR を選択するための IPv4 および IPv6 フィルタも含まれます。
2	IPv6 アドレスが UE に割り当てられている場合、追加の手順である Router Solicitation および Router Advertisement が必要です。セッションが確立されると、UE が Router Solicitation メッセージをネットワークに送信してリンク層アドレスを受信します。UPF はこのメッセージを SMF に転送し、SMF は UE の IPv6 アドレスを構成するために必要なパラメータを含む Router Advertisement メッセージを送信します。
3	UPF と SMF 間の RS/ RA は、GTP-u カプセル化されています。さらに、SMF は、Session Establishment と Modification 手順中に追加の PDR のペアを送信し、ここでは GTP-u トンネル ID が GTP-u トンネリング用に交換されます。
4	SMF から送信される追加の PDR のペアは次のとおりです： • UE から SMF に IPv6 Router Solicitation を転送する場合、1 つの PDR の送信元インターフェイスはアクセスに設定され、その接続先インターフェイスは CP 機能に設定されます。SDF フィルタは、UPF が UE からの IPv6 Router Solicitation に対してこの特定の PDR を選択するために存在します。 • たとえば、permit in 58 from any to ff01::2 any です。

ステップ	説明
5	RS/RA 手順が完了すると、UE は IPv6 通信を PDN に送信します。
6	この PFCP セッションの IPv4 通信に対して追加の手順は必要ありません。

N4 Session/Node-level Reporting 手順を構成する

この項では、N4 Session/Node-level Reporting 手順の構成方法について説明します。

GTP-u Echo Request 手順を有効にする

GTP-u Echo Request 手順を有効にするために、**gtpu-service** の既存の CLI（コマンド ライン インターフェイス）を使用します。

```
configure
   gtpu-service service_name
      echo-interval seconds
      echo-retransmission-timeout seconds
      max-retransmissions num
      path-failure detection-policy gtp echo
      end
```

注：

- **gtpu-service** *service_name*：GTP-u を作成し、現在のコンテキストに対して GTP-u サービス構成モードを開始します。*service_name* は、GTP-u サービスの名前を指定します。
- **echo-interval** *seconds*：GTP v1-u エコーパケットが送信されるレートを構成します。*seconds* は、GTP-uv1 エコーパケットの送信間隔を秒単位で指定します。60 ー 3600 の範囲の整数で指定する必要があります。
- **echo-retransmission-timeout** *seconds*：このサービスの GTP-u echo メッセージ再送信のタイムアウトを設定します。*seconds* は 、GTP-u サービスのエコー再送信タイムアウトを秒単位で指定します。1 ～ 20 の範囲の整数で指定する必要があります。デフォルト値は 5 です。
- **max-retransmissions** *num*：GTP-u echo 再送信の最大再試行回数を設定します。*num* は、パス障害エラー状態をトリガーする前に許可される GTP-u echo メッセージの再送信回数を指定します。0 ～ 15 の範囲の整数で指定する必要があります。
- **path-failure detection-policy gtp echo**：最大再試行回数分再送信された GTP-u echo メッセージのパス障害検出ポリシーを構成します。**.gtp echo** は、検出ポリシーを設定して、GTP-u echo メッセージの再送信最大回数に達した際に、障害を検出します。

次に、GTP-u Echo Request 手順を有効にするための設定例を示します。

```
configure
   gtpu-service n3-gtpu-service
```

```
  echo-interval 60
  echo-retransmission-timeout 5
  max-retransmissions 5
  path-failure detection-policy gtp echo
  end
```

N4 Session/Node-level Reporting 手順構成を確認する

この項では、N4 Session/Node Level Reporting 手順の構成を確認する方法について説明します。

N4 Session Node Level Reporting 手順の OA および M サポート

show gtpu statistics コマンドを使用して、Error Indication および GTP-u Echo 要求と応答の GTP-u 統計を表示します。次に、**show gtpu statistics** コマンドの出力例を示します。

```
show gtpu statistics
Path Management Messages:
    Echo Request Rx:                  0 Echo Response Rx:            7
    Echo Request Tx:                 19 Echo Response Tx:            0
    SuppExtnHdr Tx:                   0  SuppExtnHdr   Rx:            0

  Peer Stats:
    Total GTPU Peers:                              1
    Total GTPU Peers with Stats:                   1

  Tunnel Management Messages:
    Error Indication Tx:                           0
    Error Indication Rx:                           0
    Error Indication Rx Discarded:
```

show sx-service statistics all コマンドを使用して、ノードレポート要求と応答統計を表示します。次に、**show sx-service statistics all** コマンドの出力例を示します。

```
show sx-service statistics all
Node Report Request:
 Total TX:                          1   Total RX:                      0
 Initial TX:                        1   Initial RX:                    0
 Retrans TX:                        0   Retrans RX:                    0
 No Rsp received TX:                0   Discarded:                     0

Node Report Response:
 Total TX:                          0   Total RX:                      1
 Initial TX:                        0   Initial RX:                    1
 Accepted:                          0   Accepted:                      1
 Denied:                            0   Denied:                        0
 Retrans TX:                        0   Discarded:                     0
```

show user-plane-service statistics all コマンドを使用して、N4 PFCP メッセージパラメータの統計を表示します。次に、**show user-plane-service statistics all** コマンドの出力例を示します。

```
show user-plane-service statistics all
N4 Statistics:
    URR : Created        :              0
          Deleted        :              0
          Queried by ID  :              0
          Queried by all :              0
          Total Queried  :              0
    FAR : Created        :              0
          Updated        :              0
```

```
      Removed        :              0
PDR : Predef rule    :              0
```

（注） 統計は累積され、すべてのセッションマネージャの合計として表示されます。

フィールドの説明を次に示します。

- 作成済みURR：ローカルまたはSMFの要求により作成されたURRの総数を表示します。
- 削除された URR：ローカルまたは SMF の要求により削除された URR の総数を表示します。
- ID でクエリされた URR：具体的な ID を使用して URR のサブセットをクエリするために受信したメッセージの総数を表示します。
- すべてでクエリされた URR：セッションのすべての URR をクエリするために受信したメッセージの総数を表示します。
- クエリされたURRの合計：[IDでクエリ（Queried by ID）]および[すべてでクエリ（Queried by all）] の応答として SMF に報告された URR の総数を表示します。
- 作成済み FAR：作成された FAR の総数を表示します。
- 更新済み FAR：更新された FAR の総数を表示します。
- 削除済み FAR：削除された FAR の総数を表示します。
- PDR 事前定義ルール：事前定義されたルールが設定された CREATE PDR の総数を表示します。1 つの事前定義済みルールの場合、2 つの PDR を受信しているため、カウンタは 2 に更新されます。

（注） 事前定義されたルールが削除されても、事前定義カウンタの合計は更新されません。SMFは、事前定義されたルール名を含まないRemove PDR メッセージのみを送信します。既存の事前定義ルールの場合、HO 時に、PDR が削除され、再度作成されます。これにより、同じセッションに対してPDRが2回カウントされます。

SNMP トラップ

次のトラップを使用して、状態および条件の GTP-u パス障害を追跡できます。

- EGTPUPathFailure：このトラップは、GTP-u Echo 要求に対する応答を受信せず、ピア EPC ノードへのデータパス障害が検出された場合に生成されます。
- EGTPUPathFailureClear：このトラップは、ピアノードへのデータパスが知用可能な場合に生成されます。

グレースフル セッション終了の拡張された PFCP 関連付けのリリース手順

表 *80 :* 機能の履歴

機能	リリース	説明
UPF からの PFCP Association Update 要求の開始	2024.03.0	この機能により、UPF は PFCP Session Release の通知を cnSGWc および SMF に送信します。UPF 通知は、UPF および SMF または UPF および cnSGWc で同時にコールをクリアすることを示します。 SMF または cnSGWc に通知されない場合、UPF が cnSGWc から次の Session Modify 要求を受信するまで、コールは接続されたままになります。これにより、回線の使用状況レポートが失われます。ここで、Enhanced PFCP Association Release（EPFAR）機能により、シグナリングの効率と、SMF または cnSGWc による使用状況レポートの効果的な処理が向上します。 **デフォルト設定**： 無効：有効にするには構成が必要

UPF がエラーまたは部分的なセッションの障害によりコールをクリアすることを決定すると、UPF はコールのクリアについて SMF または cnSGWc に通知せずに、コールをローカルでクリアします。UPF が SMF または cnSGWc から次の Session Modification 要求を受信するまで、コールは接続されたままになります。

コールクリア中の使用状況レポートの損失を防ぎ、シグナリング効率を向上させるために、UPF に Enhanced PFCP Association Release（EPFAR）機能を適用し、Session Report 要求を開始して、UPF と SMF または、UPF と cnSGWc び間のセッションを同時に正常にクリアします。この機能は、3GPP TS 29.244 のリリース 16.9.0、セクション 5.18.1 およびセクション 5.18.2 に準拠しています。

EPFAR 交渉

EPFAR 機能の交渉は、UPF および SMF または UPF および cnSGWc 間の集約通信です。UPF および SMF または UPF および cnSGWc が EPFAR 機能をサポートしている場合、セッションとアソシエーション解除アクションが実行されます。UPF が SMF および cnSGWc とのアソシエーションを解除する必要がある場合は、構成コマンドを使用して EPFAR 機能を有効にすることができます。

アソシエーション解除プロセスには、次の手順が含まれます。

1. UPF が開始した PFCP セッションのリリース
2. UPF によって開始された拡張 PFCP 関連付けのリリース

UPF が開始した PFCP セッションのリリース

UPF-initiated PFCP Session Release プロセスは、これらの手順に従って実行されます。

1. UPF は、Association Setup 手順中にネゴシエートされた場合、ピアノードに対して EPFA 機能を有効にします。UPF は、エラーまたは部分的な障害により PFCP セッションを削除する必要がある場合、影響を受けるセッションの PFCP Session Report 要求を開始します。SMF は、Report Type and Usage Report Trigger IE と共に、PFCP Session Report 要求を SMF または cnSGWc に送信します。
   - PFCP セッションの使用状況がゼロ以外のレポートがある場合、レポート タイプは USAR（使用状況レポート）に設定され、送信する使用状況レポートがない場合は UISR（UP 開始セッション要求）に設定されます。
   - 使用状況レポートがゼロ以外の場合、Usage Report Trigger を TEBUR（Termination By UP function Report）に設定します。
2. UPF は、PFCP セッション レポート要求メッセージでピア ノードに原因 IE を送信します。Cause IE は、次の値を使用してセッション削除の原因を伝達します。
   - 201：サブスクライバによるクリア
   - 202：UP によって開始された関連付けのリリース
   - 203：復元失敗
   - 204：IP ソース違反
   - 205：PFCP 原因自己保護での終了
3. UPF が PSDBU（PFCP セッションが UP 機能によって削除されました）フラグを 1 に設定して、PFCP セッションの削除を示します。
4. UPF は、SMF または cnSGWc から PFCP Session Report 応答を受信し、UPF と SMF または UPF と cnSGWc でセッションをローカルに削除します。

（注） SMF には、1 秒あたり 500 セッションの明確なレート制限があります。したがって、セッションレポートのスロットルレートは UPF のインターフェイスごとに 500 セッションに維持されます。

UPF でサブスクライバセッションをクリアする

UPF でサブスクライバセッションをクリアするには、**clear subscribers all** コマンドの **pace-out-interval** 値を入力します。

手順

ステップ 1 式を使用して、**pace-out-interval** 値を計算します。

例：

```
pace_per_sessmgr = throttle rate / num_of_smgr
pace-out-interval = max session in one smmgr / pace_per_sessmgr

Throttle Rate = 500 sessions / second
Subscriber data-rate = 203000
Total number of smgrs = 22
pace_per_sessmgr = throttle rate / num_of_smgr = 500 / 22 = 22
pace-out-interval = maximum sessions in one smmgr / pace_per_sessmgr = (203000 / 22) / 22  = 420
```

ステップ 2 コマンドに対して、**pace-out-interval** 値を入力します。

例：

```
[local]upf# clear subscribers all pace-out-interval pace-out-interval

[local]upf# clear subscribers all pace-out-interval 420
```

原因レベルの統計を確認する

show sx-service statistics all コマンドを使用して、ノードレベルの統計からの原因レベルの情報を検証します。

手順

show コマンドを入力して、原因レベル情報を表示します。

例：

```
[local]qvpc-si# show sx-service statistics all

Session Management Messages:
...
...
```

```
...
Session Report Request:
 Total TX:                                350   Total RX:                    0
 Initial TX:                              0   Initial RX:                  0
 Retrans TX:                              0  Retrans RX:                   0
 Discarded:                               0  No Rsp RX:                    0
 Causes:
     User Initiated Session Deletion from UP  36
     Association Release initiated by UP      310
     Recovery Failure                         0
     IP Source Violation                      4
```

UPF によって開始された拡張 PFCP 関連付けの解除

1. SMF または cnSGWc および UPF の両方が、EPFAR 機能をサポートする場合、UPF は、PFCP Association Release の UPF から、PARPS（PFCP Association Release Preparation Start）フラグが設定されている PFCP Association Report リクエストを開始するか、SMF または cnSGWc は、UPF の選択を停止します。
2. UPF は、PFCP Session Release 手順を開始し、すべてのレポートが送信されたら、UPF は、PFCP Association Update 要求を送信し、影響を受ける PFCP Sessions Sent に対して、URSS（ゼロではない使用状況レポート）フラグを 1 に設定します。
3. SMF または cnSGWc から正常な Update 応答を受信すると、UPF は、構成可能な正常なクリーンアップ タイマーを開始し、アソシエーションを解除します。構成コマンドを使用して解除タイマーを有効にすると、タイマーをセットできます。SMF または cnSGWc は、影響を受けるセッションの削除を開始します。
4. UPF は、SMF または cnSGWc から PFCP Association Update 要求を受信すると、タイマーを停止してアソシエーションを解放します。そうでない場合、UPF はタイマーの期限切れ後にアソシエーションを解除します。

（注） セッション レポートのスロットル レートは、Association Release 手順の UPF でピアインターフェイスごとに 500 セッションで維持されます。

EPFAR なしの PFCP Association Release

ピアノードが EPFAR 機能をサポートしていないか、EPFAR がUPF で有効でない場合、PFCP Association Release は、これらの手順で実行されます。

1. PFCP Association Release は、構成コマンドを使用して、UPF で開始されます。
2. UPF は、PFCP Association Release Request IE で SARR フラグが設定された PFCP Association Update 要求を送信します。
3. UPF は、SMF または cnSGWc から Update 応答を受信した後、タイマーを開始します。SMF または cnSGWc は、影響を受けるセッションを削除します。

4. タイマーが期限切れになると、UPF は影響を受けるすべての PFCP セッションと PFCP アソシエーションをローカルで削除します。

EPFAR 機能の有効化

sx-protocol supported-features epfar コマンドを使用して、UPF で EPFAR 機能を有効にします。

手順

ステップ 1 UP で、コンテキスト構成モードを開始します。

例：

[local]UPF1(config)# **context EPC2-UP**

ステップ 2 Sx サービスモードで、*service-name* と入力します。

例：

[EPC2-UP]UPF1(config-ctx)# **sx-service name** *service_name*

ステップ 3 UPF で EPFAR を有効にして、セッションまたはアソシエーションの解除を開始します。デフォルトでは、EPFAR 機能は無効状態です。

例：

[EPC2-UP]UPF1(config-sx-service)# **sx-protocol supported-features epfar**

no sx-protocol supported-features epfar コマンドを使用して、EPFAR を無効にします。

ステップ 4 設定を保存します。

ステップ 5 show コマンドを使用すると、EPFAR 機能が有効か無効かを確認できます。

例：

```
[local]qvpc-si# show sx peers full address 192.0.2.0
  Peer IP                     : 192.0.2.0
  Sx Service Id               : 5
  Group Name                  : cp1
  Current Session             : 0
  Max Session                 : 0
  Negotiated feature
  Load Control                : Disabled
  Overload Control            : Disabled
  EPFAR                 : Enabled
```

Sx サービスのアソシエーション解除を開始する

clear sx-association peer-node-id ipv4-address コマンドは、UPF の IPv4 または IPv6 ピアノード ID と Sx アソシエーションのアソシエーション解除を開始します。

手順

peer-node-id に Sx association と入力し、IPv4 または IPv6 ピアの IP アドレスを指定します。

例：

```
[local]UPF1# clear sx-association peer-node-id ipv4-address
 IPv4 Address
[local]UPF1#clear sx-association peer-node-id ipv6-address
 IPv6 Address
clear sx-association peer-node-id ipv4-address 192.0.2.0
```

アソシエーションの解除タイマーを有効にする

sx-protocol association release-timeout コマンドを使用すると、UPF のアソシエーションの解除タイマーを有効にできます。

手順

ステップ 1 UP に対して Context Configuration mode コマンドを開始します。

例：

```
[local]UPF1(config)# context EPC2-UP
```

ステップ 2 Sx サービスモードで *service-name* と *release-timer* と入力します。タイマーは 30 ～ 900 秒の範囲で設定できます。release-timeout のデフォルト値は 90 秒です。

例：

```
[EPC2-UP]UPF1(config-ctx)# sx-service epc
[EPC2-UP]UPF1(config-sx-service)# sx-protocol association release-timeout 100
```

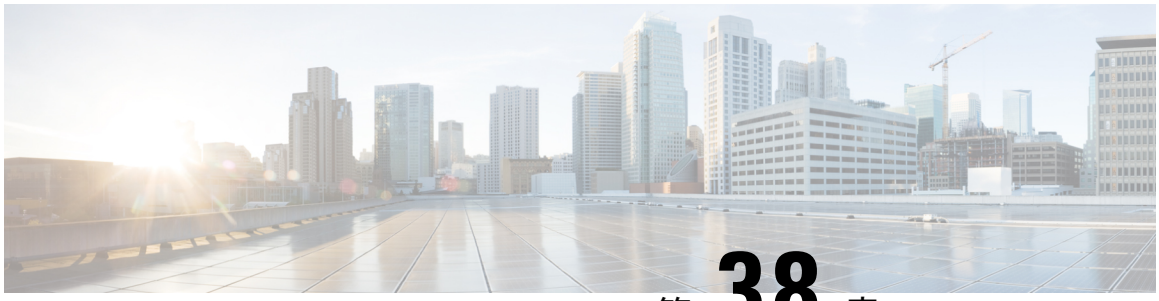
ステップ 3 show コマンドを入力して、Sx サービスに関するアソシエーションの解除タイムアウトとEPFAR 機能情報を確認します。

例：

```
[local]qvpc-si# show sx-service name sxu

  Service name                          : sxu
  Service-Id                            : 4
  Context                               : ingress
  ...
  SX Association Reattempt Timeout      : 900 (sec)
  SX Association Release Timeout        : 30 (sec)
  ...
  SX PDI Optimisation                   : Enabled
```

```
Supported Features :
     EPFAR                          : Enabled
```



第 38 章

NRF のサポート

- 機能の概要と変更履歴 （441 ページ）
- 機能説明 （442 ページ）
- 機能の仕組み （443 ページ）
- NRF 管理サービスを構成する （444 ページ）
- モニタリングおよびトラブルシューティング （446 ページ）

機能の概要と変更履歴

要約データ

表 *81* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

表 *82* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.04.0

機能説明

5Gサービスベースのアーキテクチャでは、ネットワークリポジトリ機能（NRF）が、オペレータのネットワークで使用可能なすべての5Gネットワーク機能（NF）の更新されたリポジトリを維持します。NRFには、5G NFによって提供されるサービスの詳細も含まれており、5G NFは、手動による介入なし、または手動介入を最小限に抑えて、インスタンス化、スケーリング、および終了できます。

NRFは、5Gコアネットワーク内のすべてのNFと相互作用し、次のサービスを提供します。

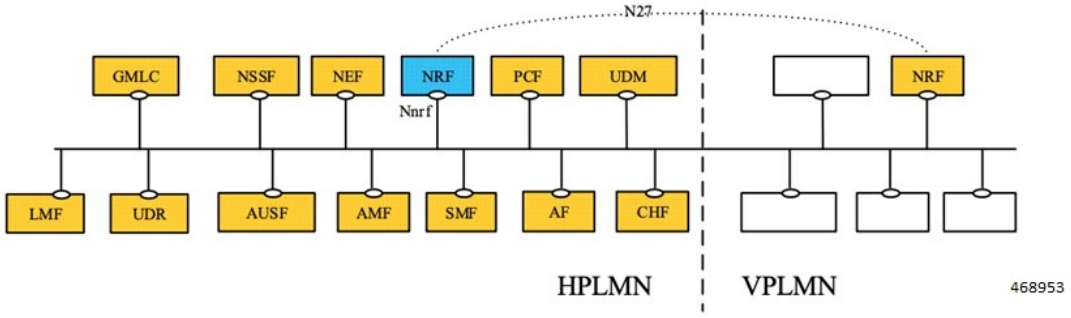
- 管理サービス
- 検出サービス
- OAuth2承認
- ブートストラップ

UPFは、NRF管理サービスのみをサポートします。

NRF管理サービス

NRF管理（Nnrf_NFManagement）サービスは、稼働中のPLMNのNFインスタンスを有効にして、NRFでプロファイルを登録、更新または登録解除します。ここで説明されているNFインスタンスとは、UPF StarOSベースのインスタンスのことです。

図 *24 : NRF* 管理



現在、Nnrf_NFManagementサービスは次の操作を提供します。

- **NFインスタンスを登録する**（NFRegister）：NFインスタンスは、提供するサービスのリストとともに、NRFにそのプロファイルを登録します。
- **NFインスタンスを更新する**（NFUpdate）：NFインスタンスは、NRFのNF profileパラメータを部分的に更新または置き換えます。また、提供されているサービスも追加または削除します。

  現在、NFUpdateは、次の操作をサポートしています。

- NF プロファイルの属性の更新
- NF のハートビート

- **NF インスタンスを登録解除する**（NFDeregister）：NF インスタンスは、その NF プロファイルと、5G ネットワークで提供するサービスの登録を解除します。

機能の仕組み

この機能により、UPF と NRF の間で管理サービスが有効になります。

UPF 登録

最小限の構成が完了すると、UPF は NRF に対する登録手順をトリガーします。Nrfmgr proclet は SessCtrl から設定を受信し、優先順位が最も低いエンドポイントを選択します。Nrfmgr が再試行のために NRF からの応答を受信しない場合、Nrfmgr は次に優先順位が低いエンドポイントを選択します。このプロセスは、すべてのエンドポイントで無限に続行されます。このプロセスを停止するには、構成を削除する必要があります。

UPF ハートビート

登録が完了すると、Nrfmgr は「nr hb-enable」オプションが設定されているかどうかを確認します。「nr hb-enable」がすでに構成されている場合、Nrfmgr は Heartbeat 要求メッセージを作成または送信します。Nrfmgr は、ピア NRF から受信したハートビートタイマー値を使用してタイマーを開始します。ハートビートタイマー値まで Heartbeat 応答が受信されない場合、Nrfmgr は次に優先順位番号が小さいエンドポイントを選択します。このプロセスは、すべてのエンドポイントに対してround-robin方式で無限に続行されます。このプロセスを停止するには、構成を削除する必要があります。

UFP 登録解除

構成が削除されると、UPF は Nrfmgr から NRF に NRF Deregistration を送信し、NRF は、UPF の登録を解除します。

標準準拠

NRF サポート機能は、*3GPP TS 29.510 "5G System; Network function repository services; Stage 3"* に準拠しています。

NRF 管理サービスを構成する

NRF プロファイルの構成

NRF プロファイルの構成により、UPF には NRF に送信する必要があるオプションのパラメータを定義する柔軟性または制御が提供されます。たとえば、NNRF Mgmt プロファイルでローカリティを構成し、NF プロファイルが NNRF サービスに関連付けられている場合、ローカリティは NRF に送信されます。

UPF で NRF プロファイルを設定するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    user-plane-nnrf
      nnrf-mgmt-format profile_name
        priority number
        locality string
        sst sst_number [ sd sd_number ]
        smf-serving-area area_n
      exit
    exit
```

注：

- **user-plane-nnrf**：UPF NRFプロファイルを構成します。
- **nnrf-mgmt-format** *profile_name*：NNRF 管理プロファイルを構成して、NRF に送信するパラメータを制御します。
- **priority** *number*：UPF の優先順位を指定します。構成されている場合、値は NRF に送信されます。

  number は、1 ～ 100 の整数で指定する必要があります。デフォルト：NRF に値は送信されません。
- **locality** *string*：UPF のローカリティを指定します。構成されている場合、この値が NRF に送信されます。*string* の最大長は、63 バイトです。
- **sst** *sst_number* **[sd** *sd_number* **]**：UPF のスライス情報を指定します。構成されている場合、この値が NRF に送信されます。

  sst *sst_number* は、0 ～ 255 の整数で指定する必要があります。デフォルト：スライス/SST は NRF に送信されません。

  sd *sd_number* は、0 ～ 16777215 の整数で指定する必要があります。構成されていない場合、SD は NRF に送信されません。
- **smf-serving-area** *area_n*：UPF の SMF サービス提供先を指定します。最大 5 つの SMF エリアを構成できます。

  area_n の最大長は、63 バイトです。構成されている場合、値は NRF に送信されます。

NRF サービスの構成

UPF で NRF サービスを構成するには、次の CLI コマンドを使用します。

```
configure
  context context_name
    nnrf-nfm-service service_name
      associate nnrf-mgmt-format profile_name
      uri-scheme { http | https }
      hb-enable
      retransmission-timeout timeout_value
      max-retransmissions max_retries
      certificate path [ key path ] [ ca-certificate path ]
      endpoint-name endpoint_name
        priority number
        ipv4-address ipv4_address [ portv4 port_number ] [ ipv6-address
ipv6_address ] [ portv6 port_number ]
        exit
      bind ipv4-address ipv4_address [ portv4 port_number ] [ ipv6-address
ipv6_address ] [ portv6 port_number ]
    exit
    user-plane-service userplane_service
      associate nnrf-nfm-service service_name
      nf-instance-id number
    exit
  exit
exit
```

注：

- **nnrf-nfm-service** *service_name*：NRF サービスを構成します。
- **associate nnrf-mgmt-format** *profile_name*：NNRF 管理プロファイル構成を関連付けます。関連付けられていない場合、*priority/slice/smfarea* などのプロファイル構成は、NFMgmt メッセージで NRF に送信されません。
- **uri-scheme { http | https }**：NRF（HTTP または HTTPS） にメッセージを送信するために使用される URI スキーマを指定します。デフォルト値：HTTP
- **[no] hb-enable**：NRF への Heartbeat メッセージを有効または無効にします。
- **retransmission-timeout** *timeout_value*：エンドポイントが NRF にメッセージを送信するための再試行タイマー間隔を秒単位で指定します。 *timeout_value* は、1 ～ 100 の整数で指定する必要があります。デフォルト値：15 秒。
- **max-retransmissions** *max_retries*：NRF にメッセージを送信するための最大再試行回数を指定します。*max_retries* は、1 ～ 20 の整数で指定する必要があります。デフォルト値：3 回の再試行。
- **certificate** *path* **[key** *path* **] [ca-certificate** *path* **]**証明書または CA 証明書およびキー URL へのパスを指定します。

- **endpoint-name** *endpoint_name*：NRF エンドポイントを指定します。UPF から NRF へのメッセージをトリガーするには、少なくとも 1 つのエンドポイントを構成する必要があります。
- **priority** *number*：NFR のエンドポイント優先順位を指定します。

  number は、1 ～ 100 の整数で指定する必要があります。デフォルト値：50。
- **bind ipv4-address** *ipv4_address* **[portv4** *port_number* **] [ipv6-address** *ipv6_address* **] [portv6** *port_number* **]**：NRF への IPv4 アドレスまたは IPv6 アドレスをバインドします。この構成は、UPF から NRF へのメッセージをトリガーために必要です。構成されている場合、IPv6 は IPv4 よりも優先されます。
- **user-plane-service** *userplane_service*：**user-plane-service** から **nnrf-nfm-service** のアソシエーションと NF インスタンスを定義します。この構成は、UPF から NRF へのメッセージをトリガーために必要です。
- **associate nnrf-nfm-service** *service_name*：関連する **nnrf-nfm-service** サービスを指定します。
- **nf-instance-id** *number*：UUID フォーマットで NF インスタンス ID を指定します。

モニタリングおよびトラブルシューティング

この項では、この機能のモニタリングと障害対応で使用できる CLI コマンドについて説明します。

show コマンドと出力

この項では、この機能の clear コマンドと show コマンドについて説明します。

- **clear nrf statistics**
- **show nrf statistics**
- **show nrf nnrf-nfm-service all**
- **show nrf nnrf-nfm-service name** *service_name*

  次に、このコマンドの出力例を示します。

```
  Service name:             nrf-svc1
 VPN Name / Id:             ingress / 2
  State       :             Started
  Timer Value :             15
  Max Retries :             3
  Heartbeat   :             Enabled
 Bind IPv4Addr:             209.165.201.2
 Bind IPv4Port:             0
 Bind IPv6Port:             0
   URI Scheme :             HTTPS
   NRF profile:             prof1
```

- **show nrf nnrf-nfm-service name** *service_name* **statistics**

次に、このコマンドの出力例を示します。

```
Service  name:             nrf-svc1
  Curr Endpoint:             end1
  Curr State   :             NRFMGMT_STATE_PENDING_REG

Statistics for endpoint name end1
=====================================================================

Num PUT Req      : 3                    Num PATCH Req           : 0

Num PUT Success  : 0                    Num PATCH Success       : 0

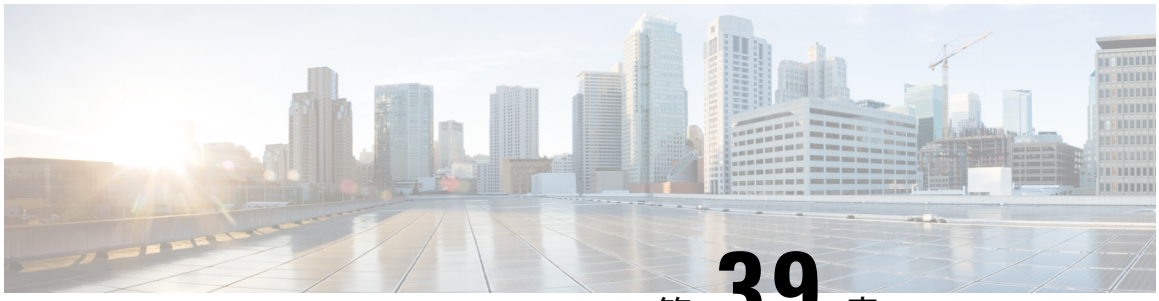
Num PUT Failed   : 3                    Num PATCH Failed        : 0

Num DEL Req      : 0               Last Conn Req Time      : 2022-08-05+19:11:14

Num DEL Success  : 0                    Last Conn Resp Time     : NA

Num DEL Failed   : 0
```

- **mon-pro support** *18*



第 39 章

パスワード期限切れ通知

- 機能の概要と変更履歴 （449 ページ）
- 機能説明 （450 ページ）
- Save Configuration コマンドを使用したアップグレードとダウンロードの手順 （451 ページ）

機能の概要と変更履歴

要約データ

表 *83* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点：	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

表 *84* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.0

機能説明

データの有効期限が切れる前に、パスワードがリセットされない場合、UPDからロックされます。管理者が手動でパスワードをリセットした場合のみ、再度ログインできます。

StarOS は、コンテキスト、AAA、および RADIUS ユーザーにパスワードの有効期限通知を送信します。UPFは、管理者、設定管理者、インスペクタ、およびオペレータのパスワードの設定と有効期限をサポートします。次のプロビジョニングがサポートされています。

- パスワードの警告間隔を指定します。パスワードの有効期限に関する警告が表示されます。
- パスワード猶予期間を指定します。この猶予期間中、ユーザーは毎回管理者に連絡するのではなく、自身でパスワードを変更できます。
- 警告間隔と猶予期間については、コンテキストの下にグローバル設定があります。ユーザーレベルの設定でこれらの値のいずれも指定されていない場合は、コンテキストのグローバル値が有効になります。

パラメータのデフォルト値は、セキュリティガイドラインに従っています。

- 有効期限間隔：パ氏の最大有効期限（デフォルト：90 日）
- 警告間隔：パスワードの有効期限が切れるまでの警告機関（デフォルト：30 日）パスワードの有効期限が近づいていることに関する警告が表示されます。パスワードを変更せずに続行できます。
- 猶予間隔：パスワードの有効期限が切れた後も、旧パスワードを使用できる日数。猶予期間を過ぎると、古いパスワードではログインできなくなります。管理者がパスワードをリセットする必要があります。

次に例を示します。

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

パスワード有効期限通知のアップグレードおよびダウングレード強化

パスワード有効期限通知機能によって、**max-age**、**exp-grace-interval**、**exp-warn-interval** などのさまざまな新しいキーワードがサブスクライバ構成に導入されました。これらの新しいパラメータは、コンテキスト グローバル レベルで設定されます。コンテキスト グローバル レベルのパラメータは、ユーザーレベルごとの設定がデフォルト値で設定されていない場合に使用されます。たとえば、パスワードの **max-age** の場合、デフォルト値は 90 日です。

ユーザーレベルごとに「有効期限」が設定されていないユーザープロファイルの場合、スタートアップ構成では、そのユーザーの有効期限が 90 日になります。この問題はスタートアップ構成ファイルを手動で編集することで解決できますが、ユーザーが複数の場所に分散している場合はこのソリューションによって問題が発生します。

ダウングレードが必要な場合、新しいキーワードが古いリリースでは無効になるため、ユーザープロファイルは失われます。

パスワード有効期限通知の機能強化に伴い、アップグレード手順が更新され、新しい **save config** CLI オプション、**legacy-password-expiry** を使用してダウングレードプロセスが変更されます。

Save Configuration コマンドを使用したアップグレードとダウンロードの手順

次のアップグレードプロセスを使用します。

- アップグレードの前に、スタートアップ構成でユーザーが設定されているすべてのコンテキストで、コンテキストレベルで **no password max-age** コマンドを追加します。
- 更新されたスタートアップ構成を使用してイメージをリロードする場合、有効期限なしで設定されているすべてのユーザーは、デフォルトでコンテキストレベルの設定を取得し、ユーザーレベル **no-max-age** キーワードを自動的に設定します。

次のダウングレードプロセスを使用します。

保存されていない新しいキーワードに基づいて、save config コマンドで、新しい CLI オプションである **legacy-password-expiry** を使用します。構成は、以前のリリースで認識される形式で保存されます。

次のプロンプトが Exec モードで表示されます。

```
configure
   context host_name
      save configuration url [ confd | ignore-locks | obsolete-encryption
 | showsecrets | verbose ] [ -redundant ] [ -noconfirm ] [
legacy-password-expiry ]
```

注：

- **save configuration** *config-file-path* **legacy-password-expiry**：

新しい Expiry Notification キーワードを削除して、後方互換性ファイルを生成します。**save config** CLI オプションにより、古い UPF バージョンとの構成の互換性が確保されます。



第 40 章

UPF での QCI 80 のサポート

- 機能の概要と変更履歴 （453 ページ）
- 機能説明 （454 ページ）
- 機能の仕組み （454 ページ）
- ADC ルールを構成する （456 ページ）
- モニタリングおよびトラブルシューティング （458 ページ）

機能の概要と変更履歴

要約データ

表 *85* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

表 *86* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.1

機能説明

5G-UPFは、アプリケーションが特定の接続先に通信を送信するときにGBR QoS以外のフローを確立するため、3GPP TS 23.203 に基づく新しい標準規格 QoS Class Index (QCI) 80 をサポートします。

機能の仕組み

検出された通信に基づくダイナミック QoS フローの確立

通信の検出時にダイナミック QoS フローを確立するために、UPF は Gx を介したアプリケーションの検出と制御（ADC）機能を使用します。

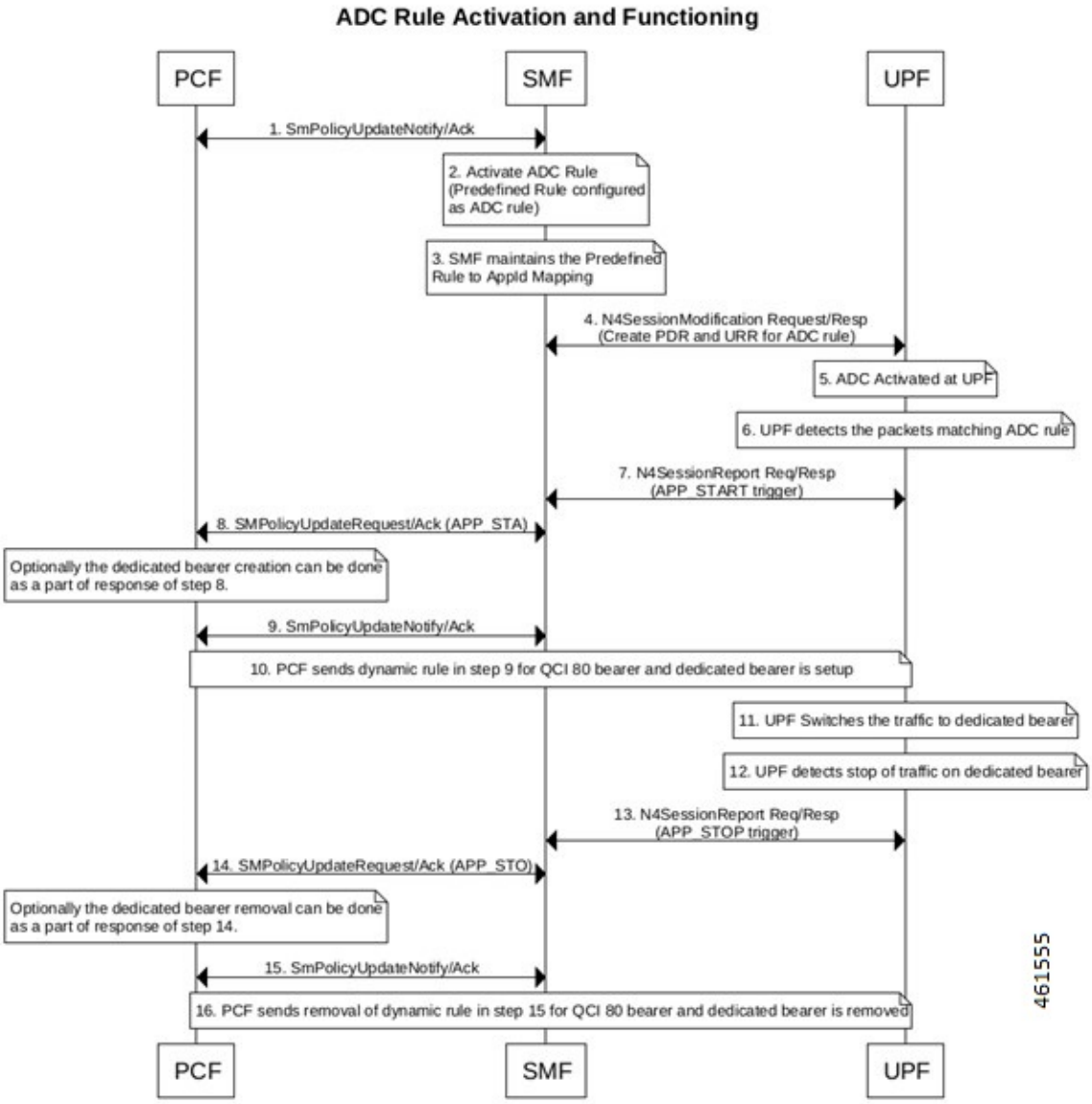
アプリケーションの検出と制御のためにデフォルトの 5G QoS 識別子（5QI）を介した PCC 事前定義済みルールを受信すると、SMF はアプリケーション通信を検出するように UPF に指示します。UPFはデフォルトのQFIを使用してGx ADC PDRをインストールし、ルール名はSMFに報告するためのアプリケーション ID と見なされます。

Gx ADC の事前定義ルールにヒットする新しいフローを検出すると、UPF は Application Start イベントをトリガーします。アプリケーション通信が、アプリケーション識別子によって特定されると、SMF は、アプリケーションの開始を PCF に報告します。

次に、PCF は、受信した情報に基づいてポリシーを決定し、対応する更新された PCC ルール（QCI-80）を SMF に送信します。

通話フロー

次の図は、5G コアシステムでのコールフローの詳細とメッセージ交換を示しています。



ステップ	説明
1	PCF は SmPolicyUpdateNotify を SMF に送信し、確認応答を受信します。
2	SMF が ADC ルール（事前定義されたルール）をアクティブにします。
3	SMF は、アプリケーション ID マッピングの事前定義されたルールを維持します。
4	SMF は、N4 Session Modification 要求を UPF に送信し、UPF からレスポンスを受信します。
5	ADC は UPF でアクティブ化されます。

ステップ	説明
6	UPF は、ADC ルールに一致するパケットを検出します。
7	UPF は、N4SessionUpdate 要求を SMF に送信し、SMF から応答をレスポンスします。UPF がアプリケーションの開始をトリガーします。
8	SMF は SmPolicyUpdate 要求を PCF に送信し、PCF から確認応答を受信します。必要に応じて、レスポンスの一部として専用ベアラーが作成されます。
9	PCF は SmPolicyUpdateNotify を SMF に送信し、SMF から確認応答を受信します。
10	PCF は QCI 80 ベアラーのダイナミックルールを送信し、専用ベアラーがセットアップます。
11	UPF は、通信を専用ベアラーに切り替えます。
12	UPF が専用ベアラーでの通信の停止を検出します。
13	UPF は、N4SessionUpdate 要求を SMF に送信し、SMF から応答をレスポンスします。UPF がアプリケーションの停止をトリガーします。
14	SMF は SmPolicyUpdate 要求を PCF に送信し、PCF から確認応答を受信します。必要に応じて、レスポンスの一部として専用ベアラーが削除されます。
15	PCF は SmPolicyUpdateNotify を SMF に送信し、SMF から確認応答を受信します。
16	PCF は QCI 80 ベアラーのダイナミックルールの削除を送信し、専用ベアラーが削除されます。

制限事項

このリリースにおけるこの機能の制限事項は次のとおりです。

- Gx ADC 事前定義ルールは、デフォルトベアラー 5QI でのみインストールされます。

ADC ルールを構成する

事前定義された ADC ルールの有効化をサポートするには、適切なアクション優先順位と **adc** キーワードに基づいて SMF の ADC ルールを構成する必要があります。以下に設定サンプルを示します。

```
active-charging service service_name
    rulebase rulebase_name
        action priority action_priority dynamic-only adc ruledef ruledef_name
 charging-action charging_action_name
    exit
ruledef ruledef_name
   ip server-ip-address ipv4/ipv6_address/mask
   ip server-ip-address ipv4/ipv6_address/mask
   exit
exit
```

レポートをミュートにするには、rulebase の構成で次の CLI コマンドを使用します。

```
action priority action_priority dynamic-only adc mute ruledef ruledef_name
charging-action charging_action_name
```

アプリケーションレポートをアプリケーションごとに最適化するには、rulebase構成で次のCLIコマンドを使用します。

```
adc app-notification once-per-app
```

アプリケーションレポートをアプリケーションごとフローごとに最適化するには、rulebase 構成で次の CLI コマンドを使用します。

```
adc app-notification once-per-ipflow
```

注：

- **rulebase** *rulebase_name*：Active Charging Service Rulebase 構成を有効にします。
- **action priority** *action_priority*：rulebase の ruledef に優先順位を割り当てます。優先順位は、1 ～ 65535 の範囲の一意の整数値で指定する必要があります。
- **dynamic-only**：フローにおけるこのアクション優先順位について、ダイナミックルールと静的ルールの照合を有効にします。
- **adc**：ADC ルールとして指定される ruledef を指定します。
- **ruledef** *ruledef_name* ：指定された ruledef を現在の rulebase に追加します。
- **charging-action** *charge_action_name*：課金アクションを指定します。
- **description** *description*：指定されたテキストをルールとアクションに追加します。
- **ip server-ip-address** *ipv4/ipv6_address/mask*：サーバー IP とサブネットマスクビットを指定します。アップリンクパケット（サブスクライバからネットワーク）の場合、このフィルターは、IP ヘッダーの接続先 IP アドレスと一致します。ダウンリンクパケット（ネットワークからサブスクライバ）の場合、このフィールドは、IP ヘッダーの送信元 IP アドレスと一致します。
- **once-per-app**：アプリ IP ごとに、APP_START または APP_STOP 通知を 1 回送信します。

  アプリケーションの通信が検出されるたびに、UPF は、APP-START 通知を、アプリケーションの最初のデータフローのフロー ID としてのアプリケーション インスタンス識別子として SMF に送信します。このアプリケーション インスタンス ID は、ユーザープレー

ンでキャッシュされます。アプリケーションの最後のデータフローが終了すると、キャッシュされたアプリケーション インスタンス ID は、APP-STOP に送信されます。これにより、PCF は、APP-START および APP-STOP をより適切に関連付けることができます。

- **once-per-ipflow**：IP フローごとにアプリ ID ごとに APP_START または APP_STOP 通知を送信します。

モニタリングおよびトラブルシューティング

この項では、この機能を監視して、障害対応を行うために使用可能なCLIコマンドについて説明します。

PDRと URR を表示する show コマンド

UPF で、次のコマンドを使用して、ADC が有効になっている PDR を表示します。

show subscribers user-plane-only callid *callid_value* **pdr full all**

UPF で次のコマンドを使用して、ADC が有効になっている URR を表示します。

show subscribers user-plane-only callid *callid_value* **urr full all**

ADC 統計を表示する show コマンド

UPF で以下のコマンドを使用すると、ADC 統計を表示できます。

show subscribers user-plane-only callid *callid_value* **adc statistics**



第 41 章

Ruledefs の QoS グループのサポート

- 機能の概要と変更履歴 （459 ページ）
- 機能説明 （460 ページ）
- 機能の仕組み （460 ページ）
- OAM のサポート （462 ページ）

機能の概要と変更履歴

要約データ

表 *87* : 要約データ

該当製品または機能エリア	5G-UPF
該当するプラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2023.01.0

機能説明

Ruledef の QoS グループ機能により、PCF はサブスクライバごとに fair usage policy （FUP）を適用できます。Ruledef の QoS グループは、QGR または SGQ とも呼ばれます。

QGR 機能では、名前付き QGR に対して異なるサブスクライバに異なるQoS パラメータが設定されるため、サブスクライバの fair usage policing が保証されます。

機能の仕組み

QGR 機能は、charging-action 構成でフロー状態と帯域幅幅制限を実行します。UPF は、RCM を使用して QGR の静的構成を適用します。

パケットが ruledef と一致すると、UPF は QGR 照合を実行して、一致した ruledef またはグループに QGR が存在するかどうかを確認します。UPF は、最も優先順位の高い QGR を返します。

- QGR が一致した場合、UPF は charging-action で flow-action を適用し、次に charging-action でパケットが許可されている場合はQGR で適用します。パケットがドロップされた場合、QGR レベルの flow-action 適用はスキップされます。
- QGR の flow-action によってパケットが許可されている場合、UPF は、パケットで QoS Enforcement Rule（QER）制限を適用します。パケットが QGR でドロップした場合、UPF は QER の制限をスキップします。
- UPF は charging-action で QER 制限を実行し、charging-action でパケットが許可されている場合は、QGR で QER 制限を実行します。

UPF は、ACS サービスで QoS -group-of-ruledef 構成をサポートします。

次に、ACS での QGR 構成例を示します。

```
configure
   active-charging service acs
     qos-group-of-ruledefs QGR1
        add-group-of-ruledef group
        add-ruledef http
        #exit
     rulebase test
        action priority 2 ruledef http charging-action standard
        action priority 5 ruledef catchall charging-action standard
        route priority 1 ruledef http-rule analyzer http
        end
```

次に、PCRF 経由で受信した QoS グループ「QGR1」の構成例を示します。

```
-qos-group-rule-install
--qgr-name QGR1
--qgr-mon-key 1
--qgr-flow-status 2
--qgr-precedence 1
--qgr-eqos-information
--qgr-eqos-mbr 1000 2000
--qgr-eqos-mbr-burst-size 1000 2000
```

```
--qgr-eqos-mbr-limit-conform-action 0 -1 0 -1
--qgr-eqos-mbr-limit-exceed-action 1 -1 1 -1
```

IE のサポート

UPF は、プライベート IE（QGR-INFO-LIST）を使用して、Session Establishment 要求または Session Modification 要求で QGR をプッシュします。QGR のダイナミックパラメータに変更がある場合、UPF は Update FAR または QER をトリガーします。UPF は、Session Establishment 要求または Session Modification 要求で更新された値を送信します。

現在、UPF は QGR の monitoring-key パラメータをサポートしません。したがって、UPF は Session Establishment 要求または Session Modification 要求で QGR に関連付けられた URR を送信しません。

プライベート IE の名前とフォーマットは次のとおりです。

```
QGR-INFO-LIST:
Value:
Number of QGRs: 2
QGR INFO:
NAME: qgr-gor
PRECEDENCE: 3
OPERATION: QGR ADD
FAR ID: 0x8005
QER ID: 0x0004
QGR INFO:
NAME: qgr2
PRECEDENCE: 9
OPERATION: QGR ADD
FAR ID: 0x8006
QER ID: 0x0005
```

次の表で、FAR フォーマットについて説明します。

表 *88 : FAR* 形式

FAR ID	固有 ID
Apply Action	QGR で定義された Flow-action
Extended Apply Action	QGR FAR と通信するためのプライベート IE。プライベート IE には、Flow-Action—Discard Uplink、Discard Downlink および Terminate フローがあります。
転送パラメータ	接続先インターフェイスとリダイレクト情報（ある場合）が含まれます。

次の表で、QER フォーマットについて説明します。

表 *89 : QER* 形式

QER ID	固有 ID

最大ビットレート	Kbps 単位の QGR の最大ビットレート。
	`UL MBR`
	`DL MBR`

バースト サイズ	バーストサイズを構成するプライベート IE。
	`UL Burst`
	`DL Burst`

適合アクション	適合アクションを構成するプライベート IE :
	`Uplink ToS`
	`Downlink ToS`

超過アクション	超過アクションを設定するプライベート IE。
	`Uplink Action`
	`Uplink ToS`
	`Downlink Action`
	`Downlink ToS`

show subscribers user-plane-only callid *call_id* **{ far | qer } full all** コマンドを使用すると、FAR と QER 値を表示できます。

制限事項

QGR 機能には、次の制限があります。

- QGR に関連付けられているモニタリングキーは、監視されている使用状況ではありません。つまり、UPF は、URR 作成と適用をサポートしません。
- UPF では、静的 QGR 定義にダイナミックルールを含めることはできません。
- UPF は、フロー状態リダイレクトと強制終了フローはサポートしていません。
- UPF は、Drop としての QoS Group Conform アクションをおよび ALLOW または MARK_DSCP としての Exceed アクションをサポートしていません。
- UPF は、64 の QGR の最大構成を静的にサポートします。
- UPF は、SMF から受信した最大 64 の QGR をサポートします。

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

show コマンドのサポート

この項では、QGR 機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show subscribers user-plane-only callid call_id far full all

このコマンドは、Extended Apply Action IE 情報を表示します。

```
[local]qvpc-si# show subscribers user-plane-only callid 00004e21 far full all
FAR-ID                   : 0x8004
        Destination Interface    : Core
        Apply Action             : FORWARD
        Outer Header Creation    :
        Remote TEID              : 0x0
        Transport Level Marking         : N/A
        Transport Level Marking Options :
          Copy Inner:                     No
          Copy Outer:                     No
        Inner Packet Marking            : N/A
        Remote IP Address        :
        Remote Port              : N/A
        Number of Associated PDRs: 0
        Associated with QGR       : Yes
            Extended Apply Action : ULDROP DLDROP
```

show subscribers user-plane-only callid call_id qer full all

このコマンドは、UPF の QGR に関連付けられた帯域幅パラメータを表示します。

```
[local]qvpc-si# show subscribers user-plane-only callid 00004e21 qer full all

        QER-id                  : 0x00000003        Correlation-id          : n/a
        GBR uplink (bps)        : 0                 GBR downlink (bps)      : 0

        UL Gate Status          : OPEN              DL Gate Status          : OPEN
        Number of Associated PDRs  :0
        Associated with QGR     : Yes
        MBR uplink (bps)        : 1000              MBR downlink (bps)     : 2000
        UL Burst         : 1000                    DL Burst               :
1000
           UL Conform Action          : ALLOW                  DL Conform
Action     : ALLOW
          UL DSCP Value              : NA                    DL DSCP Value
         : NA
           UL Exceed Action           : DROP                   DL Exceed
Action      : DROP
          UL DSCP Value              : NA                    DL DSCP Value
         : NA
```

show subscribers user-plane-only callid call_id qos-group all

このコマンドは、UPF の QGR-INFO-LIST IE からの QGR 情報を表示します。

```
[local]qvpc-si# show subscribers user-plane-only callid call_id qos-group
all       name   statistics
[local]qvpc-si# show subscribers user-plane-only callid 00004e21 qos-group all
```

```
Callid: 00004e21
Interface Type: Sxb
    QGR-Name:      Priority:       FAR-ID:         QER-ID:         URR-ID:
    ---------      ---------       -------         -------         ------
     QGR1           5               0x8003          0x0002          0x0000
     QGR2           1               0x8004          0x0003          0x0000

Total Number of QGRs found: 2
```

show subscribers user-plane-only callid call_id qos-group statistics

このコマンドは、UPF の QoS グループ統計を表示します。

```
[local]qvpc-si# show subscribers user-plane-only callid 00004e21 qos-group statistics
all       name      |         <cr>
QoS-Group-of-Ruledef:
    Total Uplink Pkts:                0     Total Dnlink Pkts:                0
    Total Uplink Bytes:               0     Total Dnlink Bytes:               0
    Uplink Pkts Allowed:              0     Dnlink Pkts Allowed:              0
    Uplink Bytes Allowed:             0     Dnlink Bytes Allowed:             0
    Uplink FP Pkts:                   0     Dnlink FP Pkts:                   0
    Uplink FP Bytes:                  0     Dnlink FP Bytes:                  0
     Flow-Status Statistics:
       Total Uplink Packets:           0     Total Downlink Packets:           0
       Total Uplink Bytes:             0     Total Downlink Bytes:             0
       Uplink Packets Redirected:      0     Downlink Packets Redirected:      0
       Uplink Bytes Redirected:        0     Downlink Bytes Redirected:        0
       Uplink Packets Dropped:         0     Downlink Packets Dropped:         0
       Uplink Bytes Dropped:           0     Downlink Bytes Dropped:           0
       Uplink Packets Term-Flow:       0     Downlink Packets Term-Flow:       0
       Uplink Bytess Term-Flow:        0     Downlink Bytes Term-Flow:         0
     Bandwidth-Control Statistics:
       Total Uplink Packets:           0     Total Downlink Packets:           0
       Total Uplink Bytes:             0     Total Downlink Bytes:             0
       Uplink Packets QoS-Exceed:      0     Downlink Packets QoS-Exceed:      0
       Uplink Bytes QoS-Exceed:        0     Downlink Bytes QoS-Exceed:        0
       Uplink Packets QoS-Conform:     0     Downlink Packets QoS-Conform:     0
       Uplink Bytes QoS-Conform:       0     Downlink Bytes QoS-Conform:       0
       Uplink Packets Dropped:         0     Downlink Packets Dropped:         0
       Uplink Bytes Dropped:           0     Downlink Bytes Dropped:           0
       Uplink Packets Marked:          0     Downlink Packets Marked:          0
       Uplink Bytes Marked:            0     Downlink Bytes Marked:            0

Total qos-group-of-ruledefs matched: 2

Total subscribers matching specified criteria: 1
```

show subscribers user-plane-only full all

このコマンドは、UPF が正常にアクティブ化されたサブスクライバごとの QoS グループの数と、データパケットと一致した QoS グループ統計を表示します。

```
[local]qvpc-si# show subscribers user-plane-only full all

  Local SEID      : [0x0004000000000000] 1125899906842624
  Remote SEID     : [0x0004000000000000] 1125899906842624
  State           : Connected
  Connect Time    : Wed Mar 18 07:53:57 2020
  Idle time       : 18h53m24s
  Access Type: uplane-ipv4               Network Type: IP
  user-plane-service-name: user-plane-service
  Callid: 00004e21
  Rulebase: prepaid
```

```
  Interface Type: Sxb
  Card/Cpu: 1/0                          Sessmgr Instance: 1
  IP address: 10.0.0.1
  Source context: ingress                Destination context: egress
  PDN-Instance: intershat
  User-plane-Sx-addr: 192.60.182.1
  Control-plane-Sx-addr: 192.60.181.1
  Number of associated PDRs : 0
  Number of associated ADC PDRs : 0
  Number of associated FARs : 1
  Number of associated QERs : 2
  Number of associated URRs : 3
  …..
  …..
  …..
  CC Dropped Uplink bytes: 0                      CC Dropped Downlink Bytes: 0
  Uplink Inflight Pkts: 0                         Downlink Inflight Pkts: 0
  Total QoS-Group(s) Active: 1

  Flow information:
    Current Active Flows:
      TCP: 0
      UDP: 0
    Total Flows:
      TCP: 2
      UDP: 0
      FP:  0

Static & Predef Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  -----------------
http                          2       1352          2        250          4
  0          0/0              0/0
catchall                      4        160          8        320         12
  0          0/0              0/0

Dynamic Rule Match stats:
PDR Id   Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)    FP-Up(Pkts/Bytes)
-------- ---------- ---------- ---------- ---------- ---------- --------------
-------------------    -----------------

Post-Processing Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  -----------------
QoS-Group Statistics:
QGR Name  Pkts-Down   Bytes-Down    Pkts-Up    Bytes-Up    Hits
Match-Bypassed   FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------- ----------   ----------   ---------  ----------  ------
--------------   -------------------  -----------------
QGR1       3           756          5           285         8        0
               0/0                    0/0
```

show user-plane-service qos-group-of-ruledefs

このコマンドは、PDF 経由の UPF で受信した静的 QoS グループ構成を表示します。

```
[local]qvpc-si# show user-plane-service qos-group-of-ruledefs
all       name
[local]qvpc-si# show user-plane-service qos-group-of-ruledefs all
  QOS-Group-of-Ruledefs Name: QGR1
   Ruledef Name
   ============
   group

Total QoS group(s) of ruledefs found: 1
```

show user-plane-service statistics qos-group sessmgr

このコマンドは、すべての QoS グループの累積統計を表示します。

```
[local]laas-si-setup# show user-plane-service statistics qos-group sessmgr
1..1152   all

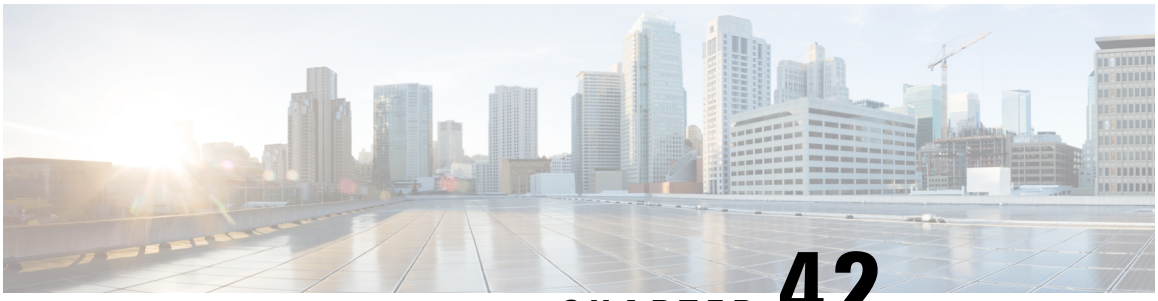
Sessmgr Instance: 1
      Total Uplink Pkts:                 5       Total Dnlink Pkts:                 3
      Total Uplink Bytes:              274     Total Dnlink Bytes:                756

      Uplink FP Pkts:                    0       Dnlink FP Pkts:                    0
      Uplink FP Bytes:                   0       Dnlink FP Bytes:                   0
      Flow-Status Statistics:
        Total Uplink Packets:            5       Total Downlink Packets:            3
        Total Uplink Bytes:              274     Total Downlink Bytes:              756

        Uplink Packets Redirected:       0       Downlink Packets Redirected:       0
        Uplink Bytes Redirected:         0       Downlink Bytes Redirected:         0
        Uplink Packets Dropped:          0       Downlink Packets Dropped:          0
        Uplink Bytes Dropped:            0       Downlink Bytes Dropped:            0
        Uplink Packets Term-Flow:        0       Downlink Packets Term-Flow:        0
        Uplink Bytess Term-Flow:         0       Downlink Bytes Term-Flow:          0
      Bandwidth-Control Statistics:
        Total Uplink Packets:            5       Total Downlink Packets:            3
        Total Uplink Bytes:              274     Total Downlink Bytes:              756

        Uplink Packets QoS-Exceed:       0       Downlink Packets QoS-Exceed:       0
        Uplink Bytes QoS-Exceed:         0       Downlink Bytes QoS-Exceed:         0
        Uplink Packets QoS-Conform:      5       Downlink Packets QoS-Conform:      3
        Uplink Bytes QoS-Conform:        274     Downlink Bytes QoS-Conform:        756

        Uplink Packets Dropped:          0       Downlink Packets Dropped:          0
        Uplink Bytes Dropped:            0       Downlink Bytes Dropped:            0
        Uplink Packets Marked:           0       Downlink Packets Marked:           0
        Uplink Bytes Marked:             0       Downlink Bytes Marked:             0
```



CHAPTER 42

ローミングのサポート

- 機能の概要と, on page 467
- 機能説明, on page 468
- 機能の仕組み, on page 472
- UPF の HR ローミングサポートを構成する, on page 491
- モニタリングおよびトラブルシューティング, on page 494

機能の概要と

要約データ

Table 90: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 91: マニュアルの変更履歴

改訂の詳細	リリース
UPF は、5G セッションの PLMN 間ローミングモビリティとセカンダリ PDR をサポートします。	2023.03.0
UPF は、次のローミング機能をサポートしています。 • Source Interface Type IE じゃ、3GPP インターフェイスタイプを示します。 • Subscriber Params IE は、ローミング状態を示します。	2023.02.0
最初の導入。	2021.02.0

機能説明

モバイルネットワーク事業者は、自社ネットワークの到達範囲を超える地域のサブスクライバにシームレスなサービスを提供するため、ローミングパートナーシップを構築します。通信事業者ネットワークの境界は、Public Land Mobile Network（PLMN）によって指定されます。サブスクライバのホームネットワークはHPLMNと呼ばれ、モバイルサービスを提供する訪問先ネットワークは VPLMN と呼ばれます。

VPLMNはパケットコアにアクセスネットワークサービスとパケットルーティングを提供し、HPLMN はサブスクライバにデータ ネットワーク アクセスを提供します。この機能により、UPFはホームルーテッド（HR）ローミングと呼ばれるルーティング方式をサポートできます。

Visited UPF（vUPF）は次の機能をサポートしています。

- 関連する FAR アクションでダミーの PDR をバッファとして処理する
- ルール照合の前に受信パケットをバッファリングする
- パケットのデバッファリングのために SMF からの QoS および FAR の更新を処理する
- PDR と照合した後、バッファリングされたパケットを送信する
- Fast Path 経由で vUPF 通信を送信する
- N9 インターフェイス GTP-U トンネルを送信する
- UPF LI サポートをローミングに拡張する
- MonSub CLI コマンドおよび PCAP ファイルのサポート

vUPF およびホーム UPF（hUPF）は、次の機能をサポートします。

- UPF の QoS フローベースの課金（QBC）
- PDR の Source Interface Type IE が UPF で 3GPP インターフェイスタイプを示す
- create PDR の PDI IE で受信した 3GPP インターフェイスタイプを受信することで GTP-U サービスを選択する
- Subscriber Params IE がUPF でローミング状態を障害雌

関係性

ローミング状態機能は、ローミングの以下の種類を示す UPF 入力インターフェイス機能に関連しています。

- ホーマー
- ルーマー
- アクセスした LBO
- アクセスした HR

UPF は、さまざまな GTP-U 入力インターフェイスをサポートしています。これにより、N3 インターフェイスと N9、S5u、および S8u インターフェイス用に個別のネットワークを使用できます。

ローミングコールとアウトバウンドコールを処理する GTP-U 入力インターフェイスには、次のものがあります。

- N3：N3 は、gNodeB と UPF 間のインターフェイスです。5G ホームコールを処理するには、N3 インターフェイスがプライベート IP アドレスである必要があります。
- N9：N9 インターフェイスは、2つの UPF を接続します。これは、異なる PLMN を接続する中間 I-UPF と UPF セッションアンカー間のインターフェイスです。5G アウトバウンドローミング コールを処理するには、N9 インターフェイスがパブリック IP アドレスである必要があります。
- S5u：S5u は、2 つの UPF を接続する N9 インターフェイスに似ています。インターフェイスは、中間の I-UPF と UPF セッションアンカーを接続します。 4G インバウンドコールを処理するには、S-GW を有効にするために SGW-U がパブリックであるため、S5u はパブリック IP 設定されます。
- S8u：S8u は S5u インターフェイスの PLMN 間バリアントです。4G アウトバウンド ローミング コールを処理するには、S8u インターフェイスがパブリック IP アドレスである必要があります。

詳細については、「*UPF* 入力インターフェイス」章を参照してください。

アーキテクチャ

この項では、ホーム ルーティング ローミング サポート機能のアーキテクチャについて説明します。

vUPF でバッファリングとデバッファリングを行う

UPF HR ローミングの vUPF でのバッファリングとでバッファリング手順は以下のとおりです。

1. 2 つのダミーPDR（UL または DL）は、最初に vSMF が vUPF で作成し、デフォルト値は QFI、バッファリングは FAR アクションです。
2. N3 および N9 インターフェイスから受信するパケットは、パケットの分類とポリシーの適用を実行する前に、FAR アクションに基づいてバッファリングされます。
3. バッファリングされたパケット数が設定された制限を超えると、後続のパケットはドロップされます。
4. バッファリングされたパケットは、vSMF からの変更要求で転送としてのアクションおよび更新された TEID を含む Update FAR を受信した後、分類およびポリシーの適用のために送信されます。
5. vSMF は、アクション転送で Update FAR を送信中にデフォルトのQER と URR の削除を開始し、必要な QER と URR を含む新しい PDR を送信します。
6. パケットは、新しい QER で定義された QFI に基づいて必要なインターフェイスに送信されます。
7. TEID と QFI が一致する PDR がインストールされていない場合、バッファリングされたパケットはドロップされます。

課金：hUPF の Predef ルールとダイナミックルール

hUPF の課金の predef およびダイナミックルールは次のとおりです。

1. SMF は、FBC URR + QBC URR + Session URR をダイナミック PDR に関連付けます。
2. SMF は QBC URR + Session URR を predef PDR に関連付けます。
3. UPF は、インストールされたグローバル PDR が作成した URR を、受信した predef PDR QBC URR + Sess URR に関連付けます。
4. QBC URR には Linked URR がありません。
5. QBC URR には、FBC URR または Session URR の使用状況レポートは含まれません。
6. UPF は、Session URR を Linked URR として FBC URR にリンクします。
7. Session URRR には、FBC URR と QBC URR の使用状況レポートが含まれます。
8. UPF は、QBC および Sess URR の各更新または削除を SMF に依存します。

課金：hUPF の静的ルール

hUPF での課金の静的ルールは次のとおりです。

1. SMF は、FBC URR + QBC URR + Session URR を RB PDR に関連付けます。
2. UPF は、インストールされたグローバル PDR によって作成された URR を、受信した RB PDR QBC URR + Sess URR に関連付けます。
3. UPF は、QBC URR を URR とリンクしません。
4. UPF は、静的 FBC URR を Session URR にリンクします。
5. UPF は、使用状況レポートのために Linked URR として Session URR を FBC URR にリンクします。
6. UPF は、QBC および SMF URR の各更新または削除を SMF に依存します。

PLMN 間モビリティサポート

Inter-Public Land Mobile Network（Inter-PLMN）モビリティ機能を使用すると、PLMN は、User Equipment（UE）がホームネットワークからアクセス先ネットワークまたはその逆方向に移動する際に、home-PLMN から visited-PLMN に代わります。この機能は、さまざまなタイプの PLMN 間モビリティケースをサポートします。

PLMN 間ハンドオーバーに関連するコールフローの詳細については、「仕組み」項を参照してください。

H-UPF データパスの仕様：

- Homer コールのセカンダリ PDR の最適化
- 最適化による PLMN 間および PLMN 内ハンドオーバーのサポート
- Homer コールの GTPU サービスのサポート
- PDR のセカンダリ PDR 情報の KPI サポート
- ハンドオーバー統計

UPF は、様々な PLMN 間モビリティに関する以下のシナリオをサポートします。

- 5G ホーマーから 5G ルーマー
- 5G ホーマーから 4G ルーマー
- 4G ホーマーから 5G ルーマー
- 4G ホーマーから 4G ルーマー
- 5G ルーマーから 5G ホーマー
- 5G ルーマーから 4G ホーマー
- 4G ルーマーから 5G ホーマー

- 4G ルーマーから 4G ホーマー

UPF は、様々な PLMN 内モビリティに関する以下のシナリオをサポートします。

- 5G ホーマーから 4G ホーマー
- 4G ホーマーから 5G ホーマー
- 5G ルーマーから 4G ルーマー
- 4G ルーマーから 5G ルーマー
- EUTRAN から Wi-Fi へのハンドオーバーとその逆のハンドオーバー

機能の仕組み

この項では、UPF のローミング機能に関連するコールフローについて説明します。

PDU Session Establishment 手順

このコールフローでは、UPF のPDU Session Establishmentn 手順について説明します。

Figure 25: PDU セッション確立コール フロー

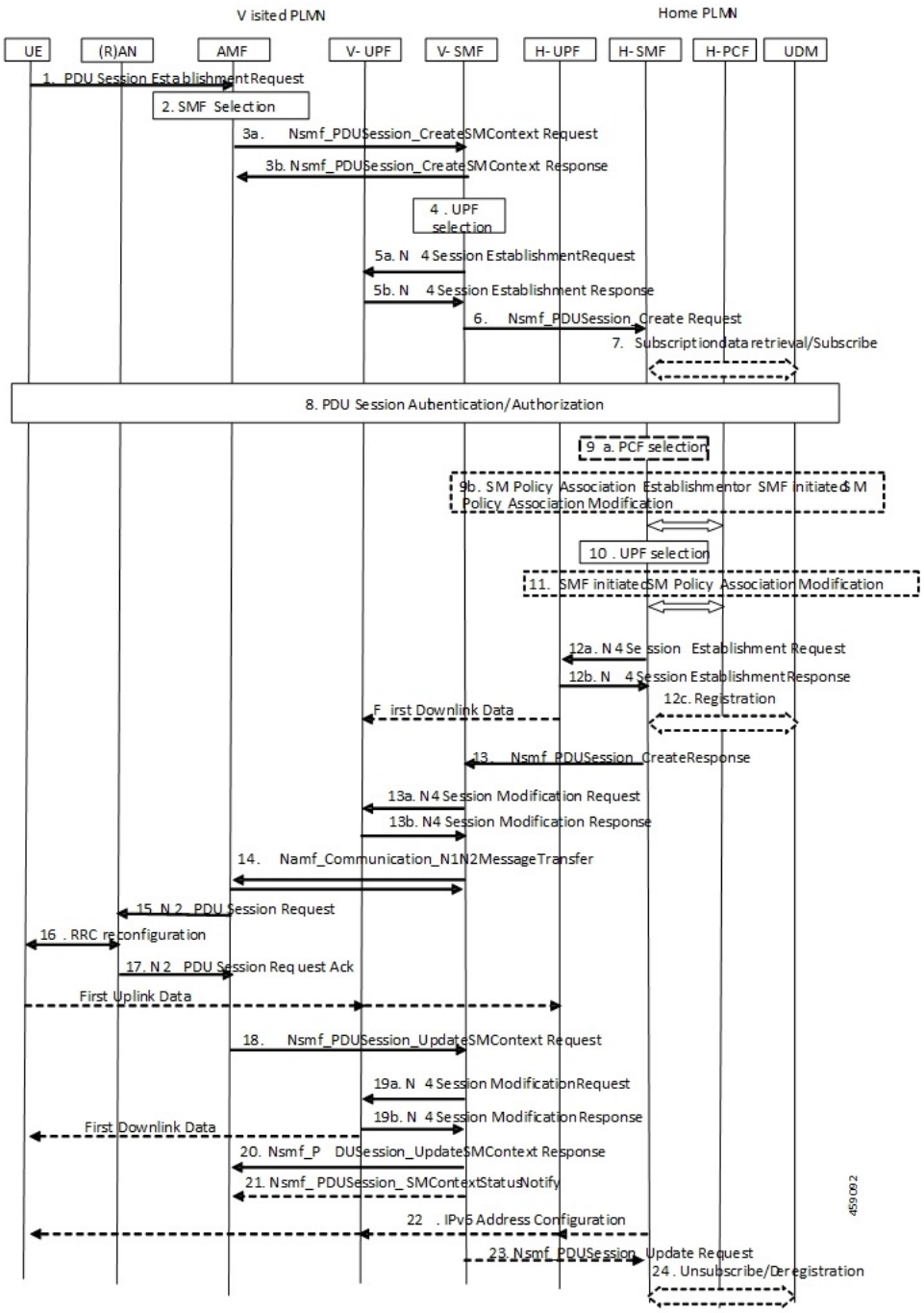


Table 92: PDU セッション確立コール フローの説明

ステップ	説明
1	UE は、PDU Session Establishment 要求を AMF に送信します。
2	AMF は SMF を選択します。
3a	AMF は、Nsmf_PDUSession_CreateSMContext 要求を呼び出し、それを vSMF に送信します。
3b	vSMF は、Nsmf_PDUSession_CreateSMContext 応答を AMF に送信します。
4	vSMF は VPLMN で UPF を選択します。
5a	vSMF は、ダミーの PDR、FAR、QER、または URR を使用して、N4 Session Establishment 要求を vUPF に送信します。この要求では、vSMF は、vUPF に。CN トンネル情報を N3 と N9 インターフェイスに割り当てるように通知します。vSMF は、Access PDR で N3 3GPP Access (11) として、ローミングに対して、Core PDR で N9 (21) として Source Interface Type IE を送信します。
5b	vUPF は、N3 および N9 CN トンネル情報を作成し、N4 Session Establishment 応答でこの情報を送信することで確認します。
6	vSMF は、Nsmf_PDUSession_Create 要求を hSMF に送信します。
7	hSMF は、指定された PDU セッションにたいして UDM を登録します。
8	SMF は、DN- AAA サーバーによる PDU セッションの確立中にセカンダリ承認または認証を実行します。
9a	hSMF は PCF を選択します。
9b	SMF は、SM Policy Association Establishment 手順を実行して、PCF との SM Policy アソシエーションを確立し、PDU セッションのデフォルトの PCC ルールを取得します。
10	hSMF は UPF を選択します。
11	hSMF は、SM Policy Association Modification 手順を開始します。
12a	hSMF は、選択した UPF に対して、N4 Session Establishment 手続きを開始します。vUPF からの N9 CN トンネル情報は、FAR で hUPF に転送されます。hSMF は、コールを登録する RAT およびローミング状態に応じて、Access PDR で N3 3GPP ACCESS (11) または S5u インターフェイスとして Source Interface Type を送信します。
12 b	UPF は、N4 セッション確立応答を送信することにより確認応答します。hUPF は、N9 CN トンネル情報を vUPF に提供します。

ステップ	説明
12c	ダウンリンクパスは、hUPF と vUPF の間に確立され、データパケットはバッファリングされる vUPF に送信されます。
13	hSMF は、Nsmf_PDUSession_Create 応答メッセージを vSMF に送信します。
14	vSMF は、Namf_Communication_N1N2MessageTransfer メッセージを AMF に送信します。
15	AMF は、N2 PDU Session 要求内の SMF から受信した UE および N2 SM 情報を対象とした PDU Session ID と PDU Session Establishment Accept を含む NASメッセージを RAN に送信します。
16	RAN は、SMF から受信した情報に関連する UE との特定のシグナリング交換を発行します。
17	RAN は、N2 PDU Session 応答メッセージを AMF に送信します。
18	AMF は、Nsmf_PDUSession_UpdateSMContext 要求メッセージを vSMF に送信します。AMF は、RAN から受信した N2 SM 情報を SMF に転送します。
19a	SMF は vUPF に対して N4 Session Modification 手続きを開始します。vSMF は、AN トンネル情報、H-CN トンネル情報、V-CN トンネル情報など、このPDU セッションの vUPF にインストールされるパケット検出、適用、およびレポート ルールを提供します。
19b	vUPF は、N4 Session Modification 要求を vSMF に提供します。この手順の後、vUPF はこの PDU セッション用にバッファされている可能性のあるダウンリンクパケットを UE に配信します。
20	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
21	vSMF は、Nsmf_PDUSession_SMContextStatusNotify メッセージを AMF に送信します。
22	PDU セッションのタイプが、IPv6 または IPv4v6 向けの場合、hSMF は、IPv6 Router Advertisement を生成して、N4 インターフェイス、hUPF、vUPF で経由でそれを UE に送信します。
23	手順 18 で受信した vSMF が、RAN が一部の QFI を拒否したことを示している場合、vSMF は Nsmf_PDUSession_Update 要求経由で hSMF に通知します。hSMF は、それに応じて、UE の QoS ルールに関連する QoS フローに対応する QoS ルールと QoS Flow level QoS パラメータを更新します。

ステップ	説明
24	手順 4 の後に PDU セッション確立が失敗した場合、SMF は次の手順を実行します。 • SMF が、この（DNN、S-NSSAI）に対応する UE の PDU セッションを処理しなくなった場合、hSMF は、Nudm_SDM_Unsubscribe を使用して、対応する（SUPI、DNN、S-NSSAI）のセッション管理サブスクリプションデータの変更の登録を解除します。 • hSMF は、Nudm_UECM_Deregistration（SUPI、DNN、PDU セッション ID）を使用して、指定された PDU セッションの登録を解除します。

PDU Session Modification 手順

このコールフローでは、UPF のPDU Session Modification 手順について説明します。

Figure 26: PDU セッション変更コール フロー

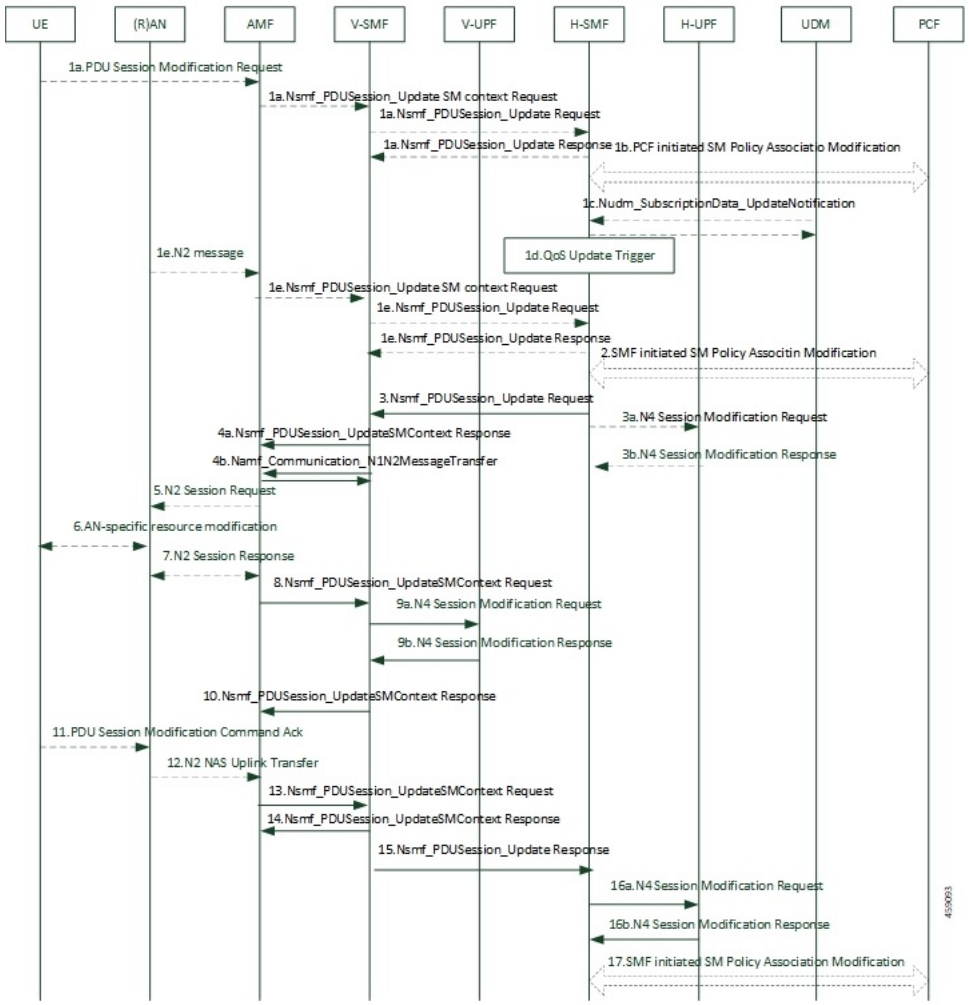


Table 93: PDU セッション変更のコール フローの説明

ステップ	説明
1a	• UE は、NASメッセージを AMF に送信することで PDU Session Modification 手順を開始します。 • AMF は、Nsmf_PDUSession_UpdateSMContext メッセージを開始します。 • vSMF は、Nsmf_PDUSession_Update 要求メッセージを hSMF に送信します。 • hSMF は、vSMF を確認し、Nsmf_PDUSession_Update 応答メッセージを送信します。

ステップ	説明
1b	PCF は、PCF が開始する SM Policy Association Modification 手順を実行して、ポリシーの変更に関して SMF に通知します。
1c	UDM は、Nudm_SDM_Notification を使用して hSMF のサブスクリプションデータを更新します（SUPI、セッション管理サブスクリプションデータ）。hSMF は、セッション管理サブスクリプションデータを更新し、（SUPI）で Ack を返すことによって UDM を確認します。
1d	SMF は、PUD セッションを変更する場合があります。この手順は、ローカルに構成されたポリシーに基づいてトリガーされることも、RAN からトリガーされることもあります。
1e	RAN は、通知制御が設定されているかどうかに関係なく、QoS フローがマッピングされる AN リソースが解放されたときに SMF に示します。RAN は、N2 メッセージを AMF に送信します。AMF は、Nsmf_PDUSession_UpdateSMContext 手順を呼び出します。 vSMF は、Nsmf_PDUSession_Update 要求メッセージを hSMF に送信します。 hSMF は、vSMF を確認し、Nsmf_PDUSession_Update 応答メッセージを送信します。
2	SMF は、SMF によって開始された SM Policy Association Modification 手順を実行することにより、サブスクライブされたイベントを PCF に報告します。
3	hSMF は、vSMF に対して Nsmf_PDUSession_Update Request サービス操作を呼び出します。
3a	SMF は hUPF に対して N4 Session Modification 手続きを開始します。
3b	hUPF は確認応答を返し、N4 Session Modification 応答メッセージを hSMF に送信します。
4a	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
4b	vSMF は、Nsmf_PDUSession_SMContextStatusNotify メッセージを AMF に送信します。
5	AMF は、N2 PDU Session 要求内の SMF から受信した UE および N2 SM 情報を対象とした PDU Session ID と PDU Session Establishment Accept を含む NAS メッセージを RAN に送信します。
6	RAN は、SMF から受信した情報に関連する UE との特定のシグナリング交換を発行します。
7	AMF は、Nsmf_PDUSession_UpdateSMContext 要求メッセージを vSMF に送信します。AMF は、RAN から受信した N2 SM 情報を SMF に転送します。

ステップ	説明
8	AMF は、Nsmf_PDUSession_UpdateSMContext 要求メッセージを vSMF に送信します。AMF は、RAN から受信した N2 SM 情報を SMF に転送します。
9a	SMF は vUPF に対して N4 Session Modification 手続きを開始します。vSMF は、AN トンネル情報、H-CN トンネル情報、V-CN トンネル情報など、このPDU セッションの vUPF にインストールされるパケット検出、適用、およびレポート ルールを提供します。
9b	vUPF は、N4 Session Modification 要求を vSMF に提供します。この手順の後、vUPF はこの PDU セッション用にバッファされている可能性のあるダウンリンクパケットを UE に配信します。
10	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
11	UE は、PDU Session Modification Command Ack メッセージを RAN に送信します。
12	RAN は、AMF との N2 NAS Uplink Transfer を開始します。
13	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
14	vSMF は、Nsmf_PDUSession_SMContextStatusNotify メッセージを AMF に送信します。
15	vSMF は、Nsmf_PDUSession_Update 応答を使用して、hSMF に応答します。この応答には、UE から vSMF に送信された SM PDU Session Modification Command Ack メッセージで UE が提供した PCO などの情報が含まれます。hSMF は、PDU セッションコンテキストを変更します。
16a	SMF は vUPF に対して N4 Session Modification 手続きを開始します。vSMF は、AN トンネル情報、H-CN トンネル情報、V-CN トンネル情報など、このPDU セッションの vUPF にインストールされるパケット検出、適用、およびレポート ルールを提供します。
16b	vUPF は、N4 Session Modification 要求を vSMF に提供します。この手順の後、vUPF はこの PDU セッション用にバッファされている可能性のあるダウンリンクパケットを UE に配信します。
17	hSMF は、SM Policy Association Modification 手順を開始します。

PDU Session Release 手順

このコールフローでは、UPF PDU Session Release 手順について説明します。

Figure 27: PDU セッションの解放コール フロー

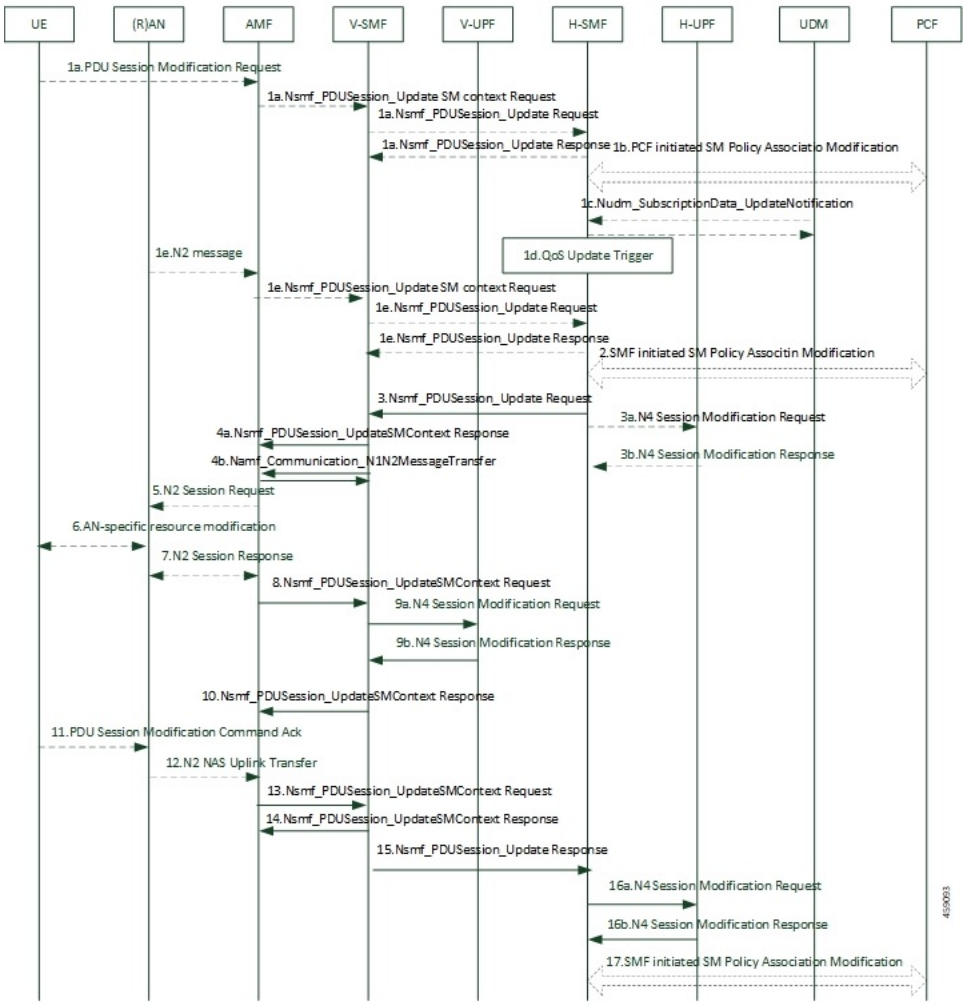


Table 94: PDU Session Release コールフローの説明

ステップ	説明
1a	• UE は、NAS メッセージを AMF に送信することで、UE Requested PDU Session Release 手順を開始します。 • AMF は、Nsmf_PDUSession_UpdateSMContext サービス操作を呼び出し、N1 SM コンテナと RAN から受信した User Location Information（ULI）を SMF に提供します。 • vSMF は N4 Session Modification を開始して、アップリンク通信の転送を停止するように vUPF に指示します。 • vSMF は、Nsmf_PDUSession_Update Request 操作を呼び出し、hSMF が PUD セッションを解放するように要求します。hSMF は即座に要求に応答します。
1b	• AMF は、Nsmf_PDUSession_ReleaseSMContext サービス操作を呼び出し、PDU セッションの解放を要求します。 • vSMF は N4 Session Modification を開始して、アップリンク通信の転送を停止するように vUPF に指示します。 • vSMF は、Nsmf_PDUSession_Release 要求を呼び出して、hSMF で PDU セッションの解放を開始します。
1c	• PCF は、SM Policy Association Termination 手順を呼び出して、PDU セッションの解放を要求します。 • hSMF は N4 Session Modification を開始して、ダウンリンク通信の転送を停止するように hUPF に指示します。
1d	• RAN は、PDU セッションのすべての QoS フローが解放されたときに PDU セッション関連のリソースが解放されることを vSMF に示します。 • vSMF は N4 Session Modification を開始して、アップリンク通信の転送を停止するように vUPF に指示します。 • vSMF は hSMF への Nsmf_PDUSession_Update 要求を開始し、hSMF は応答で確認応答します。
1e	SMF はPDU セッションの解放を決定します。hSMF は N4 Session Modification を開始して、ダウンリンク通信の転送を停止するように hUPF に指示します。

ステップ	説明
1f	AMF は、解放指示が指定された Nsmf_PDUSession_UpdateSMContext サービス操作を呼び出して、PDU セッションの解放を要求します。 vSMF は N4 Session Modification を開始して、アップリンク通信の転送を停止するように vUPF に指示します。vSMF は、hSMF に向けて Nsmf_PDUSession_Update 要求を呼び出します。
2a	hSMF は、N4 Session Release Request (N4 Session ID) メッセージを PDU セッションの hUPF に送信します。hUPF は、PDU セッションの残りのパケットをドロップし、N4 セッションに関連付けられているすべてのトンネルリソースとコンテキストを解放します。
2b	hUPF(s) は、N4 Session Release 応答メッセージを hSMF に送信して、N4 Session Release 要求で確認応答します。
3a	SMF は、AMF with the Nsmf_PDUSession_UpdateSMContext 応答に応答します。
4a	vSMF は、N4 Session Release 要求を vUPF に送信します。
4b	vUPF は確認応答を返し、N4 Session Release 応答を hSMF に送信します。
5a	vSMF は、Nsmf_PDUSession_ReleaseSMContext 応答メッセージを AMF に送信します。
5b	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
5c	N1N2 Message Transfer 手順は、AMF および vSMF で発生します。
6	hSMF は、AMF に送信されたメッセージの N2 SM Resource Release 要求を含め、その後 AMF は、NAS メッセージを UE に送信します。
7	RAN が、PDU セッションに関連付けられている AN リソースを肺胞する N2 SM 要求を受信した場合、RAN は、UE との AN 固有シグナ理イング交換を発行し、対応する AN リソースを解放します。
8	RAN が、AN リソースを解放する N2 SM 要求を受信した場合、RAN は、N2 SM Resource Release Ack メッセージを AMF に送信して、N2 SM Resource Release 要求に確認応答します。
9	AMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを vSMF に送信します。
10	vSMF は、AMF with an Nsmf_PDUSession_UpdateSMContext 応答に応答します。
11	UE は、RAN 経由で NAS メッセージを送信することで PDU Session Release コマンドに確認応答します。
12	AMF は、Nsmf_PDUSession_UpdateSMContext を vSMF に呼び出します。

ステップ	説明
13	SMF は Nsmf_PDUSession_UpdateSMContext 応答で AMF に応答します。
14	vSMF は、手順 3a で呼び出された Nsmf_PDUSession_Update 要求で hSMF に応答し、PDU セッションの解放を確認します。
15	SMF は vUPF に対して N4 Session Modification 手続きを開始します。vSMF は、AN トンネル情報、H-CN トンネル情報、V-CN トンネル情報など、このPDU セッションの vUPF にインストールされるパケット検出、適用、およびレポート ルールを提供します。
15a	hSMF は、SM Policy Association Termination 手順を呼び出すことにより、PCF 内の SM ポリシー制御アソシエーションを解放します。
15c	PDU Session Release が HPLMN によって開始された場合、hSMF は、対応するユーザープレーンリソースを解放します。
15d	hSMF は、Nudm_UECM_Deregistration サービス操作を呼び出します。
16a	は、Nsmf_PDUSession_StatusNotify (Release) 操作を呼び出すことで、PDU セッションに関連付けられているすべてのコンテキストを解放するように vSMF に要求します。
16b	vSMF は、Nsmf_PDUSession_SMContexStatusNotify (Release) を呼び出すことで、PDU セッションに関連付けられているすべてのコンテキストを解放するように AMF に要求します。AMF は、vSMF ID と PDU セッション ID の間のアソシエーションを解放します。

5G から 4G へのハンドオーバー

このコールフローでは、5G から 4G へのハンドオーバーについて説明します。

Figure 28: 5G から 4G へのハンドオーバーコールフロー

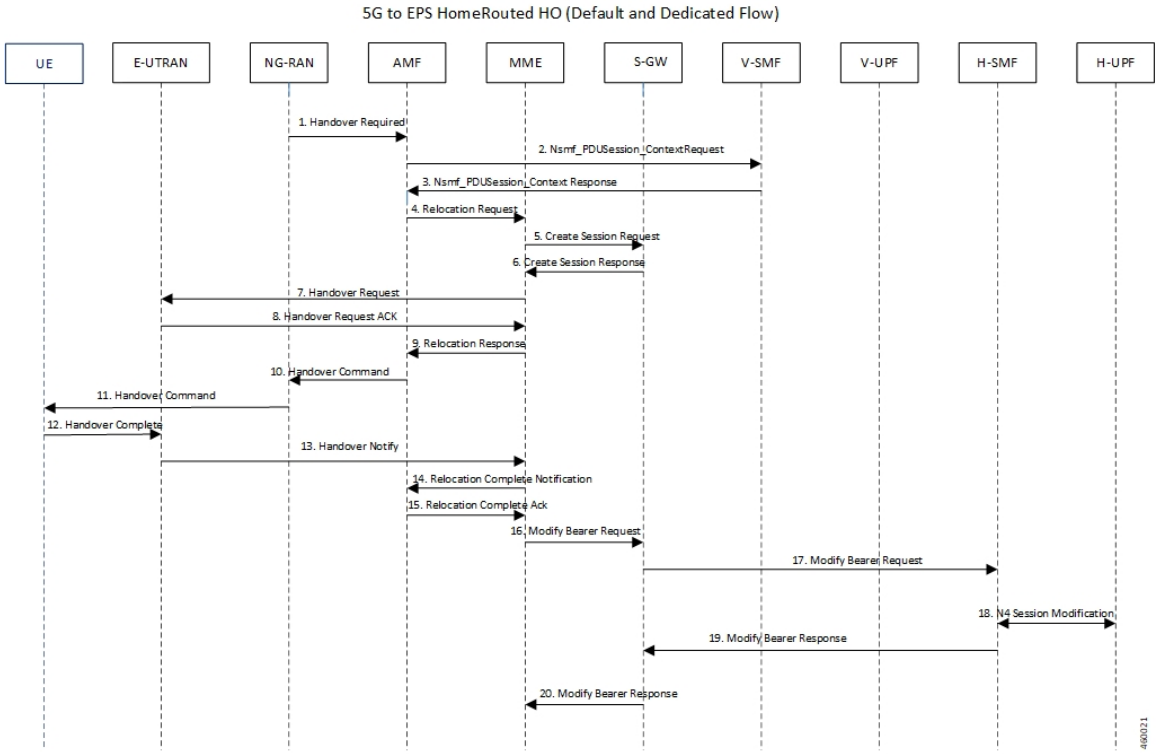


Table 95: 5G から 4G へのハンドオーバーコールフローの説明

ステップ	説明
1	5G セッションが確立された後、NG-RAN は AMF に Handover Required メッセージを送信してハンドオーバープロセスを開始します。
2	AMF は Nsmf_PDUSession_Context 要求を呼び出し、vSMF に送信します。
3	vSMF は、Nsmf_PDUSession_Context 応答を AMF に送信します。
4	AMF は、Relocation 要求を MME に送信します。
5	MME は、Create Session Request を S-GW に送信します。
6	S-GW は、Create Session 応答メッセージを MME に送り返します。
7	MME は、Handover 要求メッセージを E-UTRAN に送信します。
8	E-UTRAN は、確認応答を返し、Handover Request ACK メッセージを MME に送信します。
9	MME は、Relocation Response メッセージを AMF に送信します。
10	AMF は、Handover Commandメッセージを NG-RAN に送信します。

ステップ	説明
11	NG-RAN は、Handover Command を送信して、対象のアクセスネットワークにハンドオーバーするように UE に指示します。
12	UE は、Handover Complete メッセージを使用して、E-UTRAN に応答し、アップリンクデータパスを確立します。
13	E-UTRAN は、UE が NG-RAN に引き渡されることを MME に通知します。
14	MME は、Relocation Complete Notification メッセージを AMF に送信します。
15	AMF は応答確認を返し、Relocation Complete Ack メッセージを MME に送信します。
16	MME が、S-GW にベアラー変更要求を送信します。
17	S-GW は、Modify Bearer 要求メッセージを hSMF に転送します。
18	hSMF は、hUPF に対して N4 Session Modification 手順を開始します。
19	hSMF Modify Bearer 応答メッセージを使用して、S-GW に応答し、ダウンリンクデータパスを確立します。
20	S-GW は、Modify Bearer 応答メッセージを MME に送信します。

4G から 5G へのハンドオーバー

このコールフローでは、4G から 5G へのハンドオーバーについて説明します。

Figure 29: 4G から 5G へのハンドオーバーコールフロー

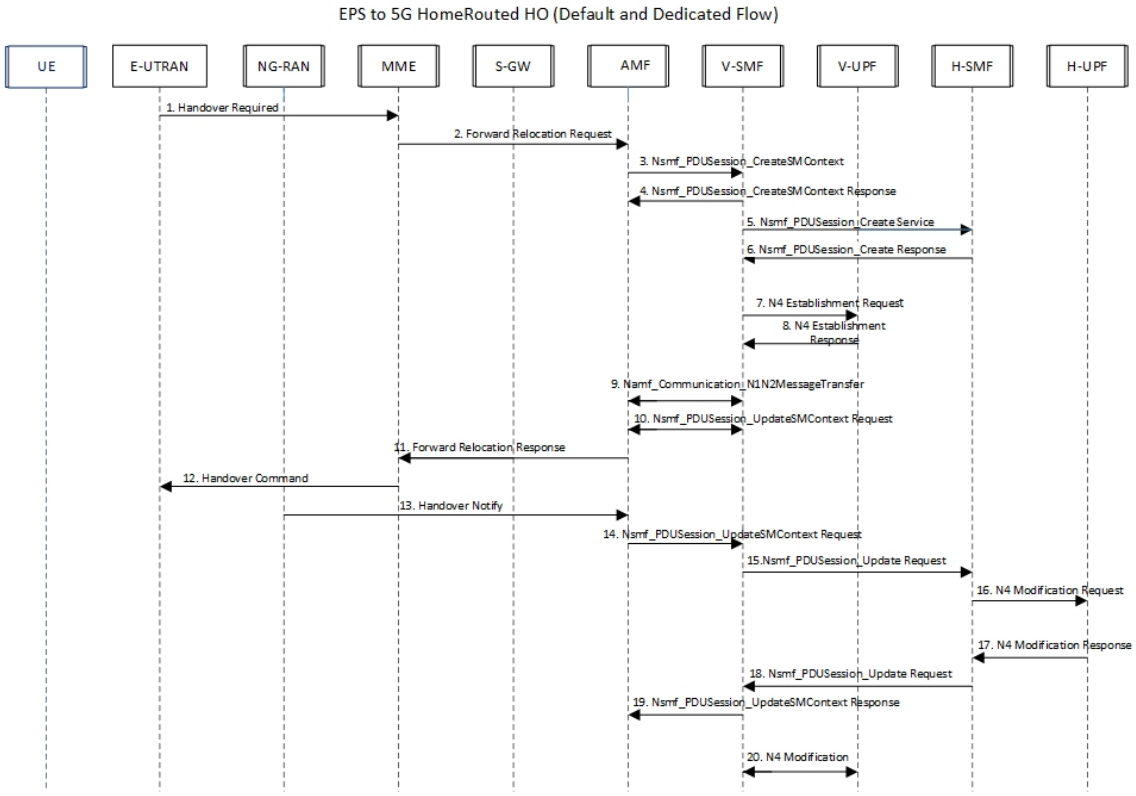


Table 96: 4G から 5G へのハンドオーバーコールフローの説明

手順	説明
1	4G セッションが確立された後、E-UTRAN は MME に Handover Required メッセージを送信してハンドオーバープロセスを開始します。
2	MME は、Forward Relocation 要求を AMF に送信します。
3	AMF は、Nsmf_PDUSession_CreateSMContext 要求を呼び出し、それを vSMF に送信します。
4	vSMF は、Nsmf_PDUSession_CreateSMContext 応答を AMF に送信します。
5	vSMF は、Nsmf_PDUSession_Create Service メッセージを送信して、hSMF で新しい PDU セッションを作成します。
6	hSMF は、Nsmf_PDUSession_Create 応答メッセージを使用して応答します。
7	SMF は、N4 Establishment 要求を vUPF に送信します。
8	vUPF は、N4 Establishment 応答 を送信することにより確認応答します。

手順	説明
9	vSMF は、Namf_Communication_N1N2MessageTransfer メッセージを AMF に送信します。
10	AMF は、Nsmf_PDUSession_UpdateSMContext 要求メッセージを vSMF に送信します。
11	AMF は、Forward Relocation 応答メッセージを MME に送信します。
12	MME は、Handover Command を E-UTRAN に送信します。
13	NG-RAN は、UE が NG-RAN に引き渡されることを AMF に通知します。
14	AMF は、Nsmf_PDUSession_UpdateSMContext 要求メッセージを vSMF に送信します。
15	vSMF は、hSMF に対して Nsmf_PDUSession_Update 要求を開始します。
16	hSMF は、PDR、FAR、QER または URR を使用して、N4 Modification 要求を hUPF に送信します。
17	hUPF は、N4 Modification 応答メッセージを使用して応答します。
18	hSMF は、vSMF に対して Nsmf_PDUSession_Update Request サービス操作を呼び出します。
19	vSMF は、Nsmf_PDUSession_UpdateSMContext 応答メッセージを AMF に送信します。
20	SMF は vUPF に対して N4 Modification 手続きを開始します。

Note ローミング状態機能をサポートするために、PDU Session Establishment またはハンドオーバー中に、Subscriber Params に Roaming Status IE を送信します。

ホーマーからルーマーへの PLMN 間 5G HO

このコールフローでは、v-SMF 挿入を使用した PLMN 間 5G ハンドオーバー（HO）手順について説明します。

UE は、H-PLMN のホームを V-PLMN のローマーに移動します。V-SMF が新しく挿入されると、SMF は H-SMF に移行します。

Figure 30: ホーマーからローマーへの ***PLMN*** 間 ***5G HO***

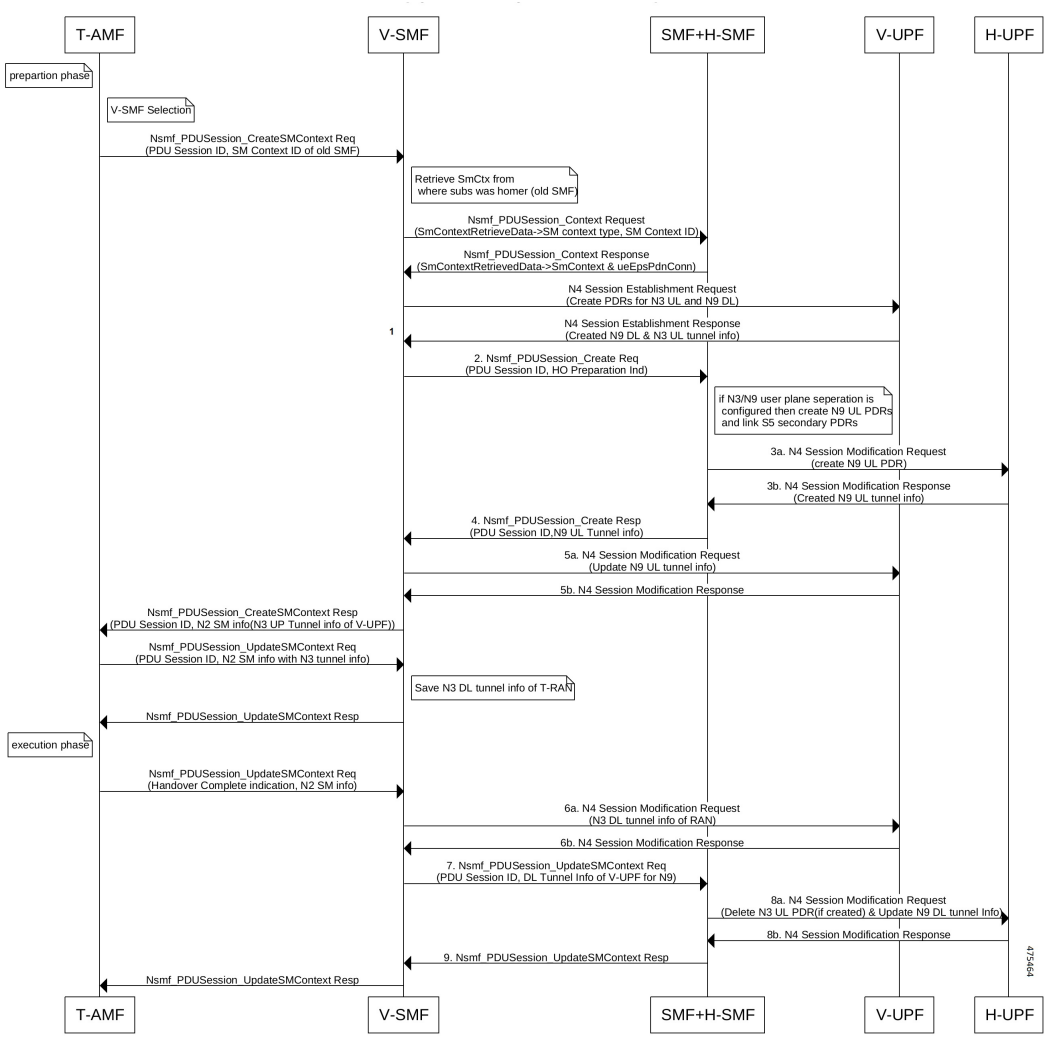


Table 97: ホーマーからローマーへの ***PLMN*** 間 ***5G HO*** コールフローの説明

手順	説明
1	UE が H-PLMN（5G ホーマー）から V-PLMN（5G ローマー）に移動します。
2	SMF は、HO Preparation Ind を使用して、Nsmf_PDUSession_Create 要求を H-SMF に送信します。
3a	H-SMF は、N4 Session Modification 要求で次の Create PDR を H-UPF に送信します。 • 送信元インターフェイスタイプが N9 で、S5U Create PDR で割り当てられたものと同じ FTEID を持つローカル FTEID を使用する プライマリ Create PDR。 • 送信元インターフェイスタイプが N9 で、S5U Create PDR で割り当てられたものと同じ FTEID を持つローカル FTEID を使用する セカンダリ Create PDR。

手順	説明
3b	は、作成された N9 UL Tunnel とともに 、N4 Session Modification 応答を H-SMF に送信します。
4	H-SMF は、N9 UL Tunnel とともに 、Nsmf_PDUSession_Create 応答を V-SMF に送信します。
5a	V-SMF は、N9 UL Tunnel とともに 、N4 Session Modification 要求を V-UPF に送信します。
5b	V-UPF は、N4 Session Modification 応答を V-SMF に送信します。
6a	は、RAN の N3 DL Tunnel 情報とともに 、N4 Session Modification 要求を V-UPF に送信します。
6b	V-UPF は、N4 Session Modification 応答を V-SMF に送信します。
7	V-SMF は、N9 の V-UPF の DL トンネル情報とともに Nsmf_PDUSession_UpdateSMContext 要求を H-SMF に送信します。
8a	H-SMF は N3 UL PDR（作成されている場合）を削除し、N4 Session Modification 要求内の N9 DL トンネル情報を更新して、H-UPF に送信します。H-SMF は、Sx-Modify で Create N9 DL FAR、Remove old N3 PDR、Remove old S5 PDR、Remove FAR、Create Core QER、Update Core PDR を送信します。
8b	H-UPF は、N4 Session Modification 要求を H-SMF に送り返します。
9	SMF は、Nsmf_PDUSession_UpdateSMContext 応答を V-SMF に送り返します。

5G ローマーから 4G ホーマーへの PLMN 間 HO

このコールフローでは、5G ローマーから 4G ホーマーへの PLMN 間 HO について説明します。

Figure 31: 5G ローマーから *4G* ホーマーへの *PLMN* 間 *HO* のコールフロー

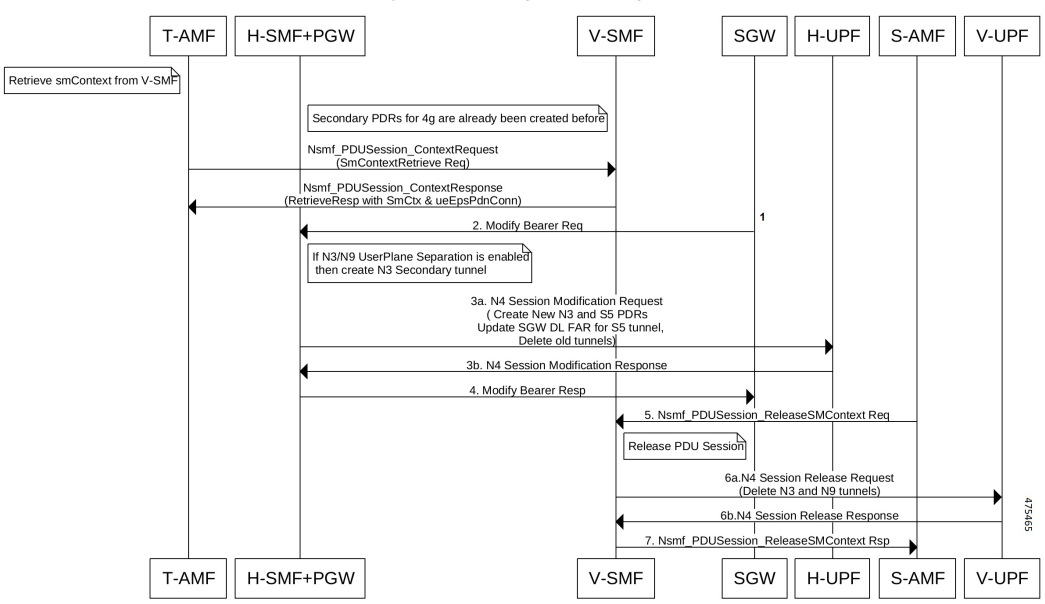


Table 98: 5G ローマーから *4G* ホーマーへの *PLMN* 間 *HO* のコールフローの説明

手順	説明
1	UE が H-PLMN（5G ローマー）から V-PLMN（4G ホーマー）に移動します。
2	S-GW は、Modify Bearer 要求を H-SMF に送信します。ここで、N3/N9 UserPlane Separation が有効になっている場合は、N3 セカンダリトンネルを作成します。
3a	H-SMF は、次の IE で N4 Session Modification 要求を H-UPF に送信します。Create S5 PDR（古い S5-U FTEID）、Create N3 PDR（新しい FTEID の CH ビットセット）、Create S5 DL FAR、Remove old N9 PDR、Remove old S5 PDR、Remove FAR、Update Core QER
3b	H-UPF は、N4 Session Modification 要求を H-SMF に送り返します。
4	H-SMF は、Modify Bearer 応答を S-GW に送り返します。
5	S-AMF は、Release PDU Session を含む Nsmf_PDUSession_ReleaseSMContext 要求を V-SMF に送信します。
6a	V-SMF は、Delete N3、N9 トンネルを含む N4 Session Release 要求を V-UPF に送信します。
6b	V-UPF は、N4 Session Release 応答を V-SMF に送り返します。
7	V-SMF は、Nsmf_PDUSession_ReleaseSMContext 応答を S-AMF に送り返します。

標準準拠

HR ローミングサポート機能は、次の標準規格に準拠しています。

- 3GPP TS 23.502 "Procedures for the 5G System"
- 3GPP TS 29.061 "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)"
- 3GPP TS 29.244 16.5.0 "Interface between the Control Plane and the User Plane nodes"

制限事項

HR ローミングサポート機能には、次の制限があります：

- Router Advertisement（RA）または Router Solicitation（RS）パケットは、vUPF のデフォルト QFI PDR で課金およびカウントされます。
- vUPF では、QER 適用ポリシングはサポートされていません。
- vUPF では、LI はサポートされていません。
- UPF は、入力インターフェイスで 2 つの GTPU エンドポイントをサポートします。
- セカンダリ PDR 最適化のサポートは、既存のコールには有効になりません。
- アップグレード後、Create PDR で送信元インターフェイスタイプが使用できない場合、既存のコールでは、サービスは、インターフェイスタイプに基づいて選択されません。
- N9、S5U、および S8U インターフェイスタイプは、同じパブリック IP でのみサポートされ、異なる IP ではサポートされません。
- PLMN 間ハンドオーバーは、セカンダリ PDR 最適化でのみ機能します。
- アクセス側の PDR 処理が失敗した場合、UPF は、両方の PDR（プライマリとセカンダリ）ではなく、失敗した PDR ID のみを報告します。

UPF の HR ローミングサポートを構成する

この項では、UPF の HR ローミングサポート機能を構成する方法について説明します。

vUPF でビジターコールのバッファリングサポートを構成する

vUPF でビジターコールのバッファリングサポートを構成するには、次の CLI コマンドを使用します。

```
config
  user-plane [converged mode | buffered-packet-count [ instance-limit
 instance_limit_value { session-limit session_limit_value} | { session-limit
```

```
session_limit_value { instance-limit instance_limit_value} ] ]
  exit
```

注：

- **buffering-packet-count**：パケットをバッファリングするための最大セッションとインスタンス制限を構成します。
- **instance-limit** *instance_limit_value*：各 SessMgr インスタンス事にすべてのセッションに対してバッファリングするパケットの最大数を構成します。デフォルト範囲は、1 ～ 10000 です。
- **session-limit** *session_limit_value*：各セッションでバッファリングするパケットの最大数を構成します。デフォルト範囲は、1 ～ 255 です。

vUPF でビジターコールのバッファリングサポートを確認する

vUPF でビジターコールの通信のバッファリング制限のサポートを確認するには、**show configuration** CLI コマンドを使用します。

以下のコードは、CLI コマンドの出力例です。

```
[local]qvpc-si# show configuration
...
...
    #exit
  user-plane buffered-packet-count session-limit 5 instance-limit 10
  context ingress
…
…
```

GTP-U サービスと N9 インターフェイス アソシエーションを構成する

GTP-U サービスと N9 インターフェイスのアソシエーションを構成するには、次の CLI コマンドを使用します。

```
config
  context ingress
    user-plane-service user-plane-service
          associate gtpu-service service_name [ cp-tunnel | pgw-ingress
 | sgw-egress | sgw-ingress | upf-egress | upf-ingress | interface-type
 [ n9 | s5u | s8u | n3 | n9-s5u-s8u ] ]
          no associate gtpu-service upf-egress
    exit
  exit
exit
```

注：

- **upf-egress**：N9 インターフェイスに使用する UPF エグレスとしてインターフェイスタイプを構成します。
- **interface-type [n9 | s5u | s8u | n3 | n9-s5u-s8u]**：希望する GTP-U 入力インターフェイスタイプを構成します。

単一のパブリック IP アドレスが N9、S5u、および S8u インターフェイスタイプに使用されている場合は、**n9-s5u-s8u** インターフェイスタイプを使用します。

- **no associate gtpu-service upf-egress**：GTP-U サービスおよび N9 インターフェイス アソシエーションを削除するように構成します。

GTP-U サービスと N9 インターフェイス アソシエーションを確認する

GTP-U サービスと N9 インターフェイス アソシエーションを確認するには、**show user-plane-service all** CLI コマンドを使用します。

以下のコードは、CLI コマンドの出力例です。

```
[local]qvpc-si# show user-plane-service all

Service name                          : user-plane-service
  Service-Id                          : 6
  Context                             : ingress
  Status                              : STARTED
  UPF Ingress GTPU Service            : sx-gtpu-service
  UPF Egress GTPU Service             : sx-upf_egress_gtpu
  SGW Ingress GTPU Service            : sx-sgw_ingress_gtpu
  SGW Egress GTPU Service             : sx-sgw_egress_gtpu
….
[local]qvpc-si# show configuration context ingress
config
  context ingress
....
...
   user-plane-service user-plane-service
      associate gtpu-service sx-gtpu-service upf-ingress
      associate gtpu-service sx-upf_egress_gtpu upf-egress
      associate gtpu-service sx-sgw_ingress_gtpu sgw-ingress
      associate gtpu-service sx-sgw_egress_gtpu sgw-egress
      associate gtpu-service up-gtpu cp-tunnel
      associate sx-service sxu
      associate control-plane-group g1
    exit
...
```

サブパラメータ IE のローミングステータス

次に、ローミング 状態を表示する Sub-Params IE の例を示します。

```
SUBSCRIBER PARAMS:
Type: 226
Rat-Type: 3
SGSN-Address: 20.20.20.17
ULI: ECGI=216354001234c800
GGSN-Address: 20.20.20.3
Roaming-Status: Homer/Roamer/Visitor-hr/Visitor-LBO
```

Source Interface Type IE

Source Interface Type IE は、送信元インターフェイスの 3GPP インターフェイスタイプを示します。

3GPP Interface Type IE は、PDR IE 内の送信元インターフェイスの 3GPP インターフェイスタイプ、またはFAR IE内の接続先インターフェイスの3GPPインターフェイスタイプを示します。

次に、送信元インターフェイスタイプを表示する Create PDR の例を示します。

```
CREATE PDR:
    Type: 1
    Value:
PDR ID:
    Type: 56
    Value:
        RULE ID: 0x0002
PRECEDENCE:
    Type: 29
    Value: 0x00000001

PDI:
Type: 2
Value:
SOURCE INTERFACE:
    Type: 20
    Value: CORE (1)
Traffic Endpoint ID:
    Type: 131
    Value: 0x0001
SOURCE INTERFACE TYPE:
    Type: 160
    Value: N9 (0x0F)
FAR ID:
    Type: 108
    Value: 0x8002
RULEBASE:
    Type: 207
    Value:
QER ID:
    Type: 109
    Value: 0x80000001
```

モニタリングおよびトラブルシューティング

のこ項では、この機能の障害対応情報について説明します。

show user-plane-service statistics all

ユーザープレーンサービスの統計をモニターするには、次の CLI コマンドを使用します。

show user-plane-service statistics all

次に、出力例を示します。

```
[local]qvpc-si# show user-plane-service statistics all

…
PDNs By PLMN-Type:
 Homer Subscriber PDNs:
    Active:                          0    Setup:                          0
    Released:                    0
 Roamer Subscriber PDNs:
    Active:                          0    Setup:                          0
```

```
    Released:                        0
  Visited-Home-Routed Subscriber PDNs:
    Active:                             0    Setup:                                0
    Released:                        0
  Visited-Local-Breakout Subscriber PDNs:
    Active:                             0    Setup:                                0
    Released:                        0
…
Inter-PLMN Handover Statistics:
   Attempted  : 0                     Succeeded  : 0
   Failed.        : 0

  Intra-PLMN Handover Statistics:
   Attempted   : 0                     Succeeded  : 0
    Failed.        : 0
…
  PDNs Rejected By Reason:
…
…
  Data Statistics Related To Paging:
    Packets Buffered:                   5    Bytes Buffered:                   420
    Packets Discarded:                  1    Bytes Discarded:                   84

  Total Data Statistics:
```

show subscribers user-plane-only full all

ユーザープレーンサービスを使用しているすべてのサブスクライバを表示するには、次のCLIコマンドを使用します。

show subscribers user-plane-only full all

次に、出力例を示します。

```
….
Converged Session: No                 Converged Peer Callid:      n/a
Visited Call: Yes
Subscriber Parameters:
…..
Interface Type: N4
….
Subscriber Parameters:
IMSI: 123456789012345
….
Old Rat Type: 6
…
Session-ID: 1414146500000001
Roaming Status: Homer
Old Roaming Status: Homer
…
```

show subscribers user-plane-only callid pdr full all

show subscribers user-plane-only callid *call_id* **pdr full all** コマンドは、すべての PDR 情報を表示します。

[送信元インターフェイスタイプ（Source Interface Type）] フィールドには、SMF から受信した Source Interface Type IE が表示されます。

次に、このコマンドの出力例を示します。

show subscribers user-plane-only callid *call_id* **pdr full all**

```
show subscribers user-plane-only callid 0098e4b0 pdr full all
Callid: 0098e4b0
Interface Type: N4
…
Matched Bytes:            0
Matched Packets:          0
Precedence:               0
Source Interface:         Access
Source Interface Type:    N9
Local F-TEID:    0x16001
Local F-TEID IP Addr:
  IPv4:          20.20.20.15
  IPv6:          N/A
…
Bearer Level Info-id:   N/A
Secondary Pdr Info:
   Pdr ID :   2 / NA
   Local F-TEID:    0x1a001
   Local F-TEID IP Addr:
         IPv4:          20.20.20.15
         IPv6:          N/A
   QoS Flow Identifier: 1 / NA
   Source Interface Type:  S5U
```

show user-plane-service gtpu statistics gtpu-service n9-egress

以下は、UPF にアクセスするためのこのコマンドの出力例です。

```
[local]Test-UPF4# show user-plane-service gtpu statistics gtpu-service n9-egress

Total Data Stats:
Uplink Packets: 10 Uplink Bytes: 2400
Downlink Packets: 10 Downlink Bytes: 2400
Packets Discarded: 0 Bytes Discarded: 0

QoS Stats:

QCI 1:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 2:
Uplink Packets: 8 Uplink Bytes: 1920
Downlink Packets: 8 Downlink Bytes: 1920
Packets Discarded: 0 Bytes Discarded: 0

QCI 3:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 4:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 5:
Uplink Packets: 0 Uplink Bytes: 0
```

```
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 6:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 7:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 8:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 9:
Uplink Packets: 2 Uplink Bytes: 480
Downlink Packets: 2 Downlink Bytes: 480
Packets Discarded: 0 Bytes Discarded: 0

QCI 65:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 66:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 69:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 70:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 80:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 82:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 83:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

Non-Std QCI(Non-GBR):
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
```

```
Packets Discarded: 0 Bytes Discarded: 0

Total uplink packets GBR QCI's: 8
Total uplink Bytes GBR QCI's: 1920
Total Downlink packets GBR QCI's: 8
Total Downlink Bytes GBR QCI's: 1920
Total uplink packets Non-GBR QCI's: 2
Total uplink Bytes Non-GBR QCI's: 480
Total Downlink packets Non-GBR QCI's: 2
Total Downlink Bytes Non-GBR QCI's: 480

Path Management Messages:
Echo Request Rx: 29 Echo Response Rx: 10
Echo Request Tx: 10 Echo Response Tx: 29
SuppExtnHdr Tx: 0 SuppExtnHdr Rx: 0

Peer Stats:
Total GTPU Peers: 1
Total GTPU Peers with Stats: 1

Tunnel Management Messages:
Error Indication Tx: 0
Error Indication Rx: 0
Error Indication Rx Discarded: 0
```

show user-plane-service gtpu statistics gtpu-service n9-ingress

以下は、ローミング UPF に対するこの コマンド の出力例です。

```
[local]Test-UPF3# show user-plane-service gtpu statistics gtpu-service n9-ingress

Total Data Stats:
Uplink Packets: 25 Uplink Bytes: 6000
Downlink Packets: 24 Downlink Bytes: 5760
Packets Discarded: 0 Bytes Discarded: 0

QoS Stats:

QCI 1:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 2:
Uplink Packets: 19 Uplink Bytes: 4560
Downlink Packets: 18 Downlink Bytes: 4320
Packets Discarded: 0 Bytes Discarded: 0

QCI 3:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 4:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 5:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0
```

```
QCI 6:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 7:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 8:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 9:
Uplink Packets: 6 Uplink Bytes: 1440
Downlink Packets: 6 Downlink Bytes: 1440
Packets Discarded: 0 Bytes Discarded: 0

QCI 65:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 66:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 69:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 70:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 80:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 82:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

QCI 83:
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

Non-Std QCI(Non-GBR):
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0
Uplink Packets: 0 Uplink Bytes: 0
Downlink Packets: 0 Downlink Bytes: 0
Packets Discarded: 0 Bytes Discarded: 0

Total uplink packets GBR QCI's: 19
```

```
Total uplink Bytes GBR QCI's: 4560
Total Downlink packets GBR QCI's: 18
Total Downlink Bytes GBR QCI's: 4320
Total uplink packets Non-GBR QCI's: 6
Total uplink Bytes Non-GBR QCI's: 1440
Total Downlink packets Non-GBR QCI's: 6
Total Downlink Bytes Non-GBR QCI's: 1440

Path Management Messages:
Echo Request Rx: 10 Echo Response Rx: 31
Echo Request Tx: 31 Echo Response Tx: 10
SuppExtnHdr Tx: 0 SuppExtnHdr Rx: 0

Peer Stats:
Total GTPU Peers: 1
Total GTPU Peers with Stats: 1

Tunnel Management Messages:
Error Indication Tx: 0
Error Indication Rx: 0
Error Indication Rx Discarded: 0
```



第 43 章

セキュリティグループタグ（SGT）ベースのアクセスコントロール

- SGACL 経由のユーザーアクセスコントロール （502 ページ）
- ISE 統合向け SGACL の仕組み （504 ページ）
- UPF でのセカンダリ ISE サーバーの統合 （506 ページ）
- ISE 統合向け SGACL 構成 （510 ページ）
- モニタリングおよびトラブルシューティング （515 ページ）

SGACL 経由のユーザーアクセスコントロール

表 *99 :* 機能の履歴

機能名	リリース情報	説明
セキュリティグループタグ（SGT）ベースのアクセス コントロール リスト（SGACL）によるユーザー アクセス制御	2024.03.0	UPF は、ダウンリンクパケットへの SGACL の適用のための Cisco ISE 統合をサポートしています。SGACL とは、セキュリティ グループ メンバーの承認を制御および管理するアクセス制御リスト（ACL）です。 UPF は、接続先 SGT（D-SGT）に基づく API クエリ経由で ISE から SGACL マトリックスをフェッチします。D-SGT は、SMF から Sx または N4 インターフェイス経由で受信されます。次に、UPF は、ダウンリンクパケットの D-SGT と送信元 SGT（S-SGT）マッピングに基づいて SGACL を適用します。したがって、Cisco ISE からのポリシーの適用が有効になります。 **デフォルト設定**：無効：有効にするには設定が必要。
UPF での Cisco Identity Services Engine（ISE）統合向けセキュリティグループタグ（SGT）	2023.03	UPF は、SMF から受信した SGT を処理するための ISE 統合をサポートしています。SMF は、RADIUS サーバーから SGT を受信します。次に、SMF は Session Establishment 要求中に、Sx または N4 インターフェイス経由で UPF に SGT を送信します。 SGT は、Cisco ISE または SMF の静的ポリシーに従って作成されます。UPF では、アップリンクパケットの Cisco Meta Data（CMD）ヘッダーに SGT を挿入する必要があります。 **デフォルト設定**：該当なし

セキュリティグループタグ（SGT）は、信頼されたネットワーク内における通信の送信元の権限を指定します。TrustSec または ISE にセキュリティグループを追加すると、セキュリティ グループ アクセスは、自動で SGT を生成します。Cisco ISE は、集中管理型ポリシーエンジンとして、他のシスコのパケットコア要素に対して統合されたポリシー管理体験を提供します。

S-SGT は 16 ビット値で、レイヤ 2 イーサネットフレームの [Cisco Meta Data（CMD）] フィールドで送信されます。CMDヘッダーは、「.1Q」タグの後に挿入されます（ある場合）。「.1Q」タグがない場合、CMD は MAC 送信元アドレスの直後に続きます。

ISE 統合で SGT をサポートするには：

- SMF は、ISE サーバーから D-SGT を受信します。
- SMF は N4 拡張機能を使用して UPF に対して D-SGT を更新します。
- UPF はパケットを識別し、D-SGT と S-SGT の組み合わせを N6 DL パケットに適用します。

セキュリティ グループ アクセス コントロール リスト（SGACL）とは、セキュリティ グループ メンバーの承認を制御および管理するアクセス制御リスト（ACL）です。SGACL は、セキュリティ グループ タグ マトリックス（SGT マトリックス）で表される SGACL ポリシーを作成します。

SGT マトリックスは、権限マトリックスとも呼ばれ、TrustSec ドメインの SGACL ポリシーを表します。このマトリックスは、セキュリティグループ番号と接続先セキュリティグループ番号で構成され、2 つのエンドポイントの通信方法を示します。適用可能なポリシーは、Permit と Deny です。SGT マトリックスと SGACL の内容は、REST API を使用して ISE サーバーからダウンロードされます。

UPF は、N6 インターフェイス経由で送信されるアップリンクパケットの D-SGT 値を挿入します。UPF は、N6 インターフェイス経由でダウンリンクパケットの S-SGT 値を受信します。この S-SGT 値は、マトリックスルックアップに使用され、N3 インターフェイスを介した発信ダウンリンクパケットの送信中に削除されます。

接続先 SGT（D-SGT）と送信元 SGT（S-SGT）間のマッピングに基づいて、ポリシーは UPF で適用され、適切な SGACL がダウンリンクパケットに適用されます。

UPF は、次の SGT 値によるダウンリンクパケットの SGACL 適用に向けて ISE 統合をサポートしています。

- 接続先 SGT（D-SGT）：UPF は、N4 インターフェイス経由のサブスクライバセッションごとに、Session Establishment 要求の SMF からこの値を受信します。SMF は、RADIUS Access Accept メッセージで ISE から D-SGT を受信します。この機能では、SMF は N4 インターフェイスの proprietary IE で SGT を UPF に送信する必要があります。
- 送信元 SGT（S-SGT）：ダウンリンクパケットの CMDヘッダーで受信します。ワイヤレス LAN コントローラ（WLC）またはアクセススイッチは、この値を挿入します。

（注）

- SMF は、Access Accept メッセージで ISE から D-SGT を受信します。この機能では、SMF は N4 インターフェイスの proprietary IE で SGT を UPF に送信する必要があります。
- SGACL 経由でユーザー アクセス コントロールが有効になっている場合、サブスクライバ セッションが D-SGT を受信すると、SGACL がダウンリンクパケットに適用されます。この場合、APN ACL は、これらのサブスクライバセッションには適用されません。
- SGACL 経由でユーザー アクセス コントロールを有効にしない場合、または UPD が、N4 Session Establishment 要求中に D-SGT を受信しない場合、APN ACL は、既存の構成に従って適用されます。

ISE サーバープロファイルは、**ise-server-profile** *profile_name* CLI コマンドを使用して定義でき、ISE サーバープロファイルは、**associate ise-server-profile name** *server_profile_name* CLI コマンドを使用して、UPF を関連付けることができます。

ISE 統合向け SGACL の仕組み

この項では、ISE 統合用の SGACL の仕組みについて説明します。

- SMF は RADIUS 経由で ISE から対応する SGT 値をフェッチし、N4 インターフェイスで UPF に送信します。
- 各 UPF は、ISE サーバーでネットワークアクセスデバイス（NAD）として登録されます。
- UPF は、REST API を使用して ISE サーバーから SGT マトリックスおよび対応する SGACL をダウンロードします。UPF は、D-SGT から S-SGT へのマッピングに基づいて、フローに対して SGACL を適用します。
- 非リアルタイムの更新は、UPF からの定期的またはトリガ ベースのプルを通じて利用できます。
- セッションリカバリと ICSR ベースのリカバリでは、D-SGT 値をチェックポイント指定する必要があります。

通話フロー

次の図は、SGT フェッチと SGACL 適用のコールフローを示しています。

ステップ	説明
1	SMF は、N4 Session Establishment 要求を UPF に送信します。この要求の一部として、UPF は SMF から D-SGT 値を受信します。
2	UPF は、N4 Session Establishment 応答を SMF に送信します。

ステップ	説明
3	特定の D-SGT の最初のセッションの場合、UPF は ISE サーバーに REST API要求を送信して D-SGT 列の値をフェッチします。
4	ISE は、REST API 応答を UPF に送信します。この応答には、D-SGT に対してマッピングされた S-SGT 値と、SGACL 名を含む SGACL マトリックス情報と更新タイマーが含まれます。 SGT マトリックスセルエントリと SGACL は UPF に保存されます。各 D-SGT 列には、ISE で設定された更新タイマーがあります。
5	UPF は、REST API 要求を ISE サーバーに送信して、必要な SGACL をフェッチします。 ISE は、SGACL 定義を使用して、REST API 応答を UPF に送信します。
6	N3 はアップリンク（UL）データを UPF に送信します。
7	UPF はイーサネットヘッダーに D-SGT を追加し、UL データを N6 インターフェイスに送信します。
8	N6 はダウンリンク（DL）データを N3 インターフェイスに送信します。
9	UPF は D-SGT と S-SGT のマッピングをチェックし、SGACL を適用します。
10	UPF は、SGT を使用せずに DL データを N3 インターフェイスに転送します。

制限事項

この機能には、次の既知の制限事項があります。

- PFCP Session Establishment 要求は、N4 インターフェイス経由で D-SGT 値に送信されます。D-SGT は変更できませんが、S-SGT は変更できます。
- ACL は特定の SGT ペアの組み合わせに対してスタックできるため、SGACL は特定の SGT ペアに対して受信した ACL の順序に従って適用されます。
- 推奨されるマトリックスの組み合わせの最大数は、150 D-SGT 列 × 150 S-SGT 行で、デフォルトの SGACL を含む 255 の異なる SGACL があります。
- 1 つのセルに含まれる SGACL の最大数は 16 に制限されています。
- UPF は、一度に 1 つのデフォルト SGACL のみを保存できます。したがって、デフォルトの SGACL が変更されると、更新された SGACL 情報のみが UPF に保存されます。

UPF でのセカンダリ ISE サーバーの統合

表 *100* : 機能の履歴

機能名	リリース情報	説明
UPF でのセカンダリ ISE サーバーのサポート	2025.03.0	

機能名	リリース情報	説明
		この機能により、ネットワークオペレータは UPF でセカンダリ ISE サーバーを統合できます。 セカンダリ ISE サーバー統合は、プライマリ ISE サーバーがダウンしたときに SGACL のシームレスな適用を保証する障害メカニズムを提供します。 **コマンドの拡張**： • **[secondary-server { ipv4_address** *ipv4_address* **| ipv6-address** *ipv6_address* **}]**：この CLI は、セカンダリサーバー IP アドレスを構成します。 • **[secondary username** *user_name* **password** *password* **]**：この CLI は、セカンダリユーザー名とパスワードを構成します。 • **[secondary-certificate** *certificate_path* **]**：この CLI は、セカンダリ証明書パスを構成します。 • **[secondary-ca-certificate** *ca_certificate_path* **]**：この CLI は、セカンダリ CA 証明書を構成します。 • **[secondary-key** *key_path* **]**：この CLI は、セカンダリキーパスを構成します。 **導入されたコマンド**： • **max-retransmissions** *max_retrans_count*：この CLI は、最大再試行回数を構成します。 • **retransmission-timeout** *timeout_duration*：この CLI は、は再送信タイムアウト

機能名	リリース情報	説明
		を構成します。 • **backoff-period** *backoff_duration*：この CLI は、バックオフ期間を構成します。 **デフォルト設定**：無効：有効にするには構成が必要です

ISE サーバーは、UPF にポリシーを適用します。ただし、ISE サーバーに到達できないまたは ISE サーバーが停止しているなど、ISE サーバーでのサービス障害が原因で、UPF はポリシーを更新またはリフレッシュできない場合があります。

セカンダリ ISE サーバーを統合すると、UPF はポリシーの動作状態を維持し、シームレスなポリシーの適用を保証できます。

セカンダリ ISE サーバー統合の仕組み

process_workflow

これらの段階は、UPF でのセカンダリ ISE サーバーサポートのプロセスの概要です。

1. UPF は、プライマリ ISE サーバーを「アクティブ」としてマークします。アクティブなプライマリ ISE サーバーは、すべての REST API 要求を受信します。
2. UPF がプライマリ ISE サーバーとの接続を試行したが、プライマリ ISE サーバーが応答しない場合、UPF は設定された再送信回数と再送信タイムアウトに従って再接続を試行します。
3. 再接続の試行が失敗した場合、UPF は現在の「アクティブ」サーバーを「非アクティブ」としてマークします。次に、UPF は、構成に従って、セカンダリ ISE サーバーを「アクティブ」としてマークします。セカンダリ ISE サーバーを設定するには、「セカンダリ ISE サーバープロファイルを構成する」項を参照してください。

   ネットワークオペレータは、CLI を使用してアクティブな ISE サーバーを手動で選択できます。

   手動設定の詳細については、「アクティブな ISE サーバーに手動で切り替える」 項を参照してください。
4. 現在「アクティブ」とマークされているサーバーは、同じ REST API 要求の受信を開始します。
5. ISE サーバーからポリシーをまだ受信していない場合、UPF は、デフォルトのポリシーまたはポリシー使用不可処理を適用します。

6. UPF は、サーバーを「アクティブ」としてマークする前に、セカンダリ ISE サーバーが最近「非アクティブ」とマークされていないことを確認します。両方のサーバーに到達不能な場合に UPF がループする問題を防ぎます。

   プライマリ ISE サーバーで障害を検出した後、UPF がセカンダリ ISE サーバーでも障害を検出した場合、またはその逆の場合、UPF は代替サーバーへの再試行を行わないはずです。これにより、UPF がループ内の ISE サーバーに到達するのを防ぎます。

   UPF は、構成されたバックオフ期間を使用してこの動作を制御します。

バックオフ期間

プライマリ ISE サーバーからセカンダリ ISE サーバーに、またはその逆に切り替えている間、両方のサーバーが到達不能な場合、UPF はループ状態になります。これを回避するために、UPF がプライマリまたはセカンダリ ISE サーバーとの接続を試行する前に、バックオフ期間が待機期間として使用されます。

バックオフ期間は、継続的な再試行による過剰なネットワーク通信とリソースの消費を防ぎます。

バックオフ期間は、ISE サーバープロファイルで設定できます。

セカンダリ ISE サーバー統合の制限事項

次に、UPF でのセカンダリ ISE サーバー統合の既知の制限事項を示します。

- ISE サーバーのエラーは、次回の REST API コールでのみ検出されます。
- プライマリまたはセカンダリ ISE サーバーの正常性に対するアクティブなモニタリングはありません。
- フェールオーバー中の REST API の場合、追加される遅延には、障害検出時間（再送信試行に基づく）およびアクティブな ISE サーバーからの接続時間または応答時間が含まれます。
- 認証の失敗によって、セカンダリ ISE サーバーへのスイッチオーバーがトリガーことは想定されていません。
- 関連する REST API 間でスイッチオーバーが発生する可能性があるため、プライマリ ISE サーバーとセカンダリ ISE サーバー間での SGT または SGACL のデータベース同期を前提としています。
- UPF は、ピアサーバー間のデータベースバージョンの不一致を検出しません。
- 定期的な更新または CLI がトリガーした更新は、以前にフェッチされたポリシーと同期していることを前提に、現在のアクティブなサーバーで実行されます。
- アクティブな ISE サーバーへのスイッチオーバーが発生すると、UPF は既存の SGACL またはポリシーを再学習しません。

再学習により遅延が増えるため、すべてのフローをオンボーディングする必要があるため、スループットに影響します。

ISE 統合向け SGACL 構成

この項では、ISE 統合向け SGACL を構成する手順について説明します。

API Manager を有効にする

API Manager は、REST API 経由で API 要求と応答の統合を可能にする機能です。

（注） API マネージャの有効化は、SGACL 統合の前提条件です。

手順

ステップ 1 構成モードを開始します。

ステップ 2 **require apimgr** コマンドを入力します。

例：

```
config
   require apimgr
end
```

この CLI コマンドは、新しいプロシージャを生成する起動構成の一部です。

次のタスク

1. ISE サーバープロファイルを構成する
2. ISE サーバープロファイルを関連付ける

ISE サーバープロファイルを構成する

次の手順では、ISE サーバープロファイルを設定します。

始める前に

ISE サーバープロファイルを設定する前に、API マネージャを有効にする必要があります。API マネージャの設定の詳細については、「API マネージャを有効にする」項を参照してください。

手順

ステップ 1 CLI **[no] ise-server-profile** *profile-name* を使用して、コンテキスト EPC モードで ISE サーバープロファイルのインスタンスを作成します。

例：

```
[local]UPF1(config)# context EPC
[local]UPF1(config-ctx)# ise-server-profile ise_1
[local]UPF1(config-ctx)#
```

ステップ 2 CLI **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address***}** を使用して、バインド IPv4 および IPv6 アドレスを指定します。

例：

```
[local]UPF1(config-ctx)# bind ipv4-address 192.0.2.1
[local]UPF1(config-ctx)#
```

ステップ 3 CLI **server { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **} [secondary-server { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}]** を使用して、プライマリ ISE サーバーとセカンダリ ISE サーバーを構成します。

例：

```
[local]UPF1(config-ctx)# server ipv4-address 192.0.2.254 secondary-server ipv4-address
 198.51.100.1
```

ステップ 4 CLI **username** *user_name* **encrypted | password** *password* **[secondary username** *user_name* **password** *password* **]** を使用してプライマリ ISE サーバーとセカンダリ ISE サーバーのユーザー名とパスワードを構成します。

例：

```
[local]UPF1(config-ctx)# username ise1 password cisco1
cisco2secondary username ise2 password  cisco2
[local]UPF1(config-ctx)#
```

（注） show configuration 出力では、パスワードは暗号化された形式で表示されます。

ステップ 5 プライマリおよびセカンダリ ISE サーバーの証明書、CA 証明書、およびキーを構成します。

a) CLI **certificate** *certificate_path* **[secondary-certificate** *certificate_path* **]** を使用して、証明書を構成します。

例：

```
[local]UPF1(config-ctx)# certificate /root/certificate/client/client.cert.pem
secondary-certificate /root/certificate/client/client2.cert.pem
[local]UPF1(config-ctx)#
```

b) CLI **ca-certificate** *ca_certificate_path* および **[secondary-ca-certificate** *ca_certificate_path* **]** を使用して CA 証明書を構成します。

例：

```
[local]UPF1(config-ctx)# ca-certificate /root/certificate/ca.cert.pem
secondary-ca-certificate /root/certificate/ca.cert2.pem
[local]UPF1(config-ctx)#
```

c) CLI **key** *key_path* **[secondary-key** *key_path* **]** を使用して、キーを構成します。

例：

```
[local]UPF1(config-ctx)# key /root/certificate/client/client.key.pem
secondary-key /root/certificate/client/client2.key.pem
[local]UPF1(config-ctx)#
```

ステップ 6 CLI **policy-unavailable-treatment [drop | pass]** GACL マトリックスが具体的な D-SGT に対して使用できない場合の通信処理を指定します。

例：

```
[local]UPF1(config-ctx)# policy-unavailable-treatment drop
[local]UPF1(config-ctx)#
```

ステップ 7 最大再送信回数、再送信タイムアウト、およびバックオフ期間を設定します。

a) CLI **max-retransmissions** *max_retrans_count* を使用して、サーバーが応答しない場合の最大再送信回数を構成します。

例：

```
[local]UPF1(config-ctx)# max-retransmissions 6
[local]UPF1(config-ctx)#
```

CLI **max-retransmissions** *max_retrans_count* は、最大再試行回数を 0 ～ 15 の範囲で構成します。デフォルト値は 3 です。

b) CLI **retransmission-timeout** *timeout_duration* を使用して再送信タイムアウトを構成します。

例：

```
[local]UPF1(config-ctx)# retransmission-timeout 4000
[local]UPF1(config-ctx)#
```

retransmission-timeout *timeout_duration* 要求を ISE サーバーに再送信する前にタイムアウト期間を 1 ～ 300 秒の間で構成します。デフォルト値は 3 秒です。

c) CLI **backoff-period** *backoff_duration* を使用して、バックオフ期間を構成します。現在の構成モードを保存して終了します。

例：

```
[local]UPF1(config-ctx)# backoff-period 400
[local]UPF1(config-ctx)# exit
```

CLI **backoff-period** *backoff_duration* は、ISE サーバー y への再試行が保留される期間を構成します。デフォルト値は、200 秒です。

次のタスク

ISE サーバープロファイルを設定したら、それを既存のユーザープレーンサービスに関連付ける必要があります。詳細については、「ISE サーバープロファイルを関連付ける」項を参照してください。

アクティブな ISE サーバーに手動で切り替える

次の手順では、現在アクティブな ISE サーバーに手動で切り替えることができます。

始める前に

現在アクティブな ISE サーバーに手動で切り替える前に、ISE サーバープロファイルでセカンダリ ISE サーバーを構成します。「ISE サーバープロファイルを構成する」 項を参照してください。

手順

実行モードで、コマンド **select ise-server { primary | secondary}** を実行し、手動でアクティブな ISE SNMP に切り替えます。

例：

```
[local]laas-si-setup# select ise-server secondary
```

- 手動切り替え後、UPF は、古いあアクティブ ISE サーバーからの未処理の REST API レスポンスを受信し、UPF はそれらを処理します。
- 保留中のすべての再試行は、ISE サーバーに適用されます。このサーバーは、再試行リクエストを受信します。
- コマンド **select** は、隠しキーワードです。

ISE サーバープロファイルを関連付ける

定義されると、ISE サーバープロファイルは、既存の UPF サービス構成と関連付けられます。

始める前に

ISE サーバープロファイルを構成する

手順

ステップ 1 ユーザープレーンサービス構成モードを開始します。

ステップ 2 定義された ISE サーバープロファイルを、既存の UPF サービス構成と関連付けます。

例：

```
user-plane-service UPlane1
      associate ise-server-profile name ise_1
  #exit
```

D-SGT 列を更新する

各 D-SGT 列には、ISE で設定された更新タイマーがあります。更新タイマーの構成に基づいて、または UPF CLI トリガー経由で、D-SGT 列の値が REST API クエリ経由で ISE サーバーから再度取得されます。ISE からの API レスポンスに基づいて、SGT マトリックスまたは SGACL のバージョンが変更された場合、UPF はそれぞれのマトリックスセルまたは SGACL 情報をローカルで更新します。必要に応じて、更新後に対応する SGACL がダウンロードされます。

始める前に

1. ISE サーバープロファイルを構成する
2. ISE サーバープロファイルを関連付ける

手順

ステップ 1 Exec モードを開始します。

ステップ 2 **refresh-sgt-column** *d_sgt* コマンドを入力して、ISE サーバーから列の値をフェッチして、D-SGT 列の更新をトリガーします。

例：

```
refresh-sgt-column d-sgt
```

（注） CLI はすぐに返されますが、バックグラウンドでのポリシーのダウンロードには時間がかかるため、更新の完了にも時間がかかる場合があります。

以下は、**refresh-sgt-column** *d_sgt* CLI コマンドの出力例で、*d_sgt* 値は、*65535* に設定されます。

```
refresh-sgt-column 65535
```

モニタリングおよびトラブルシューティング

SGACL と SGT 統合を確認する

この項では、SGACL と SGT の統合機能に関する show コマンドとその出力について説明します。

show subscribers user-plane-only full callid *callid_value*

この CLI コマンドの出力が強化され、UPF の ISE 統合の D-SGT 関連情報を表示する **SGT Value** フィールドと SGACL 経由でユーザーアクセスコントロール関連の情報を表示する **SGACL match stats** フィールドが追加されました。

```
show subscribers user-plane-only full callid 00004e3a
   Local SEID      : [0x0004000000000003] 1125899906842627
  Remote SEID     : [0x00000436b7616206] 4633051357702
  State           : Connected

....

  input pkts: 20                                  output pkts: 16
  input bytes: 9246                               output bytes: 11248
  input bytes dropped: 0                          output bytes dropped: 5624
  input pkts dropped: 0                           output pkts dropped: 8

....

  SGT Value: 0x001a

....

QoS-Group Statistics:
QGR Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
------------------- ---------- ---------- ---------- ---------- ---------- --------------
  ------------------  -----------------

SGACL Match stats:
ACL Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
--------------------- ---------- ---------- ---------- ---------- -------------
ACL2611                       4       1432          0          0             2
ACL2612                       4       4112          0          0             2
ACL2621                       8       5704          0          0             4
....

Total subscribers matching specified criteria: 1
```

show subscribers user-plane-only callid *callid_value* flows full

この CLI コマンドの出力は、SGACL 経由のユーザー アクセス コントロール関連の情報を表示する **Uplink SGT**、**Downlink SGT** および **Matched SGACL** フィールドで拡張されています。

```
show subscribers user-plane-only callid 00004e21 flows full
  Callid: 00004e21
  Interface Type: Sxab
  IP address: n/a
```

```
  Flow ID: 1:1
  Uplink pkts: 1                    Downlink pkts: 1
  Uplink bytes: 1040                Downlink bytes: 40
…
  Downlink Sfp Id: NA
  Uplink SGT: 0xA1
  Downlink SGT: 0xB5
  Matched SGACL: ACL_123
```

show user-plane-service sgt-column summary

このCLIコマンドの出力には、UPFで使用可能なすべてのD-SGT値とISEサーバーから受信した更新タイマーの概要が表示されます。

次の出力例では、**D-SGT Columns fetched**および**D-SGT Version**フィールドのD-SGT値を示しています。

```
show user-plane-service sgt-column summary
 D-SGT Columns fetched:
 D-SGT      Version
 ---------------------------------------
 65535         0
   7           0
 Total D-SGT column(s) found: 2
```

show user-plane-service sgt-column dsgt

このCLIコマンドの出力は、D-SGTクエリ中にISEから受信したD-SGTおよびS-SGTごとのSGACLマトリックスの概要を表示します。

以下の出力例では、**D-SGT**、**Refresh TimeS-SGT**、**SGACL Name**、**Version**および**Total SGT column(s) found**フィールドを示しています。

```
show user-plane-service sgt-column dsgt 26
```

```
    D-SGT: 26            Refresh Time: 86400
    S-SGT: 1
    SGACL Name           Version
    ---------------------------------------
    ACL2611                              0
    ACL2612                              0

    S-SGT: 2
    SGACL Name                      Version
    ---------------------------------------
    ACL2621                              0

  Total SGT column(s) found: 1
```

show user-plane-service sgacl name

このCLIコマンドの出力には、SGACLクエリ中にISEから受信した具体的なSGACL定義ルール行を表示します。

```
show user-plane-service sgacl name AACL2
 SGACL Name: AACL2
```

```
permit ip
Total SGACL(s) found: 1
```

show user-plane-service statistics sgacl all

この CLI コマンドの出力には、SGACL に従ったパケット一致統計が表示されます。

```
show user-plane-service statistics sgacl all

ACL Name              Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
--------------------- ---------- ---------- ---------- ---------- -------------
SGACL1-REFRESH2          6           1156       0          0          2
SGACL1-REFRESH1         13           9344       0          0          6
Allow All                0              0       0          0          0

Total SGACL(s) : 3
```

show user-plane-service statistics drop-counter

この CLI コマンドの出力は、SGACL アプリケーションが原因でドロップされたパケットを表示するように拡張されています。

```
show user-plane-service statistics drop-counter
Packet Drop Data Statistics:
        ------------------------------------------------
...
        FastPath Misc Drops:
            Overload Protection:                    0
            Invalid Client:                         0
            Stream ID 0:                            0
            Invalid Stream ID:                      0
        OHR Mismatch Packet Drops:                  0
       SGACL Packet Drops:                      8
        SGACL No Policy Packet Drops:              2
        No Default SGT cell Packet Drops:          0
```

（注）

- **No Default SGT cell Packet Drops** は、廃止されたカウンタです。既存の設計では、デフォルトの ACL が使用できない場合にのみパケットを通過させることができます。
- ISE server REST API 要求および応答の統計がサポートされています。

show apimgr statistics ise-server

show apimgr statistics ise-server には、ISE サーバー統計の状態が表示されます。

```
[local]qvpc-si# show apimgr statistics ise-server

Ise-Server Connection Statistics:

Server: 10.10.10.30           Current state: Active
Last Inactive Time:          0000:00:00:00:00:00
Request sent:                          5
Response Success:                      4
Response Fail:                         1

Server: 10.10.10.40           Current state: Inactive
```

```
Last Inactive Time:            2025:01:16:12:30:11
Request sent:                         0
Response Success:                     0
Response Fail:                        0
```

SNMP トラップ

UPF た、別の ISE サーバーに切り替わるたびに、トラップ **ISEServerSwitchoverOccured** が生成されます。

OAM のサポート

バルク統計情報

SGACL 機能によるユーザー アクセス コントロールでは、次の新しいバルク統計がサポートされています。

スキーマ：**UPF**	
統計	**説明**
downlink-total-pkts-sgacl-matched	SGACL と一致したダウンリンクパケットの総数
downlink-total-bytes-sgacl-matched	SGACL と一致したダウンリンクバイトの総数
downlink-total-pkts-sgacl-dropped	SGACL との一致が原因でドロップしたダウンリンクパケットの総数
downlink-total-bytes-sgacl-dropped	SGACL との一致が原因でドロップされたダウンリンクバイトの総数



第 44 章

セッションリカバリ

- 機能の概要と変更履歴 （519 ページ）
- 機能説明 （520 ページ）
- 機能の仕組み （520 ページ）
- セッションリカバリをサポートするためのシステムの設定 （521 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：ライセンスが必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

堅牢なハードウェアフェールオーバーと冗長性保護により、システム上のハードウェアやソフトウェアの障害を迅速に修正できます。ただし、さまざまな理由でソフトウェアの障害が発生する可能性があり、ほとんどの場合、何の前触れもありません。

この章では、ハードウェアまたはソフトウェアに障害が発生した場合に、サブスクライバセッション情報のシームレスなフェールオーバーと再構築を行うセッションリカバリ機能について説明します。



重要 セッションリカバリは、シスコのライセンス対象機能です。別の機能ライセンスが必要になる場合があります。特定のライセンス要件の詳細については、シスコのアカウント担当者にお問い合わせください。

機能の仕組み

この項では、この機能の実装方法とリカバリプロセスについての概要を示します。

セッションリカバリ機能は、システム内のハードウェアまたはソフトウェアに障害が発生した場合に、サブスクライバセッション情報のシームレスなフェールオーバーと再構築を行い、完全に接続されたユーザーセッションが切断されるのを防ぎます。

セッションリカバリは、システム内の重要なソフトウェアプロセス（セッションマネージャやAAA マネージャなど）をミラーリングすることによって実行されます。これらのミラー化されたプロセスはアイドル状態（スタンバイモード）を維持し、ソフトウェア障害が発生した場合（セッションマネージャのタスクが中止された場合など）に必要になるまでいかなる処理も実行しません。

セッションリカバリが適切に動作しない場合があります。セッションリカバリ動作中に、新たなソフトウェアまたはハードウェアの障害が発生します、たとえば、AAA マネージャは、そこに含まれていた状態情報が、新たにアクティブになったセッションマネージャのタスクの入力に使用されている間に失敗します。



重要 セッションリカバリ動作の後、マネージャごと（AAA マネージャ、セッションマネージャなど）に収集および保持された統計など、一部の統計は、通常は回復されません。アカウンティングおよび課金関連の情報のみがチェックポインティングされ、回復します。

セッションリカバリをサポートするためのシステムの設定

次に、現在、動作している運用システム（着信コールを受け入れることができる）か、動作していないシステム（実稼働ネットワークに含まれておらず、そのためライブサブスクライバ/カスタマーのデータを処理していない）のいずれかに対してセッションリカバリ機能を設定する手順を示します。



重要 機能使用キーがある場合でも、デフォルトでは、セッションリカバリ機能はシステム上で無効になっています。

セッションリカバリの有効化

前述したように、アウトオブサービス（OOS）でコンテキストがまだ設定されていないシステム、または現在コールを処理できるインサービスシステムで、セッションリカバリを有効にすることができます。ただし、システムがインサービスである場合は、セッションリカバリ機能が有効になる前に再起動する必要があります。

アウトオブサービスシステムでのセッションリカバリの有効化

次に、コンテキストが設定されていないシステムの場合の手順を示します。

サービス停止中のシステムでセッションリカバリ機能を有効にするには、次の手順を実行します。この手順は、EXEC モードプロンプトで開始することを前提としています。

手順

ステップ 1 EXEC モードのプロンプトで、**show license info** コマンドを実行し、システム上のセッションと機能の使用ライセンスを介してセッションリカバリ機能が有効になっていることを確認します。

セッションリカバリ機能の現在のステータスが [Disabled] になっている場合は、ライセンスキーをシステムにインストールするまで、この機能を有効にすることはできません。

ステップ 2 セッションリカバリを有効にするには、次の設定例を使用します。

```
configure
  require session recovery
  end
```

（注） このコマンドを設定した後で、設定を保存してからシャーシをリロードし、コマンドを有効にする必要があります。設定ファイルを保存してシャーシをリロードする方法については、使用している展開の『System Administration Guide』を参照してください。

ステップ 3 「設定の確認と保存」の説明に従って、設定を保存します。

起動すると、システムはセッションリカバリを有効にし、ミラーリングされた「スタンバイモード」のタスクをすべて作成し、パケット処理カードの予約やその他の操作を自動的に実行します。

ステップ 4 システムが構成され、稼働状態になったら、「セッションリカバリ状態を表示する」に記載されている通りこの機能をサポートするためにシステムの準備が整ったかどうかを確認します。

インサービスシステムでのセッションリカバリの有効化

すでに保存されている設定があるシステムでセッションリカバリを有効にすると、セッションリカバリコマンドは、設定ファイル内のサービス構成コマンドの前に自動的に配置されます。

稼働中のシステムでセッションローカライズ変数機能を有効にするには、以下の手順を実行します。この手順は、EXEC モードプロンプトで開始することを前提としています。

手順

ステップ 1 EXEC モードのプロンプトで、**show license info** コマンドを実行し、システム上のセッションと機能の使用ライセンスを介してセッションリカバリ機能が有効になっていることを確認します。

セッションリカバリ機能の現在のステータスが [Disabled] になっている場合は、ライセンスキーをシステムにインストールするまで、この機能を有効にすることはできません。

ステップ 2 セッションリカバリを有効にするには、次の設定例を使用します。

```
configure
  require session recovery
  end
```

この機能は、システムが再起動されるまでは有効になりません。

ステップ 3 「設定の確認と保存」の説明に従って、設定を保存します。

ステップ 4 **reload** コマンドを入力して、システムの再起動を実行します。

次のプロンプトが表示されます。

```
Are you sure? [Yes|No]:
```

Yes と入力して、システム再起動の実行を確認します。

再起動すると、システムはセッションリカバリを有効にし、ミラーリングされた「スタンバイモード」のタスクをすべて作成し、パケット処理カードの予約やその他の操作を自動的に実行します。

ステップ 5 システムを再起動したら、「セッションリカバリ状態を表示する」に記載されている通りこの機能をサポートするためにシステムの準備が整ったかどうかを確認します。

上級ユーザーはテキストユーザーなどの手段を使用して、**require session recovery** コマンドシンタックスを既存の設定ファイルに挿入してから、設定ファイルを手動で適用することもできます。このコマンドが既存の設定ファイルの最初の数行の間に配置されるようにする際は注意してください。これは、ローカル以外のコンテキストの作成よりも前に表示される必要があります。

セッションリカバリ機能の無効化

システムでセッションリカバリ機能を無効にするには、グローバル構成モードのプロンプトから **no require session recovery** コマンドを入力します。



重要 このコマンドがインサービスシステムで発行された場合は、**reload** コマンドを発行してシステムを再起動する必要があります。

セッション リカバリ ステータスの表示

システムがセッションリカバリを実行できるかどうかを確認するには、イネーブルにして、Exec モードプロンプトから **show session recovery status verbose** コマンドを入力します。

このコマンドの出力は、次に示す例のようになります。

```
[local]host_name# show session recovery status
Session Recovery Status:
     Overall Status             :  SESSMGR Not Ready For Recovery
     Last Status Update         :  1 second ago

[local]host_name# show session recovery status
Session Recovery Status:
    Overall Status              :  Ready For Recovery
    Last Status Update          :  8 seconds ago

[local]host_name# show session recovery status verbose
Session Recovery Status:
    Overall Status              :  Ready For Recovery
    Last Status Update          :  2 seconds ago

               ----sessmgr----       ----aaamgr----         demux
 cpu state     active    standby     active    standby      active    status
---- -------   ------    -------     ------    -------      ------    -------------
 1/0 Active    7         1           7         1            7         Good
[local]host_name#
```

再作成されたセッション情報を表示する

セッション状態情報とセッション再作成状態を表示するには、次のコマンドを入力します。

show subscriber debug-info callid *id*

次に、このコマンドのセッションリカバリ操作が実行される前と後の両方の出力例を示します。わかりやすくするために、この例の [Redundancy Status] フィールドを太字で示しています。

```
username: user1              callid: 01ca11b1                  msid: 0000100003
    Card/Cpu: 4/2
    Sessmgr Instance: 7
    Primary callline:
   Redundancy Status: Original Session
      Checkpoints        Attempts        Success        Last-Attempt       Last-Success
          Full:               69             68             29800ms            29800ms
          Micro:             206            206             20100ms            20100ms
      Current state: SMGR_STATE_CONNECTED
      FSM Event trace:
            State                             Event
            SMGR_STATE_OPEN                   SMGR_EVT_NEWCALL
            SMGR_STATE_NEWCALL_ARRIVED        SMGR_EVT_ANSWER_CALL
            SMGR_STATE_NEWCALL_ANSWERED       SMGR_EVT_LINE_CONNECTED
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_LINK_CONTROL_UP
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_AUTH_REQ
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_IPADDR_ALLOC_SUCCESS
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_UPDATE_SESS_CONFIG
            SMGR_STATE_LINE_CONNECTED         SMGR_EVT_LOWER_LAYER_UP
    Data Reorder statistics
    Total timer expiry:               0        Total flush (tmr expiry):    0
            Total no buffers:         0        Total flush (no buffers):    0
            Total flush (queue full): 0        Total flush (out of range):  0
            Total flush (svc change): 0        Total out-of-seq pkt drop:   0
            Total out-of-seq arrived: 0
    IPv4 Reassembly Statistics:
              Success:                0        In Progress: 0
              Failure (timeout):      0        Failure (no buffers): 0
              Failure (other reasons): 0
    Redirected Session Entries:             Allowed:
  2000            Current:                                  0
                Added:                                    0               Deleted:
                                  0
                Revoked for use by different subscriber: 0
    Peer callline:
     Redundancy Status: Recreated Session
    Checkpoints        Attempts        Success        Last-Attempt        Last-Success
          Full:               0              0                0ms                 0ms
          Micro:              0              0                0ms                 0ms
      Current state: SMGR_STATE_CONNECTED
      FSM Event trace:
            State                                                       Event
            SMGR_STATE_LINE_CONNECTED           SMGR_EVT_LOWER_LAYER_UP
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED                SMGR_EVT_REQ_SUB_SESSION
            SMGR_STATE_CONNECTED                SMGR_EVT_RSP_SUB_SESSION
            SMGR_STATE_CONNECTED                SMGR_EVT_ADD_SUB_SESSION
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
            SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
```

```
        SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_REQ
        SMGR_STATE_CONNECTED                SMGR_EVT_AUTH_SUCCESS
Data Reorder statistics
        Total timer expiry:        0         Total flush (tmr expiry):  0
        Total no buffers:          0         Total flush (no buffers):  0
        Total flush (queue full):  0         Total flush (out of range):0
        Total flush (svc change):  0         Total out-of-seq pkt drop: 0
        Total out-of-seq arrived:  0
IPv4 Reassembly Statistics:
          Success:                   0       In Progress:               0
          Failure (timeout):         0       Failure (no buffers):      0
          Failure (other reasons):   0
Redirected Session Entries:
          Allowed:                2000        Current:             0
          Added:                              Deleted:             0
          Revoked for use by different subscriber:  0
```



第 45 章

Session Report Rejection 手順

- 機能の概要と変更履歴 （527 ページ）
- 機能説明 （527 ページ）
- OAM のサポート （529 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G SMF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.02.0

機能説明

SMF は、SMF と UPF の課金設定に不一致がある場合、特定の原因コードで UPF が発信したセッション レポート要求を拒否します。

SMF によるセッション レポートの拒否の場合、UPF はローカルでセッションを消去します。SMF は消去処理を認識せず、N4 メッセージを UPF に送信し続けます。このアクションにより、ローカルでパージされたセッションの SMF に「コンテキストが見つかりませんでした」というメッセージが UPF が送信されます。

この動作は、UE エクスペリエンスに影響を与え、課金データが失われます。そのため、セッション レポート エラーの処理の現在の実装は、UPF でのセッションのローカル消去を回避し、セッションのグレースフル クリアをサポートするように変更されています。

この変更により、UPF はセッション レポート エラー応答を無視します。SMF がセッション削除要求をトリガーし、その後セッション レポートの拒否が続きます。UPF は削除要求に応答し、セッションをグレースフルにクリアします。

他の機能との関係

この機能には、SMF と UPF にいくつかの動作変更を実装することが関係しています。SMF の新しいCLI構成は、この動作を制御するのに役立ちます。SMF の動作変更の詳細については、『*UCC 5G SMF* の構成およびアドミニストレーション ガイド』の「*Session Report Rejection* 手順をサポートする」章を参照してください。

通話フロー

次の図は、Session Report Rejection 手順のフローを説明しています。

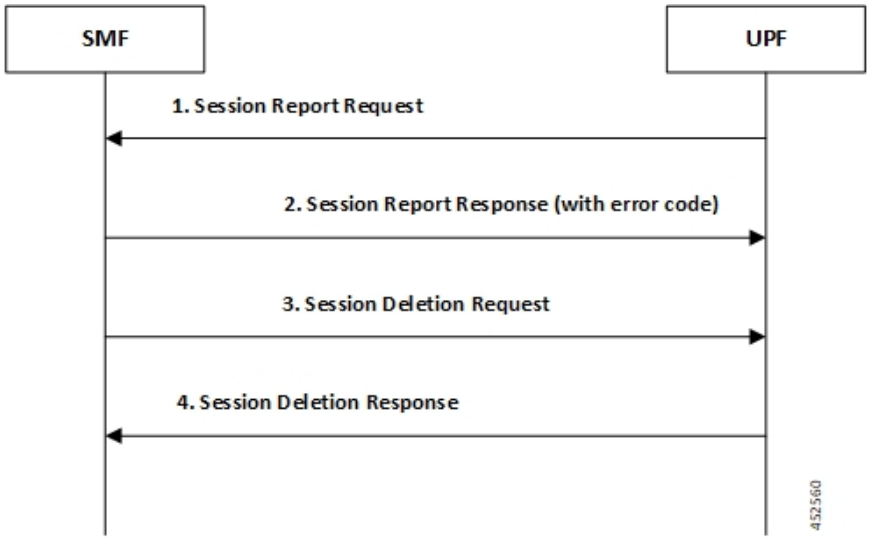


表 *101 : Session Report Rejection* 手順コールフロー

ステップ	説明
1	UPF が、Session Report メッセージを SMF に送信します。 （SX_SESSION_REPORT_REQUEST）

ステップ	説明
2	SMF は、いくつかのエラーコードでメッセージを拒否します。 （エラーコード付き SX_SESSION_REPORT_RESPONSE）
3	UPF は、Session Report エラー応答を無視します。 SMF は、Session Delete 要求を開始して、セッションを正常に切断します。 （SX_SESSION_DELETION_REQUEST）
4	UPF は削除要求に応答し、セッションを正常にクリアします。 （SX_SESSION_DELETION_RESPONSE）

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンスに関して説明します。

Show コマンドや出力

show user-plane-service statistics all

カウンタ「Skapped Local Purge」が、「理由による PDN リリース」項の **show user-plane-service statistics all** CLI コマンドに追加されました。

- **スキップしたローカル消去**：SMF/CP から UPF/UP にセッションレポートエラーがトリガーされると増分します。



第 46 章

ソフトウェア管理の運用

- 機能の概要と変更履歴 （531 ページ）
- 概要 （532 ページ）
- SNMP トラップ （533 ページ）
- 制限事項 （533 ページ）
- 正常性チェック （534 ページ）
- ビルドアップグレード （536 ページ）
- UPF アップグレード （538 ページ）
- UPF のダウングレード （538 ページ）

機能の概要と変更履歴

要約データ

表 *102* : 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点：	N/A
関連資料	該当なし

更新履歴

表 *103* : マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.2

概要

5G UPF は、SMF および UPF でのソフトウェアリリースの後方互換性をサポートします。この機能により、1 つ前のリリース（N-1）との間でソフトウェアをシームレスにアップグレードまたはダウングレードできます。この機能には、次のサポートが含まれます。

- ICSR モードの 2 つの UP におけるソフトウェアリリースの N-1 互換性：UPF 1:1 冗長性シナリオで、UPF をバージョン間でシームレスにアップグレードできます。
- SMF と UPF 間のソフトウェアリリースの N-1 互換性：関連付けられた SMF または UPF をバージョン間でシームレスにアップグレードできます。
- マルチ Sx を使用した SMF と UPF 間のソフトウェアリリースの N-1 互換性：マルチ Sx シナリオで、関連付けられた SMF または UPF をバージョン間でシームレスにアップグレードできます。

重要 ソフトウェアバージョンをアップグレードまたはダウングレードする前に、シスコのアカウント担当者に連絡して、手順に関するサポートを受けてください。

SMF と UPF 間のバージョン交換

SMF と UPF がペアペアリングされると、バージョンまたはリリース情報が交換されます。リリース情報は、UPF がアクティブとスタンバイ間で交換された Heartbeat メッセージ経由のスタンバイ UPF（1:1 冗長化シナリオ）とペアリングされた場合に交換されます。

互換性のないリリースがペアリングされると、アラーム（SNMP トラップ）が発生します。詳細については、「SNMP トラップ」項を参照してください。

リリース情報の交換中にピアバージョンを示すために、関連付け要求およびハートビート要求メッセージに次の新しい IE が含まれています。

情報要素	P	条件/コメント	IE の長さ	IE ID
ピアバージョン	O	ピア GR/PFCP バージョンと StarOS バージョンを指定するために使用されます。	4 バイト	245
		ビット		

情報要素	P	条件/コメント						IE の長さ		IE ID
	オクテット	8	7	6	5	4	3	2	1	
	1 ～ 2	ピアバージョン IE タイプ = 245（10 進数）								
	3 ～ 4	長さ = n バイト								
	5 ～ 8	ピア GR/PFCP バージョン								
	9 ～ 12	StarOS GR バージョン								
	13 ～ 13	StarOS バージョン文字列長								
	可変長	StarOS バージョン文字列値								

SNMP トラップ

互換性のないリリースとのペアリングが行われると、次の SNMP トラップが発生します。

SNMP トラップ	説明
SRPPeerUnsupportedVersion	上位バージョンのアクティブ/スタンバイ UPF は、ピアのバージョンが N-1 よりも下位の場合に SNMP トラップを発生させます。
SRPPeerUnsupportedVersionClear	上位バージョンのアクティブ/スタンバイ UPF は、SNMP トラップを発生させて SRPPeerUnsupportedVersion をクリアします。
SxPeerUnsupportedVersion	上位バージョンの UPF は、ピアのバージョンが N-1 よりも下位の場合に SNMP トラップを発生させます。
SxPeerUnsupportedVersionClear	上位バージョンの UPF は、SNMP トラップを発生させて SxPeerUnsupportedVersion をクリアします。

制限事項

この機能には次の既知の制限事項があります。

- ピアバージョンがサポートされている N-1 バージョンよりも低いと判断された場合、関連付けとペアリングが許可されますが、同じ機能の側面は保証されません。

注意 互換性のないバージョンからはアップグレードしないでください。アップグレードパスや手順については、シスコのアカウント担当者にお問い合わせください。

- 一部の CLI コマンドは、N+1 バージョンではサポートされていない場合があります。
- SMF バージョンは、UPF バージョンと互換性がある必要があります。
- ハードウェア構成は、アクティブとスタンバイの両方の UPF で同様である必要があります。
- SNMP トラップは、StarOS バージョンに関しては最新バージョンのノードによって発生します。詳細については、この章の「SNMP トラップ」項を参照してください。
- リリース 2022.01.2 以降、RCM はチェックポイントに依存せず、将来の UPF リリースのサポートを可能にします。現在、RCM は N-1 互換性のみをサポートしています。

正常性チェック

シャーシのアップグレード、ダウングレード、またはリロードの各操作の後に、次の正常性チェックを実行します。

1. アクティブシャーシのサービス冗長性プロトコル（SRP）情報を確認して、SRP スイッチオーバー中の問題を回避し、SRP スイッチオーバーの前にプロアクティブな分析の実施が必要かどうかを判断します。次の CLI コマンドを使用します。
   - **srp validate-configuration**
   - **srp validate-switchover**
   - **show srp info**

   次に、出力例を示します。

   ```
   Peer Configuration Validation: Complete
   Last Peer Configuration Error: None
   Last Peer Configuration Event: Wed Mar 18 15:34:02 2022  (1602 seconds ago)
   Last Validate Switchover Status: None
   Connection State: Connected
   ```

   次のパラメータを確認します。
   - **Peer Configuration Validation: Complete**：「進行中」と表示されている場合は、15 秒ほど待機してから **show srp info** CLI コマンドを実行します。
   - **Last Peer Configuration Error: None**：「ピアチェックサム検証エラー」と表示されている場合は、アクティブシャーシとスタンバイシャーシ間で構成の相違があり、修正しなければならないこと示しています。

（注） **Last Peer Configuration Error** でエラーが見つかった場合、アクティブ UPF とスタンバイ UPD の両方で **show configuration srp** CLI コマンドを使用して構成を検証します。

- **Last Validate Switchover Status: None**：出力は、「None」と表示される必要があります。また、**srp validate-configuration** および **srp validate-switchover** CLI コマンドが実行された場合、出力は、*Remote Chassis - Ready for Switchover (XX seconds ago)* となる必要があります。
- **Connection State: Connected**：出力は、「Connected」と表示される必要があります。

2. アクティブシャーシとスタンバイシャーシの両方のサブスクライバ数を確認します。

   セッションが起動したら、アクティブシャーシで **show subscribers summary | grep Total** CLI コマンドを実行します。次に、出力例を示します。

```
show subscribers summary | grep Total
   Total Subscribers:  100
```

   スタンバイシャーシで、**show srp checkpoint statistics | grep allocated** CLI コマンドを実行します。次に、出力例を示します。

```
show srp checkpoint statistics | grep allocated
   Current pre-allocated calls:  100
```

3. **show license information** CLI コマンドを実行して、ライセンスの状態を確認します。状態は [期限切れ（Expired）] ではなく、[良好（冗長化）（Good (Redundant)）] である必要があります。

4. **show session recovery status verbose** CLI コマンドを実行して、セッション リカバリ ステータスを確認します。次に、出力例を示します。

```
Session Recovery Status:
  Overall Status        : Ready For Recovery
  Last Status Update    : 7 seconds ago

              ----sessmgr---  ----aaamgr----  demux
 cpu state    active standby  active standby  active  status
1/0  Active     8      1        8      1        17     Good
```

5. **show srp checkpoint statistics | grep Sessmgrs** CLI コマンドを実行して、スタンバイシャーシのすべての SessMgr が [スタンバイで接続済み（Standby-Connected）] 状態であることを確認します。次に、出力例を示します。

```
Number of Sessmgrs:        1
Sessmgrs in Active-Connected state:  0
Sessmgrs in Standby-Connected state: 8
Sessmgrs in Pending-Active state:    0
```

6. すべてのカードのステータスを確認して、[Active] 状態か [Standby] 状態かを確認します。次に、出力例を示します。

```
show card table
```

```
Slot          Card Type              Oper State  SPOF  Attach
------------ ---------------------- ----------- ----- ------
1: VC        5-Port Virtual Card     Active        -
```

7. **show task resources | grep -v good** CLI コマンドを実行します。出力には SessMgr とセッションの総数のみが表示される必要があります。
8. **show crash list** CLI コマンドを実行して、新しいクラッシュがあるかどうかを確認します。
9. **show service all** CLI コマンドを実行して、状態が [初期化済み（Initialized）] ではなく [起動済み（Started）] と表示されていることを確認します。

ビルドアップグレード

バックアップ設定

1. 現在の構成をバックアップする：ダウングレードやアップグレードに使用した現在の構成を保存します。これには、現時点で存在する可能性のあるすべての機能と構成が含まれます。
2. 変更またはアップグレードを実行する前に、アクティブシャーシとスタンバイシャーシの両方で **show support details** を収集します。
3. ヘルスチェックを実行します。

アップグレード手順

1. 両方のノードでシャーシのヘルスチェックを実行します。
2. スタンバイ状態のセカンダリシャーシ（ICSR）で、起動優先順位を N+1 ビルドに変更します。
3. 最新のビルドバージョンにリロードします。
4. スタンバイシャーシで新しい構成の変更を行います（たとえば、新しいCLI、ライセンス、または設定の変更）。
5. リロードされたシャーシで正常性チェックを実行します。クラッシュやエラーを確認します。

スイッチオーバーの実行

1. 両方のシャーシで SRP をアクティブからスタンバイに切り替える前に、以下の点を確認します。
    1. アクティブシャーシ：**show subscriber summary | grep Total**
    2. スタンバイシャーシ：**show srp checkpoint statistics | grep allocated**

（注） カウントは、両方のシャーシで同じである必要があります。

3. アクティブおよびスタンバイシャーシ：**show sx peer**

   次に例を示します。

```
|||||  Sx Service                                                    No of
|||||  ID                                                                Restart
|||||  |                                                 Recovery              |
   Current    Max        Peer
vvvvv  v     Group Name    Node ID         Peer ID     Timestamp             v
   Sessions   Sessions   State
----- ---- ---------------- ------------------------ ------------------- ------
 --------- --------- --------
CAAXD  22    CPGROUP21   209.165.200.225   50331649    2021-03-17:02:33:55    0
        0          0      NONE

Total Peers:    1
```

（注） ピアの状態はアクティブであり、関連付けられている必要があります。ピアIDは両方のシャーシで一致する必要があります。

4. スタンバイシャーシ：**show srp checkpoint statistics | grep Sessmgrs**

（注） 「Number of Sessmgrs」は「Sessmgrs in Standby-Connected state」と同じである必要があります。

5. アクティブシャーシ：

   1. **srp validate-configuration**：この CLI コマンドは、アクティブシャーシで構成検証チェックを開始します。検証結果、エラーが無い場合は、この CLI コマンドの出力は空欄になります。
   2. **srp validate-switchover**：アクティブシャーシとスタンバイシャーシの両方で計画 SRP スイッチオーバーの準備ができていることを検証します。スイッチオーバーの準備ができている場合、この CLI コマンドの出力は空欄になります。
   3. **show srp info | grep "Last Validate Switchover Status"** ：この CLI コマンドの出力は次のようになります。

      ```
      Last Validate Switchover Status: Remote Chassis - Ready for Switchover
      ```

   4. **show srp info debug**：アクティブシャーシとスタンバイシャーシの出力は同じである必要があります。

2. アクティブシャーシ：**srp initiate-switchover**

1. 両方のノードでシャーシのヘルスチェックを実行します。また、「スイッチオーバーを実行する」の項の手順 1a と手順 1c を確認します。5% の差が生じる場合があります。
2. 新しいセッションは新しいアクティブシャーシで処理されるため、コールテストを実行します。
3. 「アップグレード手順」の項のステップ 2 からステップ 5 で説明されているように、古いアクティブシャーシをアップグレードします。

UPF アップグレード

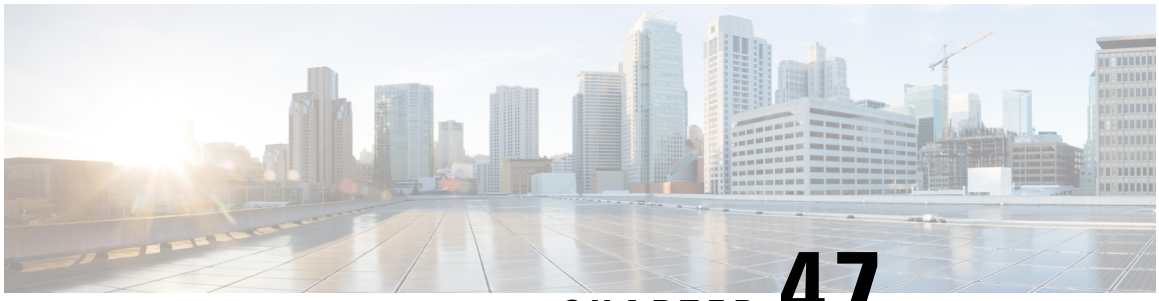
この項では、UPF アップグレードの手順について説明します。

1. 「正常性チェック （534 ページ）」項で言及されている両方の UPF ノードで Health Check 手順を実効します。
2. 「ビルドアップグレード （536 ページ）」項で言及されているスタンバイ UPF でアップグレードを実行します。
3. アップグレードされたスタンバイシャーシで「sx-peer configuration」を実行します。
4. 両方の UPF ノードで、正常性チェックを実行してから、UPF スイッチオーバーを実行します。
5. 「ビルドアップグレード （536 ページ）」項で言及されている新しいスタンバイ UPF をアップグレードします。

UPF のダウングレード

UPF をダウングレードには、次の手順を実行します。

1. UPF で正常性チェックを実行します。
2. スタンバイ UPF でブートの優先順位を N-1 ビルドに変更します。スタンバイ UPF をリロードします。
3. ダウングレードされたスタンバイ UPF で「sx-peer configuration」を実行します。
4. 両方の UPF ノードで正常性チェックを実行してから、UPF スイッチオーバーを実行します。
5. 新しいスタンバイ UPF で、手順 1 ～ 3 を実行します。



CHAPTER 47

標準 QCI のサポート

- 機能の概要と変更履歴, on page 539
- 機能説明 （540 ページ）
- 構成 （540 ページ）

機能の概要と変更履歴

要約データ

Table 104: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2021.02.0

機能説明

5G-UPF は、Mission Critical and Push-to-Talk（MC/PTT） アプリケーションに関する 3GPP TS 23.203 リリース 12 に基づいて、新しい標準規格の QoS Class Index（QCI）をサポートします。

この機能の一環として、次の機能がサポートされます。

- 新しい標準規格の非 GBR QCIs（69、70、80）を使用したデフォルトベアラー QCI/QFI が設定されている LTE/WiFi/5G-NR コールの確立。これらは、MC- PTT および 5G-NSA QCI です。
- 新しい標準規格 GBR/非 GBR QCI（65、66、69、70、80、82、83）を使用したダイナミックルールの確立。
- 新しい標準規格 QCI（80、82、および 83）での DCNR 対応 UE の拡張 QoS ビットレートのサポート。
- LTE から 5G および 5G から LTE HO、WiFi から 5G および 5G から WiFi HO、および LTE から WiFi および WiFi から LTE HO がサポートされています。
- 新しい標準規格 QCI に基づく UL および DL 方向の DSCP マーキング。

制限事項

このリリースでは、新しい標準QCIに合わせて事前定義されたルールはサポートされません。

構成

新しい標準 QCI を有効にするために SMF または UPF で必要な構成（またはライセンス）はありません。

SMF で、拡張 QoS ビットレートを有効にするには、次の構成が必要です。

```
configure
  profile dnn name
    dcnr { true | false }
    end
```

- **dcnr**：新しい無線（DCNR）とのデュアル接続を指定します。



第 48 章

システム ログ

この章では、さまざまなタイプのロギングに関連するパラメータを設定する方法と、その内容を表示する方法について説明します。内容は次のとおりです。

- 機能の概要と変更履歴 （541 ページ）
- システムログのタイプ （542 ページ）
- イベントロギングパラメータの設定 （543 ページ）
- アクティブログの設定 （550 ページ）
- ファシリティの指定 （550 ページ）
- トレースロギングの設定 （560 ページ）
- モニターログの設定 （561 ページ）
- ロギング設定と統計情報の表示 （561 ページ）
- CLI を使用したイベントログの表示 （562 ページ）
- クラッシュログの設定と表示 （563 ページ）
- 過剰なイベントロギングの削減 （566 ページ）
- ログのチェックポインティング （567 ページ）
- ログファイルの保存 （568 ページ）
- イベント ID の概要 （570 ページ）

機能の概要と変更履歴

要約データ

表 *105 :* 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要

このリリースでの関連する変更点：	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

表 *106 :* マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

システムログのタイプ

システムで設定および表示できるログには、次の 5 つのタイプがあります。

重要 すべてのイベントログをすべての製品で設定できるわけではありません。設定可能性は、使用されているハードウェア プラットフォームとライセンスによって異なります。

- **イベント**：イベントロギングを使用して、システムのステータスを判断し、システムで使用されているプロトコルとタスクに関する重要な情報をキャプチャできます。これは、すべてのコンテキスト、セッション、およびプロセスに適用されるグローバル機能です。
- **アクティブ**：アクティブログは、 CLI instance-by-CLI インスタンスベースでオペレータが設定可能です。1 つの CLI インスタンスで管理ユーザーによって設定されたアクティブログは、別の CLI インスタンスの管理ユーザーによって表示することはできません。各アクティブログは、システムに対してグローバルに設定されているものとは独立したフィルタプロパティと表示プロパティを使用して設定できます。イベントが生成されると、アクティブログがリアルタイムで表示されます。
- **トレース**：トレースロギングを使用して、接続されている特定のサブスクライバセッションで発生する可能性のある問題を迅速に分離できます。トレースは、特定のコール ID（callid）番号、IP アドレス、モバイルステーション ID（MSID）番号、またはユーザー名に対して実行できます。
- **モニター**：モニターロギングは、特定のセッションに関連付けられているすべてのアクティビティを記録します。この機能は、特定のサブスクライバのモニタリング機能に関する司法当局の要請を遵守するために使用できます。モニターは、サブスクライバの MSID またはユーザー名に基づいて実行できます。
- **クラッシュ**：クラッシュロギングには、システムソフトウェアのクラッシュに関する有用な情報が保存されています。この情報は、クラッシュの原因を特定するのに役立ちます。



重要 ステートフルファイアウォールと NAT は、ロギングがファイアウォールに対して有効になっている場合に、画面上のさまざまなメッセージのロギングをサポートします。これらのログは、critical、error、warning、および debug などのさまざまなレベルで詳細なメッセージを提供します。ステートフルファイアウォールと NAT 攻撃ログは、攻撃によってドロップされたパケットの送信元 IP アドレス、宛先 IP アドレス、プロトコル、または攻撃タイプに関する情報も提供します。また、システムで設定されている場合は、syslog サーバーにも送信されます。ステートフル ファイアウォールおよび NAT のロギングサポートの詳細については、『*PSF* アドミニストレーション ガイド』または『*NAT* アドミニストレーション ガイド』の「*Logging Support*」の章を参照してください。

イベントロギングパラメータの設定

システムは、ユーザー定義のフィルタに基づいてログを生成するように設定できます。フィルタは、システムがモニターするファシリティ（システムタスクまたはプロトコル）と、イベントエントリの生成をトリガーするシビラティ（重大度）レベルを指定します。

イベントログはシステムメモリに保存され、CLI を使用して表示できます。イベントロギング情報を保存する 2 つのメモリバッファがあります。最初のバッファには、アクティブなログ情報が保存されます。2 番目のバッファには、非アクティブなロギング情報が保存されます。非アクティブバッファは一時的なリポジトリとして使用され、データを上書きせずにログを表示できます。ログは、手動による介入によってのみ非アクティブバッファにコピーされます。

各バッファには最大 50,000 のイベントを保存できます。これらのバッファがキャパシティに達すると、最も古い情報が削除され、最新の情報を保存するための領域が確保されます。

ログデータの損失を防ぐために、ネットワーク インターフェイスを介して syslog サーバーにログを送信するようにシステムを設定できます。

イベントログフィルタの設定

Exec モードおよびグローバル構成モード レベルでイベントログの内容をフィルタリングできます。

Exec モードのフィルタリング

これらのコマンドを使用すると、グローバル ロギング パラメータを変更することなく、ログに含まれるデータの量を制限できます。

Exec モードのコマンドを介してログをフィルタ処理するには、次の例に従います。

アクティブなフィルタリング

logging active [copy runtime filters] [event-verbosity *event_level* **] [pdu-data** *format* **] [pdu-verbosity** *pdu_level* **]**

注：

- **copy runtime filters** ：ランタイムフィルタをコピーし、そのコピーを使用して現在のロギングセッションをフィルタ処理します。
- **event-verbosity** *event_level*：イベントのロギングで使用する verboseness のレベルを次のいずれかに指定します。
  - *min*：イベントに関する最小限の情報を表示します。情報には、イベント名、ファシリティ、イベント ID、シビラティ（重大度）レベル、日付、および時刻が含まれます。
  - *concise*：イベントに関する詳細情報を表示しますが、システム内にイベントの送信元を提供しません。
  - *full*：イベントが生成されたシステム内の場所を識別する送信元情報など、イベントに関する詳細情報を表示します。
- **pdu-data** *format*：ログに記録された場合のパケットデータユニットの出力形式を次のいずれかに指定します。
  - *none*： RAW 形式（未フォーマット）
  - *hex*：16 進数形式
  - *hex-ascii*：メインフレームのダンプと同様の 16 進数および ASCII
- **pdu-verbosity** *pdu_level*：パケットデータユニットのロギングに使用する verboseness のレベルを 1 ～ 5 の整数で指定します。5 が最も詳細なものです。

インスタンスによるフィルタリングの無効化または有効化

logging filter active facility *facility* **level** *severity_level* **[critical-info | no-critical-info]**

logging filter { disable | enable } facility *facility* **{ all | instance** *instance_number* **}**

注：

- **active**：アクティブプロセスのみにロギングオプションを設定するように指示します。
- **disable**：特定のインスタンスまたはすべてのインスタンスのロギングを無効にします。このキーワードは、aaamgr、hamgr、および sessmgr ファシリティでのみサポートされています。
- **enable**：特定のインスタンスまたはすべてのインスタンスのロギングを有効にします。このキーワードは、aaamgr、hamgr、および sessmgr ファシリティでのみサポートされています。デフォルトでは、aaamgr、hamgr、および sessmgr のすべてのインスタンスに対してロギングが有効になっています。

- **facility** *facility* and **level** *severity_level*：どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。
- **all | instance** *instance_number*：すべてのインスタンス、または aaamgr、hamgr、または sessmgr の特定のインスタンスに対して、ロギングを無効にするか有効にするかを指定します。**show session subsystem facility** *facility* コマンドを実行して、特定のインスタンス番号を識別します。

（注） これらのキーワードは、**disable** および **enable** キーワードでのみサポートされています。

- **level** *severity_level*：次のリストからログに記録される情報のレベルを指定します。このレベルは、最高から最低の順に並べられます。
  - critical ：エラーイベントを表示
  - error：エラーイベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - warning：警告イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - unusual ：異常イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - info：情報イベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - trace：トレースイベントおよびシビラティ（重大度）レベルが高いすべてのイベントを表示
  - debug：すべてのイベントを表示

（注） このキーワードは、**active** キーワードとの組み合わせでのみサポートされています。

- **critical-info**：重要な情報のカテゴリ属性を持つイベントを表示するように指定します。これらのタイプのイベントの例は、システムプロセスとタスクが開始される際のブートアップ時に表示されます。これがデフォルトの設定です。

  no-critical-info ：重要な情報のカテゴリ属性を持つイベントを表示しないように指定します。

（注） これらのキーワードは、**active** キーワードとの組み合わせでのみサポートされています。

重要 ファシリティの単一のインスタンスにおけるロギングを有効にするには、まずファシリティのすべてのインスタンスを無効にしてから、（**logging filter disable facility** *facility* **all**）次に特定のインスタンスのロギングを有効にする必要があります（**logging filter enable facility** *facility* **instance** *instance_number*）。デフォルトの動作に復元するには、すべてのインスタンスのロギングを再度有効にする必要があります（**logging filter enable facility** *facility* **all**）。

Exec モードの **show instance-logging** コマンドを使用して、ファシリティごとに有効にされたインスタンスのインスタンス番号を表示できます。

グローバル構成モードのフィルタリング

Exec モードおよびグローバル構成モード レベルでイベントログの内容をフィルタリングできます。

システムの実行時間イベントロギングパラメータを設定するには、次の例に従います。

```
configure
  logging filter runtime facility facility level report_level
  logging display { event-verbosity | pdu-data | pdu-verbosity }
  end
```

注：

- **facility** *facility* and **level** *severity_level*：どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。
- ログに記録するすべてのファシリティに対して手順を繰り返します。
- オプション：**logging disable eventid** コマンドを追加して、イベント ID の制限を設定します。システムは、特定のイベント ID またはある範囲のイベント ID の送信を制限して、ログに記録されるデータの量が最も有用なレベルとなるよう最小限に抑える機能を提供します。追加のイベント ID またはイベント ID の範囲のロギングを無効にするには、この手順を繰り返します。
- 管理者が上記のコマンド（**logging disable eventid**）を使用してイベント ID またはイベント ID 範囲のイベントロギングを制限すると、システムは重大なイベントログ「cli 30999 critical」と、無効にされた特定のイベント ID またはイベント ID 範囲を持つ SNMP トラップ「1361 (DisabledEventIDs)」を生成します。

  このリリースでは、これらのイベントログとトラップはデフォルトで有効になっており、無効にすることはできません。

- 管理者がロギングレベルを下げる（**logging filter runtime facility** ***facility*** **level** ***report_level*** コマンドを使用して、デフォルトレベルである「error」より下にする）と、システムは重大なイベントログ「cli 30998 Critical」と、無効にされた特定のイベント ID またはイベント ID 範囲を持つ SNMP トラップ「1362 (LogLevelChanged)」を生成します。

  このリリースでは、これらのイベントログとトラップはデフォルトで有効になっており、無効にすることはできません。

次の例は、イベントロギングまたはログレベルが変更された場合に生成されるトラップの CLI 出力を示しています。

```
show snmp trap statistics
SNMP Notification Statistics:
  ...
Trap Name                               #Gen #Disc  Disable Last Generated
----------------------------------- ----- -----  ------- --------------------
…
DisabledEventIDs                           1     0       0  2021:05:11:15:35:25
LogLevelChanged                            2     0       0  2021:05:11:15:28:03

show snmp trap history
There are x historical trap records (5000 maximum)

Timestamp                Trap Information
-------------------------
```

```
…
Thu May 11 15:28:03 2021 Internal trap notification 1362 (LogLevelChanged) Logging level
 of facility resmgr is changed to critical by user #initial-config# context local privilege
 level Security Administrator ttyname /dev/pts/0 address type IPV4 remote ip address
209.165.202.129
…
Thu May 11 15:35:25 2021 Internal trap notification 1361 (DisabledEventIDs) Event IDs
from 100 to 1000 have been disabled by user adminuser context context privilege level
security administrator ttyname tty address type IPV4 remote ip address 209.165.202.134
…
Mon May 15 10:14:56 2021 Internal trap notification 1362 (LogLevelChanged) Logging level
 of facility sitmain is changed to critical by user staradmin context local privilege
level Security Administrator ttyname /dev/pts/1 address type IPV4 remote ip address
209.165.202.120
```

syslog サーバの設定

syslog アーキテクチャ

システムロギング（syslog）は、MSUP から UDP トランスポート層経由でイベント情報を生成し、一元化されたイベントメッセージコレクタに送信するアーキテクチャです。syslog はクライアント/サーバーアーキテクチャを使用します。

- **syslog クライアント**：UPF で実行されている一連のプロセスであり、イベントメッセージの送信デバイスとして動作します。
- **syslog サーバー**：MSUP から送信されたイベントメッセージを受信するように設定された外部サーバーです。

MSUP は、受信の確認応答を必要とせずに、syslog プロトコルを使用してイベントメッセージを転送します。システムは、syslog サーバーがメッセージを受信できるかどうかに関係なく、イベントメッセージを転送します。

外部 syslog サーバーへイベントメッセージを送信するようにするシステムの設定

実行時イベントロギングのフィルタで生成された情報は、永続ストレージ用の syslog サーバーに送信できます。

重要 syslog サーバーに送信されるデータは、情報提供のために使用することを目的としています。課金やパフォーマンスのモニタリングなどの機能は、syslog には基づかないようにする必要があります。

重要 システムはコンテキストごとに syslog サーバーを設定する柔軟性を備えていますが、ネットワークトラフィックからのログトラフィックを分離するために、すべてのサーバーをローカルコンテキストで設定することを推奨します。

Syslog サーバーを設定するには、次の例を使用します。

```
configure
   context  context_name
logging syslog ip_address [ event-verbosity { min | concise | full } |
facility facilities |  msg-format { rfc3164 | rfc5424 } | pdu-data { none
 | hex | hex-ascii } | pdu-verbosity pdu_level |  port number  |  rate
value ]
     end
```

注：

- **syslog** *ip_address*：ネットワーク上のシステムログサーバーの IP アドレスを、IPv4 のドット付き 10 進表記か、または IPv6 のコロンで区切られた 16 進表記で指定します。
- **event-verbosity { min | concise | full }**：イベントのロギングで使用する詳細レベルを指定します。詳細レベルは次のいずれかである必要があります。
  - **min**：最小限の詳細を表示します。
  - **concise**：概要の詳細を表示します。
  - **full**：完全な詳細を表示します。
- **facility** *facilities*：システムロギングサーバーのロギングオプションを適用するローカルファシリティを指定します。ローカルファシリティは次のいずれかである必要があります。
  - **local0**：syslog シビラティレベル 0 の Emergency（致命的）に関するものです。
  - **local1**：syslog シビラティレベル 1 の Alert に関するものです。

- **local2**：syslog シビラティレベル 2 の Critical に関するものです。
- **local3**：syslog シビラティレベル 3 の Error に関するものです。
- **local4**：syslog シビラティレベル 4 の Warning（注意）に関するものです。
- **local5**：syslog シビラティレベル 5 の Notice に関するものです。
- **local6**：syslog シビラティレベル 6 の Informational に関するものです。
- **local7**：syslog シビラティレベル 7 の Debug に関するものです。

デフォルト：**local7**

ローカルファシリティが指定されていない場合は、**local7** がデフォルトで適用されます。

複数のシステムログサーバーは、指定のローカルファシリティのロギングオプションを共有できます。これにより、システムログサーバーの論理的なグループ化と、同じローカルファシリティに関連付けられたすべてのログサーバーに影響するオプションが可能になります。

- **msg-format { rfc3164 | rfc5424 }**：RFC3164 または RFC5424 に従って、各システムログサーバーのメッセージフォーマットを設定します。デフォルト：rfc3164。
- **pdu-data { none | hex | hex-ascii }**：ログに記録された場合のパケットデータユニットの出力形式を指定します。形式は次のいずれかである必要があります。
  - **none**：raw 形式でデータを表示します。
  - **hex**：16 進数形式でデータを表示します。
  - **hex-ascii**：メインフレームのダンプと同様の 16 進数および ASCII 形式でデータを表示します。
- **pdu-verbosity** *pdu_level*：パケットデータユニットのロギングに使用する詳細度を 1 ～ 5 の整数で指定します。5 が最も詳細なものです。
- **port** *number* ：システムログサーバーの代替ポート番号を指定します。デフォルト：514。

  number は、1 ～ 65535 の整数で指定する必要があります。
- **rate** *value*：システムログサーバーにログエントリの送信を許可する頻度を指定します。指定された 1 秒間隔内で、*value* で指定された数値を超えて、システムログサーバーに送信されることはありません。

  value は、0 ～ 100000 の整数で指定する必要があります。デフォルト：1000。
- その他の syslog サーバーを構成する場合は、この手順を繰り返します。設定可能な syslog サーバーの数に制限はありません。

アクティブログの設定

アクティブログは、CLI instance-by-CLI インスタンスでオペレータが設定可能なイベントログです。1 つの CLI インスタンスで管理ユーザーによって設定されたアクティブログは、別の CLI インスタンスの管理ユーザーには表示されません。各アクティブログは、システムに対してグローバルに設定されているものとは独立したフィルタプロパティと表示プロパティを使用して設定できます。アクティブログは、生成時にリアルタイムで表示されます。

アクティブなログは、デフォルトではアクティブなメモリバッファに書き込まれません。アクティブなログをアクティブなメモリバッファに書き込むには、グローバル構成モードで次のコマンドを実行します。

logging runtime buffer store all-events

アクティブなログがアクティブなメモリバッファに書き込まれると、すべての CLI インスタンスのすべてのユーザーが使用できるようになります。

次の例を使用して、グローバル構成モードでアクティブロギングを設定します。

logging filter runtime facility *facility* **level** *report_level*

注意：

- どのシステムファシリティをどのレベルでログに記録するかを決定するロギングフィルタを設定します。
- ログに記録するすべてのファシリティに対して手順を繰り返します。
- オプション：**logging disable eventid** コマンドを追加して、イベント ID の制限を設定します。システムは、特定のイベント ID またはある範囲のイベント ID の送信を制限して、ログに記録されるデータの量が最も有用なレベルとなるよう最小限に抑える機能を提供します。追加のイベント ID またはイベント ID の範囲のロギングを無効にするには、この手順を繰り返します。

必要なすべての情報が収集されたら、EXEC モードで次のコマンドを入力して、アクティブなログの表示を停止できます。

no logging active

ファシリティの指定

次のファシリティは、イベントデータをロギングするように設定できます。

- **a10**：A10 インターフェイス ロギング ファシリティ
- **a11**：A11 インターフェイス ロギング ファシリティ
- **a11mgr**：A11 Manager ロギング ファシリティ
- **aaa-client**：Accounting and authentication クライアント ロギング ファシリティ

- **aaamgr**：Accounting and authentication マネージャ ロギング ファシリティ
- **aaaproxy**：AAAProxy ロギングファシリティ
- **aal2**：AAL2 プロトコル ロギング ファシリティ
- **acl-log**：Access Control List ロギングファシリティ
- **acsctrl**：アクティブ課金 Subsystem Controller
- **acsmgr**：アクティブ課金 Subsystem Manager
- **alarmctrl**：Alarm Controller ロギングファシリティ
- **alcap**：ALCAP プロトコル ロギング ファシリティ
- **alcapmgr**：ALCAPMgr ロギングファシリティ
- **all**：すべてのファシリティ
- **apimgr**：API Manager ロギングファシリティ
- **bfd**：BFD プロトコル ロギング ファシリティ
- **bgp**：BGP プロトコル ロギング ファシリティ
- **bindmux**：IPCF BindMux Manager
- **bngmgr**：BNGMGR（BNG DemuxMgr）ロギングファシリティ
- **bssap+**：Bssap+ ロギングファシリティ
- **bssgp**：BSSGP プロトコル ロギング ファシリティ
- **bulkstat**：Statistics ロギングファシリティ
- **cactrl**：CACTRL アプリケーション ロギング ファシリティ
- **callhome**：CALLHOME アプリケーション ロギング ファシリティ
- **cap**：CAP プロトコル ロギング ファシリティ
- **cbsmgr**：CBSMGR ロギングファシリティ
- **cdf**：CDF ロギングファシリティ
- **cfctrl**：コンテンツ フィルタリング コントローラ
- **cfgmgr**：構成マネージャ ロギング ファシリティ
- **cfmgr**：コンテンツ フィルタリング マネージャ
- **cgw**：Converged Gateway ファシリティ
- **chmgr**：Checkpoint Manager ロギングファシリティ
- **cli**：CLI ロギング ロギング ファシリティ

- **cmp**：CMPv2 ロギングファシリティ
- **confdmgr**：ConfD Manager - confd との通信用 Proclet
- **connectedapps**：CONNECTEDAPPS ライブラリ ロギング ファシリティ
- **connproxy**：Connection Proxy ロギングファシリティ
- **credit-control**：Credit Control ファシリティ
- **cscf**：IMS/MMD CSCF
- **cscfcpmgr**：CSCFCPMGR ロギングファシリティ
- **cscfmgr**：SIP CSCF Manager ファシリティ
- **cscfnpdb**：CSCF NPDB ロギングファシリティ
- **cscfrtcp**：MS/MMD CSCF RTCP ログァシリティ
- **cscfrtp**：IMS/MMD CSCF RTP ログァシリティ
- **cscfttmgr**：SIP CSCFTT Manager ファシリティ
- **csp**：Card Slot Port コントローラ ロギング ファシリティ
- **css**：CSS ファシリティ
- **css-sig**：CSS RADIUS シグナリングファシリティ
- **cx-diameter**：Cx Diameter メッセージ
- **data-mgr**：データ マネージャ フレームワーク のロギングファシリティ
- **dcardctrl**：Daughtercard Controller ロギングファシリティ
- **dcardmgr**：Daughtercard Manager ロギングファシリティ
- **demuxmgr**：Demux Manager API ファシリティ
- **dgmbmgr**：Diameter Gmb アプリケーション マネージャのロギングファシリティ
- **dhcp**：Dynamic Host Configuration Protocol ロギングファシリティ
- **dhcpv6**：DHCPV6
- **dhost**：分散ホストのロギングファシリティ
- **diabase**：Diabase メッセージ
- **diactrl**：Diactrl proclet ロギング
- **diameter**：Diameter エンドポイントのロギングファシリティ
- **diameter-acct**：Diameter アカウンティング
- **diameter-auth**：Diameter 認証

- **diameter-dns**：Diameter DNS サブシステム
- **diameter-ecs**：ECS Diameter シグナリング
- **diameter-engine** ：Diameterv2 エンジン ロギング ファシリティ
- **diameter-hdd**：Diameter HDD インターフェイス
- **diameter-svc**：Diameter サービス
- **diamproxy** ：DiamProxy ロギングファシリティ
- **doulosuemgr**：Doulos UE Manager ファシリティ
- **dpath**：IPSEC Data Path ロギングファシリティ
- **drvctrl**：ドライバコントローラのロギングファシリティ
- **eap-ipsec** ：EAP
- **eap-sta-s6a-s13-s6b-diameter**：EAP/STA/S6A/S13/S6B Diameter メッセージ
- **ecs-css**：ACSMGR <-> Session Manager Signalling Interface ロギングファシリティ
- **egtpc**：EGTP コントロールプレーン
- **egtpmgr**：EGTP Demux マネージャ
- **egtpu**：EGTP ユーザープレーン
- **embms**：eMBMS Gateway ファシリティ
- **emctrl**：Element Manager Controller ロギングファシリティ
- **epdg**：EPDG ロギングファシリティ
- **event-notif**：Event Notification Interface ロギングファシリティ
- **evlog**：Event-logger ロギングファシリティ
- **famgr**：外部エージェントマネージャのロギングファシリティ
- **fapi**：VPP Fastpath API ロギングファシリティ
- **femgr**：Forwarding Element Manager ロギングファシリティ
- **firewall**：ファイアウォールのロギングファシリティ
- **fng**：FNG ロギングファシリティ
- **gbmgr**：SGSN Gb インターフェイス マネージャ ファシリティ
- **gmm**：GMM Protocol ロギングファシリティ
- **gprs-app**：GPRS アプリケーションのロギングファシリティ
- **gprs-ns**：GPRS-NS Protocol ロギングファシリティ

- **gq-rx-tx-diameter** ：Gq/Rx/Tx Diameter メッセージ
- **gss-gcdr**：GSS GCDR ファシリティ
- **gtpc**：GTP-C Protocol ロギングファシリティ
- **gtpcmgr**GTP-C Protocol Manager ロギングファシリティ
- **gtpp**：GTP-PRIME Protocol ロギングファシリティ
- **gtpu**：GTP-U Protocol ロギング ファシリティ
- **gtpumgr**：GTPU Demux マネージャ
- **gx-ty-diameter**：Gx/Ty Diameter メッセージ
- **gy-diameter**：Gy Diameter メッセージ
- **hamgr**：ホーム エージェント マネージャのロギングファシリティ
- **hat**：High Availability Task プロセス ロギング ファシリティ
- **hdctrl**：HD コントローラのロギングファシリティ
- **henbapp**：HENB App ファシリティ
- **henbgw** ：HENBGW ファシリティ
- **henbgw-pws**：Henbgw Public Warning System Data ロギングファシリティ
- **henbgw-sctp-acs**：HENBGW access sctp ファシリティ
- **henbgw-sctp-nw**：HENBGW network sctp ファシリティ
- **henbgwdemux**：HENBGW Demux ファシリティ
- **henbgwmgr**：ENBGW Manager ファシリティ
- **hnb-gw** ：HNB-GW（3G Femto GW）ロギングファシリティ
- **hnbmgr**：HNBMGR（3G Femto GW DemuxMgr）ロギングファシリティ
- **hss-peer-service**：HSS Peer Serviceファシリティ
- **iftask**：iftask ロギングファシリティ
- **igmp**：IGMP
- **ikev2**：IKEv2
- **ims-authorizatn**：IMS Authorization Service ファシリティ
- **ims-sh**：HSS SH Service ファシリティ
- **imsimgr** ：SGSN IMSI Manager ファシリティ
- **imsue**：IMSUE

- **ip-arp** ：IP Address Resolution Protocol ロギングファシリティ
- **ip-interface**：IP インターフェイス ロギング ファシリティ
- **ip-route**：IP ルートロギングファシリティ
- **ipms** ：IPMS ロギングファシリティ
- **ipne**：IPNE ファシリティ
- **ipsec**：IP セキュリティ ロギング ファシリティ
- **ipsecdemux**：IPSecdemux ロギングファシリティ
- **ipsg**：IP サービス ゲートウェイ インターフェイスのロギングファシリティ
- **ipsgmgr**：IP Service Gateway ファシリティ
- **kvstore**：KV Store ファシリティ
- **l2tp-control**：L2TP Protocol Control ロギングファシリティ
- **l2tp-data**：L2TP Protocol Data ロギングファシリティ
- **l2tpdemux**: L2TP Demux マネージャのロギングファシリティ
- **l2tpmgr**：L2TP Protocol Manager ロギングファシリティ
- **lagmgr**：LAGMGR ロギングファシリティ
- **lcs**：LCS Service ロギングファシリティ
- **ldap**：LDAP メッセージ
- **li**：合法的傍受ロギングファシリティ
- **linkmgr**：SGSN/SS7 Links Manager ファシリティ
- **llc**：LLC Protocol ロギングファシリティ
- **lmisf**Lmisf ロギングファシリティ
- **local-policy**：ローカル ポリシー サービス ファシリティ
- **location-service** ：Location Service ファシリティ
- **m3ua** ：M3UA Protocol ロギングファシリティ
- **magmgr**：Mobile Access Gateway ロギングファシリティ
- **map**：MAP Protocol ロギングファシリティ
- **mcctrl**：SDN Mobility Controller - Controller ロギングファシリティ
- **mcdemux**：SDN Mobility Controller - DEMUX ロギングファシリティ
- **mcmgr**：SDN Mobility Controller - Manager ロギングファシリティ

- **megadiammgr**：Megadiameter Manager（SLF Service）
- **mme-app**：MME アプリケーション ファシリティ
- **mme-misc** ：MME その他のロギングファシリティ
- **mmedemux**：MME Demux Manager ファシリティ
- **mmemgr**：MME マネージャファシリティ
- **mmgr**：Primary Manager ロギングファシリティ
- **mobile-ip**：Mobile IP コントロール ロギング ファシリティ
- **mobile-ip-data**：Mobile IP データロギングファシリティ
- **mobile-ipv6**：Mobile IPv6 コントロール ロギング ファシリティ
- **mpls**：MPLS プロトコル ロギング ファシリティ
- **mrme**：MRME ロギングファシリティ
- **mseg-app**：MSEG アプリケーション ロギング ファシリティ
- **mseg-gtpc**： MSEG GTPC アプリケーション ロギング ファシリティ
- **mseg-gtpu**MSEG GTPU アプリケーション ロギング ファシリティ
- **msegmgr**：MSEGMGR（MSEG DemuxMgr）ロギングファシリティ
- **msgproxy**：Messege Proxy ロギングファシリティ
- **mtp2** ：MTP2 Service ロギングファシリティ
- **mtp3**：MTP3 Protocol ロギングファシリティ
- **multicast-proxy**：マルチキャストプロキシのロギングファシリティ
- **nas**：NAS 4G Protocol ロギングファシリティ
- **npuctrl**：Network Processor Unit Control ロギングファシリティ
- **npumgr**：Network Processor Unit Manager ロギングファシリティ
- **npumgr-acl**：NPUMGR ACL のロギングファシリティ
- **npumgr-drv**：NPUMGR DRV のロギングファシリティ
- **npumgr-flow**：NPUMGR FLOW のロギングファシリティ
- **npumgr-fwd**：NPUMGR FWD のロギングファシリティ
- **npumgr-init** ：NPUMGR INIT ロギングファシリティ
- **npumgr-lc**：NPUMGR LC のロギングファシリティ
- **npumgr-port**：NPUMGR PORT のロギングファシリティ

- **npumgr-recovery**：NPUMGR RECOVERY のロギングファシリティ
- **npumgr-rri** ：NPUMGR RRI ロギングファシリティ
- **npumgr-vpn**：NPUMGR VPN のロギングファシリティ
- **npusim**：NPUSIM ロギングファシリティ
- **nrfmgr**：NRF Manager ロギングファシリティ
- **nsh**：NSH ロギングファシリティ
- **ocsp**：OCSP ロギングファシリティ
- ospf：OSPF プロトコルのロギングファシリティ
- **ospfv3**：OSPFv3 プロトコルのロギングファシリティ
- **p2p**：Peer-to-Peer 検出ロギングファシリティ
- **pagingmgr**：PAGINGMGR のロギングファシリティ
- **pccmgr**IPCF PCC Manager ライブラリ
- **pdg**：PDG ロギングファシリティ
- **pdif**：PDIF ロギングファシリティ
- **pgw**：PDN Gateway ファシリティ
- **plugin**：Plugin ロギングファシリティ
- **pmm-app** ：PMM アプリケーション ロギング ファシリティ
- **ppp**：PPP リンクおよびパケット ロギング ファシリティ
- **pppoe**：PPPOE ロギングファシリティ
- **proclet-map-frwk**：Proclet mapping frameowrk ロギングファシリティ
- **push**：VPNMGR CDR プッシュのロギングファシリティ
- **radius-acct**：RADIUS アカウンティング ロギング ファシリティ
- **radius-auth**：RADIUS 認証のロギングファシリティ
- **radius-coa**：RADIUS change of authorization and radius disconnect ロギングファシリティ
- **ranap**：RANAP Protocol ロギングファシリティ
- **rct**：リカバリ制御タスクのロギングファシリティ
- **rdt**：リダイレクトタスクのロギングファシリティ
- **resmgr**：Resource Manager のロギングファシリティ
- **rf-diameter**：Rf Diameter メッセージ

- **rip**：RIP プロトコル ロギング ファシリティ
- **rlf**：RLF ロギングファシリティ
- **rohc**：RObust ヘッダー圧縮
- **rsvp**：予約プロトコルのロギングファシリティ
- **rua**：RUA（3G Femto GW - RUA メッセージ）ロギングファシリティ
- **s102**：S102 プロトコルのロギングファシリティ
- **s102mgr**：S102Mgr プロトコル ロギング ファシリティ
- **s1ap**：S1AP Protocol ロギングファシリティ
- **sabp**：SABP ロギングファシリティ
- **saegw**：SAE Gateway ファシリティ
- **sbc**：SBc プロトコルのロギングファシリティ
- **sccp**：SCCP Protocol ロギングファシリティ
- **sct**：共有設定タスクのロギングファシリティ
- **sctp**：SCTP Protocol ロギングファシリティ
- **sef_ecs**：sef apis printing ファシリティ
- **sess-gr**：SM GR ファシリティ
- **sessctrl**：セッションコントローラのロギングファシリティ
- **sessmgr**：セッションマネージャのロギングファシリティ
- **sesstrc**：Session trace ロギングファシリティ
- **sfcctrl**：Service Funcion Chain Controller ロギングファシリティ
- **sfcmgr**：Service Funcion Chain Manager ロギングファシリティ
- **sft**：スイッチファブリックタスクのロギングファシリティ
- **sgmbmgr**：eMBMS Gateway Demux ファシリティ
- **sgs**：SGs プロトコル ロギング ファシリティ
- **sgsn-app**：SGSN-APP interface ロギングファシリティ
- **sgsn-failures**：SGSN call failures ロギングファシリティ
- **sgsn-gtpc** ：SGSNs GTP-C Protocol ロギングファシリティ
- **sgsn-gtpu**：SGSNs GTP-U Protocol ロギングファシリティ
- **sgsn-mbms-bearer**：SGSNs MBMS bearer app（SMGR）ロギングファシリティ

- **sgsn-misc**：SGSN その他のロギングファシリティ
- **sgsn-system** ：SGSNs System Components ロギングファシリティ
- **sgsn-test**：SGSN Tests ロギングファシリティ
- **sgtpcmgr**：SGSN GTPC Manager ファシリティ
- **sgw**：サービング ゲートウェイ ファシリティ
- **sh-diameter** ：Sh Diameter メッセージ
- **sitmain**：システム初期化タスクのメインロギングファシリティ
- **slmgr**：Smart License Manager ロギングファシリティ
- **sls**：SLs プロトコル ロギング ファシリティ
- **sm-app**：SM プロトコルのロギングファシリティ
- **sms**：SMS Service ロギングファシリティ
- **sndcp**：SNDCP Protocol ロギングファシリティ
- **snmp**：SNMP のロギングファシリティ
- **sprmgr**：IPCF SPR Manager ライブラリ
- **srdb**：スタティック評価データベース
- **srp**：Service Redundancy Protocol ロギングファシリティ
- **sscfnni**：SSCFNNI Protocol ロギングファシリティ
- **sscop**：SSCOP Protocol ロギングファシリティ
- **ssh-ipsec**：SSH IP Security ロギングファシリティ
- **ssl**：SSL（セキュア ソケット レイヤ メッセージ）ロギングファシリティ
- **stat**：統計情報のロギングファシリティ
- **supserv**：Suplementary Services ロギングファシリティ
- **sx**：SX Manager ロギングファシリティ
- **mmedemux**：MME Demux マネージャのロギングファシリティ
- **system**：システムのロギングファシリティ
- **tacacsplus**：TACACS+ プロトコル ロギング ファシリティ
- **tcap**：TCAP プロトコルのロギングファシリティ
- **tcpdemux**：TCP Demux Manager ロギングファシリティ
- **testctrl**：テストコントローラのロギングファシリティ

- **testmgr**：テストマネージャのロギングファシリティ
- **threshold**：Threshold ロギングファシリティ
- **tsmon**：Traffic Steering Monitor Server ファシリティ
- **ttg**：TTG ロギングファシリティ
- **tucl**：TUCL ロギングファシリティ
- **udr**：UDR ファシリティ
- **uplane**：User Plane ロギングファシリティ
- **user-data**：User Data ロギングファシリティ
- **user-l3tunnel**：User layer-3 tunnel ロギングファシリティ
- **usertcp-stack**：User Tcp スタック
- **vnfma**：VNFM Proxy Agent ロギングファシリティ
- **vpn**：仮想プライベートネットワークのロギングファシリティ
- **vpp**：vpp ロギングファシリティ
- **wimax-data** ：WiMAX DATA
- **wimax-r6**：WiMAX R6
- **wsg**：WSG ロギングファシリティ
- **x2gw-app**：X2GW アプリケーション ロギング ファシリティ
- **x2gw-demux**：X2GW demux タスクのロギングファシリティ

トレースロギングの設定

トレースロギングは、現在アクティブな特定のセッションの問題を迅速に解決するのに役立ちます。これらは、Exec モードで **logging filter** コマンドを使用して設定されたグローバル イベントログフィルタに依存しない修飾子に基づいて生成される一時的なフィルタです。ただし、イベントログと同様に、ログによって生成される情報は、アクティブなメモリバッファに保存されます。

選択したコールに関連付けられているすべてのデバッグレベルイベントが保存されます。



重要 トレースログは、セッションの処理に影響します。デバッグ目的でのみ実装する必要があります。

Exec モードでトレースログを設定するには、次の例を使用します。

logging trace { callid *call_id* **| ipaddr** *ip_address* **| msid** *ms_id* **| username** *username* **}**

必要なすべての情報が収集されたら、次のコマンドを入力して、トレースログを削除できます。

no logging trace { callid *call_id* **| ipaddr** *ip_address* **| msid** *ms_id* **| username** *username* **}**

モニターログの設定

モニターロギングは、特定のサブスクライバのすべてのセッションに関連付けられているすべてのアクティビティを記録します。この機能は、特定のサブスクライバのモニタリング機能に関する司法当局の要請を遵守している場合に使用できます。

モニターは、サブスクライバのMSIDまたはユーザー名に基づいて実行できます。また、司法当局によって規定された限定期間にのみ使用することを目的としています。したがって、必要なモニタリング期間の直後に終了する必要があります。

この項では、モニターログを有効または無効にする手順について説明します。

モニターログの有効化

モニターログのターゲットを設定するには、次の例を使用します。

```
configure
  logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

モニターログの追加のターゲットを設定するには、この手順を繰り返します。

モニターログの無効化

モニターログを無効にするには、次の例を使用します。

```
configure
  no logging monitor { ip_addr | ipv6_addr | msid id | username name }
  end
```

ロギング設定と統計情報の表示

ロギング設定と統計情報を確認するには、Exec モードで次のコマンドを入力します。

show logging [active | verbose]

キーワードを指定しなかった場合は、グローバルフィルタ設定が表示され、有効になっている他のタイプのロギングに関する情報も表示されます。

次の表に、**verbose** キーワードを使用したときに表示される統計情報の説明を示します。

表 *107 :* ロギング設定コマンドと統計情報コマンド

フィールド	説明
General Logging Statistics	
Total events received	システムによって生成されたイベントの合計数が表示されます。
Number of applications receiving events	イベントを受信しているアプリケーションの数が表示されます。
Logging Source Statistics	
Event sequence ids by process	生成されたイベントがあるシステムプロセスのリストと、生成されたイベントの参照識別番号が表示されます。
Msg backlog stat with total cnt	生成されたイベントの合計数と比較してログに記録されたイベントメッセージの数が表示されます。
LS L2 filter drop rate	ロギングソース（LS）のレイヤ2（L2）イベントのドロップのパーセンテージが表示されます。
Abnormal Log Source Statistics	異常なロギングソース（LS）の統計情報が表示されます（存在する場合）。
Runtime Logging Buffer Statistics	
Active buffer	現在アクティブなメモリバッファに記録されているイベントの数と、バッファ内の最も古いエントリと最新のエントリのタイムスタンプが表示されます。
Inactive buffer	非アクティブなメモリバッファに現在ログインしているイベントの数が表示されます。

CLI を使用したイベントログの表示

システムによって生成されるイベントログは、次のいずれかの方法で表示できます。

- **syslog サーバーから、次のようにします。**システムが syslog サーバーにログを送信するように設定されている場合、ログは syslog サーバーで直接表示できます。
- **システム CLI から、次のようにします。**システムのメモリバッファに保存されているログは、CLI から直接表示できます。
- **コンソールポートから、次のようにします。**デフォルトでは、CLI セッションがアクティブになっていない場合、システムはコンソールインターフェイスを介して端末にイベントを自動的に表示します。

この項では、CLI を使用してイベントログを表示する手順を説明します。これらの手順は、Exec モードのルートプロンプトを使用していることが前提になります。

手順

ステップ 1 アクティブなログメモリバッファを非アクティブなログメモリバッファにコピーします。

アクティブなログメモリバッファが非アクティブなログメモリバッファにコピーされると、非アクティブなログメモリバッファ内の既存の情報が削除されます。

アクティブと非アクティブの両方のイベントログメモリバッファは、Exec モードの CLI を使用して表示できます。ただし、データが上書きされないようにするために、非アクティブなログを表示することをお勧めします。アクティブなログバッファからの情報は、次のコマンドを入力して非アクティブなログバッファにコピーできます。

```
logs checkpoint
```

ステップ 2 次のコマンドを入力してログを表示します。

```
show logs
```

クラッシュログの設定と表示



（注） CN-5G 2025.02 リリースでは、クラッシュ対応 URL が構成されておらず、クラッシュコアは `/var/lib/systemd/coredump/` に配置されます

ソフトウェアのクラッシュが発生した場合は、クラッシュの原因を特定するのに役立つ情報をシステムが保存します。この情報はシステムメモリ内で維持することも、ネットワークサーバーに転送して保存することもできます。

システムでは、次の 2 種類のログを生成することができます。

- **クラッシュログ**：クラッシュログには、ソフトウェアクラッシュに関するあらゆる情報が記録されます（完全なコアダンプ）。サイズが原因で、システムメモリに保存することはできません。したがって、ログを保存できるローカルデバイスか、またはネットワークサーバーを指定する Universal Resource Locator（URL）を使用して設定されている場合にのみ、これらのログが生成されます。
- **クラッシュログの要約**：クラッシュイベントレコードは、ソフトウェアクラッシュが発生したときに自動的に生成され、管理カード上のフラッシュメモリに保存されます。クラッシュログの要約には、関連付けられたダンプファイルとともに、クラッシュイベントのレコードのリストが含まれています。このログは、CLI コマンドを使用してイベントレコードとダンプファイルを表示します。

クラッシュロギングのアーキテクチャ

クラッシュログは、クラッシュイベント情報の永続的なリポジトリです。各イベントには番号が付けられており、CPU（minicore）、NPU、またはカーネルクラッシュに関連するテキストが含まれます。ログに記録されたイベントは、固定長レコードに記録され、/flash/crashlog2.に保存されます。

クラッシュが発生するたびに、次のクラッシュ情報が保存されます。

1. イベントレコードは、/flash/crashlog2 ファイル（クラッシュログ）に保存されます。
2. 関連する minicore、NPU、またはカーネルダンプファイルは、/flash/crsh2 ディレクトリに保存されます。
3. 完全なコアダンプは、ユーザーが設定したディレクトリに保存されます。

ソフトウェアクラッシュログ接続先の設定

システムは、ソフトウェアのクラッシュログ情報を次のいずれかの場所に保存するように設定できます。

- VPC 上
  - **フラッシュメモリ**：仮想マシンからアクセス可能です。
  - **USB メモリスティック**：プラットフォームの USB スロットに取り付けられています（USB スロットはハイパーバイザを介して有効になっています）。
- **ネットワークサーバー**：システムが Trivial File Transfer Protocol（TFTP）、File Transfer Protocol（FTP）、Secure File Transfer Protocol（SFTP）、または Hypertext Transfer Protocol（HTTP）を使用してアクセスできるネットワーク上のワークステーションまたはサーバーです。これは、複数のシステムが同じ設定を必要とする大規模なネットワークの展開に推奨されます。

クラッシュログファイル（完全なコアダンプ）は、指定された場所で発生すると一意の名前で書き込まれます。名前の形式は、*crash-card-cpu-time-core* です。*Card* はカードスロット、*cpu* はカード上の CPU の数、*time* は 16 進表記の Portable Operating System Interface（POSIX）のタイムスタンプです。

次の例を使用して、グローバル構成モードでソフトウェアのクラッシュログの接続先を設定します。

```
configure
  crash enable [ encrypted ] url crash_url
  end
```

注意：

- 追加のソフトウェアのクラッシュログの接続先を設定するには、この手順を繰り返します。設定可能な接続先の数に制限はありません。

CLI を使用して要約されたクラッシュログ情報の表示

管理カード（**/flash/crashlog2**）上のフラッシュメモリに一連のイベントレコードとして保存されている要約されたクラッシュ情報を表示できます。各クラッシュイベントレコードには、表示可能な（minicore、NPU、またはカーネル）関連のダンプファイル(**/flash/crsh2**)があります。

システムで発生したソフトウェアクラッシュイベントを表示するには、この項の手順に従ってください。これらの手順は、Execモードのルートプロンプトを使用していることが前提になります。

手順

ステップ 1 次の Exec モードコマンドを入力して、ソフトウェアクラッシュイベントのリストを表示します。

show crash { all | list | number *crash_num* **}**

注意：

- **Show crash list** を実行して、特定のクラッシュイベントの番号を取得します。
- **Show crash number** *crash_num* を実行して、ターゲットクラッシュイベントの出力を表示します。

結果として得られる出力は、すべてのプラットフォームで同じとは限りません。

同様のクラッシュイベントに関する情報は、このコマンドの出力では抑制されます。

ステップ 2 特定のクラッシュイベントに関連付けられているダンプファイルを表示します。

ダンプファイルに含まれる情報は、ソフトウェアがクラッシュする原因となっている内部または外部の要因を特定して診断するのに役に立ちます。

- クラッシュ #：クラッシュイベントをログに記録するときに StarOS によって割り当てられた一意の番号
- SW バージョン：StarOS ビルドリリース形式：RR.n(bbbbb)
- 同様のクラッシュカウント：類似したクラッシュの数
- 最初のクラッシュ時刻：YYYY-MMM-DD+hh:mm:ssの形式で最初のクラッシュが発生したときのタイムスタンプ
- 失敗メッセージ：イベントメッセージのテキスト
- 関数：コード識別子
- プロセス：クラッシュが発生した場所（カード、CPU、PID など）
- クラッシュ時間：クラッシュが発生したときのタイムスタンプ（YYYY-MMM-DD+hh:mm:ss タイムゾーン）
- 最近の errno：最新のエラー番号のテキスト。
- スタック：メモリスタック情報
- ラストバウンス：クラッシュ前に受信したメッセージングに関する情報

- レジスタ：メモリレジスタの内容
- 現在の着信メッセージ：現在の着信メッセージの 16 進情報
- アドレス マップ
- 最近のヒープアクティビティ（最も古いもの）
- 最近のイベント（最も古いもの）
- プロファイルの深さ

過剰なイベントロギングの削減

イベントロギング（evlogd）は、StarOS ファシリティによって送信されたイベントメッセージをキャプチャする共有メディアです。1 つまたは複数のファシリティが継続的に大量のイベントメッセージを送信し続けると、残りの通常に動作している機能が影響を受けます。このシナリオでは、特にログを生成するファシリティの数が増えるにつれて、システムパフォーマンスが低下していきます。

イベントメッセージロギングのレートコントロールは、ログの送信元パスで処理されます。基本的に、カウンタは秒ごとに 0 に設定され、evlogd に送信されたログイベントごとに増分します。カウントが 1 秒経過する前にしきい値に達した場合、イベントが送信またはキューに格納されます。ただし、evlogd メッセンジャーキューがいっぱいの場合はイベントが破棄されます。

メッセージロギングのレートに対するこのコマンドで設定された上限しきい値を超過するファシリティがあり、同じ状態が長時間続く場合、StarOS は SNMP トラップまたはアラーム経由でユーザーに通知します。

新しい threshold コマンドを使用すると、ファシリティイベントキューを満杯とするパーセンテージを指定できます。このしきい値を超えると、問題のあるファシリティを指定する SNMP トラップとアラームが生成されます。

このコマンドに関連付けられている SNMP トラップの形式は次のとおりです。

- **ThreshLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshLSLogsVolume) threshold
<upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

- **ThreshClearLSLogsVolume**

```
<timestamp> Internal trap notification <trap_id> (ThreshClearLSLogsVolume) threshold
 <upper_percent>%
measured value <actual_percent>% for facility <facility_name> instance <instance_id>
```

ポーリング間隔内にトリガー条件が発生した場合は、そのポーリング間隔が終了するまではアラートやアラームは生成されません。

両方のトラップを有効または抑制するには、グローバル構成モードの **snmp trap** コマンドを使用します。

ログソースのしきい値の設定

ログソースのしきい値の設定と実装に関連する3つのグローバル構成モードコマンドがあります。

1. **threshold ls-logs-volume**：トラップやアラームをそれぞれ生成およびクリアするための上限および下限しきい値のパラメータを設定します。
2. **threshold poll ls-logs-volume interval**：このしきい値のポーリング間隔を設定します。
3. **threshold monitoring ls-logs-volume**：このしきい値のモニタリングをオンまたはオフにします。

Syslog サーバーを設定するには、次の例を使用します。

```
configure
  [ default ] threshold ls-logs-volume upper_percent [ clear lower_percent ]
  [ default ] threshold poll ls-logs-volume interval duration
  [ no ] threshold monitoring ls-logs-volume
  end
```

注：

- *upper_percent* と *lower_percent* は、0 ～ 100 の整数として表わされます。*upper_percent* のデフォルト値は 90% です。*lower_percent* が指定されていない場合、デフォルトのクリア値は *upper_percent* です。
- **threshold poll ls-logs-volume interval** はポーリング間隔を秒単位で設定します。デフォルトの間隔は 300 秒（5 分）です。
- **threshold monitoring ls-logs-volume** はこの機能を有効または無効にします。

このしきい値の設定を確認するには、Exec モードの **show threshold** コマンドを実行します。

ログのチェックポインティング

チェックポインティングは、ログに記録されたデータが以前に表示されたものか、マークされたものかを識別します。チェックポインティングを使用すると、最後のチェックポイント以降のログ情報のみを表示できます。

個々のログには、アクティブログに最大50,000のイベントが含まれている場合があります。ログのチェックポイントを実行すると、最大50,000のイベントが非アクティブなログファイルに記録されます。これにより合計で最大100,000イベントとなり、これらはログに記録された各ファシリティで使用できます。

特殊なアクティビティが実行される前に、EXEC モードの logs checkpoint コマンドを使用してログデータをチェックポイント処理し、ログの内容を既知の時点に設定します。また、このコマンドを定期メンテナンスの一環として含めて、ログデータを管理することもできます。

ログのチェックポインティングでは、現在のログデータを非アクティブなログに移動します。最後にチェックポインティングされたデータが、非アクティブログに保持されます。後続のログのチェックポインティングによって、以前にチェックポインティングされた非アクティブなログデータがクリアされ、新たにチェックポインティングされたデータに置き換えられます。チェックポインティングされたログデータは表示できません。



重要 ログファイルがいっぱいになるのを防ぐために、ログのチェックポインティングを定期的に実行する必要があります。50,000 のイベントが記録されたログは、新しいイベントがログに記録されると、最も古いイベントを最初に破棄します。

ログファイルの保存

ログファイルは、URL で指定されたローカルまたはリモートの場所にあるファイルに保存できます。ログファイルを保存するには、次の EXEC モードコマンドを使用します。

save logs { *url* } **[active]] [inactive] [callid** *call_id* **] [event-verbosity** *evt_verboseness* **] [facility** *facility* **] [level** *severity_level* **] [pdu-data** *pdu_format* **] [pdu-verbosity** *pdu_verboseness* **] [since** *from_date_time* **[until** *to_date_time* **]] [| { grep** *grep_options* **| more }]**

オプション：

- *url*：ログファイルを保存する場所を指定します。*url* は、ローカルまたはリモートファイルを参照する場合があり、次のフォーマットで入力する必要があります。
- **active**：アクティブログからのデータを保存します。
- **inactive**：非アクティブなログからのデータを保存します。
- **callid** *call_id*：4 バイト 16 進数として保存するログ情報のコール ID を指定します。
- **event-verbosity** *evt_verboseness*：イベントデータの表示に使用する詳細度を、次のいずれかとして指定します。
  - *min*：イベントに関する最小限の情報をログに記録します。情報には、イベント名、ファシリティ、イベント ID、シビラティ（重大度）レベル、日付、および時刻が含まれます。
  - *concise*：イベントが生成されたシステム内の場所を識別する送信元情報など、イベントに関する詳細情報をログに記録します。
  - *full*：イベントい関する詳細な情報をログに記録します。これには、送信元情報が含まれ、イベントが生成されたシステムの場所を指揮熱
- **facility** *facility*：ログに記録された情報のフィルタを変更するファシリティを指定します。
- **level** *severity_level*：次のリストからログに記録する情報のレベルを指定します。リストは、最高から最低の順に並べられます。

- *critical*：重要なイベントをログに記録します。
- *error*：エラーイベントとすべてのより高いシビラティ（重大度）レベルのイベントをログに記録します。
- *warning*：警告イベントとすべてのより高いシビラティレベルのイベントをログに記録します。
- *unusual*：異常なイベントとすべてのより高いシビラティレベルのイベントをログに記録します。
- *info*：情報イベントとすべてのより高いシビラティレベルのイベントをログに記録します。
- *trace*：トレースイベントとすべてのより高いシビラティレベルのイベントをログに記録します。
- *debug*：すべてのイベントをログに記録します。

- **pdu-data** *pdu_format*：パケットデータの表示に使用する出力フォーマットを、次のいずれかとして指定します。
  - *none*：RAW 形式（未フォーマット）。
  - *hex*：16 進数フォーマット。
  - *hex-ascii*：16 進数 およびメインフレームダンプと類似する ASCII。
- **pdu-verbosity** *pdu_verboseness* ：パケットデータユニットの表示に使用する詳細度レベルを、1 ～ 5 の値で指定します。5 が最も詳細です。
- **since** *from_date_time*：*from_date_time* よりも直近で収集されたログ情報のみを保存します。
- **until** *to_date_time*：*to_date_time* よりも直近のログ情報を保存しません。省略した場合、デフォルト値は現在の時刻です。
- *from_date_time* および *to_date_time* YYYY:MM:DD:HH:mm または YYYY:MM:DD:HH:mm:ss フォーマットで指定する必要があります。場所：
  - YYYY = 4 桁の年
  - MM = 01 ～ 12 の範囲の 2 桁の月
  - DD = 01 ～ 31 の範囲の 2 桁の日
  - HH = 00 ～ 23 の範囲の 2 桁の時間
  - mm = 00 ～ 59 の範囲の 2 桁の分
  - ss = 0 ～ 59 の範囲の 2 桁の秒

  to_date_time は、*from_date_time* よりも新しい日時で指定する必要があります。

until キーワードを使用すると、ログ情報の時間範囲を指定できます。**since** キーワードのみを使用すると、現在の時刻までのすべての情報を表示します。

- **grep** *grep_options* | **more**：このコマンドの出力を指定のコマンドに送信しますこのコマンドの出力送信先コマンドを指定する必要があります。

イベント ID の概要



重要 イベント ID の使用は、プラットフォームのタイプとプラットフォームで実行されているライセンスによって異なります。

識別番号（ID）は、システムでロギングが有効になっている場合に発生するイベントを参照するために使用されます。前述したように、ログはファシリティごとに収集されます。各ファシリティには、次の表に示すように、独自の範囲のイベント ID があります。

表 *108 :* システムファシリティとイベント *ID* の範囲

ファシリティ	説明	イベント ID の範
a10	A10 プロトコルファシリティ	28000 ～ 28999
a11	A11 プロトコルファシリティ	29000 ～ 29999
a11mgr	A11 マネージャファシリティ	9000 ～ 9999
aaa-client	AAA クライアントファシリティ	6000 ～ 6999
aaamgr	AAA マネージャファシリティ	36000 ～ 36999
aaaproxy	AAA プロキシファシリティ	64000 ～ 64999
aal2	AAL2 プロトコルファシリティ	173200 ～ 17329
acl-log	IP アクセスコントロールリスト（ACL）ファシリティ	21000 ～ 21999
acsctrl	アクティブ チャージング サービス コントローラ（ACSCtrl）ファシリティ	90000 ～ 90999
acsmgr	アクティブ チャージング サービス マネージャ（ACSMgr）ファシリティ	91000 ～ 91999
afctrl	Ares ファブリックコントローラ（ASR 5500 のみ）	186000 ～ 18699
afmgr	Ares Fabric Manager（ASR 5500 のみ）	187000 ～ 18799
alarmctrl	アラーム コントローラ ファシリティ	65000 ～ 65999
alcap	Access Link Control Application Part（ALCAP）プロトコルファシリティ	160900 ～ 16139

ファシリティ	説明	イベント ID
alcapmgr	ALCAP マネージャファシリティ	160500 ～ 16
asf	ASF ファシリティ	73000 ～ 739
asfprt	ASFPRT ファシリティ	59000 ～ 599
asngwmgr	アクセス サービス ネットワーク（ASN）ゲートウェイ マネージャ ファシリティ	100000 ～ 10
asnpcmgr	ASNページング/ロケーション レジストリ マネージャ ファシリティ	100500 ～ 10
bcmcs	ブロードキャスト/マルチキャストサービス（BCMCS）ファシリティ	109000 ～ 10
bfd	Bidirectional Forwarding Detection（BFD）プロトコルファシリティ	170500 ～ 17
bgp	ボーダー ゲートウェイ プロトコル（BGP）ファシリティ	85000 ～ 859
bindmux	BindMux マネージャ ファシリティ [インテリジェントポリシー制御機能（IPCF）]	158200 ～ 15
bngmgr	ブロードバンドネットワーク ゲートウェイ（BNG）マネージャファシリティ	182000 ～ 18
bssap	Base Station System Application Part+（BSSAP+）サービスファシリティ	131000 ～ 13
bssgp	Base Station System GPRS Protocol（BSSGP）ファシリティ	115050 ～ 11
callhome	Call Home ファシリティ	173600 ～ 17
cap	CAMEL Application Part（CAP）ファシリティ	87900 ～ 880
chatconf	CHATCONF ファシリティ	74000 ～ 749
cli	CLI（コマンドラインインターフェイス）のロギングファシリティ	30000 ～ 309
connproxy	接続プロキシファシリティ	190000 ～ 19
crdt-ctl	クレジット制御ファシリティ	127000 ～ 12
csg	Closed Subscriber Groups（CSG）ファシリティ	188000 ～ 18
csg-acl	CSG アクセスコントロールリスト（ACL）ファシリティ	189000 ～ 18
csp	カード/スロット/ポート（CSP）ファシリティ	7000 ～ 7999
css	コンテンツ ステアリング サービス（CSS）ファシリティ [ESC]	77000 ～ 774
css-sig	コンテンツ サービス セレクション（CSS）RADIUS シグナリング ファシリティ	77500 ～ 775
cx-diameter	Cx Diameter メッセージファシリティ	92840 ～ 928
dcardctrl	ドーターカードコントローラファシリティ	62000 ～ 629

ファシリティ	説明	イベント ID の範
dcardmgr	ドーターカード マネージャ ファシリティ	57000 ～ 57999
demuxmgr	Demux マネージャファシリティ	110000 ～ 11099
dgmbmgr	Diameter Gmb（DGMB）アプリケーションマネージャ ファシリティ	126000 - 126999
dhcp	DHCP ファシリティ	53000 ～ 53999
dhcpv6	DHCPv6 プロトコルファシリティ	123000 ～ 12399
dhost	分散型ホストマネージャファシリティ	83000 ~ 83999
diameter	Diameter エンドポイントファシリティ	92000 ～ 92599
diabase	Diabase メッセージファシリティ	92800 ～ 92809
diameter-acct	Diameter アカウンティング プロトコル ファシリティ	112000 ～ 11299
diameter-auth	Diameter 認証プロトコルファシリティ	111000 ～ 11199
diameter-dns	Diameter DNS サブシステムファシリティ	92600 ～ 92699
diameter-ecs	ECS Diameter シグナリングファシリティ	81990 ～ 81999
diameter-hdd	Diameter Horizontal Directional Drilling（HDD）インターフェイス ファシリティ	92700-92799
diameter-svc	Diameter サービスファシリティ	121200 ～ 12199
diamproxy	Diameter プロキシファシリティ	119000 ～ 11999
dpath	IPSec ファシリティのデータパス	54000 ～ 54999
drvctrl	ドライバ コントローラ ファシリティ	39000 ～ 39999
ds3mgr	DS3 および DS3/E ラインカード マネージャ ファシリティ（NPU マネージャ コントローラ ファシリティの一部）	40000 ～ 40999
eap-diameter	Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）Diameter ファシリティ	92870 ～ 92879
eap-ipsec	EAP IPSec ファシリティ	118000 ～ 11899
ecs-css	ACS セッションマネージャ（ACSMgr）シグナリングインターフェイス ファシリティ	97000 ～ 97099
edr	イベントデータレコード（EDR）ファシリティ	80000 ～ 80999
egtpc	eGTP-C ファシリティ	141000 ～ 14199
egtpmgr	eGTP マネージャファシリティ	143000 ～ 14399
egtpu	eGTP-U ファシリティ	142000 ～ 14299
epdg	Evolved Packet Data Gateway（ePDG）ファシリティ	178000 ～ 17899
evlog	イベントログファシリティ	2000 ～ 2999

ファシリティ	説明	イベント ID
famgr	外部エージェント（FA）マネージャファシリティ	33000 ～ 339
ファイアウォール	ファイアウォール機能	96000 ～ 969
fng	フェムト ネットワーク ゲートウェイ（FNG）ファシリティ	149000 ～ 14
gbrmgr	Gb-Manager ファシリティ	201900 ～ 20
gcdr	GGSN 課金データレコード（G-CDR）ファシリティ	66000 ～ 669
gmm	GPRS Mobility Management（GMM）ファシリティ	88100 ～ 882
gprs-app	General Packet Radio Service（GPRS）アプリケーション ファシリティ	115100 ～ 11
gprs-ns	GPRS-NS プロトコルファシリティ	115000 ～ 11
gq-rx-tx-diameter	Gq/Rx/Tx Diameter メッセージファシリティ	92830 ～ 928
gss-gcdr	GTPP ストレージサーバーの GCDR ファシリティ	98000 ～ 980
gtpc	GTPC プロトコルファシリティ	47000 ～ 479
gtpcmgr	GTPC シグナリング デマルチプレクサ マネージャ ファシリティ	46000 ～ 469
gtpp	GTP-PRIME プロトコルファシリティ	52000 ～ 529
gtpu	GTPU プロトコルファシリティ	45000 ～ 459
gtpumgr	GTPU マネージャ ファシリティ	157200 ～ 15
gx-ty-diameter	Gx/Ty Diameter メッセージファシリティ	92820 ～ 928
gy-diameter	Gy Diameter メッセージファシリティ	92810 ～ 928
h248prt	H.248 プロトコルファシリティ	42000 - 4299
hamgr	ホームエージェント（HA）マネージャファシリティ	34000 ～ 349
hat	高可用性タスク（HAT）ファシリティ	3000 ～ 3999
hdctrl	ハードディスク（HD）コントローラファシリティ	132000 ～ 13
hddshare	HDD 共有ファシリティ	184000 ～ 18
henb-gw	Home eNodeB-GW ファシリティ	195000 ～ 19
henbapp	Home eNodeB アプリケーションファシリティ	196000 ～ 19
henbgwdemux	Home eNodeB-GW Demux ファシリティ	194000 ～ 19
henbgwmgr	Home eNodeB-GW マネージャファシリティ	193000、193
hnb-gw	Home NodeB（HNB）ゲートウェイファシリティ	151000 ～ 15
hnbmgr	HNB マネージャファシリティ	158000 ～ 15
hss-peer-service	ホーム サブスクライバ サーバー（HSS）ファシリティ [MME]	138000 ～ 13

ファシリティ	説明	イベント ID の範
igmp	Internet Group Management Protocol（IGMP）	113000 ～ 11399
ikev2	IKEv2 ファシリティ	122000 ～ 12299
ims-authorizatn	IMS 承認サービス ライブラリ ファシリティ	98100 ～ 98999
ims-sh	IMS SH ライブラリファシリティ	124000 ～ 12499
imsimgr	International Mobile Subscriber Identity（IMSI）マネージャファシリティ	114000 ～ 11499
imsue	IMS User Equipment（IMSUE）ファシリティ	144000 ～ 14599
ip-arp	IP Address Resolution Protocol（ARP）ファシリティ	19000 ～ 19999
ip-interface	IP インターフェイスファシリティ	18000 ～ 18999
ip-route	IP ルートファシリティ	20000 ～ 20999
ipms	インテリジェントパケットモニタリングシステム（IPMS）ファシリティ	134000 ～ 13499
ipne	IP Network ENABLER（IPNE）ファシリティ	192000 ～ 19299
ipsec	IPSec プロトコルファシリティ	55000 ～ 56998
ipsg	IP サービスゲートウェイ（IPSG）ファシリティ	128000 ～ 12899
ipsgmgr	IPSG マネージャ（IPSGMgr）ファシリティ	99000 ～ 99999
ipsp	IP プール共有プロトコル（IPSP）ファシリティ	68000 ～ 68999
kvstore	Key/Value ストア（kvstore）ファシリティ	125000 ～ 12599
l2tp-control	L2TP Control PDU Protocol ファシリティ	50000 ～ 50999
l2tp-data	L2TP Data PDU Protocol ファシリティ	49000 ～ 49999
l2tpdemux	L2TP Demux ファシリティ	63000 ～ 63999
l2tpmgr	L2TP マネージャファシリティ	48000 ～ 48999
lagmgr	Link Aggregation GROUP（LAG）マネージャファシリティ	179000 ～ 17999
ldap	Lightweight Directory Access Protocol（LDAP）リクエストファシリティ	160000 ～ 16049
li	合法的傍受（LI）ログファシリティ	69000 ～ 69999
linkmgr	リンク マネージャ ファシリティ	89500 ～ 89999
llc	論理リンク制御（LLC）レイヤファシリティ（GPRS）	115700 ～ 11579
local-policy	ローカルポリシー設定ファシリティ	161400 ～ 16239
m3ap	M3 アプリケーション プロトコル（M3AP）ファシリティ	211500 ～ 21199

ファシリティ	説明	イベント ID
m3ua	MTP レベル 3（M3UA）プロトコルファシリティ [SIGTRAN]	87500 ～ 876
magmgr	モバイルアクセス ゲートウェイ（MAG）マネージャファシリティ	137500 ～ 13
map	モバイル アプリケーション パート（MAP）プロトコルファシリティ [SS7]	87100 ～ 872
megadiammgr	MegaDiameter マネージャファシリティ	121000 ～ 12
mme-app	モビリティマネージメントエンティティ（MME）アプリケーションファシリティ	147000 ～ 14
mme-embms	MME evolved Multimedia Broadcast Multicast Service（eMBMS）ファシリティ	212000 ～ 21
mme-misc	MME その他のファシリティ	155800 ～ 15
mmedemux	MME Demux マネージャファシリティ	154000 ～ 15
mmemgr	MME マネージャファシリティ	137000 ～ 13
mmgr	マスターマネージャ（MMGR）ファシリティ	86000 ～ 863
mobile-ip	モバイル IP（MIP）プロトコルファシリティ	26000 ～ 269
mobile-ip-data	MIP トンネルデータファシリティ	27000 ～ 279
mobile-ipv6	モバイル IPv6 ファシリティ	129000 ～ 12
mpls	マルチ プロトコル ラベル スイッチング（MPLS）ファシリティ	163500 ～ 16
mseg-app	Mobile Services Edge Gateway（MSEG）アプリケーション ファシリティ 本リリースではサポートされていません。	172300 ～ 17
mseg-gtpc	MSEG GTPC アプリケーション ファシリティ 本リリースではサポートされていません。	172000 ～ 17
mseg-gtpu	MSEG GTPU アプリケーション ファシリティ 本リリースではサポートされていません。	172200 ～ 17
msegmgr	MSEG マネージャファシリティ 本リリースではサポートされていません。	171000 ～ 17
mtp2	Message Transfer Part 2（MTP2）サービスファシリティ [SS7]	116900 ～ 11
mtp3	Message Transfer Part 3（MTP3）サービスファシリティ [SS7]	115600 ～ 11
multicast-proxy	マルチキャスト プロキシ ファシリティ	94000 ～ 949
nas	ネットワーク アクセス シグナリング（NAS）ファシリティ	153000 ～ 15

ファシリティ	説明	イベント ID の範
netwstrg	ネットワーク ストレージ ファシリティ	78000 ～ 78999
npuctrl	ネットワーク処理ユニット（NPU）制御ファシリティ	16000 ～ 16999
npudrv	NPU ドライバファシリティ	191000 ～ 19199
npumgr	NPU マネージャ（NPUMGR）ファシリティ	17000 ～ 17999
npumgr-acl	NPUMGR ACL ファシリティ	169000 ～ 16999
npumgr-drv	NPUMGR ドライバファシリティ	185000 ～ 18599
npumgr-flow	NPUMGR フローファシリティ	167000 ～ 16799
npumgr-fwd	NPUMGR 転送ファシリティ	168000 ～ 16899
npumgr-init	NPUMGR 初期化ファシリティ	164000 ～ 16499
npumgr-lc	NPUMGR LC ファシリティ	180000 ～ 18099
npumgr-port	NPUMGR ポートファシリティ	166000 ～ 16699
npumgr-recovery	NPUMGR リカバリファシリティ	165000 ～ 16599
npumgr-vpn	NPUMGR VPN ファシリティ	181000 ～ 18199
npusim	NPUSIM ファシリティ	176000 ～ 17699
ntfy-intf	イベント通知インターフェイス ファシリティ	170000 ～ 17049
orbs	orbs：オブジェク リクエスト ブローカ（ORB）システムファシリティ	15000 ～ 15999
ospf	Open Shortest Path First（OSPF）プロトコルファシリティ	38000 ～ 38999
ospfv3	OSPFv3 プロトコルファシリティ [IPv6]	150000 ～ 15099
p2p	ピアツーピア（P2P）ファシリティ	146000 ～ 14699
pccmgr	Policy Charging and Control（PCC）マネージャファシリティ	159000 ～ 15949
pdg	Packet Data Gateway（PDG）ファシリティ	152010 ～ 15299
pdgdmgr	PDG TCP Demux Manager（pdgdmgr）ファシリティ（顧客固有のファシリティ）	162400 ～ 16299
pdif	Packet Data Interworking Function（PDIF）ファシリティ	120000 ～ 12099
pgw	Packet Data Network Gateway（PGW）ファシリティ	139000 ～ 13999
pmm-app	パケット モビリティ マネージメント（PMM）アプリケーション ファシリティ [SGSN]	89200 ～ 89499
ppp	Point-To-Point Protocol（PPP）ファシリティ	25000 ～ 25999
pppoe	Point-to-Point Protocol over Ethernet（PPPoE）ファシリティ	183000 ～ 18399

ファシリティ	説明	イベント ID
ptt	PTT ファシリティ	76000 ～ 769
push	PUSH（VPNMgr CDR Push）ファシリティ	133000 ～ 13
radius-acct	RADIUS アカウンティング プロトコル ファシリティ	24000 ～ 249
radius-auth	RADIUS 認証プロトコルファシリティ	23000 ～ 239
radius-coa	RADIUS 許可の変更（CoA）と接続解除ファシリティ	70000 ～ 709
ranap	Radio Access Network Application Part（RANAP）ファシリティ	87700 ～ 878
rct	リカバリ制御タスク（RCT）ファシリティ	13000 ～ 139
rdt	リダイレクタタスク（RDT）ファシリティ	67000 ～ 679
resmgr	Resource Manager (RM) ファシリティ	14000 ～ 149
rf-diameter	Rf Diameter メッセージファシリティ	92860 ～ 928
rip	Routing Information Protocol（RIP）ファシリティ	35000 ～ 359
rohc	Robust Header Compression（ROHC）プロトコルファシリティ	103000 ～ 10
rsvp	RSVP プロトコルファシリティ	93000 ～ 939
rua	RANAP User Adaptation（RUA）プロトコルファシリティ	152000 ～ 15
s1ap	S1 アプリケーション プロトコル（S1AP）ファシリティ	155200 ～ 15
saegw	System Architecture Evolution ゲートウェイファシリティ	191000 ～ 19
sccp	Signalling Connection Control Part（SCCP）プロトコルファシリティ [SS7]	86700 ～ 868
sct	共有設定タスク（SCT）ファシリティ	32000 ～ 320
sctp	Stream Control Transmission Protocol（SCTP）プロトコルファシリティ	87300 ～ 874
sess-gr	SESS-GR ファシリティ	77600 ～ 779
sessctrl	セッション コントローラ ファシリティ	8000 ～ 8999
sessmgr	セッション マネージャ ファシリティ	10000 ～ 129
sesstrc	セッション トレース ファシリティ	155000 ～ 15
sft	スイッチファブリックタスク（SFT）ファシリティ	58000 ～ 589
sgs	SG インターフェイスプロトコルファシリティ [MME]	173000 ～ 17
sgsn-app	SGSN アプリケーション インターフェイス ファシリティ	115900 ～ 11
sgsn-failures	SGSN コール失敗ファシリティ	89100 ～ 891
sgsn-gtpc	SGSN GTP-C プロトコルファシリティ	116000 ～ 11

ファシリティ	説明	イベント ID の範
sgsn-gtpu	SGSN GTP-U プロトコルファシリティ	86900 ～ 87099
sgsn-mbms-bearer	SGSN MBMS ベアラーアプリケーション（SMGR）ファシリティ	116600 ～ 11679
sgsn-misc	SGSN その他のファシリティ	88800 ～ 89099
sgsn-system	SGSN システム コンポーネント ファシリティ	86400 ～ 86499
sgsn-test	SGSN テストファシリティ	88700 ～ 88799
sgsn2	SGSN2 ファシリティ	114000 ～ 11799
sgtpcmgr	SGSN GTP-C（SGTPC）マネージャファシリティ	117000 ～ 11799
sgw	サービングゲートウェイ（SGW）ファシリティ	140000 ～ 14099
sh-diameter	Sh Diameter メッセージファシリティ	92850 ～ 92859
sipcdprt	SIPCDPRT ファシリティ	95000 ～ 95999
sitmain	システム開始タスク（SIT）メインファシリティ	4000 ～ 4999
sm-app	ショート メッセージ サービス（SMS）ファシリティ	88300 ～ 88499
sms	SMS サービスファシリティ	116800 ～ 11689
sndcp	Sub Network Dependent Convergence Protocol（SNDCP）ファシリティ	115800 ～ 11589
snmp	Simple Network Management Protocol（SNMP）ファシリティ	22000 ～ 22999
sprmgr	Subscriber Policy Register（SPR）マネージャファシリティ	159500 ～ 15999
srdb	スタティック評価データベースファシリティ	102000 ～ 10299
srp	サービス冗長性プロトコル（SRP）ファシリティ	84000 ～ 84999
sscfnni	SSCFNNI プロトコルファシリティ [ATM]	115500 ～ 11559
sscop	SSCOP Protocol ファシリティ [ATM]	115400 ～ 11549
ssh-ipsec	SSH IP セキュリティファシリティ	56999 ～ 56999
ssl	SSL ファシリティ（顧客固有のファシリティ）	156200 ～ 15719
stat	統計情報ファシリティ	31000 ～ 31999
system	システムファシリティ	1000 ～ 1999
tacacs+	TACACS+ プロトコルファシリティ	37000 ～ 37999
taclcp	TACLCP ファシリティ	44000 ～ 44999
tcap	Transaction Capabilities Application Part（TCAP）プロトコルのロギングファシリティ [SS7]	86500 ～ 86699
testctrl	テスト コントローラ ファシリティ	174000 ～ 17499
testmgr	テスト マネージャ ファシリティ	175000 ～ 17599

ファシリティ	説明	イベント ID
threshold	しきい値ファシリティ	61000 ～ 619
ttg	Tunnel Termination Gateway（TTG）ファシリティ	130000 ～ 13
tucl	TCP/UDP コンバージェンスレイヤ（TUCL）ファシリティ [SS7]	88500 ～ 886
udr	ユーザーデータレコード（UDR）ファシリティ	79000 ～ 799
user-data	ユーザーデータファシリティ	51000 ～ 519
user-l3tunnel	ユーザー L3 トンネルファシリティ	75000 ～ 759
usertcp-stack	ユーザー TCP スタックファシリティ	173300 ～ 17
vim	ボイス インスタント メッセージ（VIM）ファシリティ	60000、6099
vinfo	VINFO ファシリティ	82000、8299
vmgctrl	仮想メディアゲートウェイ（VMG）コントローラファシリティ	41000、4199
vmgctxmgr	VMG コンテキスト マネージャ ファシリティ	43000、4399
vpn	バーチャル プライベート ネットワーク（VPN）ファシリティ	5000 ～ 5999
wimax-data	WiMAX データファシリティ	104900 ～ 10
wimax-r6	WiMAX R6 プロトコル（シグナリング）ファシリティ	104000 ～ 10

イベントのシビラティ（重大度）

システムにより、ロギングが有効になっている場合に表示される情報のレベルを柔軟に設定できます。次のレベルがサポートされます。

- **クリティカル**：システムまたはシステムのコンポーネントの機能を停止させる重大なエラーが発生したことをログに記録します。これが最高のシビラティ（重大度）レベルです。
- **エラー**：システムまたはシステムのコンポーネントの動作を低下させるエラーが発生したことをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **警告**：潜在的な問題を示す可能性があるイベントをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **異常**：きわめて異常であり、調査する必要がある可能性のあるイベントをログに記録します。このレベルは、シビラティ（重大度）レベルが高いイベントもログに記録します。
- **情報**：シビラティ（重大度）がより高い情報イベントおよびイベントをログに記録します。
- **トレース**：トレースに役立つイベントやより高いシビラティ（重大度）を持つイベントをログに記録します。

- **デバッグ**：シビラティ（重大度）に関係なく、すべてのイベントをログに記録します。

上記のレベルはそれぞれ、イベント ID の「シビラティ（重大度）」レベルに対応します。したがって、「シビラティ（重大度）」レベルがロギングレベルと等しいイベント ID のみが表示されます。

ログ出力のイベント ID 情報の概要

この項では、ロギングが有効になっておりときに表示されるイベント情報について説明します。

次に、ログに記録されたイベントの出力例を示します。

```
2011-Dec-11+5:18:41.993 [cli 30005 info] [8/0/609 cli:8000609 _commands_cli.c:1290]
[software internal system] CLI session ended for Security Administrator admin on device
 /dev/pts/2
```

次の表で、出力例に含まれている要素について説明します。

表 *109*：イベント要素の説明

要素	説明
2011-Dec-11+5:18:41.993	イベントが生成された日時を示す日付/タイムスタンプ
[cli 30005 info]	以下を含むイベントに関する情報 • イベントが属している機能 • イベント ID • イベントのシビラティ（重大度） この例では、イベントはCLI ファシリティに属しており、ID は 3005、シビラティ（重大度）は「info」です。
[8/0/609 cli:8000609 _commands_cli.c:1290]	特定の CLI インスタンスに関する情報。
[software internal system]	イベントの発生原因がシステムの動作であることを示しています。
CLI session ended for Security Administrator admin on device /dev/pts/2	イベントの詳細。イベントの詳細には、イベントの発生に固有の変数が含まれている場合と含まれない場合があります。



第 49 章

UPF 入力インターフェイス

- 機能の概要と変更履歴, on page 581
- 機能説明, on page 582
- UPF 入力インターフェイス種別の構成 （583 ページ）
- 複数の GTPU IP アドレスのサポート （589 ページ）

機能の概要と変更履歴

要約データ

Table 110: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

更新履歴

Table 111: マニュアルの変更履歴

改訂の詳細	リリース
UPF の VPP ワーカースレッド間で通信を均等に分配するために、複数の GTPU IP アドレスをバインドするためのサポートが追加されました。	2023.04.0
N3 および N9 インターフェイス用の個別のネットワークを可能にするために、インターフェイスごとの IP 分離のサポートが追加されました。	2023.03.0 2023.02.0
最初の導入。	2020.02.0

機能説明

UPF は、ユーザープレーンサービスを開始するために GTP-U 入力インターフェイスをサポートします。UPF は、N3 インターフェイスと N9、S5u、および S8u インターフェイスに個別のネットワークを許可するために、さまざまな GTP-U 入力インターフェイスをサポートしています。N9、S5u、および S8u インターフェイスは、同じパブリック IP を共有します。

サポートされている GTP-U 入力インターフェイスは次のとおりです。

- **N3**：N3 は、gNodeB と UPF 間のインターフェイスです。
- **N9**：N9 インターフェイスは 2 つの UPF を接続します。これは、異なる PLMN を接続する中間 I-UPF と UPF セッションアンカー間のインターフェイスです。
- **S5u**：S5u は、4Gの SGW-U と PGW-U 間のインターフェイスです。
- **S8u**：S8u は S5u インターフェイスの PLMN 間バリアントです。

ユーザープレーンサービスは、ユーザープレーンサービス構成モードで **associate gtpu-service** CLI コマンドを使用して GTP-U サービスに関連付けます。**upf-ingress** コマンドを有効にするには、UPF で、**require upf** コマンドを構成する必要があります。**require upf** コマンドを有効にするには、UPF ライセンスが必要です。

Note UPF は、1 つのコールに対する複数の GTP-U サービスの選択をサポートしません。

UPF 入力インターフェイス種別の構成

UPF 入力インターフェイスタイプを構成する

UPF 入力インターフェイス タイプを構成するには、次の構成を使用します。

upf-ingress コマンドを有効にするには、UPF で、**require upf** コマンドを構成する必要があります。**require upf** コマンドを有効にするには、UPF ライセンスが必要です。

```
configure
   context context_name
      user-plane-service service_name
         [ no ] associate gtpu-service gtpu_service_name upf-ingress
interface-type [ n9 | s5u | s8u | n3 | n9-s5u-s8u ]
        end
```

注：

- **associate gtpu-service** *gtpu_service_name*：GTP-U サービスとユーザープレーンサービスを関連付けます。
- **upf-ingress**：UPF イングレスとしてインターフェイスタイプを構成します。
- **interface-type [n9 | s5u | s8u | n3 | n9-s5u-s8u]**：希望する GTP-U 入力インターフェイスタイプを構成します。
- N3 GTP-U 入力サービスが存在しない場合、UPF はデフォルトのインターフェイスを使用します。
- N9、S5u、または S8u インターフェイスの構成が存在しない場合、UPF は次のアクションを実行します。
  - UPF は、最初に N9 インターフェイスを使用し、次に S5u および S8u インターフェイスを使用します。
  - GTP-U サービスがない場合、UPF はデフォルトのインターフェイスを使用します。

設定例

次に設定例を示します。

```
associate gtpu-service n3-ingress upf-ingress
associate gtpu-service n3-ingress upf-ingress interface-type n3
associate gtpu-service n9-ingress upf-ingress interface-type n9
associate gtpu-service s5-ingress upf-ingress interface-type s5
associate gtpu-service s8-ingress upf-ingress interface-type s8
```

N9 インターフェイスの Echo 応答を構成する

GTP-U サービスでの Echo 応答は、ピア UPF の可用性を提供します。

次に、hUPF での N9 インターフェイスの Echo 応答構成の例を示します。

```
gtpu-service n9-ingress
   echo-interval 60
   echo-retransmission-timeout 1
   bind ipv4-address 60.60.41.5 bearer-type all
   exit
```

次に、vUPF の N9 インターフェイスの Echo 応答構成の例を示します。

```
gtpu-service n9-egress
   echo-interval 60
   echo-retransmission-timeout 1
   bind ipv4-address 60.60.42.5 bearer-type all
   exit
```

N3 および N9 BGP ルートを分離する

以下は、hUPF の N3 および N9 BGP ルートを分離する構成例です。

```
 config
  context SAEGW
    ip vrf mpls-vrf-1
    #exit
    ip vrf mpls-vrf-2
    #exit
    mpls bgp forwarding
    bfd-protocol
    #exit
    ip prefix-list name up seq 15 permit 50.50.17.4/32
    ip prefix-list name up seq 20 permit 50.50.17.5/32
    ip prefix-list name up seq 25 permit 50.50.17.6/32
    ip prefix-list name up seq 40 permit 50.50.17.7/32
    ip prefix-list name n9-up1 seq 50 permit 60.60.17.5/32
    ip prefix-list name n9-up1 seq 55 permit 60.60.17.6/32
    route-map up_routes1 permit 10
      match ip address prefix-list n9-up1
    #exit
    route-map up_routes permit 10
      match ip address prefix-list up
    #exit
    router bgp 61435
      maximum-paths ebgp 4
      neighbor 20.14.35.100 remote-as 65000
      neighbor 20.14.35.100 ebgp-multihop
      neighbor 20.14.35.100 update-source 20.14.35.98
      neighbor 2001:4888:121:1435::1 remote-as 65000
      neighbor 2001:4888:121:1435::1 ebgp-multihop
      neighbor 2001:4888:121:1435::1 update-source 2001:4888:121:1435::2
      neighbor 20.14.40.100 remote-as 65000
      neighbor 20.14.40.100 ebgp-multihop
      neighbor 20.14.40.100 update-source 20.14.40.98
      address-family ipv4
        neighbor 20.14.35.100 max-prefix 8192 threshold 50
        neighbor 20.14.35.100 route-map up_routes out
        neighbor 20.14.35.100 send-community extended
        neighbor 20.14.40.100 max-prefix 8192
        neighbor 20.14.40.100 route-map up_routes1 out
        neighbor 20.14.40.100 send-community extended
        redistribute connected
        redistribute static
      #exit
```

```
  address-family ipv6
    neighbor 2001:4888:121:1435::1 activate
    redistribute connected
    redistribute static
  #exit
#exit
interface SxC loopback
  ip address 50.50.17.4 255.255.255.255
#exit
interface SxC-ipv6 loopback
  ipv6 address 2001:4888:50:50::17/128
#exit
interface gn-1
  ip address 20.14.35.98 255.255.255.0
  ipv6 address 2001:4888:121:1435::2/64 secondary
#exit
interface gn-2
  ip address 20.14.36.98 255.255.255.0
  ipv6 address 2001:4888:121:1436::2/64 secondary
#exit
interface gn-n9-ingress
  ip address 20.14.40.98 255.255.255.0
#exit
interface n9-ingress-hupf loopback
  ip address 60.60.17.5 255.255.255.255
#exit
interface pgw-gtpu loopback
  ip address 50.50.17.5 255.255.255.255
#exit
interface sgw-gtpu-egress loopback
  ip address 50.50.17.6 255.255.255.255
#exit
interface sgw-gtpu-ingress-phazr loopback
  ip address 60.60.17.6 255.255.255.255
#exit
subscriber default
exit
aaa group default
#exit
gtpp group default
  gtpp limit-secondary-rat-usage 32
#exit
gtpu-service SxC
  echo-interval 60
  echo-retransmission-timeout 1
  bind ipv4-address 50.50.17.4 ipv6-address 2001:4888:50:50::17 bearer-type all
exit
gtpu-service n9-ingress
  bind ipv4-address 60.60.17.5 bearer-type all
exit
gtpu-service pgw-gtpu
  bind ipv4-address 50.50.17.5 bearer-type all
exit
gtpu-service sgw-gtpu-egress
  bind ipv4-address 50.50.17.6 bearer-type all
exit
gtpu-service sgw-gtpu-ingress-phazr
  echo-interval 60
  echo-retransmission-timeout 1
  bind ipv4-address 60.60.17.6 bearer-type all
exit
sx-service sx-svc
  instance-type userplane
  bind ipv4-address 50.50.17.4 ipv6-address 2001:4888:50:50::17
```

```
    sxa max-retransmissions 5
    sxa retransmission-timeout-ms 1000
    sxb max-retransmissions 5
    sxb retransmission-timeout-ms 1000
    sxab max-retransmissions 5
    sxab retransmission-timeout-ms 1000
    sx-protocol heartbeat retransmission-timeout 15
    sx-protocol heartbeat max-retransmissions 3
    sx-protocol association debug-mode debug-reattempt-timeout 1
    no sx-protocol compression
  exit
  user-plane-service user_plane_svc
    associate gtpu-service pgw-gtpu upf-ingress
    associate gtpu-service n9-ingress upf-ingress interface-type n9
    associate gtpu-service sgw-gtpu-ingress-phazr sgw-ingress
    associate gtpu-service sgw-gtpu-egress sgw-egress
    associate gtpu-service SxC cp-tunnel
    associate sx-service sx-svc
    associate fast-path service
    associate control-plane-group SAEGW
    associate userplane-load-control-profile LCP
    associate userplane-overload-control-profile OLCP
  exit
```

以下は、vUPF の N3 および N9 BGP ルートを分離する構成例です。

```
context SAEGW
  router bgp 61441
    neighbor 20.14.41.100 remote-as 65000
    neighbor 20.14.41.100 ebgp-multihop
    neighbor 20.14.41.100 update-source 20.14.41.98
    neighbor 2001:4888:121:1441::1 remote-as 65000
    neighbor 2001:4888:121:1441::1 ebgp-multihop
    neighbor 2001:4888:121:1441::1 update-source 2001:4888:121:1441::2
    address-family ipv4
      redistribute connected
      redistribute static
    #exit
    address-family ipv6
      neighbor 2001:4888:121:1441::1 activate
      redistribute connected
      redistribute static
    #exit
  #exit
  interface SxC loopback
    ip address 50.50.18.4 255.255.255.255
  #exit
  interface SxC-ipv6 loopback
    ipv6 address 2001:4888:50:50::18/128
  #exit
  interface gn-1
    ip address 20.14.41.98 255.255.255.0
    ipv6 address 2001:4888:121:1441::2/64 secondary
  #exit
  interface gn-2
    ip address 20.14.42.98 255.255.255.0
    ipv6 address 2001:4888:121:1442::2/64 secondary
  #exit
  interface n9-egress loopback
    ip address 50.50.18.8 255.255.255.255
  #exit
  interface pgw-gtpu loopback
    ip address 50.50.18.5 255.255.255.255
  #exit
  interface pgw-gtpu-ipv6 loopback
```

```
  ipv6 address 2001:4888:50:50::18:5/128
#exit
interface sgw-gtpu-egress loopback
  ip address 50.50.18.6 255.255.255.255
#exit
interface sgw-gtpu-egress-ipv6 loopback
  ipv6 address 2001:4888:50:50::18:6/128
#exit
interface sgw-gtpu-ingress-phazr loopback
  ip address 50.50.18.7 255.255.255.255
#exit
interface sgw-gtpu-ingress-phazr-ipv6 loopback
  ipv6 address 2001:4888:50:50::18:7/128
#exit
subscriber default
exit
aaa group default
#exit
gtpp group default
  gtpp limit-secondary-rat-usage 32
#exit
gtpu-service SxC
  echo-interval 60
  echo-retransmission-timeout 1
  bind ipv4-address 50.50.18.4 ipv6-address 2001:4888:50:50::18 bearer-type all
exit
gtpu-service n9-egress
  bind ipv4-address 50.50.18.8 bearer-type all
exit
gtpu-service pgw-gtpu
  bind ipv4-address 50.50.18.5 ipv6-address 2001:4888:50:50::18:5 bearer-type all
exit
gtpu-service sgw-gtpu-egress
  bind ipv4-address 50.50.18.6 ipv6-address 2001:4888:50:50::18:6 bearer-type all
exit
gtpu-service sgw-gtpu-ingress-phazr
  echo-interval 60
  echo-retransmission-timeout 1
  bind ipv4-address 50.50.18.7 ipv6-address 2001:4888:50:50::18:7 bearer-type all
exit
sx-service sx-svc
  instance-type userplane
  bind ipv4-address 50.50.18.4 ipv6-address 2001:4888:50:50::18
  sxa max-retransmissions 5
  sxa retransmission-timeout-ms 1000
  sxb max-retransmissions 5
  sxb retransmission-timeout-ms 1000
  sxab max-retransmissions 5
  sxab retransmission-timeout-ms 1000
  sx-protocol heartbeat retransmission-timeout 15
  sx-protocol heartbeat max-retransmissions 3
  sx-protocol association debug-mode debug-reattempt-timeout 1
  no sx-protocol compression
exit
user-plane-service user_plane_svc
  associate gtpu-service pgw-gtpu upf-ingress
  associate gtpu-service n9-egress upf-egress
  associate gtpu-service sgw-gtpu-ingress-phazr sgw-ingress
  associate gtpu-service sgw-gtpu-egress sgw-egress
  associate gtpu-service SxC cp-tunnel
  associate sx-service sx-svc
  associate fast-path service
  associate control-plane-group SAEGW
  associate userplane-load-control-profile LCP
```

```
    associate userplane-overload-control-profile OLCP
  exit
  ip route 0.0.0.0 0.0.0.0 20.14.41.100 gn-1
  ip igmp profile default
  #exit
#exit
```



（注） RCM UPF の場合、Day 0.5 構成にすべての IP プレフィックスリストを追加します。

UPF 入力インターフェイス種別の構成を検証する

設定を確認するには、次のコマンドを使用します。

- show user-plane-service all （588 ページ）

show user-plane-service all

show user-plane-service all コマンドは、user-plane サービス情報を表示します。

次に、このコマンドの出力例を示します。

```
show user-plane-service all
Service name                          : user-plane-service
  Service-Id                          : 7
  Context                             : EPC2-UP
  Status                              : NOT STARTED
  UPF Ingress GTPU Service            : sx-gtpu-service
  UPF Ingress N3 Interface Type GTPU Service: n3-ingress
  UPF Ingress N9 Interface Type GTPU Service: n9-ingress
  UPF Ingress S5U Interface Type GTPU Service: s5u-ingress
  UPF Ingress S8U Interface Type GTPU Service: s8u-ingress
  UPF Egress GTPU Service             : Not defined
  SGW Ingress GTPU Service            : SGW-Ingress
  SGW Egress GTPU Service             : SGW-Egress
  Control Plane Tunnel GTPU Service : control_gtpu
  Sx Service                          : sxu
  Control Plane Group                 : g1
  Fast-Path service                   : Disabled
```

注：

- UPF は、単一のユーザープレーン サービスで、いずれかのインターフェイスタイプ、**pgw-ingress** または **upf-ingress** のみを構成します。

複数の GTPU IP アドレスのサポート

表 *112:* 機能の履歴

機能名	リリース情報	機能説明
複数の GTPU IP アドレスをバインドする	2023.04	UPF を使用すると、複数の GTPU IP アドレスをバインドでき、プライベート 5G のデプロイメントで高いアップリンクスループットを提供できます。UPF は、一意の GTPU 3 タプルハッシュエントリを作成して、すべての VPP ワーカースレッドで入力通信を均等に分散させます。

機能説明

アップリンク通信がダウンリンク通信よりも多いプライベート 5G ネットワークでは、gNodeB の数は制限されます。UPF は、Receive Side Scaling（RSS）の概念を使用してサブスクライバ通信の最適な分散を実現します。ただし、UPF の VPP ワーカースレッドの数が限られているため、入力通信はそれらのスレッド間で均等に分散されません。UPF がすべてのワーカースレッドを最適に使用するのを制限するため、サブスクライバのアップリンクスループットに影響を及ぼします。

UPF では、UPF のフォワーディングプレーンで一意の GTPU 3 タプルハッシュエントリを作成することで、VPP ワーカー スレッドを最適な方法で利用できます。これにより、N3 インターフェイスでの入力通信の最適な分散が保証されます。これにより、UPF は最大キャパシティまで通信処理を実行でき、プライベート 5G ネットワークで高いアップリンクスループットを確保します。

機能の仕組み

一意の 3 タプルハッシュエントリを作成することで、UPF で使用可能なすべてのワーカースレッドでの入力通信の均等な分散が保証されます。

GTPU ヘッダーの送信元 IP は、gNodeB の N3 サービスエグレス IP ですが、gNodeB でポートのランダム化のサポートがない場合、ソースポートは標準規格ポートです。これらの 2 つの値が gNodeB ごとの定数である場合、GTPU ヘッダーで実現できる唯一の変数は接続先 IP（N3 サービスイングレス IP アドレス）です。

次に、一意の 3 タプルハッシュエントリの作成方法について説明します。

- GTPU アドレスは、サブスクライバセッションの Sx Session Establishment 応答の FTEID に round-robin 方式で割り当てられます。ただし、この round-robin メカニズムは、セッションマネージャ内でのみ保証されます。

- セッションマネージャが選択されると、選択したセッションマネージャに到達するすべてのセッションに、FTEID の GTPU アドレスが round-robin 方式で割り当てられます。
- GTPU サービスまたはインターフェイスから IP アドレスを削除しても、GTPU サービスが停止することはありません。既存のコールは削除されます。ただし、削除された IP アドレスが割り当てられたサブスクライバのアップリンク通信は、UPF で受信されません。
- すべての IP アドレスが別のインターフェイスで設定されている場合、インターフェイスはループバックとして設定する必要があります（複数の非ループバック インターフェイスが同じサブネットを共有することはできません）。いずれかのインターフェイスが停止してから再び稼働しても、インターフェイスはループバックとして設定されているため、GTPU サービスは停止しません。
- すべてのアドレスペアは、GTPU サービスの 1 つの GTPU エンドポイントです。すべてのエンドポイントが同じサブネットに属している必要があります。

（注）
- 最適なパフォーマンスを得るには、GTPUバインドアドレスの数がVPP ワーカースレッドの数と同じである必要があります。
- GTPU サービスごとに最大 12 の IP アドレスペア（IPv4 または IPv6、または IPv4 + IPv6）を構成できます。

制限事項

この機能には、次の制限事項があります。

- GTPU Echo が有効になっており、最初のバインド IP アドレスが削除されると、リモートピアからの Echo 要求が UPF に到達せず、リモートピアがパス障害を検出する原因となります。そのサブスクライバの UPF からの後続のダウンリンク通信により、UPF でエラー通知が受信されます。

  GTPUサービスは、すべてのバインドIPアドレスが削除された場合にのみ停止します。これらの IP アドレスは、単一のインターフェイスまたは個別のインターフェイスに割り当てることができます。

- UPF では、GTPU サービスごとに異なる IP アドレスタイプを設定できません。つまり、IPv4 + IPv6 または IPv4 + IPv4/IPv6 の組み合わせは許可されません。IPv4 または IPv6、または IPv4 + IPv6 の組み合わせのみを設定できます。

N3 インターフェイスで複数のバインドアドレスを構成する

N3 インターフェイスで複数バインドアドレスを構成するには、次の構成例を使用します。

```
config
  context context_name
    gtpu-service service_name
```

```
      bind { ipv4-address ipv4_address | ipv6-address ipv6_address [
bearer-type { non-ims-media | ims-media | all } ] }
      exit
```

注：

- **bind { ipv4-address** *ipv4_address* **| ipv6-address** *ipv6_address* **}**：GTPU サービスを、N3 インターフェイスの IPv4 アドレスまたは IPv6 アドレスにバインドします。
- **[bearer-type { non-ims-media | ims-media | all }]**：バインドアドレスと関連付けるベアラーのタイプを指定します。 **bearer-type** では、3 種類のメディア通信を許可します。
  - **non-ims-media**：IMS 以外のメディアのみに対してバインドアドレスを構成します。
  - **ims-media**：ims-media 通信のみに対してバインドアドレスを構成します。
  - **all**：すべてのタイプのベアラー通信を処理するようにバインドアドレスを構成します。これはデフォルトの動作です。

（注） GTPU エコーが GTPU サービスで有効になっている場合、Echo 要求は GTPU サービスで設定された最初のバインドアドレスで開始されます。バインドアドレスの設定は、ソートされたリストに保存されます。その結果、GTPUエコーは、数値的に最も低いバインドIPアドレスから開始します。

設定例

以下は、N3 インターフェイスで複数の GTPU IP アドレスをバインドする構成例です。

```
config
context EPC2-UP
cups enable
interface uplane_interface
    ip address <ip_address 1> <subnet mask>
    ip address <ip_address 2> <subnet mask> secondary
    ip address <ip_address 3> <subnet mask> secondary
    ip address <ip_address 4> <subnet mask> secondary
    ip address <ip_address 5> <subnet mask> secondary
    ip address <ip_address 6> <subnet mask> secondary
    ip address <ip_address 7> <subnet mask> secondary
#exit
gtpu-service N3U-service
    bind ipv4-address <ip_address 1> bearer-type all
    bind ipv4-address <ip_address 2> bearer-type all
    bind ipv4-address <ip_address 3> bearer-type all
    bind ipv4-address <ip_address 4> bearer-type all
    bind ipv4-address <ip_address 5> bearer-type all
    bind ipv4-address <ip_address 6> bearer-type all
exit
```

設定の確認

構成を確認するには、次のコマンドを使用します：

show gtpu-service name N3U-service

次に、このコマンドの出力例を示します。

```
show gtpu-service name N3U-service

Service name:             N3U-service
  Context:                  EPC2-UP
  State:                    Started
  Echo Interval:            Disabled
  Sequence number:          Disabled
  Include UDP Port Ext Hdr: FALSE
  Max-retransmissions:         4
  Retransmission Timeout:   5 (secs)
  IPSEC Tunnel Idle Timeout:60 (secs)
  GTPU IP QOS DSCP value:10
  Allow Error-Indication:   Disabled
  Address List:
                <ip_address 1>      all
                <ip_address 2>      all
                <ip_address 3>      all
                <ip_address 4>      all
                <ip_address 5>      all
                <ip_address 6>      all
                <ip_address 7>      all
  GTPU UDP Checksum:  Enabled - Attempt Optimize Default Mode
  Path Failure Detection
  on gtp echo msgs:         Set
  Path Failure Clear Trap : non-echo
  GTPU Source-port Configuration : Use Standard Port
    GTPU Source-port Offset      : N/A
  GTPU Peer Statistics Threshold : 16000
         1
```

OAM のサポート

ここでは、この機能の操作、管理、およびメンテナンス サポートについて説明します。

モニタリングのサポート

この項では、機能レベルのモニタリングのサポート情報について説明します。

show user-plane-service gtpu local-addresses

このコマンドは、特定のバインドアドレスを使用したアクティブなベアラー/セッションの数を表示します。

シングルコンバージド 4G コールの場合：

```
show user-plane-service gtpu local-addresses
  Service name:         N3U-service
  Address List:                                                    GTPv1 Sessions:
     <ip_address 1>                                                     1
  Service name:         SGW-Egress
  Address List:                                                    GTPv1 Sessions:
     <ip_address 2>                                                     1
  Service name:         SGW-Ingress
Address List:                                                   GTPv1 Sessions:
     <ip_address 3>                                                     1
```

（注）
- 4G コールでは、ベアラーごとに 1 つの GTPU セッションが存在します。
- この CLI 出力には、GTPU アドレスごとの一意のサブスクライバの総数は表示されません。

5G コールの場合：

```
show user-plane-service gtpu local-addresses
  Service name:         N3U-service
  Address List:                                                         GTPv1 Sessions:
     <ip_address 1>                                                        1
  Service name:         SGW-Egress
  Address List:                                                         GTPv1 Sessions:
No active sessions exists
  Service name:         SGW-Ingress
  Address List:                                                         GTPv1 Sessions:
No active sessions exists
```

show user-plane-service gtpu statistics local-address

このコマンドは、GTPU バインドアドレスごとの統計を表示します。

```
show user-plane-service gtpu statistics local-address < Local IPv4/IPv6 Address>
Session Stats:
    Current:                                    1
    Current (IMS-media):                        0
    Total Setup:                                2
    Total Setup (IMS-media):                    0
    Current gtpu v0 sessions:                   0
    Current gtpu v1 sessions:                   2

  Total Data Stats:
    Uplink Packets:                    0  Uplink Bytes:                0
    Downlink Packets:                  0  Downlink Bytes:              0
    Packets Discarded:                 0  Bytes Discarded:             0
    Uplink Packets (IMS-media):                   0  Uplink Bytes (IMS-media):
       0
    Downlink Packets (IMS-media):                 0  Downlink Bytes (IMS-media):
       0
    Packets Discarded (IMS-media):                0  Bytes Discarded (IMS-media):
       0

 QoS Stats:

    QCI 1:
         Uplink Packets:               0  Uplink Bytes:                0
         Downlink Packets:             0  Downlink Bytes:              0
         Packets Discarded:            0  Bytes Discarded:             0

    QCI 2:
         Uplink Packets:               0  Uplink Bytes:                0
         Downlink Packets:             0  Downlink Bytes:              0
         Packets Discarded:            0  Bytes Discarded:             0

    QCI 3:
         Uplink Packets:               0  Uplink Bytes:                0
         Downlink Packets:             0  Downlink Bytes:              0
         Packets Discarded:            0  Bytes Discarded:             0
```

```
 QCI 4:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 5:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 6:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

QCI 7:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 8:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 9:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 65:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 66:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 69:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

  QCI 70:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 80:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 82:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0

 QCI 83:
      Uplink Packets:             0  Uplink Bytes:              0
      Downlink Packets:           0  Downlink Bytes:            0
      Packets Discarded:          0  Bytes Discarded:           0
```

```
Non-Std QCI(Non-GBR):
    Uplink Packets:              0  Uplink Bytes:                0
    Downlink Packets:            0  Downlink Bytes:         0
    Packets Discarded:           0  Bytes Discarded:           0
    Uplink Packets:              0  Uplink Bytes:                0
    Downlink Packets:            0  Downlink Bytes:         0
    Packets Discarded:           0  Bytes Discarded:           0

Total uplink packets GBR QCI's:                0
Total uplink Bytes GBR QCI's:                  0
Total Downlink packets GBR QCI's:              0
Total Downlink Bytes GBR QCI's:                0
Total uplink packets Non-GBR QCI's:            0
Total uplink Bytes Non-GBR QCI's:              0
Total Downlink packets Non-GBR QCI's:          0
Total Downlink Bytes Non-GBR QCI's:            0

 Path Management Messages:
   Echo Request Rx:                  0  Echo Response Rx:            0
   Echo Request Tx:                  0  Echo Response Tx:            0
   SuppExtnHdr  Tx:                  0  SuppExtnHdr   Rx:            0

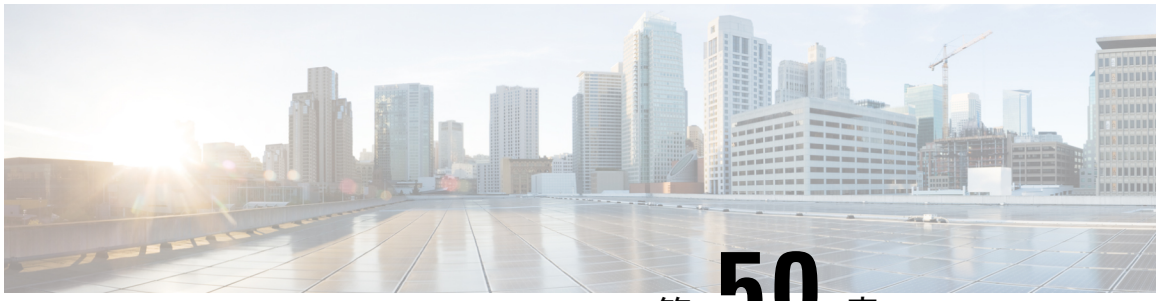
 Peer Stats:
   Total GTPU Peers:                             1
   Total GTPU Peers with Stats:                  1

Tunnel Management Messages:
    Error Indication Tx:                          0
    Error Indication Rx:                          0
    Error Indication Rx Discarded:                0
```

show npu utilization table

このコマンドは、VPP ワーカースレッドの CPU 使用率を表示します。

```
[local]UPF1# show npu utilization table
          ---------vpp--------
   lcore     now   5min  15min
--------  ------ ------ ------
 01/0/01     15%    11%    12%
 01/0/02     15%    13%    14%
 01/0/03     23%    23%    24%
 01/0/04     19%    21%    20%
 01/0/05     22%    20%    20%
 01/0/06     12%    11%    11%
 01/0/07     16%    16%    16%
 01/0/08     15%    17%    17%
 01/0/09     11%    12%    12%
```



第 50 章

UPF ローカル構成

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 597
- 機能説明, on page 598
- UPF のローカル構成サポートを構成する, on page 600

機能の概要と変更履歴

要約データ

Table 113: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 114: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

EPC ノードのコントロールおよびユーザープレーン分離（CUPS）アーキテクチャにおける静的ルールおよび事前定義ルールの処理のサポートは、ruledef、rulebase 、および課金アクションに依存します。L3/L4 の静的ルールおよび事前定義済みルールを処理する場合、この情報はCUPSアーキテクチャのコントロールプレーンで使用可能です。コントロールプレーンは、PFD management メッセージを使用して、関連するユーザープレーンにこれらすべての情報を送信します。UPF は、CN-SNF と連携するために PFD management メッセージを使用できません。この機能により、ユーザープレーン機能（UPF）のローカル構成のサポートが有効になり、UPF が CN-SNF と連携できるようになります。

機能の仕組み

Access Control System (ACS) CLI（コマンド ライン インターフェイス） は、ユーザープレーンで構成され、CLI モジュールがそれを ACS コントローラ（ACSCtrl）に送信します。ACSCtrl は、CLIを検証し、セッションコントローラ（SessCtrl）に送信します。SessCtrl は SCT に構成を保存します。

SessCtrl は、スキップリストのさまざまな構成タイプを維持および保存します。スキップリストの長さが特定の構成タイプの最大（BULK 構成の長さ）に達すると、リスト全体が Sessctrl からセッションマネージャ（SessMgr）に一括でプッシュされます。その結果、構成が 1 つのメッセージで一括で送信されるため、proclet 間のメッセンジャイベント/メッセージトランザクションの数が大幅に減少します。一括構成タイムアウト（2 秒）の期限切れ時に、セッションコントローラで常に実行されている一括構成タイマーによって、さまざまなタイプの構成が SessMgrs にプッシュされます。

- 一括構成プッシュでは、次の構成タイプがサポートされます。
- Ruledef
- 課金アクション
- アクション優先回線
- Group of ruledef 構成
- Group of ruledef 構成のルール
- rulebase L3/L4/L7 情報構成
- APN 設定
- ACS サービス構成

構成は、追加または変更された構成の一括プッシュメカニズム経由でプッシュされます。一方、構成が削除されると、一括構成プッシュタイマーからの応答を待つことなく、すぐに削除されます。削除された構成は、SCT および他の SessMgrs からすぐに削除されます。

Note 競合状態を回避するために、構成の削除をプッシュする前に、一括構成タイムアウト機能が強制的に呼び出され、保留中のすべての構成が SessMgrs にプッシュされます。

- すべての新規コールと既存のコールに適用される構成変更を次の表に示します。

Table 115: **新規および既存のコールフローの構成変更**

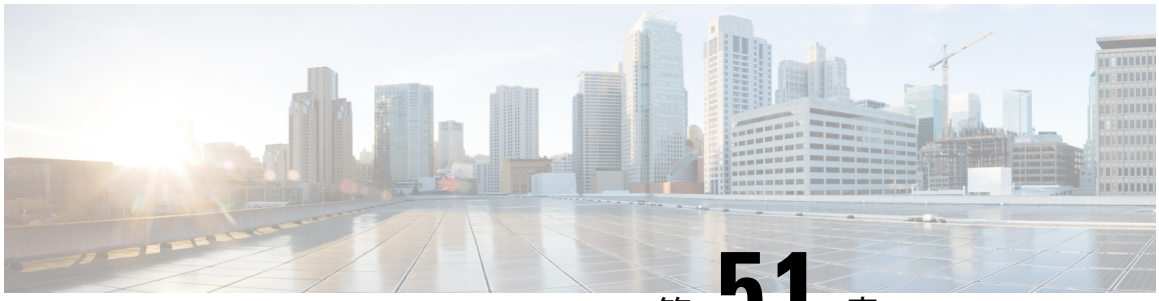
設定の変更	既存のコールおよび現在のフローへの影響	既存のコールおよび現在のフローへの影響	新規コールへの影響
既存の ruledef コンテキスト/新しいルールの追加	構成変更後、既存のフローにはルール照会は適用されません。TRM は既存のフローから切り離されません。これにより、進行中のフローの ruledef コンテンツが変更された場合に課金の問題が発生する可能性があります。	設定の変更が新しいフローに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、ruledef の変更が既存のコールの新しいフローに適用される。	設定の変更が新規コールに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、ruledef の変更が新規コールのフローに適用される。
ruledef なし	使用中のルールは削除できません。	使用中のルールは削除できません	使用中のルールは削除できません
新しい Group of Ruledefs/Changes から既存の Group of Ruledefs コンテンツ（Group of Ruledefs にルールを追加または削除）	構成変更後、既存のフローにはルール照会は適用されません。TRM は既存のフローから切り離されません。これにより、進行中のフローで Group of Ruledefs のコンテンツが変更された場合に、課金の問題が発生する可能性があります。	設定の変更が新しいフローに適用される。新しいフローの場合、あらゆる方向で新たにルール照合が発生し、Group of Ruledefs の変更が既存のコールの新しいフローに適用される。	設定の変更が新規コールに適用される。新しいフローの場合、いずれにしても、新しいコールでは新しいルールマッチングが実行され、Group of Ruledefs 変更がフローに適用されます。
Group of Ruledefs がない	使用中の Group of Ruledefs は削除できません	使用中の Group of Ruledefs は削除できません	使用中の Group of Ruledefs は削除できません
GoR にルールなし	フローは、ruledef 自体が削除されない限り、Group of Ruledefs で定義された ruledef と照会し続けます	新しいフローで新たにルール照合が行われ、設定の変更が有効になる。	新しいフローで新たにルール照合が行われ、設定の変更が有効になる。
アクションの優先順位の変更/アクションの優先順位の追加	進行中のフローでは TRM は解除されません。構成変更は既存のフローには適用されません。	設定の変更が新しいフローに適用される。	設定の変更が新規コールに適用される。

設定の変更	既存のコールおよび現在のフローへの影響	既存のコールおよび現在のフローへの影響	新規コールへの影響
アクションの優先順位なし	既存のフローへの影響なし	設定の変更が新しいフローに適用される。	設定の変更が新規コールに適用される。
rulebase パラメータの変更	一部のパラメータの変更は、既存のコールに適用されます	一部のパラメータの変更は、既存のコールに適用されます	構成変更が新規コールに適用されます
rulebase がない	rulebase はサポートされていません	rulebase はサポートされていません	rulebase はサポートされていません
APN なし	APN はサポートされていません	APN はサポートされていません	APN はサポートされていません
IP ソース違反	既存のコールへの影響なし	既存のコールへの影響なし	設定の変更が新規コールに適用される。

UPF のローカル構成サポートを構成する

次の CLI コマンドを使用して、ユーザープレーン機能（UPF）をローカルで構成します。

```
configure
  require upf
  end
```



第 51 章

N4/Sx インターフェイス経由の負荷と過負荷の制御

- 機能の概要と変更履歴 （601 ページ）
- 機能説明 （602 ページ）
- 負荷および過負荷制御の仕組み （603 ページ）
- N4 または Sx インターフェイスでの負荷および過負荷制御を有効にする （606 ページ）
- モニタリングおよびトラブルシューティング （610 ページ）

機能の概要と変更履歴

要約データ

該当製品または機能エリア	UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

表 *116 :* 機能の履歴

機能名	リリース情報	説明
N4/Sxインターフェイス経由の負荷と過負荷の制御	2024.04.1	この機能により、UPF は、負荷および過負荷制御メカニズムを有効にして、過負荷状態または自己保護状態の間メッセージを処理します。 導入されたコマンド： • **upf-load-control-profile** *profile_name* • **upf-overload-control-profile** *profile_name* • **associate { upf-load-control-profile** *profile_name* **| upf-overload-control-profile** *profile_name* **}** **デフォルト設定**：無効 - 有効にするには構成が必要です。
N4インターフェイス経由で負荷制御を報告する	2020.02.0	この機能により、UPF での負荷制御が可能になります。この機能により、UPF は、SMF に負荷情報を送信して、実効負荷に応じて、UPF 全体で PFCP セッション負荷のバランスを取ります。 **デフォルト設定**：無効 - 有効にするには構成が必要です。

機能説明

UPF には 3 つの 状態 があり、それぞれの任意の時点でのデフォルト値は次のとおりです。

- **負荷状態**：UPF の負荷が 70% 以下の場合。
- **過負荷状態**：UPF の負荷が 70 ～ 85% の場合。
- **自己保護状態**：UPF の負荷が 85 ～ 100% の場合。

（注） デフォルト値を構成できます。

負荷制御により、UPF は負荷情報を CP-F に送信し、実効負荷に応じて UPF 全体で PFCP セッションの負荷のバランスを取ることができます。負荷情報には、UPF のリソース操作状態が反映されます。負荷制御により、PFCP セッションの負荷をより適切に分散し、過負荷を防ぐことができます。

過負荷制御により、特定の UPF に対する新しいセッション要求のスロットリングが可能になります。過負荷状態および自己保護状態では、負荷が、設定されたしきい値を超えると、非優先セッションのセッション削除プロセスが開始されます。

注： UPF が高い負荷を報告した場合でも、過負荷緩和アクションはトリガーされません。

負荷および過負荷制御の仕組み

CP-F は、Sx Association 要求および応答メッセージでサポートされている負荷および過負荷機能を UPF に送信します。この情報に基づいて、UPF は負荷または、過負荷情報を CP-F ピアに送信するかを決定します。

CP-F での負荷または過負荷のサポートは、Sx サービスノード設定の一部として設定されます。この情報は、ダイナミック構成によって情報が変更された場合、Sx Association 応答または Sx Association Update 要求時に UP に送信されます。

UPF が過負荷状態の場合、OCI IE は削減メトリックとともにコントロールプレーン機能に送信されます。

（注）
- 負荷または過負荷制御機能が CP-F ノードで有効または無効になっている場合、CP-F ノードは UPF に対して Association Update 要求を開始し、更新されたサポートに通知します。
- 原因コード **PFCP_ENTITY_IN_CONGESTION** 原因が応答メッセージで受信された場合、UPF はアクションを実行しません。

負荷および過負荷係数の計算

負荷係数の計算

負荷係数は、任意の時点でのシステムの負荷合計を表します。CPU、メモリ、またはセッション数のいずれかが高い場合、UPF はロードされていると見なされます。したがって、負荷係数は、システム CPU、システムメモリ、セッション数などのシステムパラメータに基づいて計算されます。

過負荷係数の計算

負荷が、設定されているしきい値のいずれかを超える場合、UPF は過負荷と見なされます。自己保護モードでの過負荷係数の計算では、次のパラメータが考慮されます。

システムレベルのパラメータ：CPU、メモリ、セッション数

VPP：VPP CPU

CP-F への負荷および過負荷のレポート

UPF は、N4 メッセージ経由で CP-F に負荷または過負荷情報を送信します。

UPF が以下の場合...	以下を送信...
負荷状態	LCI IE
過負荷状態	OCI IE

CP-F は、LCI および OCI IE のすべての受信 N4 メッセージと N4 応答を解析します。SMF は、ピアノードから LCI IE または OCI IE を受信するたびに、その UPF ノードの負荷と過負荷のパラメータについて学習します。

CP-F ノードが、LCI IE と OCI IE をそれぞれ処理する方法の詳細については、次のガイドを参照してください。

- *UCC 5G* セッション管理機能構成およびアドミニストレーション ガイド、リリース *2024.04*.
- *UCC 5G cnSGWc* 構成およびアドミニストレーション ガイド、リリース *2024.04*

CP-F への負荷情報レポート

UPF は、負荷制御情報を送信して、ノードレベルでのリソースの動作状態を反映します。この情報により、CP-F はこの情報を使用して UPF selection 手順を強化できます。負荷制御情報は、負荷制御情報の交換で追加のシグナリングがトリガーされないように、PFCP 要求または応答メッセージでピギーバックされます。

Load Control Information IE は、UPF から CP-F に送信される以下のメッセージで表示されます。

- PFCP Session Establishment 応答
- PFCP Session Modification 応答
- PFCP Session Deletion 応答
- PFCP Session Report 要求

LCI IE の情報要素

負荷情報は、LCI IE に存在する次の要素を使用して報告されます。

- **負荷制御シーケンス番号**：この番号は、更新された負荷制御情報または新しい負荷制御情報が送信されると増分します。パラメータ **current-time** は、負荷制御シーケンス番号に使用されます。
- **Load Metric**：このパラメータは、UPF の現在の負荷レベルを示します。これは、0 ～ 100 の範囲のパーセンテージで送信されます。

（注）
- 複数の SessMgrs が、同じシーケンス番号を持つ Load Metric の同じ値を報告します。
- システムタイムスタンプはシーケンス番号として使用されます。

CP-F への過負荷情報レポート

UPF が過負荷状態の場合、N4/Sx メッセージで OCI IE を送信します。OCI IE は、次のメッセージに含まれている可能性があります。

- PFCP Session Establishment 応答
- PFCP Session Modification 応答
- PFCP Session Deletion 応答
- PFCP Session Report 要求

OCI IE の情報要素

過負荷情報は、OCI IE に存在する次の要素を使用して報告されます。

- **過負荷制御シーケンス番号**：この番号は、更新された過負荷制御情報または新しい負荷制御情報が送信されると増分します。パラメータ **current-time** は、過負荷制御シーケンス番号に使用されます。
- **過負荷削減メトリック**：自己保護モードでは、CP 機能は Sx Establishment 要求メッセージを UPF に向けてスロットリングします。メッセージは、報告された過負荷削減メトリック値に基づいてスロットリングされます。これは、0 ～ 100 の範囲のパーセンテージで送信されます。
- **Period of Validity**：このパラメータは、この パラメータは、OCI IE で指定された過負荷状態を有効と見なす期間を示します（後続の新しい過負荷制御情報によってオーバーライドされない場合）
- **Overload Control Information Flags**：このパラメータには、過負荷制御関連情報に関するフラグが含まれます。ビット 1 は、Associate OCI with Node ID（AOCI）を表します。このフラグは、OCI IE が PFCP Session Establishment 応答に含まれ、Cause IE が拒否原因値に設定されている場合、UP 機能によって「1」に設定されます。

自己保護モードでのセッションクリア

システムが自己保護モードにあり、システムの状態が低下し続けると、UPF でセッションのスロットリングが発生する可能性があります。

セッションレポートは、次の 2 つの方法で送信されます。

- EPFAR 機能がピアでサポートされているか、またはネゴシエートされている場合、UPF は、レポートタイプが「USAR」または「UISR」であるセッションの PFCP Session Report 要求メッセージを開始します。（PFCP の使用状況レポートがゼロ以外の場合）、または送信する使用状況レポートがない場合は UISR（UP Initiated Session Request）。
  - **USAR（使用状況レポート）**：PFCP の使用状況レポートがゼロ以外の場合。
  - **USIR（UP Initiated Session Request）**：送信する使用状況レポートがない場合。

  PFCP Session Report 要求の「原因」IE は、**PFCP_CAUSE_SELF_PROTECTION_TERMINATION (205)** に設定されます。Session Report 要求を送信後にセッションを削除します。
- EPFAR 機能がピアとネゴシエートされない場合、レポートタイプが「SPTER」のセッションに対して PFCP Session Report 要求メッセージを開始し、ピアがセッションの削除を正常に開始するのを待ちます。セッションの削除が 120 秒以内に開始されない場合、セッションはローカルで削除されます。

N4 または Sx インターフェイスでの負荷および過負荷制御を有効にする

次の手順を実行して、UPF で負荷と過負荷の制御を有効にします。

- 負荷制御プロファイルを構成する
- 過負荷制御プロファイルを構成する
- 負荷と過負荷制御プロファイルをユーザープレーンサービスと関連付ける

負荷制御プロファイルを構成する

負荷制御プロファイルを構成するには、次の手順を実行します。

手順

ステップ 1 **upf-load-control-profile** *dnn_profile_name* コマンドを使用して、グローバル構成モードで負荷制御プロファイルインスタンスを構成します。

例：

```
local]UPlane# config
[local]UPlane(config)# upf-load-control-profile loadcontrolprof
[local]UPlane(config-upf-load-control-profile)#
```

ステップ 2 コマンド **inclusion-frequency advertisement-interval** *interval_value* および **inclusion-frequency change-factor** *changefactor_value* を使用して、構成された負荷制御プロファイルでアドバタイズ間隔、変更係数、および有効期限を構成します。

例：

```
[local]UPlane(config-upf-load-control-profile)# inclusion-frequency advertisement-interval
 300
 [local]UPlane(config-upf-load-control-profile)# inclusion-frequency change-factor 5
```

パラメータ **inclusion-frequency** LCI IE が送信される周波数を指定します。LCI IE の送信では、次の 2 つの要因が考慮されます。

- パラメータ **advertisement-interval** は、LCI IE が送信される間隔です。デフォルト値は 300 秒です。
- パラメータ **change-factor** は、LCI IE が送信される時点における、前回の LCI 係数からの変化率（%）です。デフォルト値は 5% です。

ステップ 3 **end** コマンドを使用して現在の構成モードを終了します。

例：

```
[local]UPlane(config-upf-load-control-profile)# end
[local]UPlane# config#
```

過負制御プロファイルを構成する

過負制御プロファイルを構成するには、次の手順を実行します。

手順

ステップ 1 **upf-overload-control-profile** *dnn_profile_name* コマンドを使用して、グローバル構成モードで負荷制御プロファイルインスタンスを構成します。

例：

```
[local]UPlane# config
[local]UPlane(config)# upf-overload-control-profile ovrloadcontrolprof
[local]UPlane(config-upf-overload-control-profile)#
```

ステップ 2 過負荷制御プロファイルで過負荷しきい値パラメータ（システムレベルおよび VPP CPU）の下限と上限を設定します。

例：

```
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system cpu lower
limit 80 upper-limit 90
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system memory lower
 limit 70 upper-limit 80
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system session-count
 lower limit 80 upper-limit 90
[local]UPlane(config-upf-overload-control-profile)# overload-threshold vpp-cpu lower limit
 50 upper-limit 80
```

パラメータ **system** は、過負荷システムのしきい値を設定します。下限値を超えるとシステムは過負荷状態に移行し、上限値を超えると自己保護状態に移行します。システム状態は、システムレベルまたは VPP CPU パラメータのいずれかが原因で変化する可能性があります。

過負荷制御パラメータ	下限（過負荷制御状態）	上限（自己保護状態）
システム CPU	80	90
システム メモリ	70	80
システムセッションカウント	80	90
VPP CPU	50	80

（注） システムが自己保護状態になると、削減メトリックは 100% に設定されます。

ステップ 3 コマンド **inclusion-frequency advertisement-interval** *interval_value*、**inclusion-frequency change-factor** *changefactor_value*、**validity-period** *validity_period* を使用して、構成された負荷制御プロファイルでアドバタイズ間隔、変更係数、および有効期限を構成します。

例：

```
[local]UPlane(config-upf-overload-control-profile)# inclusion-frequency
advertisement-interval 300
[local]UPlane(config-upf-overload-control-profile)# inclusion-frequency change-factor 5
[local]UPlane(config-upf-overload-control-profile)# validity-period 300
```

パラメータ **inclusion-frequency** は、OCI IE が送信される周波数を指定します。OCI IE の送信では、次の 2 つの要因が考慮されます。

- パラメータ **advertisement-interval** は、OCI IE が送信される間隔です。デフォルト値は 300 秒です。
- パラメータ **change-factor** は、OCI IE が送信される以前の OCI 係数からの変更率です。デフォルト値は 5% です。
- パラメータ **validity-period** は、OCI 係数の有効性を示します。デフォルト値は 300 です。

ステップ 4 **end** コマンドを使用して現在の構成モードを終了します。

例：

```
[local]UPlane(config-upf-overload-control-profile)# end
[local]UPlane(config)#
```

負荷と過負荷制御プロファイルをユーザープレーンサービスと関連付ける

次の手順を実行して、負荷および過負荷制御プロファイルをユーザープレーンサービスに関連付けます。

始める前に

負荷と過負荷制御プロファイルをユーザープレーンサービスに関連付ける前に、次を構成する必要があります。

- 負荷制御プロファイル
- 過負荷制御プロファイル

手順

ステップ 1 コマンド **context** *context_name* を使用して、グローバル構成モードでコンテキストインスタンスを構成します。

例：

```
[local]UPlane# config
[local]UPlane (config)# context EPC
[EPC]UPlane (config-ctx)#
```

ステップ 2 コマンド **user-plane-service** *userplane_service_name* を使用して、構成されたコンテキストで User Plane Service インスタンスを構成します。

例：

```
[EPC]UPlane (config-ctx)# user-plane-service UPlane1
[EPC]UPlane (config-user-plane-service)#
```

ステップ 3 コマンド **load-control capacity** *session_value* を使用して、UPF でサポートされるセッションの最大数を構成します。

例：

```
[EPC]UPlane (config-user-plane-service)# load-control capacity 120000
[EPC]UPlane (config-user-plane-service)#
```

ステップ 4 コマンド **associate { upf-load-control-profile** *profile_name* **| upf-overload-control-profile** *profile_name* **}** を使用して、負荷と過負荷の制御プロファイルを構成されたユーザープレーンサービスと関連付けます。

例：

```
[EPC]UPlane (config-user-plane-service)# associate upf-load-control-profile
loadcontrolprof
[EPC]UPlane (config-user-plane-service)# associate upf-overload-control-profile
ovrloadcontrolprof
[EPC]UPlane (config-user-plane-service)#
```

ステップ 5 **end** コマンドを使用して現在の構成モードを終了します。

例：

```
[EPC]UPlane (config-user-plane-service)# end
[EPC]UPlane (config-ctx)#
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できるCLIコマンドについて説明します。

show コマンドと出力

この項では、この機能のサポートにおける show コマンドおよびコマンドの出力について説明します。

show upf-load-control-profile

show コマンド **show upf-load-control-profile [name** *name* **| all]** は、PDF の負荷制御プロファイルを表示します。

```
[local]qvpc-si# show upf-load-control-profile name lci1
UPF Load Control Profile
---------------------------------
lci1
```

```
[local]qvpc-si# show upf-load-control-profile full name lci1
UPF Load Control Profiles
---------------------------------
UPF Load Control Profile Name: lci1
 Inclusion Frequency:
   Change Factor                        : 6
   Advertisement Interval               : 300
```

show upf-overload-control-profile

show コマンド **show upf-overload-control-profile [name** *name* **| all]** は、PDF の過負荷制御プロファイルを表示します。

```
[local]qvpc-si# show upf-overload-control-profile name oci1
UPF Overload Control Profile
---------------------------------
oci1
```

```
[local]qvpc-si# show upf-overload-control-profile full name oci1
UPF Overload Control Profiles
```

```
---------------------------------

UPF Overload Control Profile Name: OC1
 System Thresholds:
   CPU Lower Limit           : 80
   CPU Upper Limit           : 90
   Memory Lower Limit        : 70
   Memory Upper Limit        : 80
   Session Count Lower Limit : 80
   Session Count Upper Limit : 90
 VPP Thresholds:
   CPU Lower Limit           : 50
   CPU Upper Limit           : 80
 Inclusion Frequency:
   Change Factor             : 5
   Advertisement Interval    : 300
 Validity Period             : 300
```

show user-plane-service statistics name

show コマンド **show user-plane-service statistics name** *service_name* は、付加および過負荷制御要素とその他の既存の統計を表示します。

```
[local]asr5000# show user-plane-service statistics name <user_plane_service_name>
  UPF Overload Stats:
    Current state                                                 :        Normal
    Overload mode count                                           :             0
    Self-protection mode count                                    :             0
    Last detected Overload state                                  :
0000:00:00:00:00:00
    Last detected Out-of Overload state                           :
0000:00:00:00:00:00
    Last reported (system) Overload Factor
      CPU                                                         :             0
      Memory                                                      :             0
      Session Capacity                                            :             0
    Last reported (VPP CPU) Overload Factor                       :             0
    Last reported Reduction Metric                                :             0

   Sessions Stats:
      Sx-Sessions removed in Self-protection mode                 :             0
      Non-Priority Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode               :             0
        Sx-Establishment reqs rejected in Self-protection mode    :             0
        Sx-Modification reqs rejected in Self-protection mode     :             0
      Unclassified Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode               :             0
        Sx-Establishment reqs rejected in Self-protection mode    :             0
        Sx-Modification reqs rejected in Self-protection mode     :             0
      IMS Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode               :             0
        Sx-Establishment reqs rejected in Self-protection mode    :             0
        Sx-Modification reqs rejected in Self-protection mode     :             0
        Sx-Establishment reqs allowed in Self-protection mode     :             0
        Sx-Modification reqs allowed in Self-protection mode      :             0
      WPS/Emergency Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode               :             0
        Sx-Establishment reqs rejected in Self-protection mode    :             0
        Sx-Modification reqs rejected in Self-protection mode     :             0
        Sx-Establishment reqs allowed in Self-protection mode     :             0
        Sx-Modification reqs allowed in Self-protection mode      :             0

    Data Stats:
```

```
    Overload Mode:
      WPS/Emergency new flows allowed                          :              0
      WPS/Emergency new flows dropped                          :              0
      Non WPS/Emergency new flows allowed                      :              0
      Non WPS/Emergency new flows dropped                      :              0
      Unclassified new flows dropped                           :              0
      Total Packets dropped                                    :              0
    Self-Protection Mode:
      WPS/Emergency new flows allowed                          :              0
      WPS/Emergency new flows dropped                          :              0
      Non WPS/Emergency new flows allowed                      :              0
      Non WPS/Emergency new flows dropped                      :              0
      Unclassified new flows dropped                           :              0
      Total Packets dropped                                    :              0

  UPF Load Stats:
    Current (system) Load Factor
      CPU                                                      :              0
      Memory                                                   :              0
      Session Capacity                                         :              0
    Last reported sequence number                              :              0
```

show user-plane-service statistics all

show コマンド **show user-plane-service statistics all** は、UPF の負荷と過負荷状態を表示します。

```
  UPF Overload Stats:
    Current state                                              :         Normal
    Overload mode count                                        :              0
    Self-protection mode count                                 :              0
    Last detected Overload state                               :
0000:00:00:00:00:00
    Last detected Out-of Overload state                        :
0000:00:00:00:00:00
    Last reported (system) Overload Factor
      CPU                                                      :              0
      Memory                                                   :              0
      Session Capacity                                         :              0
    Last reported (VPP CPU) Overload Factor                    :              0
    Last reported Reduction Metric                             :              0

   Sessions Stats:
      Sx-Sessions removed in Self-protection mode              :              0
      Non-Priority Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode            :              0
        Sx-Establishment reqs rejected in Self-protection mode :              0
        Sx-Modification reqs rejected in Self-protection mode  :              0
      Unclassified Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode            :              0
        Sx-Establishment reqs rejected in Self-protection mode :              0
        Sx-Modification reqs rejected in Self-protection mode  :              0
      IMS Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode            :              0
        Sx-Establishment reqs rejected in Self-protection mode :              0
        Sx-Modification reqs rejected in Self-protection mode  :              0
        Sx-Establishment reqs allowed in Self-protection mode  :              0
        Sx-Modification reqs allowed in Self-protection mode   :              0
      WPS/Emergency Sx Messages:
        Sx-Establishment reqs rcvd in Overload mode            :              0
        Sx-Establishment reqs rejected in Self-protection mode :              0
        Sx-Modification reqs rejected in Self-protection mode  :              0
        Sx-Establishment reqs allowed in Self-protection mode  :              0
        Sx-Modification reqs allowed in Self-protection mode   :              0
```

```
  Data Stats:
    Overload Mode:
      WPS/Emergency new flows allowed                          :          0
      WPS/Emergency new flows dropped                          :          0
      Non WPS/Emergency new flows allowed                      :          0
      Non WPS/Emergency new flows dropped                      :          0
      Unclassified new flows dropped                           :          0
      Total Packets dropped                                    :          0
    Self-Protection Mode:
      WPS/Emergency new flows allowed                          :          0
      WPS/Emergency new flows dropped                          :          0
      Non WPS/Emergency new flows allowed                      :          0
      Non WPS/Emergency new flows dropped                      :          0
      Unclassified new flows dropped                           :          0
      Total Packets dropped                                    :          0

UPF Load Stats:
  Current (system) Load Factor
    CPU                                                        :          0
    Memory                                                     :          0
    Session Capacity                                           :          0
  Last reported sequence number                                :          0
```

show user-plane-service name

show コマンド **show user-plane-service name** *service-name*は、特定のユーザープレーンサービスの負荷および過負荷制御プロファイル情報をその他の情報とともに表示します。

```
show user-plane-service name UPlane1

Service name                        : UPlane1
  Service-Id                        : 6
  Context                           : EPC
  Status                            : STARTED
  PGW Ingress GTPU Service          : pgwIngress
  UPF Ingress N3 GTPU Service       : Not defined
  UPF Ingress N9 GTPU Service       : Not defined
  UPF Ingress S5U GTPU Service      : Not defined
  UPF Ingress S8U GTPU Service      : Not defined
  UPF Ingress N9_S5U_S8U GTPU Service: Not defined
  UPF Egress GTPU Service           : Not defined
  SGW Ingress GTPU Service          : SGW1EGTPINGTPUIN
  SGW Egress GTPU Service           : SGW1EGTPOUTGTPUOUT
  Control Plane Tunnel GTPU Service : UP1SXU
  Sx Service                        : sx1
  Control Plane Group               : cp1
  Userplane Load Control Profile    : Not defined
  Userplane Overload Control Profile: Not defined
  Fast-Path service                 : Disabled
  NRF Management Service            : Not defined
  Nf-Instance-Id                    : Not defined
  Session Priority Profile          : Not defined
  Ise Server Profile                : Not defined
  UPF Load Control Profile          : ULCI1
  UPF Overload Control Profile      : UOCI1
```

show user-plane-service all

show コマンド **show user-plane-service all** は、ユーザープレーンサービスの負荷および過負荷制御プロファイル情報を他の情報とともに表示します。

```
show user-plane-service all

Service name                          : UPlane1
  Service-Id                          : 6
  Context                             : EPC
  Status                              : STARTED
  PGW Ingress GTPU Service            : pgwIngress
  UPF Ingress N3 GTPU Service         : Not defined
  UPF Ingress N9 GTPU Service         : Not defined
  UPF Ingress S5U GTPU Service        : Not defined
  UPF Ingress S8U GTPU Service        : Not defined
  UPF Ingress N9_S5U_S8U GTPU Service: Not defined
  UPF Egress GTPU Service             : Not defined
  SGW Ingress GTPU Service            : SGW1EGTPINGTPUIN
  SGW Egress GTPU Service             : SGW1EGTPOUTGTPUOUT
  Control Plane Tunnel GTPU Service : UP1SXU
  Sx Service                          : sx1
  Control Plane Group                 : cp1
  Userplane Load Control Profile      : Not defined
  Userplane Overload Control Profile: Not defined
  Fast-Path service                   : Disabled
  NRF Management Service              : Not defined
  Nf-Instance-Id                      : Not defined
  Session Priority Profile            : Not defined
  Ise Server Profile                  : Not defined
  UPF Load Control Profile            : ULCI1
  UPF Overload Control Profile        : UOCI1
```

show sx-service statistics all

show コマンド **show sx-service statistics all** は、セルフ保護状態で終了した、セッション管理メッセージを表示します。

```
show sx-service statistics all

Session Management Messages:
….
Session Report Request:
 Total TX:                          1   Total RX:                          0
 Initial TX:                        1   Initial RX:                        0
 Retrans TX:                        0   Retrans RX:                        0
 Discarded:                         0   No Rsp RX:                         0
 Causes:
  User Initiated Session Deletion from UP:                                 0
  Association Release initiated by UP:                                    0
  Recovery Failure:                                                       0
  IP Source Violation:                                                    0
  Self Protection Termination:                                            1
```

バルク統計情報

次の一括統計は、この機能の一環としてサポートされます。

変数名	データ型	キー	カウンタタイプ
%upf-num-overload-state-reached%	Int32	0	カウンター
%upf-num-self-protection-reached%	Int32	0	カウンター

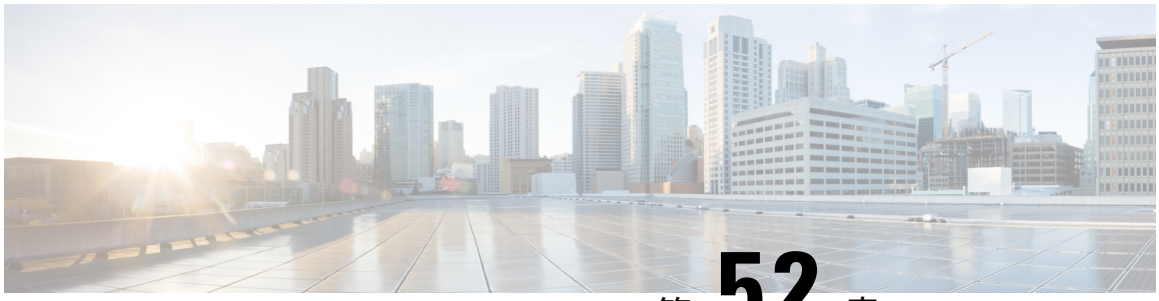
変数名	データ型	キー	カウンタタイプ
%upf-last-in-overload-state-timestamp%	Int32	0	情報
%upf-last-out-overload-state-timestamp%	Int32	0	情報
%upf-overload-reduction-metric%	Int32	0	情報
%upf-overload-factor-system-cpu%	Int32	0	情報
%upf-overload-factor-system-mem%	Int32	0	情報
%upf-overload-factor-system-sesscnt%	Int32	0	情報
%upf-overload-factor-vpp-cpu%	Int32	0	情報
%upf-load-factor-system-cpu%	Int32	0	情報
%upf-load-factor-system-mem%	Int32	0	情報
%upf-load-factor-system-sesscnt%	Int32	0	情報
%upf-load-factor-seq-num%	Int32	0	情報
%upf-num-sessions-removed-during-self-protection-mode%	Int32	0	情報
%upf-num-non-priority-session-estab-req-received-in-overload%	Int32	0	カウンター
%upf-num-non-priority-session-estab-req-reject-in-sp%	Int32	0	カウンター
%upf-num-non-priority-session-mod-req-reject-in-sp%	Int32	0	カウンター
%upf-num-unclassified-session-estab-req-received-in-overload%	Int32	0	カウンター
%upf-num-unclassified-session-estab-req-reject-in-sp%	Int32	0	カウンター
%upf-num-unclassified-session-mod-req-reject-in-sp%	Int32	0	カウンター
%upf-num-ims-session-estab-req-received-in-overload%	Int32	0	カウンター
%upf-num-ims-session-estab-req-reject-in-sp%	Int32	0	カウンター
%upf-num-ims-session-mod-req-reject-in-sp%	Int32	0	カウンター
%upf-num-ims-session-estab-req-allowed-in-sp%	Int32	0	カウンター
%upf-num-ims-session-mod-req-allowed-in-sp%	Int32	0	カウンター
%upf-num-wps-emer-session-estab-req-received-in-overload%	Int32	0	カウンター
%upf-num-wps-emer-session-estab-req-reject-in-sp%	Int32	0	カウンター

変数名	データ型	キー	カウンタタイプ
%upf-num-wps-emer-session-mod-req-reject-in-sp%	Int32	0	カウンター
%upf-num-wps-emer-session-estab-req-allowed-in-sp%	Int32	0	カウンター
%upf-num-wps-emer-session-mod-req-allowed-in-sp%	Int32	0	カウンター
%upf-num-wps-emer-new-flows-allowed-in-overload%	Int32	0	カウンター
%upf-num-wps-emer-new-flows-dropped-in-overload%	Int32	0	カウンター
%upf-num-non-wps-emer-new-flows-allowed-in-overload%	Int32	0	カウンター
%upf-num-non-wps-emer-new-flows-dropped-in-overload%	Int32	0	カウンター
%upf-num-unclassified-new-flows-dropped-in-overload%	Int32	0	カウンター
%upf-num-packets-dropped-in-overload%	Int32	0	カウンター
%upf-num-wps-emer-new-flows-allowed-in-self-protection%	Int32	0	カウンター
%upf-num-wps-emer-new-flows-dropped-in-self-protection%	Int32	0	カウンター
%upf-num-non-wps-emer-new-flows-allowed-in-self-protection%	Int32	0	カウンター
%upf-num-non-wps-emer-new-flows-dropped-in-self-protection%	Int32	0	カウンター
%upf-num-unclassified-new-flows-dropped-in-self-protection%	Int32	0	カウンター
%upf-num-packets-dropped-in-self-protection%	Int32	0	カウンター

SNMP トラップ

この機能をサポートするために、次の SNMP トラップが追加されました。

- **UPFOverloadState**：このトラップは、システムが過負荷状態になると生成されます。
- **UPFOverloadStateClear**：このトラップは、システムが過負荷状態から解放されると生成されます。
- **UPFSSelfProtectionMode**：このトラップは、システムが自己保護モードになると生成されます。
- **UPFSelfProtectionModeClear**：このトラップは、システムの自己保護モードが解除されたときに生成されます。



第 52 章

PCF 経由の使用状況の監視

- 機能の概要と変更履歴 （617 ページ）
- 機能説明 （618 ページ）

機能の概要と変更履歴

要約データ

表 *117*: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効、常時オン
このリリースでの関連する変更点：	N/A
関連資料	• *UCC 5G SMF* 構成およびアドミニストレーション ガイド • *UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2022.01.0

機能説明

UPF は、既存の N4 インターフェイスに対する使用状況モニタリング制御をサポートし、4G と 5G の両方のセッションに対して SMF の N7 インターフェイス経由で PCF から提供される使用量しきい値を報告します。UPF は Session Report 要求経由で使用量しきい値違反を SMF に報告し、SMF は PCF にデータを送信します。UPF は、usage monitoring パラメータの変更をサポートします。これには、合計ボリューム、アップリンクボリューム、ダウンリンクボリュームおよび、PCF から使用量監視しきい値または関連するトリガーを受信しなかったことに基づく、使用量監視の無効化が含まれます。

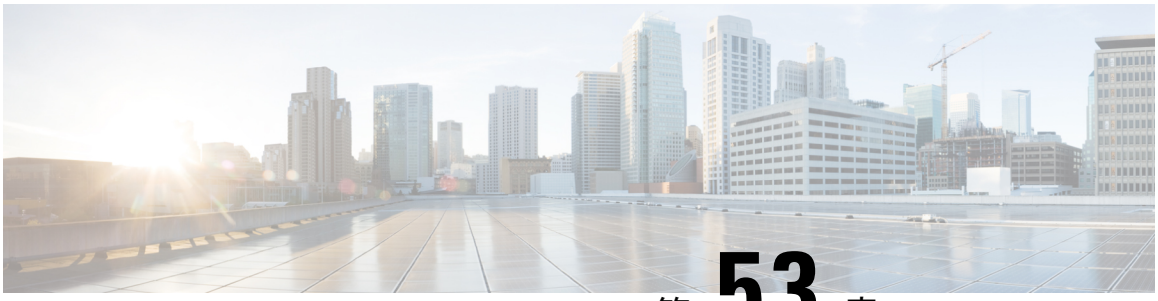
使用状況レポート

UPF は、PDU セッションまたは対応するサービス データ フローのすべてのトラフィックの量と使用時間を測定します。UPF は、PFCP セッション レポート要求または PFCP セッション変更応答のいずれかで累積使用レポートを SMF に送信します。SMF には、PCF に対する「accuUsageReports」属性に 1 つまたは複数の累計使用状況レポートを含めます。



（注） *PCF* 経由の使用状況監視機能は、SMF から有効になります。

注：SMF がこの機能を処理する方法の詳細については、『*UCC 5G SMF* 構成およびアドミニストレーション ガイド』の「ポリシーとユーザープレーンの管理」章 「*PCF* 経由の使用状況監視」項を参照してください。



第 53 章

CPU サイクルの可変解放

表 *118*：機能の履歴

機能名	リリース情報	説明
VRCC を使用した電源管理	2024.04.0	5G UPF の Variable Relinquishing of CPU Cycles（VRCC）機能は、通信の需要に基づいてパケット処理 システムの消費電力を削減するための動的 CPU 管理システムを導入しますこの機能により、CPU は通信が少ない期間にクロック周波数を減らし、省電力モードを実行できます。 この機能には有効なライセンスが必要であり、5G UPF の VPC-SI の VPP インスタンスでのみサポートされます。 **導入されたコマンド：グローバル構成モードの require power-saving vpp** **デフォルト設定**：無効：有効にするには設定が必要。

- VRCC の概要 （619 ページ）
- VRCC の仕組み （620 ページ）
- VRCC を構成する （621 ページ）

VRCC の概要

VPP について

5G UPF ネットワーク機能は、サードパーティのベクトルパケット処理（VPP）システムを使用して、ベクトルと呼ばれるバッチのパケットを処理します。UPF は、すべてのユーザープ

レーン機能と互換性を確保するために、VPP を使用して、超高速パケット転送と IP サービスおよびサードパーティ アプリケーションとの統合を実現します。

VRCC について

5G UPF の CPU サイクルの可変解放（VRCC）機能により、システムは通信の少ない期間に未使用の処理能力を解放できます。この機能により、UPF はパケット到着率に基づいて CPU サイクルを動的に管理できます。通信処理やユーザー体験に影響を与えることなく、最適なリソース使用率と電力効率を保証します。

VRCC でサポートされるプラットフォーム

VRCC 機能は、5G UPF の VPC-SI の VPP インスタンスでのみ動作します。

VRCC のライセンス要件

VRCC 機能を有効または無効にするには、ライセンスが必要です。

詳細については、シスコのアカウント担当者にお問い合わせください。

VRCC の利点

VRCC 機能には次の利点があります。

- エネルギー効率：通信量が少ない時間帯の消費電力を削減し、測定可能なエネルギーを節約できます。
- 環境への影響：ネットワーク運用に関する CO2 排出量を削減します。
- コスト削減：電力と冷却に関連するコストを削減します。
- 動的調整：リアルタイムの通信需要に基づいて CPU パフォーマンスを自動的に調整します。

VRCC の仕組み

VRCC は、各 VPP ワーカースレッド内で自己完結型であり、パケット処理エンジンのスケジューラと統合されます。VPP は、ポーリングモードドライバ（PMD）を実行し、インターフェイスの負荷に関係なく CPU を完全に使用します。

VRCC は VPP 使用率の移動平均を計算して通信負荷を測定し、短期間の CPU サイクルを定期的に停止します。このメカニズムにより、システムはスループット、遅延応答、システムの安定性、および電源管理のバランスをとることができます。

高通信と低通信を検出する

各 VPP スレッドのメインループスケジューラは、スリープ長を計算します。スリープ長は、受信ベクトルサイズの移動平均に反比例します。ベクトルサイズは、システムパフォーマンスを検出するための高通信と低通信を示します。

- 高通信：スリープ期間が短いか、スリープ期間がない場合、移動平均は大きくなります。この状態では、CPU はアクティブに維持されます。
- 低通信：スリープ期間が長いほど、移動平均は大きくなります。この状態では CPU のアクティビティが低下します。

省電力モードを有効にする

VRCC は、VPP の処理ループ内に短いスリープ期間を適用します。これらの期間中、CPU は処理を一時的に停止します。任意の短いスリープを適用することで、VPP ワーカースレッドは、CPU がクロック周波数をリアルタイムで動的に変更できるようにします。これは CPU ハードウェアを間接的にトリガーし、スリープの短時間のバーストに応答して省電力モードを実行します。

ネットワーク遅延への影響

実際のシナリオで予想されるラウンドトリップ遅延は、Ookla ベンチマークデータに従い、通常 40 ミリ秒以上です。

VRCC 機能が有効になっている場合、通常、ラボテストに基づいて、遅延がわずかに増加します（約 0.3 ~ 0.4 ミリ秒）。この増加は、実際の条件で予想される合計ラウンドトリップ遅延の約 1% ～ 2% にすぎません。

このような追加の遅延は、受信通信バーストを処理するために VPP が VRCC によって引き起こされたスリープから再開する必要があるために発生します。VPP がアクティブなままの場合、これらのスリープサイクルは発生せず、遅延は同じままです。ただし、VPP のアイドル中にバーストが到達すると、システムが完全な応答状態に戻るまで短時間の遅延が発生します。

VRCC を構成する

CPU ハードウェアを、VPP 省電力モードで実行するには、次のタスクを使用します。

始める前に

- デプロイメントに基づいて正しいコールモデルを実行していることを確認します。
- VRCC 機能を有効にするには、有効なライセンスが必要です。

手順

ステップ 1 **require power-saving vpp** CLI コマンドを使用して、省電力モードを有効にします。このコマンドはランタイム時に適用され、リロードは必要ありません。

例：

```
[local]host_name# configure
[local]host_name(config)# require power-saving vpp
[local]host_name(config)# exit
```

no require power-saving vpp CLI コマンドを使用して、省電力モードを無効にします。

ステップ 2 **show npumgr vpp vrcc** コマンドを使用して、VRCC が有効になっているかどうかを確認します。

（注） 非表示モードに入った後にのみ、**show npumgr vpp vrcc** CLI を設定できます。

例：

```
[local]host_name# show npumgr vpp vrcc
VPP VRCC : Enabled
```

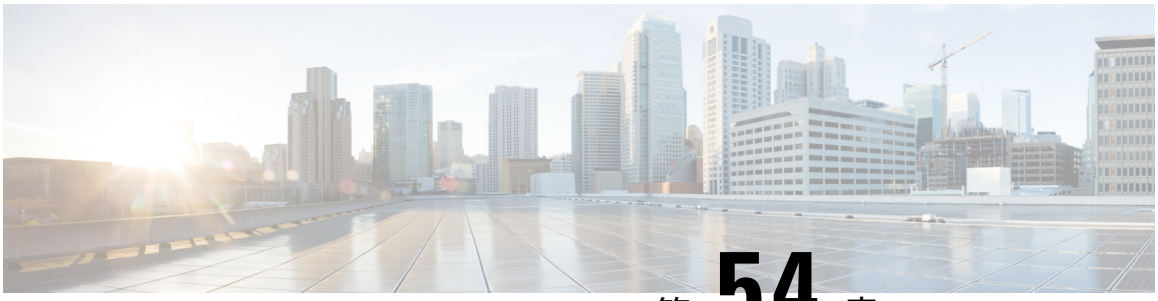
ステップ 3 ホスト CIMC で、[電力管理（Power Management）]または [電力モニタリング（Power Monitoring）] のタブを確認して、電力測定のグラフを表示します。CPU 電力ドメインの詳細を表示するには、グラフでコンポーネント CPU を参照してください。

次のコマンドを使用して CIMC CLI から電力モニタリングにアクセスできます。

例：

```
[server]# scope chassis
[server]# show power-monitoring detail
```

ステップ 4 システム KPI を確認し、システムのクラッシュや異常な動作をモニターします。また、通常のレジリエンシまたは冗長化タスクを実行します。



第 54 章

仮想ルーティングおよび転送

- 機能の概要と変更履歴, on page 623
- 更新履歴, on page 623
- 機能説明 （624 ページ）
- VRF の設定 （626 ページ）
- VRF を使用した VLAN セグメンテーション （629 ページ）
- モニタリングおよびトラブルシューティング （631 ページ）

機能の概要と変更履歴

更新履歴

Table 119: マニュアルの変更履歴

改訂の詳細	リリース
UPF は、プライベート APN/DNN に対して最大 200 の VRF をサポートします。	2023.02.0
UPFは、プライベート APN/DNN に対して最大 129 の VRFをサポートします。	2022.04.0
次の機能のサポートが追加されました。 • 重複するIP プール • SMF と UPF 間の必須の VRF 順序の削除	2021.01.0
最初の導入。	2020.02.0

機能説明

仮想ルーティングおよびフォワーディング（VRF）は、同じルータ上で同時に複数のインスタンスのルーティングテーブルを共存させるためのテクノロジーです。ルーティングインスタンスは独立しているため、VRF は、互いに競合することなく、同じ IP アドレスまたは重複する IP アドレスを使用できます。

（注） 2023.02.0 以降のリリースでは、UPF はプライベート APN または DNN に対して最大 200 の VRF をサポートします。

2023.02.0 より前のリリースでは、UPF はプライベート APN または DNN に対して最大 129 の VRF をサポートしていました。

UPF では、この機能により、IP アドレスプールと VRF とのアソシエーションが可能になります。このプールからのチャンクは、これらのプールを使用する UPF に割り当てられます。UPF で VFR が関連付けられたプールは、Static または Private の種類のいずれかです。

UPF を登録する際、PRIVATE VRF プールのチャンクは、通常のプライベートプールと同様に割り当てられます。Static VRF プールの場合、SMF は、構成中に UPF へのチャンク割り当てを行います。UPF 登録時に事前に割り当てられた静的チャンクに対して Sx-Route-Update メッセージが送信されます。

重複するIPプール

重複プールは、IP アドレス範囲を共有して、使用します。重複プールのタイプは、[静的（Static）] または [プライベート（Private）] のいずれかです。パブリックプールを重複プールとして設定することはできません。各重複プールは、異なる VRF（ルーティングドメイン）およびプールグループに属します。また、1 つの APN が使用できるプールグループは 1 つのみであるため、重複プールは異なる APN に属します。

この機能がない場合、重複プールは SMF で構成されます。ただし、2 つの重複プールからのチャンクを同じ UPF に送信することはできません。つまり、UPF は 2 つの異なる重複プールのチャンクを処理できません。同じ IP アドレス範囲には、同じ数の UPF および重複プールが必要です。

この機能がある場合、UPF は 2 つの異なる重複プールのチャンクを処理できます。つまり、単一の UPF が、同じ IP 範囲を共有する重複プールをいくつでも処理できます。

同じ UPF 内の重複プールの機能は次のとおりです。

- 特定のプールのチャンクが UPF にインストールされると、対応する vrf-name がチャンクとともに送信されます。
- UPF は、VRF 対応のチャンクであり、チャンクを対応する VRF にインストールします。チャンクデータベースは、VRF でデータが格納されます。

- コールの割り当て、リリース、リカバリなど VPNMgr へのあらゆる通信には、UPF の対応する SessMgr に vrf-id が含まれます。これにより、VPNMgr は、指定された vrf-id でその IP の正しいチャンクを選択して処理できます。

UE IP VRF は、N4 SESSION ESTABLISHMENT 要求メッセージの VRF 名をカプセル化するカスタム IE です。

UE IP VRF 情報要素

プライベート UE IP VRF の IE フォーマットを次に示します。

表 *120 : UE IP VRF* フォーマット

	ビット							
オクテット	8	7	6	5	4	3	2	1
1 ～ 2	タイプ = 242（10 進数）							
3 ～ 4	長さ = n							
5	Spare					同一 VRF フラグ	IPv6 VRF が有効	IPv4 VRF が有効
m ～ m+1	VRF-1 名の長さ = p							
m+1 ～ m+1+p	VRF-1 名							
n ～ n+1	VRF-2 名の長さ = q							
m+1 ～ m+1+q	VRF-2 名							

次の表に、[UE IP VRF] フィールドで使用可能な値を示します。

ケース	UE IP VRF	値（2 進数）		
		ビット 3	ビット 2	ビット 1
1	IPv4 および IPv6 UE IP アドレスは、VRF に関連付けられません。	0	0	0
2	IPv4 UE IP アドレスのみが、VRF に関連付けられます。	0	0	1
3	IPv6 UE IP アドレスのみが、VRF に関連付けられます。	0	1	0
4	IPv4 と IPv6 の両方の UE IP アドレスが、異なる VRF に関連付けられます。	0	1	1

5	IPv4 と IPv6 の両方の UE IP アドレスが、共通の VRFに関連付けられます。	1	1	1

識別子としての VRF 名

VRF に関連する SMF と UPF 間の通信は、vrf-id 経由で行われていました。これには、オペレータが SMF と UPF の両方ですべての VRF を同じ順序で構成する必要がありました。

この機能では、vrf-name が VRF に関連する SMF と UPF 間のすべての通信で識別子として使用されます。この機能により、UPF のすべての VRF の構成が削除されます。オペレータは、SMF と UPF で異なる順序で VRF を構成でき、両方のノードで同じ vrf-name で VRF を識別できます。

制限事項と制約事項

次に、UPF の既知の制限事項および制約事項を示します。

- UPF は、VRF ベースの重複プールのみをサポートします。UPF は、NH ベースや VLAN ベースのプールなどの重複プールをサポートしません。
- UPF は、同じ UPF グループ内に複数の UPF を持つ静的 IP プールでの PDN Type IPv4v6 ベースのコールを許可しません。
- UPF は、VRF の動的更新をサポートしません。

VRF の設定

UPF で VRF サポートを構成するには、次の手順を実行します。

SMF で：

1. APN または DNN プロファイルを作成します。
2. 重複する IP プールを作成し、コンテキストレベルでそれぞれの APN、DNN と VRF を関連付けます。
3. APN または DNN を UPF プロファイルに関連付けます。

次に、SMF の構成例を示します：

```
profile dnn intershat1
.
.
.
   upf apn mpls1.com
exit
profile dnn intershat2
.
.
.
```

```
   upf apn mpls2.com
exit
profile network-element upf upf1
.
.
.
   dnn-list [ intershat1 intershat2 ]
exit
profile network-element upf upf2
.
.
.
   dnn-list [ intershat1 intershat2 ]
exit
ipam
   source local
   address-pool pool-intershat1
      vrf-name mpls-vrf-1@isp
      tags
         dnn intershat1
      exit
      ipv4
         address-range 209.165.201.25 255.255.255.224
      exit
   exit
   address-pool pool-intershat2
      vrf-name mpls-vrf-2@isp
      tags
         dnn intershat2
      exit
      ipv4
         address-range 209.165.201.25 255.255.255.224
      exit
   exit
exit
```

UPF で：

SMF からチャンクがプッシュされる前に、UPF で VRF を構成しておくことを推奨します。構成されていない場合、IP プールトランザクション全体（VRF に属さないチャンクを含む）でエラーが発生する場合があります。SMF は、しばらくしてから再試行します。

次に、UPF の構成例を示します。

UPF 1：

```
config
  context EPC2
    sx-service sx
      instance-type userplane
      bind ipv4-address 209.165.201.11 ipv6-address bbbb:aaaa::4
    exit
    user-plane-service up
      associate gtpu-service pgw-gtpu pgw-ingress
      associate gtpu-service sgw-ingress-gtpu sgw-ingress
      associate gtpu-service sgw-engress-gtpu sgw-egress
      associate gtpu-service saegw-sxu cp-tunnel
      associate sx-service sx
      associate fast-path service
      associate control-plane-group g1
    exit

  context isp
    ip vrf mpls-vrf-1
```

```
    #exit
    ip vrf mpls-vrf-2
    #exit
    ip vrf mpls-vrf-1
        route-distinguisher 61601 11100001
        route-target export 61601 11100001
        route-target import 61606 11100001
        route-target import 65200 11100001
    #exit
    address-family ipv4 vrf mpls-vrf-1
        redistribute connected
        redistribute static
    #exit
    address-family ipv6 vrf mpls-vrf-1
        redistribute connected
        redistribute static
    #exit
    ip vrf mpls-vrf-2
        route-distinguisher 61601 11100002
        route-target export 61601 11100002
        route-target import 61606 11100002
        route-target import 65200 11100002
    #exit
    address-family ipv4 vrf mpls-vrf-2
        redistribute connected
        redistribute static
    #exit
    address-family ipv6 vrf mpls-vrf-2
        redistribute connected
        redistribute static
    #exit
    #exit
apn mpls1.com
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ip context-name isp
    exit
exit
control-plane-group g1
    peer-node-id ipv4-address 209.165.201.15
  #exit
  user-plane-group default
```

UPF 2：

```
config
  context EPC2
    sx-service sx
      instance-type userplane
      bind ipv4-address 209.165.201.12 ipv6-address bbbb:aaaa::5
    exit
    user-plane-service up
      associate gtpu-service pgw-gtpu pgw-ingress
      associate gtpu-service sgw-ingress-gtpu sgw-ingress
      associate gtpu-service sgw-engress-gtpu sgw-egress
      associate gtpu-service saegw-sxu cp-tunnel
      associate sx-service sx
      associate fast-path service
      associate control-plane-group g1
    exit
exit

  context isp
    ip vrf mpls-vrf-1
```

```
    #exit
    ip vrf mpls-vrf-2
    #exit
    apn mpls2.com
      pdp-type ipv4 ipv6
      bearer-control-mode mixed
      selection-mode sent-by-ms
      ip context-name isp
    exit
exit

control-plane-group g1
    peer-node-id ipv4-address 209.165.201.15
  #exit
  user-plane-group default
```

VRF を使用した VLAN セグメンテーション

表 *121 :* 機能の履歴

機能名	リリース情報	説明
仮想ルーティングと転送を使用した通信の VLAN セグメンテーションを有効にする	2024.01	UPF では、VRF を使用した VLAN セグメンテーションが許可されています。VRF は、確認します。 VLANに対して構成され、各VFRには、アップリンクパケットが送信されるデフォルトルートがあります。 **デフォルト設定** 無効：有効にするには構成が必要です。

機能説明

UPFは、仮想LAN（VLAN）を使用した企業通信のセグメント化をサポートしています。VLANは、1 つの物理 LAN セグメントをさらに小さな仮想ネットワークに分割し、ポートのグループ同士を、物理的に異なるセグメント上にあるかのように分離できるようにします。VLANセグメンテーションでは、異なるクラスに属するUEは、通信分離のために異なるVLANに割り当てられます。

VLAN セグメンテーションは、次の 2 つのメソッドを使用して実現できます。

1. Next Hop Forwarding
2. 仮想ルーティングおよび転送

UPFは、VRFを構成することにより、VLAN通信のセグメント化をサポートします。これは、VLAN ごとにデフォルトルートを使用して VRF を設定することで構成されるレイヤ 3 仮想化です。VRF デフォルトルートは、パケットの送信に使用されます。

VLAN セグメンテーションは、VLAN タグを SMF の IP プールに論理的にマッピングすることによって有効になります。UPF には、VRF に構成されたデフォルトルート経由で N6 インターフェイスでアップリンクパケットを転送する UPF に基づくマッピング構成が通知されます。

VRF を使用して VLAN セグメンテーションを有効にする

UPF で VRF を使用して VLAN セグメンテーションを有効にするには、次の構成を使用します。

```
config
  port ethernet slot/port
     no shutdown
     vlan vlan_tag_ID
     no shutdown
     bind interface interface_name context_name
     end
     context context_name
        ip vrf vrf_name
        { ip | ipv6 } address address subnetmask [ secondary ]
        end
```

注：

- **ip vrf** *vrf-name*：ルータに VRF を作成してVRF-ID を割り当てます。

設定例

次に、VRF を使用して VLAN セグメンテーションを有効にするための構成例を示します：

```
config
    port ethernet 1/10
       no shutdown
       vlan 400
         no shutdown
         bind interface N6_interface1 ISP
       #exit
       vlan 401
         no shutdown
         bind interface N6_interface2 ISP
       #exit
 context ISP
    ip vrf vrf1
    #exit
    ip vrf vrf2
    #exit
 interface N6_interface1
      ip vrf forwarding vrf1
      ip address 209.165.200.225 209.165.200.254
      ip address 209.165.201.1 209.165.200.254 secondary
      ipv6 address 2001:DB8::1/32 secondary
 interface N6_interface2
      ip vrf forwarding vrf2
      ip address 209.165.202.129 209.165.200.254
      ip address 209.165.201.30 209.165.200.254 secondary
      ipv6 address 2001:DB8:1::1/32 secondary
```

モニタリングおよびトラブルシューティング

この項では、機能のモニタリングと障害対応に使用できるCLIコマンドについて説明します。

showコマンドと出力

この項では、この機能のサポートにおけるshowコマンドおよびコマンドの出力について説明します。

show ip chunks

この CLI コマンドの出力には、そのコンテキストのすべてのチャンクが表示されます。

重複する IP プール機能を使用すると、**show ip chunks vrf** *vrf_name* CLI コマンドの出力には、その VRF のチャンクのみが表示されます。

- chunk-id
- chunk-size
- vrf-name
- start-addr
- end-addr
- used-addrs
- Peer Address

次に、出力例を示します。

```
==========================================
VRF Name: MPN00001
==========================================================================================================
|------------------------------|----------|------------|--------------|--------------|------------|
|          Peer Address          | chunk-id | chunk-size |   start-addr   |    end-addr
  | used-addrs |
|------------------------------|----------|------------|--------------|--------------|------------|
|                  192.10.25.23|1074790405|        8192|    36.40.128.0|  36.40.159.255|
          0|
|                  192.10.25.23|1074790406|        8192|    36.40.160.0|  36.40.191.255|
          0|
|------------------------------|----------|------------|--------------|--------------|------------|
```

show ipv6 chunks

この CLI コマンドの出力には、そのコンテキストのすべてのチャンクが表示されます。

重複する IP プール機能を使用すると、**show ipv6 chunks vrf** *vrf_name* CLI コマンドの出力は、その VRF にチャンクを表示します。

- chunk-id
- chunk-size

- vrf-name
- start-prefix
- end-prefix
- used-prefixes
- Peer Address

show ip bgp vpnv4

この CLI コマンドの出力には、すべての VPN ルーティング情報が表示されます。

重複する IP プール機能を使用すると、**show ip bgp vpnv4 vrf** *vrf_name* CLI コマンドは、その VRF に情報を表示します。

次に、出力例を示します。

```
VPNv4 Routing Table:
BGP table version is 1, local router ID is 172.31.35.36
Status Codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale,
 m Multipath
Origin Codes: i - IGP, e - EGP, ? - incomplete

Network              Next Hop             Metric LocPrf Weight Path
*>   0.0.0.0/0            172.31.35.29         0             0      65200 ?
*>   2.2.2.101/32         172.31.35.29         0             0      65200 ?
*>   2.2.3.2/32           0.0.0.0              0             32768  ?
*>   36.40.0.0/19         0.0.0.0              0             32768  ?
*>   36.40.32.0/19        0.0.0.0              0             32768  ?
*>   36.40.192.0/19       0.0.0.0              0             32768  ?

Total number of prefixes 6
```

show ip bgp vpnv6

この CLI コマンドの出力には、すべての VPN ルーティング情報が表示されます。

重複する IP プール機能を使用すると、**show ip bgp vpnv6 vrf** *vrf_name* CLI コマンドは、その VRF に情報を表示します。

次に、出力例を示します。

```
VPNv6 Routing Table:
BGP table version is 1, local router ID is 172.31.35.36
Status Codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale,
 m Multipath
Origin Codes: i - IGP, e - EGP, ? - incomplete

 Network              Next Hop             Metric LocPrf Weight Path
*>   0.0.0.0/0            172.31.35.29         0             0      65200 ?
*>   2036:adb0:40         172.31.35.29/51         0             32768  ?
*>   2036:adb0:40:2000    172.31.35.29/51           0             32768  ?
*>   2036:adb0:40:c000    172.31.35.29/51            0             32768  ?

Total number of prefixes 4
```

show mpls ilm

この CLI コマンドの出力には、FEC 情報を含む MPLS ILM テーブルが表示されます。

重複するIP プール機能を使用すると、**show mpls ilm** *fec verbose* and **show mpls ilm** *fec summary* CLI コマンドは、その VRF に情報を表示します。

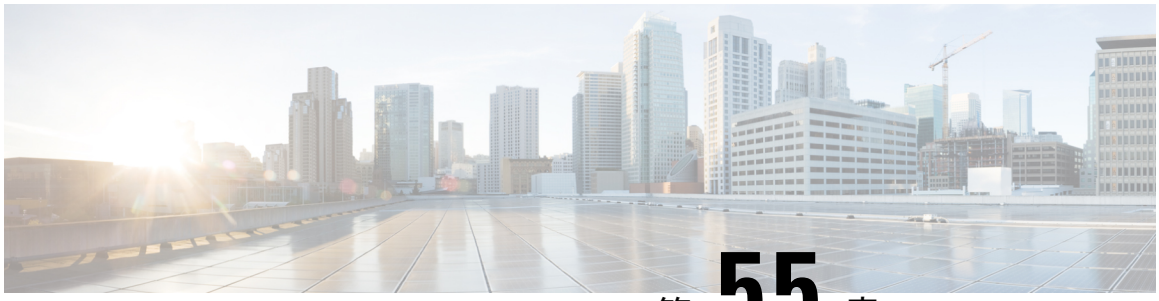
次に、カウントを表示する **show mpls ilm** *fec summary* CLI コマンドの出力例を示します。

```
Total ILM entries: 406
```

次に、詳細な MPLS ILM テーブルを表示する **show mpls ilm** *fec Verbose* CLI コマンドの出力例を示します。

```
In-segment entry with in label: 832, id: 99, in label-space: 0, row status: Active
Owner: BGP, # of pops: 1 XC Index:708
FEC: 36.40.0.0/19
FEC: 36.40.32.0/19
FEC: 36.40.192.0/19

In-segment entry with in label: 833, id: 100, in label-space: 0, row status: Active
Owner: BGP, # of pops: 1 XC Index:709
FEC: 2037:adb0:201::/51
FEC: 2037:adb0:201::/51
FEC: 2037:adb0:201::/51
```



第 55 章

音声の新しいラジオ

この章では、次のトピックについて取り上げます。

- 機能の概要と変更履歴, on page 635
- 機能説明, on page 636

機能の概要と変更履歴

要約データ

Table 122: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI SMI
機能のデフォルト設定	有効：常時オン
このリリースでの関連する変更点	N/A
関連資料	該当なし

更新履歴

Table 123: マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	2020.02.0

機能説明

UPF は、既存の Session Establishment および Modification 手順により、Voice over New Radio（VoNR）をサポートします。これらの手順では、SMF は、IMS シグナリング用の 5QI=5 Non-GBR フローの PDR と、音声通信用の 5QI=1 GBR フローの PDR を作成します。UPF では、モバイル発信またはモバイル受信のコールフローをサポートするために、特別な処理は必要ありません。

機能の仕組み

次は、IMS シグナリングの場合は 5QI 値 5、音声通信の場合は 5QI 値 1 を使用して PDR を作成するコールフローの手順です。

UPF の VoNR コールフロー

この項では、UPF での VoNR セッションとそれぞれの PDR 作成の手順について説明します。

***Figure 32: VoNR* コールフロー**

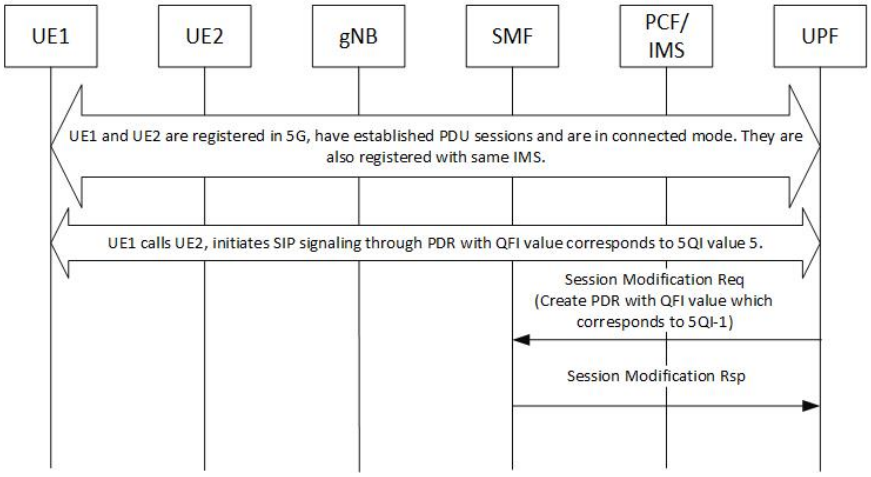
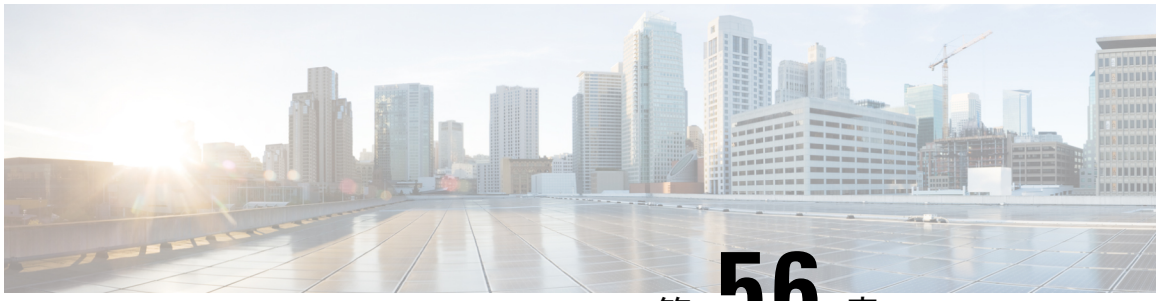


***Table 124: VoNR* コールフロー**

ステップ	説明
1	UE1 と UE2 は 5G ネットワークに登録されています。これれは、IMS PDU セッションを確立し、同じ IMS に登録されます。両方の UE は、接続モードになります。
2	IMS シグナリングの場合、非 GBR QoS PDR（UL および DL）は、5QI 値 5 に対応する QFI 値が設定されている SMF によって作成されます。
3	同様に、会話型音声通信の場合、GBR QoS フローの PDR は、5QI 値 1 に対応する QFI 値で作成されます。

ステップ	説明
4	QFI から 5QI へのマッピングは SMF によって維持されるため、QFI には 5QI と同じ値はありません。
5	上記の手順は、モバイル発信（MO）またはモバイル受信（MT）の両方のコールフローに有効です。
6	GBR または GBR 以外のフローに関する 5QI マッピングの他のタイプについては、「3GPP TS 23.501、5.7.4 項」を参照してください。



第 56 章

WPS 優先順位

表 *125 :* 機能の履歴

機能名	リリース情報	説明
UPF での WPS の優先順位	2023.04	Wireless Priority Services（WPS）機能を使用すると、複数のインターフェイスでの優先順位処理をより細かく制御できます。 UPF は、SMF によって示されるメッセージの優先順位に基づいて WPS サービスをサポートします。SMF で設定された優先順位の値は、PFCP ヘッダーの一部として N4 経由で UPF に送信されます。

- 機能説明 （639 ページ）
- 機能の仕組み （640 ページ）
- 過負荷シナリオでのメッセージの優先順位付け （643 ページ）
- WPS の優先順位を構成する （644 ページ）
- OAM のサポート （645 ページ）

機能説明

Wireless Priority Services（WPS）機能を使用すると、複数のインターフェイスでの優先順位処理をより細かく制御できます。UPF は、SMF が示すメッセージの優先順位に基づいて WPS をサポートします。

SMF で設定された優先順位の値は、PFCPヘッダーの一部として N4 経由で UPF に送信されます。SMF および cnSGWc からのメッセージの優先順位の値は、現在、Emergency（致命的）、VoLTE、および非 VoLTE IMS セッションでサポートされています。

（注） WPS は、UPF で N4（SMF）および Sxa（cnSGW）終端のみをサポートします。このリリースでは、WPS は Sxb（PGW-C）および Sxa（SGW-C）の終端をサポートしません。

RCM での WPS 優先順位のサポートについては、『*UCC 5G RCM* 構成およびアドミニストレーション ガイド』を参照してください。

SMF での WPS 優先順位のサポートについては、『*UCC 5G SMF* 構成およびアドミニストレーション ガイド』を参照してください。

機能の仕組み

この項では、UPF における WPS の優先順位の仕組みについて説明します。

優先的対応

session-priority-profile は、0 ～ 15 のセッション優先順位値を 1 ～ 4 の優先順位値にマップします。RCM やデータキュー配布などのモジュールで内部的に使用されます。

SRと ICSR

この機能が有効になっていない場合、N4/SX 経由で受信した有効な session-priority が設定されているセッションは、以前の設計に従ってSR/ICSR に対して優先されます。

この機能が有効になっている場合、Emergency セッションと WPS セッションのみが SR/ICSR に対して優先されるように変更されます。UPFのダウングレード中に、優先順位値はオフセット +1 で回復されます。

データキュー

次の表に、セッションの優先順位に基づくデータキューへの通信の分散を示します。

キュー #	詳細
3（最優先）	Sx 用に予約済み
2	優先順位 1、2 セッションに使用
1	優先順位 3、4 セッションに使用
0（最低の優先度）	データ/非優先セッションに使用されます

デフォルトの優先順位値は、次の場合に使用されます。

- session-type のみが構成され、session-priority については優先順位は定義されていない
- session-priority プロファイルで優先順位値が構成されていない

• WPS 機能が**デフォルト**の session-priority プロファイルで有効になっている

（注）
- この機能が無効になっている場合、UPF は N-1 サポートの優先順位を使用します。
- コンボコールのセッションリカバリでは、Sxa または N4 で受信した最も高い優先順位値が両方のセッションに使用されます。

セッションタイプにマッピングする

UPFは、N4経由で受信したセッション優先順位値（WPS、Emergency、およびIMS）を「associate session-priority-profile」 CLI構成を使用してセッションタイプにマッピングします。

VoLTE の非アクティブセッションの場合、マッピングは使用できません。VoLTE のアクティブセッションの場合、優先順位値「ims」が使用されますが、次の優先順位値（+1）は VoLTE の非アクティブセッションに暗黙的に使用されます。したがって、「ims+1」の優先順位は、session-priority プロファイルで構成されるべきではありません。

バージョンの互換性

1. RCM の最新バージョン (X) および UPF の以前のバージョン (X-1) の場合：
    1. 優先順位セットは、以前にサポートされていた優先順位のセット（1、2、3）に影響を与えることなく拡張されるため、RCM は以前の UPF バージョン (XN) をサポートします。
    2. スイッチオーバー時、フラッシュ シーケンスは、以前のバージョンではなく、UPF から受信した優先順位に完全に基づきます。
2. RCM の以前のバージョン (X-1) と UPF の最新バージョン (X) の場合：
    1. RCM は拡張された優先順位のセットをサポートせず、優先順位 4 で受信したチェックポイントはドロップされます。
    2. スイッチオーバー時に、優先順位 1、2、3 のコールを復元できます。

コントロールプレーンの互換性

WPS の優先順位を有効にするには、UPF を新しい構成にアップグレードします。次のシナリオでは、優先順位は保証されません。

- SMF/CP がアップグレードされていない
- 優先順位値が、N-1 サポートに基づいて送信される
- WPS の優先順位が UPF で有効になっている

コントロールプレーンから受信した優先順位値に基づき、次の組み合わせが機能します。

シリアル番号	SMF/cnSGW/PGW-C/SGW-C バージョン	UPF バージョン	UPF で有効になっている WPS の優先順位	UPF の動作
1	N-1 または 構成なしの N	N-1	N/A	WPS による優先順位なし：以前と同じ動作。
2	N-1 または 構成なしの N	N	いいえ	WPS による優先順位なし：以前と同じ動作。
3	N-1 または 構成なしの N	N	はい	セッションの優先順位は保証されません。
4	N（構成あり）	N-1	N/A	セッションの優先順位は保証されないため、これは推奨されません。優先順位が 3 の場合、RCM チェックポイントはドロップされます。
5	N（構成あり）	N	はい	WPS の優先順位が機能します。
6	N（構成あり）	N	いいえ	セッションの優先順位は保証されないため、これは推奨されません。

制限事項

WPS の優先順位機能には、次の制限があります。

- マルチ Sx/N4 シナリオでは、すべてのコントロールプレーンノードが同じプロセスを使用して MP 値を送信する必要があります。これは、同じ UPF で動作する SMF/cnSGW と PGW-C/SGW-C に適用されます。
- UPF ソフトウェアのアップグレード中に回復されたセッションは、優先順位の値を保持します。その結果、N-1 と N 間の UPF アップグレード後、既存のセッションの優先順位が期待どおりに機能せず、show CLI 出力が不確定になります。
- 既存の優先順位値を変更する SMF での構成変更、またはセッションタイプを変更する UPF での構成変更の場合、セッションタイプと優先順位は再評価されません。このような設定変更の結果として、誤った統計の更新が発生する可能性があります。

- セッション中の優先順位の変更により、一部の統計に一貫性がなくなる可能性があります。

過負荷シナリオでのメッセージの優先順位付け

表 *126 :* 機能の履歴

機能名	リリース情報	説明
過負荷シナリオでメッセージの優先順位を使用して PFCP メッセージを処理する	2024.04.1	この機能を使用すると、UPF は、メッセージ優先順位を使用して、過負荷シナリオまたは自己保護モード中でも、受信 PFCP メッセージを中断なく受信できるようにします。 メッセージの優先順位により、ネットワークオペレータは、WPS セッションの過負荷シナリオで PFCP メッセージをスロットリングする構成を使用してメッセージの優先順位を定義できます。 **拡張されたコマンド**：**session-priority-profile** *spp_name* **priority** *priority_value* **type { wps | emergency | ims } { throttle | precedence** *precedence_value* **}** **デフォルト設定**：無効-有効にするには構成が必要です。

PFCP メッセージのメッセージの優先順位

過負荷状態の場合、UPF はメッセージの優先順位を使用して受信 PFCP メッセージを処理します。UPF は、オペレータポリシーに基づいて、PFCP シグナリングでメッセージ優先順位ビットを受信します。UPF は、受信した要求メッセージのメッセージ優先度と同じメッセージ優先度を、送信するレスポンスメッセージに設定します。

UPF は、このメッセージの優先順位を構成で定義されているメッセージの優先順位と比較します。次に、UPF は、過負荷または自己保護モードでの構成に従って、スロットリングするか、スロットリングを免除します。

UPF は、優先順位の通信もスロットリングせずに要求された通信の削減を実現できない限り、優先順位の通信のスロットリングを免除します。デフォルトでは、UPF は優先順位 PFCP メッセージをスロットリングから免除します。ただし、構成で具体的に定義することで、優先順位 PFCP セッションをスロットリングできます。

優先順位 PFCP メッセージをスロットルするには、「セッション優先順位プロファイルをマッピング」 項を参照してください。

WPS の優先順位を構成する

この項では、WPS 優先順位機能の構成方法について説明します。

WPS の優先順位を有効にする

次の構成を使用して、WPS の優先順位サポートを有効または無効にし、session-priority-profile を user-plane-service に関連付けます。

```
config
  context context_name
    user-plane-service up_service_name
      [ no ] associate session-priority-profile { name | default } [
 name_string ]
      end
```

注：

- **associate session-priority-profile { name | default } [** *name_string* **]**：WPS の優先順位サポートを有効にします。
  - **name**：ユーザープレーンサービスに関連付けるセッションセッション優先順位プロファイルの名前を指定します。
  - **default**：セッション優先順位と関連付けるデフォルトの優先順位値を指定します。
  - *name-string* ：セッション優先順位に関連付ける名前文字列を指定します。
- **no associate session-priority-profile** ：WPS の優先順位サポートを無効にします。
- 特定の UPF では、合計 16 の session-priority-profile を構成できます。ユーザープレーンサービスに関連付けることができる session-priority-profile は 1 つだけです。
- セッションが N4/Sx メッセージ内のメッセージ優先順位を受信しない場合、「優先順位」の値が 0 に設定された「標準」セッションとして分類されます。
- session-priority-profile 構成で優先順位が指定されていない場合、セッションタイプは [未分類（Unclassified）] として表示され、default1 precedence 値を使用します。
- user-plane-service で session-priority-profile アソシエーションが無い場合、UPF は、既定の優先順位値が設定された既存の （N-1） 動作を使用します。これには、Emergency、IMS-VoLTE、IMS-nonVoLTE が含まれます。

セッション優先順位プロファイルをマッピングする

セッションタイプおよび優先順位の値を使用してセッション優先度の値を構成するには、次の構成を使用します。

```
config
   session-priority-profile spp_name
     priority priority_value type { wps | emergency | ims } [ throttle |
 precedence precedence_value ]
     end
```

注：

- **session-priority-profile**：セッション優先順位プロファイル名を指定します。
- **priority**：優先順位の値を、0 ～ 15 の範囲の整数で指定します。
- **type { wps | emergency | ims }**：セッションタイプを指定します
- **throttle**：過負荷/自己保護状態の優先順位セッションのフローの動作を定義します。優先順位が設定されていない場合、このキーワードのデフォルト値は、[有効（Enabled）] です。
- **precedence**：優先順位値を 1 ～ 4 の範囲の整数で指定します。
- セッション優先順位プロファイルには、**ims** に割り当てられた優先度の値の隣の値を構成しないでください。

OAM のサポート

show コマンドのサポート

ここでは、この機能をサポートする show コマンドとその出力について説明します。

show subscribers user-plane-only full all

この CLI コマンドの出力は、session-type 値を表示するように拡張されています。

次に、このコマンドの出力例を示します。

```
show subscribers user-plane-only full all | more

  Local SEID      : [0x0004000000000000] 1125899906842624
  Remote SEID     : [0x0004000000000002] 1125899906842626
  State           : Connected
  Connect Time    : Thu Jun  8 09:36:49 2023
Idle time       : 00h00m11s
  Access Type: uplane-ipv4              Network Type: IP
  user-plane-service-name: user-plane-service
  active-service-scheme-name:
  Callid: 00004e21
  Rulebase: prepaid
  Interface Type: Sxb
  eMPS Session: Yes
  eMPS Session Priority: 6
  Session-Type: wps
  Precedence-Order: 1
  Data Queue: 2
```

show user-plane-service all

このCLIコマンドの出力は、セッション優先順位プロファイル名を表示するように拡張されています。

次に、このコマンドの出力例を示します。

```
show user-plane-service all

Service name : user-plane-service
Service-Id : 7
Context : ingress
Status : STARTED
PGW Ingress GTPU Service : sx-gtpu-service
…
Nf-Instance-Id : Not defined
Session Priority Profile          : sp1
```

show user-plane-service session-priority-profile name | all

このCLIコマンドの出力には、セッション優先度プロファイル名と、各優先度のタイプおよび優先順位の値が表示されます。

次に、このコマンドの出力例を示します。

```
show user-plane-service session-priority-profile name spp1

  Session Priority Profile Name: spp1
  Priority     Type            Precedence
  ---------------------------------------
  0            unclassified    1
  1            wps             1
  2            unclassified    1
  3            emergency       2
  4            unclassified    2
  5            ims             3
  6            ims             3
  7            unclassified    2
  8            unclassified    3
  9            unclassified    3
  10           unclassified    3
  11           unclassified    3
  12           unclassified    4
  13           unclassified    4
  14           unclassified    4
  15           unclassified    4

Total session priority profile(s) found: 1
```

show user-plane-service statistics all

このコマンドの出力が強化され、WPSセッション数が表示されるようになりました。

次に、このコマンドの出力例を示します。

```
show user-plane-service statistics all
…
  eMPS PDNs Total:
    Active:                          0        Setup:                          0
    Released:                        0        Rejected:                       0

  WPS PDNs Total:
```

```
  Active:                          0        Setup:                          0
  Released:                        0        Rejected:                       0
```

show user-plane-service statistics session-priority-profile

このCLIコマンドの出力には、優先されたセッションと優先されていないセッションの数が表示されます。また、このコマンドは、「session-priority-profile」の「type」構成に基づいて優先されたセッションも表示します。

次に、このコマンドの出力例を示します。

```
show user-plane-service statistics session-priority-profile

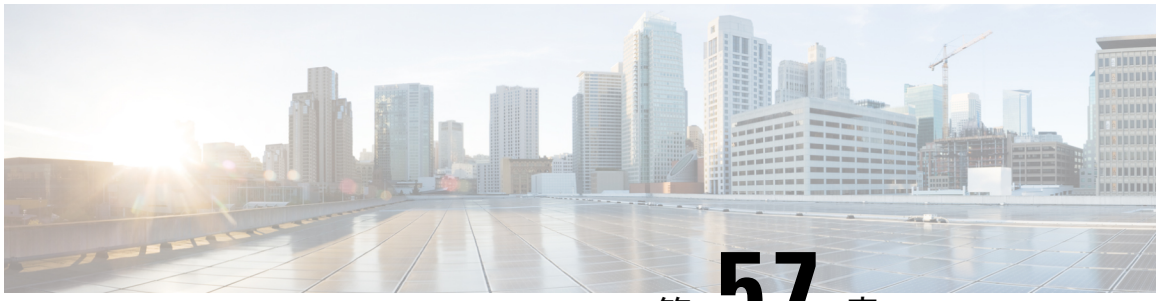
  Total Non-Prioritized (Normal) sessions: 0

  Total Prioritized sessions: 121
    WPS sessions             Total: 11           Active: 11
      Precedence             Config match        Default match
      ----------            --------------      ---------------
        1                               1                    0
        2                               0                   10
        3                               0                    0
        4                               0                    0

    Emergency sessions       Total: 110          Active: 110
      Precedence             Config match        Default match
      ----------            --------------      ---------------
        1                               0                   10
        2                               0                    0
        3                               0                  100
        4                               0                    0

    IMS sessions             Total: 0            Active: 0
      Precedence             Config match        Default match
      ----------            --------------      ---------------
        1                               0                    0
        2                               0                    0
        3                               0                    0
        4                               0                    0

    Unclassified sessions    Total: 0            Active: 0
      Precedence             Config match        Default match
      ----------            --------------      ---------------
        1                               0                    0
        2                               0                    0
        3                               0                    0
        4                               0                    0
```



第 57 章

X ヘッダーの挿入と暗号化

- 機能の概要と変更履歴 （649 ページ）
- 機能説明 （650 ページ）
- 機能の仕組み （650 ページ）
- X-Header の挿入と暗号化の設定 （652 ページ）
- X-Header の挿入および暗号化構成をモニタリングして障害対応する （654 ページ）
- アンチスプーフィングのサポート （654 ページ）

機能の概要と変更履歴

要約データ

表 *127*: 要約データ

該当製品または機能エリア	5G-UPF
該当プラットフォーム	VPC-SI
機能のデフォルト設定	無効：設定が必要
このリリースでの関連する変更点	N/A
関連資料	*UCC 5G UPF* 構成およびアドミニストレーション ガイド

マニュアルの変更履歴

改訂の詳細	リリース
X-Header エンリッチメントによるアンチスプーフィング機能のサポートを追加しました。	2023.02.0
最初の導入。	2020.02.x

機能説明

X-Header の挿入および X-Header 暗号化のプロセスは、総称してヘッダーエンリッチメント（HE）と呼ばれます。UPF は HE をサポートし、URL リクエストの HTTP ヘッダー内の既存の X-Header フィールドを削除および変更できます。

この機能により、HTTP、WSP GET および POST 要求パケットおよび、モバイルアドバタイズメントの挿入（MSISDN、IMSI、IP アドレス、ユーザーによるカスタマイズが可能、など）としてエンドアプリケーションが使用する HTTP 応答にヘッダーを追加できます。

機能の仕組み

HE には次の 2 つの動作が含まれます。

1. ヘッダーの挿入
2. ヘッダーの暗号化

X-Header の挿入

拡張ヘッダー（X-Header）フィールドは、ユーザーID、デバイスの検出などの特定の目的でプロトコルヘッダーに追加されるフィールドです。X-Header メカニズムでは、プロトコルを変更せずに追加の entity-header フィールドを定義できます。ただし、これらのフィールドは、受信者が認識できないものとします。

X-Header の挿入機能を使用すると、HTTP または WSP の GET および POST 要求パケットと HTTP 応答パケットに X-Header を挿入できます。HTTP または WSP 要求および HTTP 応答パケットに X-Header を挿入するようにルールを構成できます。ルールに関連付けられた課金アクションには、パケットに挿入される X-Header のリストが含まれます。

（注）

- パケットに X-Header が挿入されているフローはオフロードされません。
- X-Header 設定では、transmit order CLI に関係なく、すべての TCP OOO パケットがバッファされ、順序変更後に送信されます。

X-Header の暗号化

X-Header の暗号化により、挿入前に X-Header フィールドを暗号化できます。IP フローに対して（いずれかの X-Header フォーマットにより）すでに X-Header が挿入されていて、かつ現在の charging-action に [first-request-only] フラグが設定されている場合、そのフォーマットによる X-Header の挿入は行われません。charging-action に [first-request-only] フラグが設定されていな

い場合、該当する IP フローの他の適切なパケットでは、その X-Header フォーマットによる挿入が続行されます。

X-Headerのフォーマット構成を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された構成は、次の再暗号化時に、再暗号化タイムアウトが指定されている既存のコールに対して適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。



（注） この機能では、フローのリカバリはサポートされません。

制限事項

ここでは、現在のリリースに存在する制限について説明します。

- 応答パケットへの X-Header 挿入はサポートされません。
- RSA および RC4MD5 による X-Header の暗号化はサポートされていますが、AES による X-Header の暗号化はサポートされていません。
- X-Header のモニタープロトコルはサポートされていません。
- パケットでは、次の X-Header フィールドの挿入は、されていません。
  - QoS
  - UIDH
  - カスタマー ID
  - Hash Value
  - 時刻
  - RADIUS 文字列
  - Session-Id
  - 輻輳レベル
  - ユーザープロファイル
- HTTP ヘッダーの解析とバッファリングは、rulebase に明示的に delete-existing と設定されている x-header フィールドで構成された x-header フォーマットがある場合にのみ実行されます。x-header delete-existing を使用しないオペレータの場合、解析またはバッファリングによるオーバーヘッドは発生しません。

X-Header の挿入と暗号化の設定

X ヘッダーの挿入の設定

ステップ 1	X-Header を挿入する必要がある HTTP パケットを識別するための ruledef を作成または設定します。
ステップ 2	rulebase を作成または設定し、charging-action を設定します。これにより、HTTP パケットに X-headerフィールドが挿入されます。
ステップ 3 :	「*X-Header* フォーマットの作成」の説明に従って、X-Header フォーマットを作成します。
ステップ 4	「*X-Header* フォーマットを構成する」の説明に従って、課金アクションのメッセージタイプに基づいて、X-Header フォーマットを構成します。

X-Header フォーマットの作成

X-Header フォーマットを作成するには、次の構成を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
    end
```

X-Header フォーマットの設定

X-Header フォーマットを構成するには、次の構成を使用します。

```
configure
  active-charging service ecs_service_name
    xheader-format xheader_format_name
      insert xheader_field_name string-constant xheader_field_value | variable
 { bearer { 3gpp { apn | charging-characteristics | charging-id | imei
 | imsi | qos | rat-type | s-mcc-mnc | sgsn-address } | acr | customer-id
 | ggsn-address | mdn | msisdn-no-cc | radius-string |
radius-calling-station-id | session-id | sn-rulebase |
subscriber-ip-address | username } [ encrypt ] [ delete-existing ] |
http { host | url } }
       end
```

X ヘッダーの暗号化の設定

ステップ 1	「*X-Header* の挿入を構成」で説明されているように、X-Header の挿入を構成します。

ステップ 2	「*X-Header* の暗号化を構成」で説明されているように、rulebase を作成または構成し、使用する暗号化証明書と再暗号化パラメータを構成します。
ステップ 3	「暗号化証明書の設定」の説明に従って、使用する暗号化証明書を設定します。

X ヘッダーの暗号化の設定

X-Header の暗号化を構成するには、次の構成を使用します。

```
configure
   active-charging service ecs_service_name
     rulebase rulebase_name
        xheader-encryption certificate-name certificate_name
        xheader-encryption re-encryption period re-encryption_period
        end
```

注：

- この構成により、指定した rulebase に基づいて、すべてのサブスクライバに対して X-Header の暗号化が有効になります。
- 証明書が削除されても、ECS ではそのコピーが引き続き使用されます。証明書名がルールベースから削除されると、コピーは解放されます。
- X ヘッダーのフォーマット設定を変更しても、既存のコールの再暗号化はトリガーされません。ただし、新しいコールには変更された設定が適用されます。変更された設定は、次の再暗号化のときに、再暗号化のタイムアウトが指定されている既存のコールにも適用されます。データのフロー中にパラメータの暗号化が有効になった場合、暗号化された値が使用できなくなるため、そのパラメータの挿入は停止します。

暗号化証明書の設定

暗号化証明書を設定するには、次の設定を使用してください。

```
configure
   certificate name certificate_name pem { { data pem_certificate_data
private-key pem [ encrypted ] data pem_pvt_key } | { url url private-key
pem { [ encrypted ] data pem_pvt_key | url url } }
   end
```

X-Header の挿入と暗号化の構成を確認する

Exec モードで次のコマンドを入力して構成を確認します。

xheader-format *xheader_format_name*

X-Header の挿入および暗号化構成をモニタリングして障害対応する

show active-charging charging-action statistics name

このコマンドの出力には、X-Header の統計が表示されます。

- X-Header 情報：
  - 挿入された XHeader のバイト数
  - 挿入された XHeader のパケット数
  - XHeader によって消費される IP フラグメント数
  - 削除された XHeader のバイト数
  - 削除された XHeader のパケット数

show active-charging rulebase statistics name

このコマンドの出力には、ヘッダーエンリッチメントの統計が表示されます。

- HTTP ヘッダーのバッファリング制限到達

アンチスプーフィングのサポート

機能説明

UPF は、ヘッダーエンリッチメントを使用したスプーフィング検出と緩和をサポートしています。アンチスプーフィング機能により、オペレータとそのサブスクライバは、悪意のある UE デバイスによって引き起こされるスプーフィング脅威を阻止します。この機能は、外部ポータルがサブスクライバまたはコンテンツの承認に使用されている場合に、不正行為を検出します。

アンチスプーフィング機能は、HTTP 要求に対してのみサポートされます。この機能により、URL 要求の HTTP ヘッダー内の既存の X-Header フィールドを削除および変更できます。

ユーザー生成のヘッダー名が X-Header フォーマットで使用されているヘッダー名と類似している場合、X-Header フィールドを検索、削除、変更できます。X-Header フィールド名では、大文字と小文字が区別されません。たとえば、x-MSISDN フィールドと x-msisdn フィールドが、受信 HTTP 要求に存在する場合、両方のフィールドが処理されます。

user HTTP ヘッダーに、挿入するフィールドがすでにある場合、それらのフィールドに対応する値は、ヘッダーの最後の部分にあるゲートウェイからの変更された値に置き換えられます。

ヘッダーにすでに存在する 1 つのフィールドに複数のエントリがある場合、フィールドの 1 つのインスタンスがゲートウェイから挿入された値とともに選択されます。

HTTP GET 要求が複数ある場合、パケットヘッダーを、すべての GET 要求の X-header フィールドに置き換えます。暗号化が有効になっている場合は、X-Header の挿入後に実行されます。

制限事項

次に、アンチスプーフィング機能の既知の制限事項を示します。

- HTTP の GET または POST ヘッダーが、3 つのパケットで完了していない場合、アンチスプーフィングは、ヘッダーが完了する最後のパケットに対してのみ実行されます。それ以外の場合、パケットは HE なしで送信されます。
- フィールド名に「x-」を含まないフィールドは許可されますが、x- で始まらない拡張ヘッダーフィールドは削除されません。

X-Header でのアンチスプーフィングを有効にする

X-Header でアンチスプーフィングを有効にするには、次の設定を使用します。

```
configure
   active-charging service acs_service_name
      xheader-format xheader_format_name
         insert xheader_field_name variable { bearer subscriber-ip-address
} [ encrypt ] [ delete-existing ]
         exit
```

注：

- **delete-existing**：このコマンドは、X-Header ファイルのスプーフィングの検出を有効にします。
- この機能はデフォルトで無効に設定されています。
- 最大 10 の X-Header フィールドを設定するには、**delete-existing** CLI キーワードを使用します。このキーワードには、X-Header 挿入用に設定されたフィールドも含まれます。

OAM のサポート

この項では、アンチスプーフィング機能の show コマンドとそれらの出力に関する情報を示します。

show user-plane-service statistics charging-action [name | all]

このコマンドの出力には、課金アクションに関するユーザープレーン統計が表示されます。

- X-Header 情報：
  - 挿入された XHeader のバイト数

- 挿入された XHeader のパケット数
- 削除された XHeader のバイト数
- 削除された XHeader のパケット数

show user-plane-service statistics rulebase [name | all]

このコマンドの出力には、rulebase のユーザープレーン統計が表示されます。

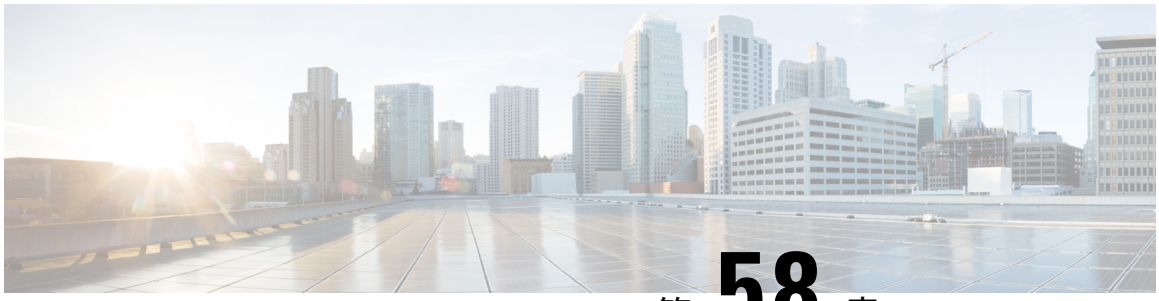
- ヘッダーの機能拡張統計
  - HTTP ヘッダーのバッファリング制限到達



第 II 部

モニタリングおよびトラブルシューティングの情報

- UPF 障害対応情報 （659 ページ）



第 58 章

UPF 障害対応情報

この章では、UPF 機能のモニタリングと障害対応に関連した次のトピックについて説明します。

- デバッグログ （659 ページ）
- 監視 CLI （660 ページ）
- 監視プロトコル （661 ページ）
- RAT タイプベースの統計 （661 ページ）
- サブスクライバレベルの CLI （666 ページ）
- VPP 統計 （674 ページ）
- SNMP サポート （678 ページ）
- UPF 機能の障害対応 （680 ページ）

デバッグログ



重要 debug logging CLIs は、システム管理者からのサポートを受けながら有効にする必要があります。debug logging CLI は、リソースを大量に消費します。

必要に応じて、次の debug CLI を使用します。

- **logg filter active facility sx level debug**
- **logg filter active facility user-data level debug**
- **logg filter active facility sessmgr level debug**
- **logg filter active facility uplane level debug**
- **logg filter active facility egtpc level debug**
- **logg filter active facility gtpu level debug**
- **logg filter active facility egtpu level debug**
- **logg filter active facility gtpumgr level debug**

- **logg filter active facility sxdemux level debug**
- **logg filter active facility user-l3tunnel level debug**
- **logg filter active facility aaamgr level debug**
- **logg filter active facility vpp level debug**
- **logg filter active facility dpath level debug**
- **logg active pdu-verbosity 5**
- **logg syslog** *ip_address* **facility** *facilities* **event-verbosity { min | concise | full }**

監視 CLI

サブスクライバレベルのメッセージ

サブスクライバレベルのメッセージには **mon sub callid** CLI コマンドを使用します。

リソースの追跡

show task resources facility *sessmgr* **all** CLI コマンドを使用して、PROCLET の CPU やメモリをトラックします。

サービスのステータス（**Service Status**）

show service all CLI コマンドを使用して、サービス状態を確認します。

Sx ピア状態

show sx peers CLI コマンドを使用して、Sx ピア状態を確認します。

この CLI の出力は、Sx ピアの自動構成作成、構成プッシュ開始時間、構成プッシュ終了時間を表示します。

```
[local]laas-si-setup# show sx peers wide
         ID                                                          Restart

|||||||  |                                        Recovery          |   Current   Max
     Peer   Config  Auto-Config  Config Push  Config Push
vvvvvvv  v    Group Name  Node ID      Peer ID     Timestamp        v  Sessions  Session
  State  Failures  Success    Start Time    End Time
------  ----  ----------- ---------   ---------  ------------------ ---- ------- -------
  ------  -------  --------    ----------   -----------
CAAXDXN  9    CPGROUP11   20.20.20.81  33554433 2025-05-14:05:36:46  0     0        0
    NONE     0         0           NA           NA
CAAXDXN  22   CPGROUP21   20.20.20.101 50331649 2025-05-14:05:36:45  0     0        0
    NONE     0         0           NA           NA

Total Peers:    2
```

監視プロトコル

monitor protocol コマンドを使用する際は、PFCP に対して オプション 49 を、GTP-U に対して オプション 26 を有効にします。

RAT タイプベースの統計

RAT タイプベースの統計機能により、ユーザーは UPF の RAT タイプによって分離されたデータ統計を表示できます。

UPF の RAT タイプベースのデータ統計では、個別のバケツが維持されます。これらのバケツは、セッション マネージャ インスタンス レベルで作成されます。バケツは、「Subscriber-Parameters」で受信した RAT Type IE に基づいて、コールセットアップ時にサブスクライバに割り当てられます。IE を受信しない場合は、そのサブスクライバに「不明な」RAT タイプバケツが割り当てられます。セッション中に、UPF がサブスクライバの新しい RAT タイプを受信すると、それに応じてバケツが変更されます。

重要　データ統計はチェックポインと指定されず、セッションリカバリ/ICSR 中に失われます。リカバリ後（コール監査時）に、「Current-Subscriber」統計のみが再計算されます。

show コマンドと出力

show user-plane-service statistics rat { 5g-nr | all | eutran | unknown | wlan } CLI コマンドは、UPF でノードレベルの RAT 統計を表示します。

注：

- **5g-nr**：5G NR サブスクライバのデータ統計を表示します。
- **all**：すべての RAT タイプのサブスクライバのデータ統計を表示します。
- **eutran**：EUTRAN サブスクライバのデータ統計を表示します。
- **unknown**：不明な RAT タイプのサブスクライバのデータ統計を表示します。
- **wlan**：WLAN サブスクライバのデータ統計を表示します。

統計

次の表は、各フィールドの説明を示しています。

表 128 : show user-plane-service statistics rat all

フィールド	説明
現在のサブスクライバ	

フィールド	説明
5G NR	現在の 5G NR サブスクライバの総数を指定します。
EUTRAN	現在の EUTRAN サブスクライバの総数を指定します。
WLAN	現在の WLAN サブスクライバの総数を指定します。
不明	不明な RAT タイプの現在のサブスクライバの総数を指定します。
データ統計	
5G NR	5G NR サブスクライバのデータ統計を指定します。
アップリンク	アップリンク方向の 5G NR サブスクライバのデータ統計を指定します。
パケットの総数	5G NR サブスクライバのアップリンクパケットの総数を指定します。
合計バイト数	5G NR サブスクライバのアップリンクバイトの総数を指定します。
ドロップされたパケットの総数	5G NR サブスクライバでドロップされたアップリンクパケットの総数を指定します。
合計廃棄バイト数	5G NR サブスクライバでドロップされたアップリンクバイトの総数を指定します。
ダウンリンク	ダウンリンク方向の 5G NR サブスクライバのデータ統計を指定します。
パケットの総数	5G NR サブスクライバのダウンリンクパケットの総数を指定します。
合計バイト数	5G NR サブスクライバのダウンリンクバイトの総数を指定します。
ドロップされたパケットの総数	5G NR サブスクライバでドロップされたダウンリンクパケットの総数を指定します。
合計廃棄バイト数	5G NR サブスクライバでドロップされたダウンリンクバイトの総数を指定します。
EUTRAN	EUTRAN サブスクライバのデータ統計を指定します。
アップリンク	アップリンク方向の EUTRAN サブスクライバのデータ統計を指定します。
パケットの総数	EUTRAN サブスクライバのアップリンクパケットの総数を指定します。
合計バイト数	EUTRAN サブスクライバのアップリンクバイトの総数を指定します。

フィールド	説明
ドロップされたパケットの総数	EUTRAN サブスクライバでドロップされたアップリンクパケットの総数を指定します。
合計廃棄バイト数	EUTRAN サブスクライバでドロップされたアップリンクバイトの総数を指定します。
ダウンリンク	ダウンリンク方向の EUTRAN サブスクライバのデータ統計を指定します。
パケットの総数	EUTRAN サブスクライバのダウンリンクパケットの総数を指定します。
合計バイト数	EUTRAN サブスクライバのダウンリンクバイトの総数を指定します。
ドロップされたパケットの総数	EUTRAN サブスクライバのダウンリンクパケットの総数を指定します。
合計廃棄バイト数	EUTRAN サブスクライバでドロップされたダウンリンクバイトの総数を指定します。
WLAN	WLAN サブスクライバのデータ統計を指定します。
アップリンク	アップリンク方向の WLAN サブスクライバのデータ統計を指定します。
パケットの総数	WLANサブスクライバのアップリンクパケットの総数を指定します。
合計バイト数	WLANサブスクライバのアップリンクバイトの総数を指定します。
ドロップされたパケットの総数	WLANサブスクライバでドロップされたアップリンクパケットの総数を指定します。
合計廃棄バイト数	WLANサブスクライバでドロップされたアップリンクバイトの総数を指定します。
ダウンリンク	ダウンリンク方向の WLAN サブスクライバのデータ統計を指定します。
パケットの総数	WLANサブスクライバのダウンリンクパケットの総数を指定します。
合計バイト数	WLANサブスクライバのダウンリンクバイトの総数を指定します。
ドロップされたパケットの総数	WLANサブスクライバのダウンリンクパケットの総数を指定します。
合計廃棄バイト数	WLANサブスクライバでドロップされったダウンリンクバイトの総数を指定します。

フィールド	説明
不明	不明な RAT タイプのサブスクライバのデータ統計を指定します。
アップリンク	アップリンク方向の不明な RAT タイプのサブスクライバのデータ統計を指定します。
パケットの総数	不明な RAT タイプのサブスクライバのアップリンクパケットの総数を指定します。
合計バイト数	不明な RAT タイプのサブスクライバのアップリンクバイトの総数を指定します。
ドロップされたパケットの総数	不明な RAT タイプのサブスクライバでドロップされたアップリンクパケットの総数を指定します。
合計廃棄バイト数	不明な RAT タイプのサブスクライバでドロップされたアップリンクバイトの総数を指定します。
ダウンリンク	ダウンリンク方向の不明な RAT タイプのサブスクライバのデータ統計を指定します。
パケットの総数	不明な RAT タイプのサブスクライバのダウンリンクパケットの総数を指定します。
合計バイト数	不明な RAT タイプのサブスクライバのダウンリンクバイトの総数を指定します。
ドロップされたパケットの総数	不明な RAT タイプのサブスクライバでドロップされたダウンリンクパケットの総数を指定します。
合計廃棄バイト数	不明な RAT タイプのサブスクライバでドロップされたダウンリンクバイトの総数を指定します。

バルク統計情報

RAT タイプベースのデータ統計イベントを追跡するために、次のバルク統計が User Plane Service スキーマに含まれています。

表 *129 : show bulkstats variables user-plane-service*

変数名	データ型	キー	カウンタタイプ
vpnname	文字列	1	情報
vpnid	Int32	1	情報
servname	文字列	1	情報
servid	Int32	1	情報
curr-pdn-rat-eutran	Int64	0	ゲージ

変数名	データ型	キー	カウンタタイプ
curr-pdn-rat-5g-nr	Int64	0	ゲージ
curr-pdn-rat-wlan	Int64	0	ゲージ
curr-pdn-rat-unknown	Int64	0	ゲージ
uplink-total-pkts-pdn-rat-eutran	Int64	0	カウンター
uplink-total-bytes-pdn-rat-eutran	Int64	0	カウンター
uplink-total-pkts-dropped-pdn-rat-eutran	Int64	0	カウンター
uplink-total-bytes-dropped-pdn-rat-eutran	Int64	0	カウンター
downlink-total-pkts-pdn-rat-eutran	Int64	0	カウンター
downlink-total-bytes-pdn-rat-eutran	Int64	0	カウンター
downlink-total-pkts-dropped-pdn-rat-eutran	Int64	0	カウンター
downlink-total-bytes-dropped-pdn-rat-eutran	Int64	0	カウンター
uplink-total-pkts-pdn-rat-5g-nr	Int64	0	カウンター
uplink-total-bytes-pdn-rat-5g-nr	Int64	0	カウンター
uplink-total-pkts-dropped-pdn-rat-5g-nr	Int64	0	カウンター
uplink-total-bytes-dropped-pdn-rat-5g-nr	Int64	0	カウンター
downlink-total-pkts-pdn-rat-5g-nr	Int64	0	カウンター
downlink-total-bytes-pdn-rat-5g-nr	Int64	0	カウンター
downlink-total-pkts-dropped-pdn-rat-5g-nr	Int64	0	カウンター
uplink-total-bytes-dropped-pdn-rat-5g-nr	Int64	0	カウンター
uplink-total-pkts-pdn-rat-wlan	Int64	0	カウンター
uplink-total-bytes-pdn-rat-wlan	Int64	0	カウンター
uplink-total-pkts-dropped-pdn-rat-wlan	Int64	0	カウンター
uplink-total-bytes-dropped-pdn-rat-wlan	Int64	0	カウンター
downlink-total-pkts-pdn-rat-wlan	Int64	0	カウンター
downlink-total-bytes-pdn-rat-wlan	Int64	0	カウンター
downlink-total-pkts-dropped-pdn-rat-wlan	Int64	0	カウンター

変数名	データ型	キー	カウンタタイプ
downlink-total-bytes-dropped-pdn-rat-wlan	Int64	0	カウンター
uplink-total-pkts-pdn-rat-unknown	Int64	0	カウンター
uplink-total-bytes-pdn-rat-unknown	Int64	0	カウンター
uplink-total-pkts-dropped-pdn-rat-unknown	Int64	0	カウンター
uplink-total-bytes-dropped-pdn-rat-unknown	Int64	0	カウンター
downlink-total-pkts-pdn-rat-unknown	Int64	0	カウンター
downlink-total-bytes-pdn-rat-unknown	Int64	0	カウンター
downlink-total-pkts-dropped-pdn-rat-unknown	Int64	0	カウンター
downlink-total-bytes-dropped-pdn-rat-unknown	Int64	0	カウンター

サブスクライバレベルの CLI

必要に応じて、次のサブスクライバレベルの CLI を使用します。

- **show subscribers user-plane-only full all**
- **show subscribers user-plane-only full msid** *msid_value*
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} pdr all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} far all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} qer all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} urr all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} bar all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} pdr full all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} urr full all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} far full all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} qer full all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} bar full all**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} pdr id** *id_value*
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} flows full**
- **show subscribers user-plane-only { seid** *seid_value* **| callid** *callid_value* **} bli full all**

show subscribers user-plane-only full msid *msid_value*

show subscribers user-plane-only full msid *msid_value* コマンドは、障害対応時のデータコレクション関連のユーザー情報をインスタンスレベルとセッションレベルで表示します。

次に、このコマンドの出力例を示します。

```
show subscribers user-plane-only full msid 404005123456789

  Local SEID      : [0x0004000000000000] 1125899906842624
  Remote SEID     : [0x0004000000000007] 1125899906842631
State           : Connected
  Connect Time    : Thu Sep 15 20:40:09 2022
  Idle time       : 00h11m25s
  Access Type: uplane-ipv4               Network Type: IP
  user-plane-service-name: UP21
  active-service-scheme-name:
  Callid: 00004e21
  Rulebase: cisco
  Interface Type: Sxb
  eMPS Session: No
  eMPS Session Priority: 0
  Card/Cpu: 1/0                          Sessmgr Instance: 1
  IP address: 11.11.12.0
  Next Hop Ip Address:
  Source context: EPC2-UP                Destination context: ISP1-UP
  PDN-Instance: starent.com
  User-plane-Sx-addr: 20.20.20.106
  Control-plane-Sx-addr: 20.20.20.101
  Number of associated PDRs : 0
  Number of associated ADC PDRs : 0
  Number of associated FARs : 0
  Number of associated QERs : 1
  Number of associated BARs : 0
  Number of associated URRs : 0
  Uplink APN AMBR (bps) : 200000       Downlink APN AMBR (bps) : 200000
  active input acl: IPV4ACL            active output acl: IPV4ACL
  active input ipv6 acl: n/a             active output ipv6 acl: n/a
  Bandwidth Policy: bw_policy1
  FW-and-NAT Policy: n/a
  FW-and-NAT Policy ID: n/a
  Firewall Policy IPv4: n/a
  Firewall Policy IPv6: n/a
  NAT Policy NAT44: n/a
  NAT Policy NAT64: n/a
  Converged Session: No                 Converged Peer Callid:      n/a
  Visited Call: No
  Subscriber Parameters:
  IMSI: 404005123456789
  IMEI: 112233445566778
  MSISDN: 9890098900
  Charging Characteristics: 0x3412
  Rat Type: 6
  MCC MNC: 123765
  SGSN Address: 20.20.20.61
  ULI: TAI=12546312ab00
  Congestion Level: 0
  GGSN Address: 20.20.20.101
  User-Name: 9890098900@starent.com
  Session-ID: 1414146500000008
  input pkts: 0                                    output pkts: 0
  input bytes: 0                                   output bytes: 0
  input bytes dropped: 0                           output bytes dropped: 0
```

```
  input pkts dropped: 0                          output pkts dropped: 0
  CF Buffered Uplink Packets: 0                  CF Buffered Downlink Packets: 0

  CF Buffered Uplink Bytes: 0                    CF Buffered Downlink Bytes: 0

  Uplink Packets in Buffer: 0                    Downlink Packets in Buffer: 0

  Buff Over-limit Uplink Pkts: 0                 Buff Over-limit Downlink Pkts: 0

  DDN buffered pkts : 0                          DDN buffered bytes : 0
  DDN buffer overflow drop pkts : 0              DDN buffer overflow drop bytes : 0

  pk rate from user(bps): 0                      pk rate to user(bps): 0
  ave rate from user(bps): 0                     ave rate to user(bps): 0
  sust rate from user(bps): 0                    sust rate to user(bps): 0
  pk rate from user(pps): 0                      pk rate to user(pps): 0
  ave rate from user(pps): 0                     ave rate to user(pps): 0
  sust rate from user(pps): 0                    sust rate to user(pps): 0
  ipv4 bad hdr: 0                                ipv4 ttl exceeded: 0
ipv4 fragments sent: 0                         ipv4 could not fragment: 0
  ipv4 bad length trim: 0
  input pkts dropped (0 mbr): 0                  output pkts dropped (0 mbr): 0

  ipv4 input acl drop: 0                         ipv4 output acl drop: 0
  ipv6 input acl drop: 0                         ipv6 output acl drop: 0
  ip source violations: 0                        ipv4 output no-flow drop: 0
  ipv6 bad hdr: 0                                ipv6 bad length trim: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Uplink Pkts Drop: 0                    APN AMBR Downlink Pkts Drop: 0

  APN AMBR Uplink Bytes Drop: 0                   APN AMBR Downlink Bytes Drop: 0

  APN AMBR Uplink Pkts IP pref lowered: 0        APN AMBR Downlink Pkts IP pref lowered:
 0
  APN AMBR Uplink Bytes IP pref lowered: 0        APN AMBR Downlink Bytes IP pref
lowered: 0
  ITC Uplink Pkts Drop: 0                        ITC Downlink Pkts Drop: 0
  ITC Uplink Bytes Drop: 0                       ITC Downlink Bytes Drop: 0
  ITC Uplink Pkts IP pref lowered: 0             ITC Downlink Pkts IP pref lowered: 0

  ITC Uplink Bytes IP pref lowered: 0            ITC Downlink Bytes IP pref lowered:
0
  ITC Terminated Flows:: 0                       ITC Redirected Flows: 0
  Flow Action Terminated Flows: 0                Flow Action Redirected Flows: 0

  ToS marked Uplink Pkts: 0                      ToS marked Downlink Pkts: 0
  CC Dropped Uplink Pkts: 0                      CC Dropped Downlink Pkts: 0
  CC Dropped Uplink bytes: 0                     CC Dropped Downlink Bytes: 0

  Uplink Inflight Pkts: 0                        Downlink Inflight Pkts: 0

  QFI Mismatch Uplink Pkts Drop: 0               QFI Mismatch Downlink Pkts Drop: 0

  Total QoS-Group(s) Active: 0
  DNS-to-EDNS Uplink Pkts: 0                    DNS-to-EDNS Uplink Bytes: 0
  EDNS Response Received: 0

  Flow information:
    Current Active Flows:
      TCP: 0
      UDP: 0
    Total Flows:
      TCP: 0
      UDP: 0
```

```
      FP:  0

Static & Predef Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

Dynamic Rule Match stats:
PDR Id   Rule Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits
Match-Bypassed  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------- -------------------- ---------- ---------- ---------- ---------- ----------
--------------  -------------------  ------------------

Post-Processing Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

Firewall-NAT Access Rule Match stats:
Firewall-Ruledef Name Pkts-Down Bytes-Down    Pkts-Up   Bytes-Up Dr-Pkts-Dn Dr-Byts-Dn
Dr-Pkts-Up Dr-Byts-Up       Hits
-------------------- ---------- ---------- ---------- ---------- ---------- ----------
---------- ---------- ----------

QoS-Group Statistics:
QGR Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

  CIoT APN Rate Control:
    Allowed UL Limit:   0                         Allowed DL limit:    0
    Remaining UL Limit: 0                         Remaining DL limit:  0
    Allowed Time unit: unrestricted               Status Validity Time: N/A


  Local SEID      : [0x0004000000000002] 1125899906842626
  Remote SEID     : [0x0004000000000009] 1125899906842633
  State           : Connected
  Connect Time    : Thu Sep 15 20:51:03 2022
Idle time       : 00h00m31s
  Access Type: uplane-ipv4              Network Type: IP
  user-plane-service-name: UP21
  active-service-scheme-name:
  Callid: 00004e23
  Rulebase: cisco
  Interface Type: Sxb
  eMPS Session: No
  eMPS Session Priority: 0
  Card/Cpu: 1/0                         Sessmgr Instance: 1
  IP address: 11.11.12.1
  Next Hop Ip Address:
  Source context: EPC2-UP               Destination context: ISP1-UP
  PDN-Instance: starent.com
  User-plane-Sx-addr: 20.20.20.106
  Control-plane-Sx-addr: 20.20.20.101
  Number of associated PDRs : 0
  Number of associated ADC PDRs : 0
  Number of associated FARs : 0
  Number of associated QERs : 1
  Number of associated BARs : 0
  Number of associated URRs : 0
```

```
  Uplink APN AMBR (bps) : 200000       Downlink APN AMBR (bps) : 200000
  active input acl: IPV4ACL            active output acl: IPV4ACL
  active input ipv6 acl: n/a             active output ipv6 acl: n/a
  Bandwidth Policy: bw_policy1
  FW-and-NAT Policy: n/a
  FW-and-NAT Policy ID: n/a
  Firewall Policy IPv4: n/a
  Firewall Policy IPv6: n/a
  NAT Policy NAT44: n/a
  NAT Policy NAT64: n/a
  Converged Session: No                 Converged Peer Callid:      n/a
  Visited Call: No
  Subscriber Parameters:
  IMSI: 404005123456789
  IMEI: 112233445566778
  MSISDN: 9890098900
  Charging Characteristics: 0x3412
  Rat Type: 6
  MCC MNC: 123765
  SGSN Address: 20.20.20.61
  ULI: TAI=12546312ab00
  Congestion Level: 0
  GGSN Address: 20.20.20.101
  User-Name: 9890098900@starent.com
  Session-ID: 141414650000000A
  input pkts: 0                                 output pkts: 0
  input bytes: 0                                output bytes: 0
  input bytes dropped: 0                        output bytes dropped: 0
  input pkts dropped: 0                         output pkts dropped: 0
  CF Buffered Uplink Packets: 0                 CF Buffered Downlink Packets: 0

  CF Buffered Uplink Bytes: 0                   CF Buffered Downlink Bytes: 0

  Uplink Packets in Buffer: 0                   Downlink Packets in Buffer: 0

  Buff Over-limit Uplink Pkts: 0                Buff Over-limit Downlink Pkts: 0

  DDN buffered pkts : 0                         DDN buffered bytes : 0
  DDN buffer overflow drop pkts : 0             DDN buffer overflow drop bytes : 0

  pk rate from user(bps): 0                     pk rate to user(bps): 0
  ave rate from user(bps): 0                    ave rate to user(bps): 0
  sust rate from user(bps): 0                   sust rate to user(bps): 0
  pk rate from user(pps): 0                     pk rate to user(pps): 0
  ave rate from user(pps): 0                    ave rate to user(pps): 0
  sust rate from user(pps): 0                   sust rate to user(pps): 0
  ipv4 bad hdr: 0                               ipv4 ttl exceeded: 0
  ipv4 fragments sent: 0                        ipv4 could not fragment: 0
  ipv4 bad length trim: 0
  input pkts dropped (0 mbr): 0                 output pkts dropped (0 mbr): 0

  ipv4 input acl drop: 0                        ipv4 output acl drop: 0
  ipv6 input acl drop: 0                        ipv6 output acl drop: 0
  ip source violations: 0                       ipv4 output no-flow drop: 0
  ipv6 bad hdr: 0                               ipv6 bad length trim: 0
  ipv4 icmp packets dropped: 0
  APN AMBR Uplink Pkts Drop: 0                   APN AMBR Downlink Pkts Drop: 0

  APN AMBR Uplink Bytes Drop: 0                  APN AMBR Downlink Bytes Drop: 0

  APN AMBR Uplink Pkts IP pref lowered: 0       APN AMBR Downlink Pkts IP pref lowered:
 0
  APN AMBR Uplink Bytes IP pref lowered: 0       APN AMBR Downlink Bytes IP pref
lowered: 0
```

```
  ITC Uplink Pkts Drop: 0                          ITC Downlink Pkts Drop: 0
  ITC Uplink Bytes Drop: 0                         ITC Downlink Bytes Drop: 0
  ITC Uplink Pkts IP pref lowered: 0               ITC Downlink Pkts IP pref lowered: 0

  ITC Uplink Bytes IP pref lowered: 0              ITC Downlink Bytes IP pref lowered:
0
  ITC Terminated Flows:: 0                         ITC Redirected Flows: 0
  Flow Action Terminated Flows: 0                  Flow Action Redirected Flows: 0

  ToS marked Uplink Pkts: 0                        ToS marked Downlink Pkts: 0
  CC Dropped Uplink Pkts: 0                        CC Dropped Downlink Pkts: 0
  CC Dropped Uplink bytes: 0                       CC Dropped Downlink Bytes: 0

  Uplink Inflight Pkts: 0                          Downlink Inflight Pkts: 0

  QFI Mismatch Uplink Pkts Drop: 0                 QFI Mismatch Downlink Pkts Drop: 0

  Total QoS-Group(s) Active: 0
  DNS-to-EDNS Uplink Pkts: 0                    DNS-to-EDNS Uplink Bytes: 0
  EDNS Response Received: 0

  Flow information:
    Current Active Flows:
      TCP: 0
      UDP: 0
    Total Flows:
      TCP: 0
      UDP: 0
      FP:  0

Static & Predef Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

Dynamic Rule Match stats:
PDR Id   Rule Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits
Match-Bypassed  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------- -------------------- ---------- ---------- ---------- ---------- ----------
--------------  -------------------  ------------------

Post-Processing Rule Match stats:
Rule Name           Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

Firewall-NAT Access Rule Match stats:
Firewall-Ruledef Name Pkts-Down Bytes-Down    Pkts-Up   Bytes-Up Dr-Pkts-Dn Dr-Byts-Dn
Dr-Pkts-Up Dr-Byts-Up       Hits
-------------------- ---------- ---------- ---------- ---------- ---------- ----------
---------- ---------- ----------

QoS-Group Statistics:
QGR Name            Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  ------------------

  CIoT APN Rate Control:
    Allowed UL Limit:   0                          Allowed DL limit:    0
    Remaining UL Limit: 0                          Remaining DL limit:  0
    Allowed Time unit: unrestricted                Status Validity Time: N/A
```

```
Total subscribers matching specified criteria: 1
```

show subscribers user-plane-only callid *callid-value* rule-match-info { [full] all | rulename *rulename*}

表 *130* : 機能の履歴

機能名	リリース情報	説明
単一のコマンドを使用して一致するルールに関連付けられた URR を特定する	2025.01.0	このリリースでは、UP の統合コマンドが導入され、次のようなサブスクライバごとの詳細の包括的な概要が提供されます。 • 一致したルールと関連する課金アクション • 関連付けられた URR-ID この拡張機能により、サブスクライバごとにこの情報を抽出して関連付けるために、UP または UP と CP 全体で複数のコマンドを使用する必要がなくなります。 **導入されたコマンド**：**show subscribers user-plane-only callid** *callid* **rule-match-info { [full] all | rulename** *rulename* **}**。 **デフォルト設定**：デフォルトで有効。

show subscribers user-plane-only callid *callid* **rule-match-info { [full] all | rulename** *rulename* **}**コマンドは、一致するルール、関連する charging-action および 関連する URR-ID を表示します。

（注）
- このコマンドは、統計と一致する静的ルール、事前定義ルールおよびダイナミックルールを表示します。後処理、ファイアウォール、その他の ruledef は表示されません。
- URR-ID に対応する情報のしきい値、およびクォータは、**show subscribers user-plane-only callid urr** *urr-ID* コマンドを使用して、取得されます。
- コマンドに表示されている URR-ID は、現在 **show subscribers user-plane-only callid** *callid* **urr full all** の出力には表示されていばい場合があります。ただし、URR-ID は最終的に入力されます。
- **rulename** フィルタを使用してこのコマンドを実行すると、CPU の負荷が大きくなる場合があります。
- リカバリ後、パケットカウントが失われると、rule-match 統計は回復しませんが、URR 詳細は回復します。

次に、**show subscribers user-plane-only callid 00004e22 rule-match-info full all** コマンドの出力例を示します。

```
[local]host_name# show subscribers user-plane-only callid 00004e22 rule-match-info full
 all
STATIC & PREDEF RULE MATCH INFORMATION:

        RULEDEF NAME: catchall
        Charging-Action name: catchall

        Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
        ---------- ---------- ---------- ---------- ---------- --------------
-------------------  ------------------
                1         40          2         80          5              0
0/0             0/0

        RULEDEF NAME: httpAnyMatch
        Charging-Action name: catchall

        Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
        ---------- ---------- ---------- ---------- ---------- --------------
-------------------  ------------------
                2        716          3        205          5              0
0/0             0/0


        URR-id: 0x80000131

         URR-id: 0x80000137

DYNAMIC RULE MATCH INFORMATION:

        RULEDEF NAME: dynamic5

        PDR Id   Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
 FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
```

```
        -------- --------   ---------- ---------- ---------- -------    ----------
 ---------------       --------------------
        0x0003            0          0          5        285          6               0
         0/0               0/0
        0x0004            3        756          0          0          4               0
         0/0               0/0

        Outer header removal:   GTP-U/UDP/IPv4
        Application ID:         N/A
        Associated FARID:       0x0003
         Destination Interface: Core
         Apply Action:          FORWARD
         Outer Header Creation:
         Remote TEID:           0x0
          Transport Level Marking:         N/A
          Transport Level Marking Options:
            Copy Inner:                    No
            Copy Outer:                    No
          Inner Packet Marking:            N/A

        Outer header removal:
        Application ID:         N/A
        Associated FARID:       0x0004
         Destination Interface: Access
         Apply Action:          FORWARD
         Outer Header Creation: GTP-U/UDP/IPv4
         Remote TEID:           0x60010f20
          Transport Level Marking:         N/A
          Transport Level Marking Options:
            Copy Inner:                    No
            Copy Outer:                    No
          Inner Packet Marking:            N/A

        URR-id: 0x00000007

Total subscribers matching specified criteria: 1
```

VPP 統計

フローが、VPP にオフロードされているか判断するには、次の CLI コマンドの出力で fastpath 統計を確認します。

- **show user-plane-service statistics all**
- **show user-plane-service statistics analyzer name ip [verbose]**
- **show user-plane-service statistics analyzer name ipv6 [verbose]**
- **show user-plane-service statistics analyzer name tcp [verbose]**
- **show user-plane-service statistics analyzer name udp [verbose]**
- **show user-plane-service statistics analyzer name http [verbose]**
- **show user-plane-service statistics analyzer name rtp [verbose]**
- **show user-plane-service statistics analyzer name ftp [verbose]**

```
show user-plane-service statistics analyzer name ftp verbose
```

```
Wednesday July 02 17:47:13 IST 2025
   FTP Session Stats:
      Current Control Sessions:         0         Current Data Sessions:          0
      Total Control Sessions:           0         Total Data Sessions:            1
      Uplink Control Bytes:             0         Downlink Control Bytes:         0
      Uplink Control Pkts:              0         Downlink Control Pkts:          0
      Uplink Data Bytes:              219         Downlink Data Bytes:         3249
      Uplink Data Pkts:                 6         Downlink Data Pkts:             9
      Uplink Error Bytes:               0         Downlink Error Bytes:           0
      Uplink Error Pkts:                0         Downlink Error Pkts:            0
      Request Succeed:                  0         Request Failed:                 0
      Unknown Requests:                 0         Unknown Responses:              0
      Uplink Bytes Retrans:             0         Downlink Bytes Retrans:         0
      Uplink Pkts Retrans:              0         Downlink Pkts Retrans:          0
      RETR commands:                    0         STOR commands:                  0
      Unknown packets received:                                                   0
      Data packet received without control connection:                           11
      Invalid packets:                                                            0
      Packets that could not be parsed:
```

- **show subscribers user-plane-only full callid** *call_id*
- **show subscribers user-plane-only callid** *callid_value* **drop-statistics**
- **show user-plane-service statistics drop-counter**
- **show subscribers user-plane-only callid** *callid_value* **flows full**
- **show subscribers user-plane-only callid** *callid-value* **flows flow-id** *flow-id*

show subscribers user-plane-only callid *callid_value* drop-statistics

show subscribers user-plane-only callid *callid-value* **drop-statistics** コマンドは、インスタンスレベルおよびセッションレベルでそれぞれの原因（ドロップ理由）とともにパケットドロップ統計を表示します。

次に、このコマンドの出力例を示します。

```
[local]UPF1# show subscribers user-plane-only callid 00004e21 drop-statistics

        Callid: 00004e21
        Interface Type: <interface-type>

        Packet Drop Data Statistics:
        ----------------------------------------------------
        NAT packets processing failure
           NAT on demand handling:                  0
           ICMP Packet translation:                 0
        FIREWALL packets processing failure
           Policy not found:                        0
        No Matching GX rule found:                  0
        Flow apply action
           Discard:                                 0
           Readdress Failure:                       0
           Packet exceeds the MTU size:                 0
      Failure in processing FAR Buffer packets:     0
      FAR Apply Action Drop:                        0
      Traffic Steering Failure:                     0
      QER Gate Status Closed:                       0
      Content-filtering Discard Action:             0
      IP Header Validation Failed:                  0
```

```
        ADF level failure
            DL TFT mismatch:                        0
        URL Blacklisting Discard Action:            0
        QGR Flow Action SGQ Discard:                0
        QGR Policer Drops:                          0

Total subscribers matching specified criteria: 1
[local]UPF1#
```

show user-plane-service statistics drop-counter

show user-plane-service statistics drop-counter コマンドは、各原因（ドロップ理由）に合わせて、インスタンスレベルまたはセッションレベルでパケットドロップ統計を表示します

次に、このコマンドの出力例を示します。

```
[local]UPF1# show user-plane-service statistics drop-counter

         Packet Drop Data Statistics:
         ------------------------------------------------------
         NAT packets processing failure
            NAT on demand handling:                     0
            IP allocation is in progress:               0
            ICMP Packet translation:                    0
         FIREWALL packets processing failure
            Policy not found:                           0
         No Matching GX rule found:                     0
         Flow apply action
            Discard:                                    0
            Readdress Failure:                          0
            Redirect-URL:                               0
         Packet exceeds the MTU size:                   0
         Failure in processing FAR Buffer packets:      0
         FAR Apply Action Drop:                         0
         Traffic Steering Failure:                      0
         QER Gate Status Closed:                        0
         Content-filtering Discard Action:              0
         IP Header Validation Failed:                   0
         ADF level failure
           UL TEID/QFI key mismatch:                    0
           DL TFT mismatch:                             0
           DL QFI mismatch:                             0
         URL Blacklisting Discard Action:               0
         DDN buffer overflow drop packets:              0
         APN AMBR Packets Drop:                         0
         ITC Packets Drop:                              0
         ACL Drop:                                      0
         CC Dropped Packets:                            0
         FastPath Misc Drops
             Overload Protection:                       0
             Invalid Client:                            0
             Stream ID 0:                               0
             Invalid Stream ID:                         0
```

注：

- **show user-plane-service statistics drop-counter** CLI コマンドの場合、様々な理由でドロップされたパケット数のカウンタは、sessmgr リカバリまたは ICSR（シャーシ間セッションリカバリ）後に回復されません。

- **show subscribers user-plane-only callid** *callid_value* **drop-statistics** CLI コマンドの場合、様々な理由でドロップされたパケット数のカウンタは、sessmgr リカバリまたは ICSR 後に回復されます。
- コマンドは、セッションレベルおよびインスタンスレベルでキャプチャされたカウンタを重複ません。
- 「Quota Exhaus FAR Apply Action Drop」によってドロップされたパケットは、「FAR Apply Action Drop」カウンタではなく、「CC Dropped Packets」に累積されます。
- 「Failure in processing FAR buffered packets」でドロップされたパケットは、「ルールに一致しない」、「TEID が見つからない」、またはその他の理由が原因である可能性があります。このようなパケットに対しては、それぞれのカウンタが増分します。
- 「redirect-url」フローアクションによってドロップされたパケットは、**show user-plane-service statistics drop-counter** CLI コマンドの「Redirect- URL 」に蓄積されます。

show subscribers user-plane-only callid *callid_value* flows full

show subscribers user-plane-only callid *callid_value* **flows full** コマンドは、デバッグを行うために必要なフローレベルの詳細情報を表示します。

次に、このコマンドの出力例を示します。

```
[local]GVK-HUPF# show subscribers user-plane-only callid 017dc662 flows full
Tuesday November 22 18:35:35 UTC 2022

Callid: 017dc662
Interface Type: N4
IP address: n/a

Flow ID: 6:2
Uplink pkts: 0 Downlink pkts: 1
Uplink bytes: 0 Downlink bytes: 1040
Fast Path Info:
Uplink pkts: 0 Downlink pkts: 0
Uplink bytes: 0 Downlink bytes: 0
Total pkts: 0
Uplink Dropped pkts: 0 Downlink Dropped pkts: 4
Uplink Stream ID: 0x0 Downlink Stream ID: 0x1000007
Uplink Stream State: n/a Downlink Stream State: Passive
Client-ID : C6
UE IP address: 12.1.0.3 UE Port: 1001
Server IP address: 100.100.100.10 Server Port: 1001
Protocol: TCP
Service Chain Name: NA
Uplink Sfp Id: NA
Downlink Sfp Id: NA

Flow ID: 6:3
Uplink pkts: 5 Downlink pkts: 2
Uplink bytes: 200 Downlink bytes: 2080
Fast Path Info:
Uplink pkts: 0 Downlink pkts: 3
Uplink bytes: 0 Downlink bytes: 3120
Total pkts: 3
Uplink Dropped pkts: 0 Downlink Dropped pkts: 0
```

```
Uplink Stream ID: 0x0 Downlink Stream ID: 0x2000008
Uplink Stream State: n/a Downlink Stream State: Active
Client-ID : C6
UE IP address: 12.1.0.3 UE Port: 1000
Server IP address: 100.100.100.10 Server Port: 1000
Protocol: TCP
Service Chain Name: NA
Uplink Sfp Id: NA
Downlink Sfp Id: NA

Total Number of Active flows : 2
```

show subscribers user-plane-only callid *callid_value* flows flow-id *flow_id*

show subscribers user-plane-only callid *callid_value* **flows flow-id** *flow_id* コマンドは、デバッグプロセスで必要なフローレベルの詳細な情報を表示します。

次に、このコマンドの出力例を示します。

```
# show sub user-plane-only callid 00004e22 flows flow-id 1:4

  Callid: 00004e22
  Interface Type: Sxb
  IP address: n/a

  Flow ID: 1:4
  Uplink pkts: 17                                 Downlink pkts: 0
  Uplink bytes: 1026                              Downlink bytes: 0
  Fast Path Info:
   Uplink pkts: 0                                 Downlink pkts: 0
   Uplink bytes: 0                                Downlink bytes: 0
   Total pkts: 0
   Uplink Dropped pkts: 0                         Downlink Dropped pkts: 0
   Uplink Stream ID: 0x0000008                    Downlink Stream ID: 0x0
   Uplink Stream State: Passive                   Downlink Stream State: n/a
   Client-ID : C2
  UE IP address: 12.2.0.13                        UE Port: 1007
  Server IP address: 100.100.100.10               Server Port: 1005
  Protocol: TCP
  Service Chain Name: NA
  Uplink Sfp Id: NA
  Downlink Sfp Id: NA

Total Number of Active flows : 1
```

SNMP サポート

システムは Simple Network Management Protocol（SNMP）を使用して、ネットワーク上の EMS サーバーまたはアラームサーバーにトラップまたはイベントを送信します。これらのデバイスと通信するには、SNMP を設定する必要があります。

「*SNMP MIB* リファレンス」では、UPF と StarOS がサポートする MIB と SNMP トラップについて説明されています。

各機能をサポートするために、次の SNMP トラップが利用可能です。

N4 Session/Node Level Reporting 手順

次のトラップを使用して、状態および条件の GTP-U パス障害を追跡できます。

- EGTPUPathFailure：このトラップは、GTP-u Echo 要求に対する応答を受信せず、ピア EPC ノードへのデータパス障害が検出された場合に生成されます。
- EGTPUPathFailureClear：このトラップは、ピアノードへのデータパスが知用可能な場合に生成されます。

UP セッションリカバリ

ユーザープレーンノードでのセッションリカバリ後に、次のトラップを使用できます。

- ManagerFailure：このトラップは、ソフトウェアマネージャでエラーが発生した場合に生成されます。
- TaskFailed：このトラップは、重要ではないタスクでエラーが発生し、適切なリカバリ手順が開始された場合に生成されます。
- TaskRestart：このトラップは、以前のエラー発生後に重要でないタスクが再開した場合に生成されます。
- SessMgrRecoveryComplete：このトラップは、セッションマネージャリカバリが完了した場合に生成されます。通常は、セッションマネージャタスクが失敗し、リカバリが正常に完了した場合に発生します。
- ManagerRestart：このトラップは、特定されたマネージャタスクが再開した場合に生成されます。

Sx の関連付け

Sx 関連付けのステータスを追跡するため、次のトラップを使用できます。

- SxPeerAssociated：このトラップは、Sx アソシエーションが検出された場合にトリガーされます。
- SxPeerAssociationRelease：このトラップは、Sx アソシエーションの解除が検出された場合にトリガーされます。

URL ブロックリスト登録登録

URL ブロックリスト登録機能のサポートで使用できる SNMP トラップを以下に示します。

- BLDBError：エラーコードが記載された blockedlisting OPTBLDB ファイルエラーを指定します。
- BLDBErrorClear：削除された blockedlisting OPTBLDB ファイルエラーを指定します。
- BLDBUpgradeError：エラーコードが記載された blockedlisting OPTBLDB ファイルエラーを指定します。
- BLDBUpgradeErrorClear：削除された blockedlisting OPTBLDB ファイルエラーを指定します。

SNMP トラップの有効化

SNMP トラップを有効にするには、次の構成を使用します。

```
configure
   snmp trap enable trap_name
   end
```

SNMP サポートの補間情報については、『*ASR 5500* システム アドミニストレーション ガイド』の「管理設定」章を参照してください。

UPF 機能の障害対応

N4 またはデータパス

N4 またはデータパス関連の問題の障害対応には、次の CLI コマンドを使用できます。

- **show gtpu statistics**
- **show user-plane-service { all | bandwidth-policy | charging-action | edr-format | group-of-ruledefs | gtpp-group | name | pdn-instance | rulebase | ruledef | statistics | xheader-format }**

  注：

  - **all**：すべてのユーザープレーンサービスを表示します。
  - **bandwidth-policy**：ユーザープレーンサービスの帯域幅ポリシーの情報を表示します。
  - **charging-action**：ユーザープレーンサービスの課金アクションの情報を表示します。
  - **edr-format**：ユーザープレーンサービスの EDR フォーマットの情報を表示します。
  - **group-of-ruledefs**：ユーザープレーンサービスで設定された Group of Ruledefs に関する情報を表示します。
  - **gtpp-group**：ユーザープレーンサービスの帯域幅ポリシーの情報を表示します。
  - **name**：特定のユーザープレーンサービス名の情報を表示します。
  - **pdn-instance**：PDN インスタンスに関する情報を表示します。
  - **rulebase**：ユーザープレーンサービスの rulebase の情報を表示します。
  - **ruledef**：ユーザープレーンサービスの ruledef の情報を表示します。
  - **statistics**：ユーザープレーンのノードレベルの統計を表示します。

    さらに、**show user-plane-service statistics { all | analyzer | charging-action | fapi | rulebase | tethering-detection }** も使用できます。
  - **xheader-format**：ユーザープレーンサービスの X-Header フォーマットの情報を表示します。

- **show user-plane-service content-filtering category policy-id (all | id** *id_value* **}**

- **content-filtering**：コンテンツフィルタリング情報を表示します。
- **category**：コンテンツフィルタリングのカテゴリ情報を表示します。
- **policy-id**：コンテンツフィルタリングのカテゴリの Policy-ID とその定義を表示します。
- **all**：すべてのコンテンツフィルタリングのカテゴリポリシーの定義を表示します。
- **id** *id_value*：具体的なポリシー ID のコンテンツフィルタリングのカテゴリ定義を表示します。*id_value* は、1 ～4,294,967,295 の範囲の整数で指定する必要があります。

- **show sx-service { all | name | statistics }**

  注：

  - **all**：すべての Sx サービスを表示します。
  - **name**：具体的な Sx サービス名の情報を表示します。
  - **statistics**：最後の restart または clear コマンド以降に収集された特定のプロトコルについての情報の合計を表示します。

コンテンツ フィルタリング

CF 関連の問題の障害対応を実行するには、次の CLI コマンドを使用します。

2022.01.0 より前のリリース：

```
show user-plane-service inline-services { content-filtering | info |
url-blacklisting }
```

2022.01.0 以降のリリース：

```
show user-plane-service inline-services { content-filtering | info |
url-blockedlisting }
```

注：

- **content-filtering**：コンテンツフィルタリング情報を表示します。
- **info**：インラインサービスの情報を表示します。
- **url-blockedlisting**：ユーザープレーンサービスの URL ブロックリスト登録パラメータを表示します。

URL のブラックリスト化

show user-plane-service url-blacklisting database { all | debug-only | facility | url } CLI コマンドを使用して、URL ブラックリスト関連の問題の障害対応を行います。

注：

- **all**：すべての URL ブラックリスト登録データベース構成を表示します。

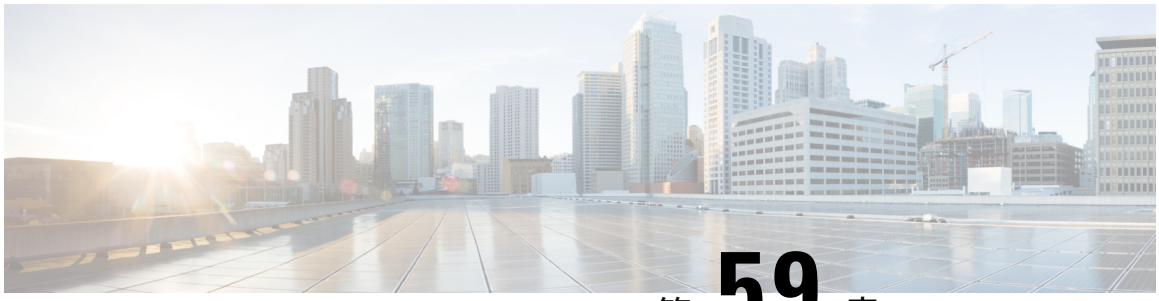
- **debug-only**：URL ブラックリスト登録に関する静的データベースのデバッグ情報を表示します。
- **facility**：ファシリティごとの URL ブラックリスト登録データベースの構成を表示します。
- **url**：URL ブラックリスト登録の特定のデータベース情報を表示します。



第 III 部

UPF の基本構成例

• UPF の構成例 （685 ページ）



第 59 章

UPF の構成例

- 設定例 （685 ページ）

設定例

以下は、選択に応じて個別に提供されたサンプルの構成ファイルです。展開の具体的なニーズに応じて、独自の構成ファイルを作成および変更する必要があります。

```
----- snip -----
  active-charging service acs
    bandwidth-policy BWP
      flow limit-for-bandwidth id 1 group-id 2
      flow limit-for-bandwidth id 2 group-id 3
      flow limit-for-bandwidth id 100 group-id 100
     group-id 2 direction uplink peak-data-rate 256000 peak-burst-size 1000 violate-action
 discard
      group-id 2 direction downlink peak-data-rate 200000 peak-burst-size 1000
violate-action discard
      group-id 3 direction downlink peak-data-rate 256000 peak-burst-size 1000
violate-action discard
     group-id 4 direction uplink peak-data-rate 300000 peak-burst-size 1200 violate-action
 lower-ip-precedence
      group-id 100 direction downlink peak-data-rate-kbps 4294967295 peak-burst-size
4294967295 violate-action discard

    ruledef L3_SERVER
      ip server-ip-address = 209.165.202.150/27
      tcp either-port = 80
    #exit
    ruledef L4_PORT
      tcp either-port = 80
      udp either-port = 80
      multi-line-or all-lines
    #exit
    ruledef L7_HTTP
      http host contains 209.165.202.150
      multi-line-or all-lines
    #exit
    ruledef http-pkts
      http any-match = TRUE
    #exit
    ruledef http-port
      tcp either-port = 80
      rule-application routing
```

```
  #exit
  ruledef ip-any-rule
    ip any-match = TRUE
  #exit
  urr-list urrs
    rating-group 10 urr-id 5
  #exit
  charging-action starent
    content-id 10
    billing-action egcdr
  #exit
  rulebase default
  #exit
  credit-control group default
    pending-traffic-treatment noquota buffer
    pending-traffic-treatment quota-exhausted pass
    usage-reporting quotas-to-report based-on-grant

  rulebase starent
    billing-records egcdr
    dynamic-rule order first-if-tied
    action priority 5 ruledef http-pkts charging-action standard
    action priority 10 ruledef L7_HTTP charging-action starent
    action priority 20 ruledef L4_PORT charging-action starent
    action priority 100 ruledef L3_SERVER charging-action starent
    action priority 10000 ruledef ip-any-rule charging-action starent
    route priority 1 ruledef http-port analyzer http
    egcdr threshold interval 1000
    bandwidth default-policy BWP
  #exit
  traffic-optimization-policy default
  #exit
#exit
context ingress
  interface N3_interface
    ip address 209.165.201.4 209.165.201.5
    ipv6 address abc0:0:0:cb::1/64 secondary
  #exit
  interface N3_interface_LOGICAL loopback
    ip address 209.165.201.4 209.165.201.5
  #exit
  interface N3_interface_LOGICAL2 loopback
    ip address 209.165.201.4 209.165.201.5
  #exit
  interface N4U_interface
    ip address 209.165.201.4 209.165.201.5
    ipv6 address abc0:0:0:cd::1/64 secondary
    ipv6 address abc0:0:0:ca::1/64 secondary
  #exit
  interface N4U_interface_LOGICAL loopback
    ip address 209.165.201.4 209.165.201.5
  #exit
 interface N4_interface
    ip address 209.165.201.4 209.165.201.5
    ipv6 address abc0:0:0:cc::1/64 secondary
  #exit
  interface N4_interface_LOGICAL loopback
    ip address 209.165.201.4 209.165.201.5
  #exit
  subscriber default
  exit
  aaa group default
  #exit
  gtpp group default
```

```
  #exit
  gtpu-service N3-GNB1
    bind ipv4-address 209.165.200.225
  exit
  gtpu-service N3-GNB2
    bind ipv4-address 209.165.201.4
  exit
  gtpu-service control_gtpu
    bind ipv4-address 209.165.201.4
  exit
  sx-service N4
    instance-type userplane
    bind ipv4-address 209.165.201.4
    sx-protocol heartbeat interval 3600
    sx-protocol heartbeat max-retransmissions 1
    sx-protocol association reattempt-timeout 30
  exit
  user-plane-service user-plane-service
    associate gtpu-service N3-GNB1 upf-ingress
    associate gtpu-service control_gtpu cp-tunnel
    associate sx-service N4
    associate fast-path service
    associate control-plane-group default
    load-control capacity 900
  exit
  user-plane-service user-plane-service1
  exit
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N4_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N4_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N3_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N3_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N4_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N3_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N4_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N3_interface
#exit
context egress
  interface N6_interface
    ip address 209.165.201.4 209.165.201.5
    ipv6 address abc0:0:0:cf::1/64 secondary
  #exit
  subscriber default
  exit
  apn starent.com
    pdp-type ipv4 ipv6
    selection-mode subscribed sent-by-ms chosen-by-sgsn
    gtpp group default accounting-context egress
    ip context-name egress
    active-charging rulebase starent
  exit
  aaa group default
  #exit
  gtpp group default
    gtpp attribute local-record-sequence-number
    gtpp dictionary custom24
    gtpp egcdr service-data-flow threshold interval 60
    gtpp egcdr service-data-flow threshold volume downlink 13000
    gtpp egcdr service-data-flow threshold volume uplink 17000
    gtpp egcdr service-data-flow threshold volume total 22222
  #exit
  ipv6 route 2:2:2:2::/64 next-hop abc0::ab:1c:2ff:def9:1ad interface N6_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N6_interface
  ip route 209.165.201.4 209.165.201.5 209.165.201.6 N6_interface
  ipv6 route 2:2:2:2::/64 next-hop abc0::ab:1c:2ff:def9:1ab interface N6_interface
```

```
    ip route 209.165.201.4 209.165.201.5 209.165.201.6 N6_interface
  #exit
  control-plane-group default
    sx-association initiated-by-cp
    peer-node-id ipv4-address 209.165.200.225 interface n4
  #exit
  user-plane-group default
  #exit
  port ethernet 1/11
    no shutdown
    vlan 203
      no shutdown
      bind interface N4U_interface ingress
    #exit
    vlan 204
      no shutdown
      bind interface N4_interface ingress
    #exit
    vlan 205
      no shutdown
      bind interface N3_interface ingress
    #exit
    vlan 206
      no shutdown
    #exit
    vlan 207
      no shutdown
      bind interface N6_interface egress
    #exit
  #exit
end
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。