S11 KPI低下のトラブルシューティング

内容

はじめに

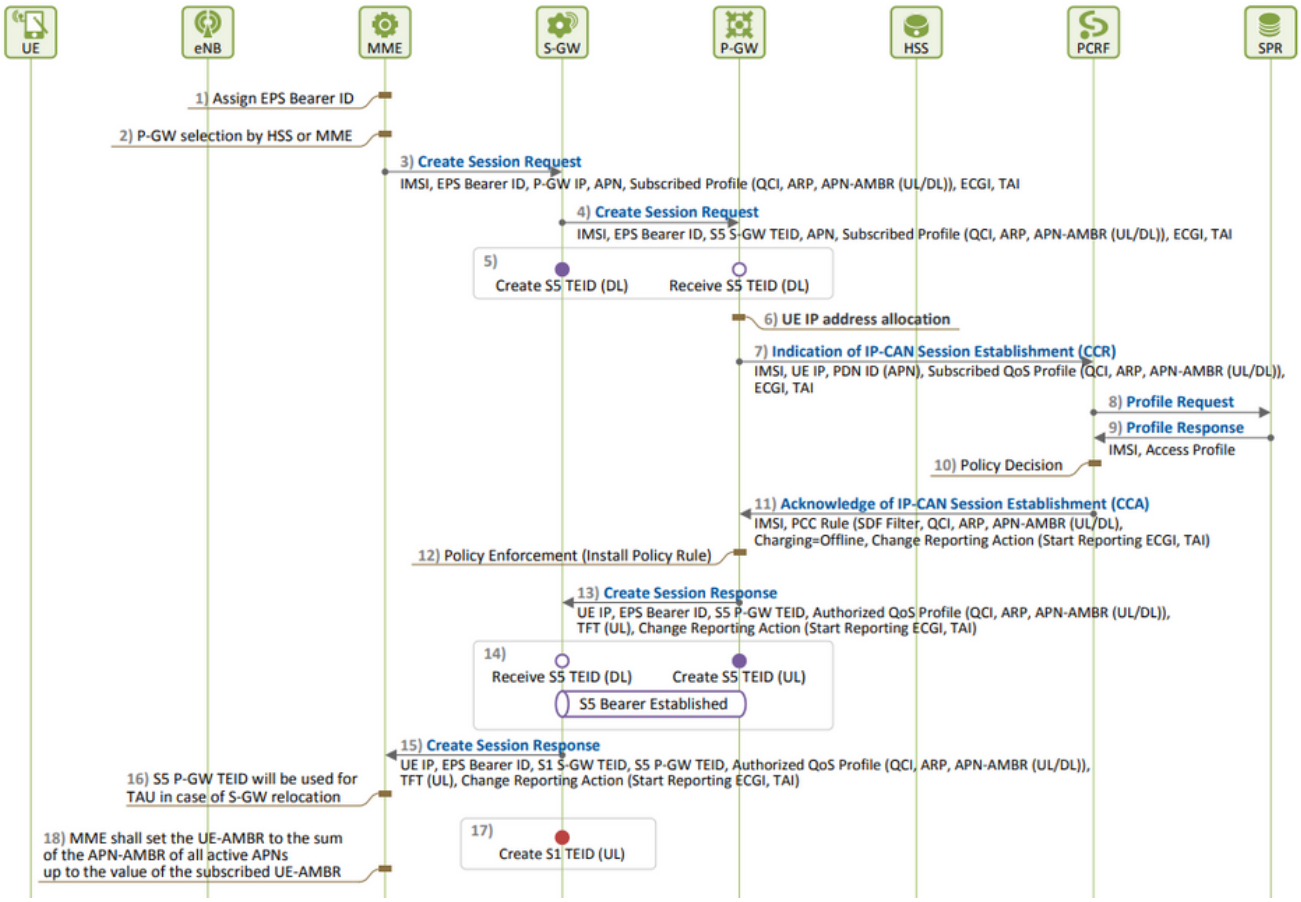
このドキュメントでは、S11重要業績評価指標(KPI)の品質低下の問題をトラブルシューティングする方法について説明します。

概要

S11は、Long Term Evolution(LTE)ネットワークでモビリティマネージメントエンティティ(MME)とサービングゲートウェイ(SGW)を接続するインターフェイスです。このインターフェイスでは、GnまたはGPRSトンネリングプロトコル制御(GTP-C)が使用されます。

S11インターフェイスのメッセージ

- セッション要求/応答の作成
- セッション要求/応答の変更
- セッション要求/応答の削除



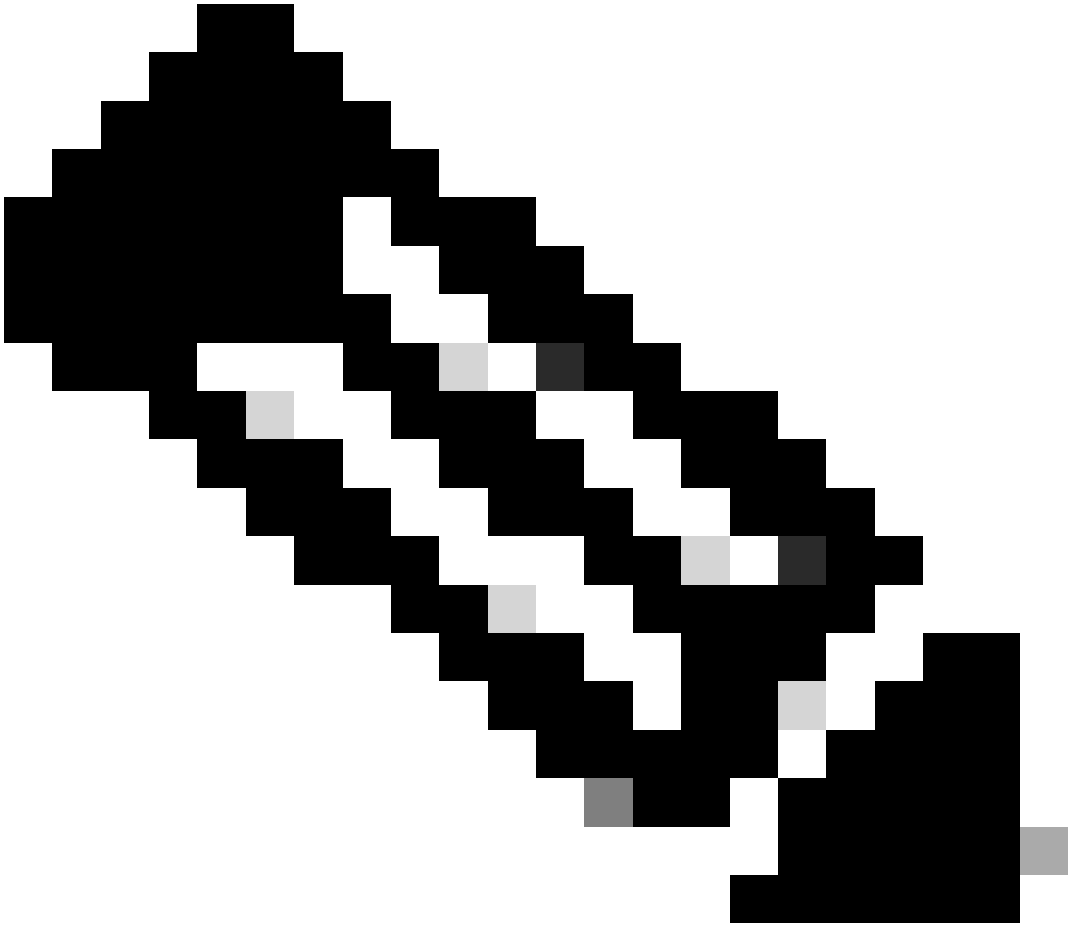
EPSセッションの確立

- S11 KPIの低下は、根本原因である必要があるCSRの試行よりも、Create Session Requests(CSR)の拒否の方が多い場合に観察されます。

KPIの測定に使用される式を把握し、式に含まれるすべてのカウンタをメモして、低下の原因となるカウンタを特定できます。

```
S11 ASR (SPGW)  = ((tun-sent-cresessrespaccept+ggsn_tun-sent-cresessrespdeniedUserAuthFailed+tun-sent-c

PDN Connectivity Success Rate (MME) : ((%esmevent-pdncon-success%) + (%esm-msgtx-pdncon-rej%))*) / (%es
```



注：計算式は、測定方法によって異なります。

初期レベルで必要なログ：

- 機能低下を示すKPIトレンド。
- 使用されているKPIフォーミュラ。
- 未処理のバルクスタットカウンタと問題の開始時からのコード傾向を引き起こします。
- 問題が発生している期間に30分間隔でノードからShow Support Details(SSD)の2つのインスタンスをキャプチャします。
- Syslogの範囲は、品質低下が発生する2時間前から現在の時刻までです。mon sub/pro tracesおよびlogging monitor msid <imsi>。

トラブルシューティングシーケンス

- S11 KPI式に含まれる各カウンタのKPIトレンドをバルクスタットを分析して評価する。

- 問題のあるタイムラインと問題のないタイムラインの間のKPIトレンドを比較します。

- 特定された問題のあるbulkstatカウンタがフローに基づいてどのように定義されているかを調べ、パターンを確立します。

- 3 ~ 5分の間隔で複数回の繰り返しによってノードから切断理由を収集します。

異なるタイムスタンプで収集された2つのSSD間の切断理由の差分を分析できます。デルタ値の大幅な増加を示す切断理由は、KPIの低下の原因と考えられます。すべての切断理由の詳細については、https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-23/Stat-Count-Reference/21-23-show-commanにある『Cisco Statistics and Counters Reference』を参照してください。

show session disconnect-reasons verbose

5. 対象のノードのタイプに基づいてegtp統計情報をチェックします。

--- SGW end -----

show egtpc statistics interface sgw-ingress path-failure-reasons
show egtpc statistics interface sgw-ingress summary
show egtpc statistics interface sgw-ingress verbose
show egtpc statistics interface sgw-ingress sessmgr-only

show egtpc statistics interface sgw-egress path-failure-reasons
show egtpc statistics interface sgw-egress summary
show egtpc statistics interface sgw-egress verbose
show egtpc statistics interface sgw-egress sessmgr-only

---- PGW end -----

show egtpc statistics interface pgw-ingress path-failure-reasons
show egtpc statistics interface sgw-ingress summary
show egtpc statistics interface sgw-ingress verbose
show egtpc statistics interface sgw-ingress sessmgr-only

--- MME end -----

show egtpc statistics interface mme path-failure-reasons
show egtpc statistics interface mme summary
show egtpc statistics interface mme verbose
show egtpc statistics interface mme sessmgr-only

6. 問題を引き起こしている特定のカウンタを特定したら、mon-sub/mon-proコールトレースをキャプチャして、さらに分析を行い、KPI低下の原因となっている特定のコールフローを特定する必要があります。さらに、外部ツールを使用してWiresharkトレースを取得し、より詳細な分析を行うこともできます。

Monサブトレースをキャプチャするコマンドは次のとおりです。

monitor subscriber with options 19, 26,33, 34, 35, 49,A,S, X, Y, verbosity +5 during the issue.

mon-pro with options 19, 26,33, 34, 35, 49,A,S, X, Y, verbosity +5 during the issue if no mon-sub is present.

More options can be enabled depending on the protocol or call flow we need to capture specifically

KPIの低下が最小限の割合に留まっているためにmon-subのようなトレースのキャプチャが実行できない場合は、代わりにシステムレベルのデバッグログをキャプチャする必要があります。これには、sessmgrとegptcのデバッグログのキャプチャ、および必要に応じたゲートウェイ固有のフローのキャプチャが含まれます。

logging filter active facility sessmgr level debug
logging filter active facility egtpc level debug
logging filter active facility sgw level debug
logging filter active facility pgw level debug

logging active ---------- to enable
no logging active ---------- to disable

Note :: Debugging logs can increase CPU utilization so need to keep a watch while executing debugging logs

7. デバッグログを分析した後、問題の原因を特定した場合は、エラーログを観察する特定のイベントのコアファイルのキャプチャに進むことができます。

logging enable-debug facility sessmgr instance <instance-ID> eventid 11176 line-number 3219 collect-cores 1

For example :: consider we are getting below error log in debug logs which we suspect can be a cause of issue
and we don;t have any call trace

[egtpc 141027 info] [15/0/6045 <sessmgr:93> _handler_func.c:10068] [context: INLAND_PTL_MME01, contextID: 6] [software internal user syslog] [m

So in this error event

facility :: sessmgr
event ID = 141027
line number = 10068

警告:デバッグログ、logging monitor、mon-sub、mon-proなどのログの収集を要求する場合は常に、これらのログが必ずメンテナンス時間帯に収集されるようにしてください。また、この間にCPUの負荷を監視することも重要です。

症状の分析と特定

-

まず、SSDからシステムに頻繁なクラッシュが発生していないかどうかを確認します。

```
show crash list
```

- ライセンスの問題が発生したかどうかを確認してください。場合によっては、Serving Packet Data Gateway(SPGW)のライセンスの期限が切れると、新しいコールを受け入れることができなくなり、その結果、コールが失敗し、S11の機能低下またはディップが発生します。

```
show resource info
```

- メモリまたはCPUの使用率が高いために、警告/オーバー状態のsessmgrインスタンスが複数あるかどうかを確認してください。このようなインスタンスが見つかった場合は、次の条件が原因で新しいコールが拒否されているかどうかを確認します。

- デバッグログから、どのインターフェイスでコール拒否エラーが発生しているかを確認できます。

「sgw-egress」コンテキストで特定のサブスクライバに対して大量のコール拒否エラーが発生し、それに続いて「sgw-ingress」コンテキストで同じサブスクライバが拒否される場合は、Packet Data Gateway(PGW)からの拒否がS11コンテキストのSGW-> MMEに送信されると推測できます。PGW側からさらに確認してトラブルシューティングするために、このIMSIのmon-subを取得できます。

```
2022-Nov-26+00:20:51.763 [egtpc 141018 unusual] [7/0/16871 <sessmgr:579> _handler_func.c:3227] [context

2022-Nov-26+00:20:51.763 [egtpc 141018 unusual] [7/0/16871 <sessmgr:579> _handler_func.c:2505] [context
```

- 場合によっては、KPIディップに対して複数の拒否理由が存在することがあるため、各理由を個別に確認し、それに応じて処理を進める必要があります。

たとえば、特定のInternational Mobile Subscriber Identity(IMSI)シリーズ（ローマー内のサブスクライバ用）でno_resource_available/user_auth_failureエラーが増加する可能性があるため、PGWからこれらを確認する必要があります。remote peer not respondingのような理由でセッション要求がSGWでタイムアウトになり、S11 KPIが低下する可能性があります。この作成セッションは、SGWからMMEへのNo_resource_availableと同様に拒否できます。これらのリジェクト原因コードは、モニタプロトコルログから確認できます。また、Create Session RequestおよびCreate Session Responsesをチェックして、これらのリジェクト原因コードの送信元である特定のIPアドレスを特定できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。