

S11 KPI 저하 문제 해결

목차

[소개](#)

[개요](#)

[S11 인터페이스의 메시지](#)

[문제 해결 순서](#)

[증상 분석 및 식별](#)

소개

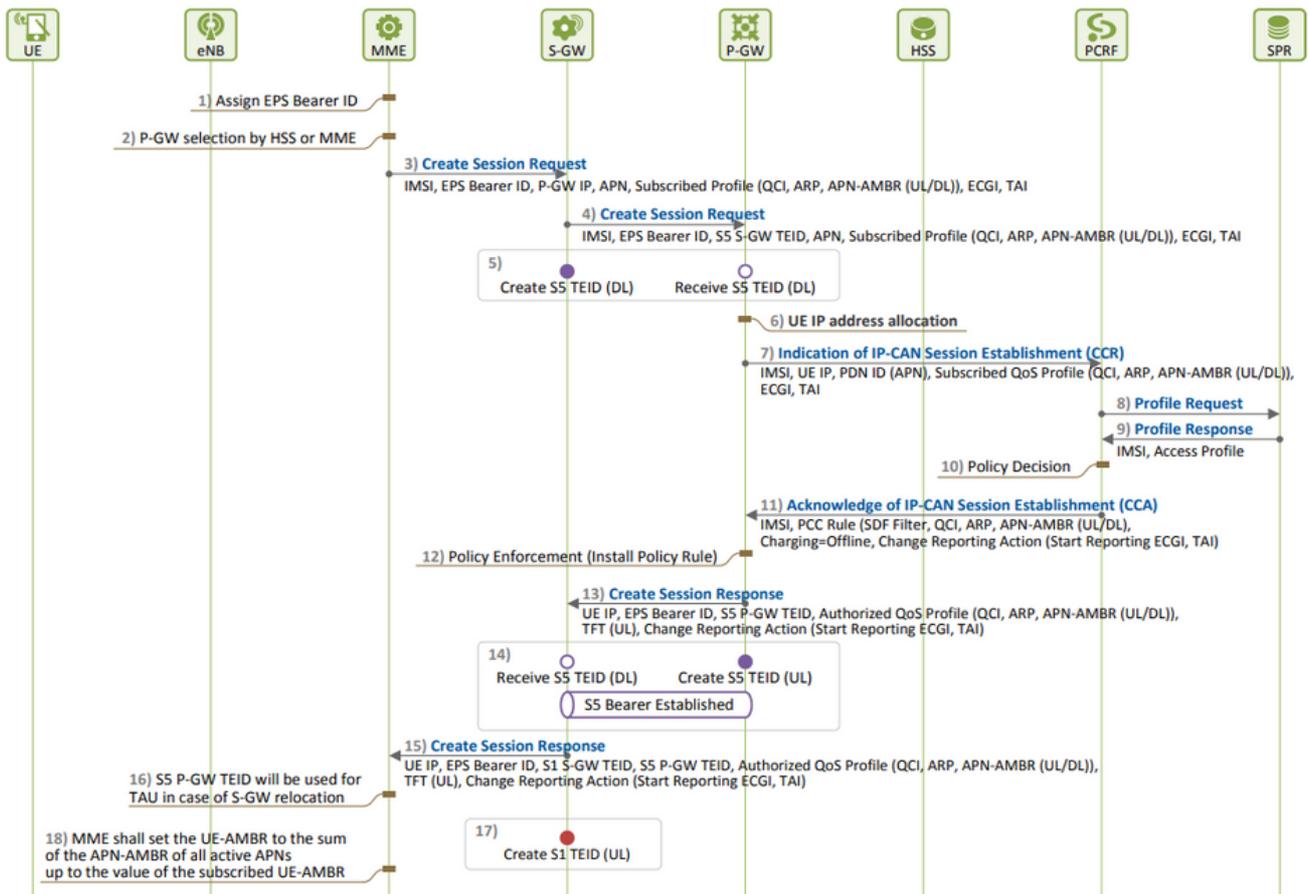
이 문서에서는 S11 KPI(핵심 성능 지표) 저하 문제를 해결하는 방법에 대해 설명합니다.

개요

S11은 LTE(Long Term Evolution) 네트워크에서 MME(Mobility Management Entity)와 SGW(Serving Gateway)를 연결하는 인터페이스이다. 인터페이스는 Gn 또는 GTP-C(GPRS Tunneling Protocol-Control)를 사용합니다.

S11 인터페이스의 메시지

- 세션 요청/응답 생성
- 세션 요청/응답 수정
- 세션 요청/응답 삭제



EPS 세션 설정:

- S11 KPI 성능 저하는 CSR 시도에 비해 CSR(Create Session Requests) 거부가 더 많이 나타날 때 관찰됩니다. CSR은 근본 원인이어야 합니다.

KPI를 측정하는 데 사용되는 공식을 알고 공식에 포함된 모든 카운터를 기록하고 성능 저하의 원인이 되는 정확한 카운터를 결정할 수 있습니다.

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

주: 공식은 측정 방법에 따라 달라질 수 있습니다.

초기 수준에 필요한 로그:

- 성능 저하를 나타내는 KPI 추세입니다.
- 사용된 KPI 공식입니다.
- Raw Bulkstat 카운터 및 문제 발생 초기부터 코드 추세를 유발합니다.
- 문제가 있는 기간 동안 30분 간격으로 노드에서 SSD(Show Support Details) 인스턴스 2개를 캡처합니다.
- Syslogs의 범위는 성능 저하가 발생하기 2시간 전부터 현재 시간까지 `mon sub/pro traces`입니다. 및 `logging monitor msid <imsi>`.

문제 해결 순서

•

bulkstats를 분석하여 S11 KPI 공식에 포함된 각 카운터의 KPI 추세를 평가합니다.

•

문제가 있는 일정의 KPI 추세를 문제가 없는 일정의 KPI와 비교합니다.

•

확인된 문제 있는 Bulkstat 카운터가 흐름을 기준으로 어떻게 정의되는지 살펴보고 패턴을 설정합니다.

•

3~5분 간격으로 여러 번 반복을 통해 노드의 연결 끊김 사유를 수집합니다.

서로 다른 타임스탬프에 수집된 두 SSD 간의 연결 끊김 사유의 델타를 분석할 수 있습니다. 델타값의 유의한 증가를 보이는 연결해제 사유는 KPI 열화의 원인으로 여겨질 수 있다. 모든 연결 해제 사유에 대한 자세한 내용은 Cisco 통계 및 카운터 참조 (https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-23/Stat-Count-Reference/21-23-show-command...)를 참조하십시오.

```
show session disconnect-reasons verbose
```

5. 노드 유형에 따라 egtp 통계를 확인합니다.

--- 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. 문제를 일으키는 특정 카운터를 식별한 후에는 mon-sub/mon-pro 통화 추적을 캡처하여 KPI 저하를 일으키는 특정 통화 흐름을 더 자세히 분석하고 식별해야 합니다. 또한 외부 툴을 사용하여 Wireshark 추적을 가져와 더 자세한 분석을 수행할 수 있습니다.

Mon 하위 추적을 캡처하는 명령은 다음과 같습니다.

```
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 저하의 최소 백분율로 인해 mon-sub와 같은 추적을 캡처할 수 없는 경우 대신 시스템 수준 디버그 로그를 캡처해야 합니다. 여기에는 sessmgr 및 egtpc에 대한 디버그 로그를 캡처하고 필요한 경우 게이트웨이별 플로우를 캡처하는 작업이 포함됩니다.

```
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. 디버그 로그를 분석한 후 문제의 원인을 파악하면 오류 로그를 관찰하는 특정 이벤트에 대한 핵심 파일을 계속 캡처할 수 있습니다

```
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
```



경고: 디버그 로그, 로깅 모니터, mon-sub 또는 mon-pro와 같은 로그 수집을 요청할 때마다 유지 관리 기간 동안 이러한 로그가 수집되었는지 확인하는 것이 중요합니다. 또한 이 시간 동안 CPU 로드를 모니터링하는 것이 중요합니다.

증상 분석 및 식별

- 먼저 SSD에서 시스템에 충돌이 자주 발생하는지 확인합니다.

show crash list

- 라이선스 문제가 발생했는지 확인하십시오. SPGW(Serving Packet Data Gateway)의 라이선스가 만료되면 더 이상 새 통화를 수락할 수 없으므로 통화가 실패하고 S11 성능 저하 또는 감축으로 이어집니다.

show resource info

- 메모리 또는 CPU 사용량이 많아 여러 esmgr 인스턴스가 경고/오버 상태에 있는지 확인하십시오. 이러한 인스턴스가 발견되면 해당 조건 때문에 새 통화가 거부되는지 확인합니다.
- 디버그 로그에서 어떤 인터페이스에서 통화 거부 오류를 받는지 확인할 수 있습니다.

"sgw-egress" 컨텍스트에서 특정 가입자에 대해 상당수의 통화 거부 오류가 발생한 후 "sgw-ingress" 컨텍스트에서 동일한 가입자가 거부되는 경우 PGW(Packet Data Gateway)의 거부가 S11 컨텍스트에서 SGW-> MME로 전송됨을 유추할 수 있습니다. PGW 쪽에서 더 확인하고 문제를 해결하기 위해 이제 이 IMSI에 대해 mon-sub를 사용할 수 있습니다.

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

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

- 때로는 KPI dip에 여러 거절 사유가 있을 수 있으므로 사유별로 따로 확인하고 그에 따라 진행해야 한다.

예를 들어, 특정 IMSI(International Mobile Subscriber Identity) 시리즈의 오류 증가가 no_resource_available/user_auth_failure 있을 수 있으며, 이는 인로머(in-roamer) 가입자용이므로 PGW에서 확인해야 합니다. SGW에서 시간이 초과되는 세션 요청을 생성하고 그런remote peer not responding 이유가 있을 수 있으며, 이는 S11 KPI의 저하를 야기할 수 있다. 이 생성 세션은 SGW에서 MME로 No_resource_available 거부될 수 있습니다. 이러한 거부 원인 코드는 모니터 프로토콜 로그에서 확인할 수 있으며, Create Session Request(세션 요청 생성) 및 Create Session Responses(세션 응답 생성)를 선택하여 이러한 거부 원인 코드가 전송되는 특정 IP 주소를 식별할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.