

SCTP 최대 MTU 크기와 관련된 패킷 삭제 트러블 슈팅

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[단편화](#)

[SCTP 청크 번들링](#)

[크기 조정에 영향을 미치는 구성](#)

[SCTP-Param-Template SCTP MTU 크기](#)

[MME 컨텍스트 이더넷 인터페이스 컨피그레이션](#)

[포트 이더넷 MTU 크기](#)

[S1APUE 무선 기능 IE 크기](#)

[사례 연구](#)

[솔루션](#)

[삭제 해결을 위한 해결 방법](#)

[해결 #1: SCTP 최대 MTU 크기 감소](#)

[해결 #2: 전송 노드 MTU 크기를 1500보다 크게 증가](#)

[관련 정보](#)

소개

이 문서에서는 Cisco MME의 SCTP 프래그먼트화 및 청크 번들링 메커니즘과 프래그먼트화 및 번들링이 패킷 삭제에 미치는 영향에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- QVPC-SI 소프트웨어 버전 21.28.m18

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SCTP(Stream Control Transmission Protocol)는 IP와 같은 연결 없는 패킷 네트워크에서 작동하는 신뢰할 수 있는 전송 프로토콜입니다. 또한 검색된 경로 MTU 크기에 맞게 데이터를 단편화하고 청크 번들링을 사용하여 여러 사용자 메시지를 단일 SCTP 패킷으로 번들링할 수 있습니다. 이 문서에서는 경로 MTU 제한으로 인해 발생하는 패킷 삭제를 해결하는 두 가지 방법을 제공합니다.

사례 연구에서는 SCTP 최대 MTU 크기의 컨피그레이션이 아니라 Cisco MME 외부에서 발생하는 패킷 삭제를 포함하여 패킷 삭제를 보여주는 프래그먼트화 및 번들링 메커니즘과 수단을 보여줍니다.

RFC 4960(Stream Control Transmission Protocol) 6.9(Fragmentation and Reassembly)에 따라:

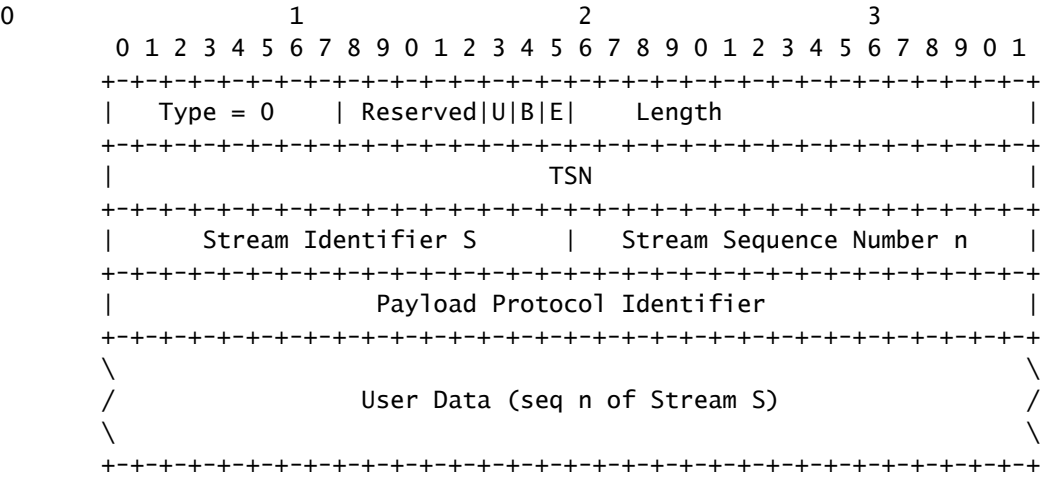
"엔드포인트가 프래그먼트화를 지원하는 경우 전송되는 사용자 메시지 크기로 인해 아웃바운드 SCTP 패킷 크기가 현재 MTU를 초과하는 경우 사용자 메시지를 프래그먼트화해야 합니다."

또한 여러 SCTP 데이터 청크를 하나의 아웃바운드 SCTP 패킷으로 번들로 묶을 수 있습니다. SCTP 패킷 및 IP 헤더를 포함한 결과 IP 데이터그램의 총 크기는 현재 경로 MTU보다 작거나 같아야 합니다. MME에서 경로 MTU는 이러한 패킷을 처리하는 IP 인터페이스에 구성됩니다.

단편화

SCTP 연결에는 SI(스트림 식별자)로 식별되는 여러 스트림이 있을 수 있습니다. SSN(Stream Sequence Number)은 특정 SCTP 스트림 내의 각 프래그먼트에 대한 순서를 식별합니다. 여러 세션에서 동일한 SCTP 스트림을 사용할 수 있습니다. TSN(Transmission Sequence Number)은 전체 SCTP 연관 내의 각 프래그먼트에 대한 순서를 식별합니다.

프래그먼트화될 때 SCTP 페이로드 데이터 청크는 B 및 E 필드에 프래그먼트가 시작 프래그먼트인지, 중간 프래그먼트인지 또는 끝 프래그먼트인지를 나타냅니다.



B	E	Description
1	0	First piece of a fragmented user message
0	0	Middle piece of a fragmented user message
0	1	Last piece of a fragmented user message
1	1	Unfragmented message

Table 1: Fragment Description Flags

스트림 시퀀스 번호의 간격은 스트림 또는 연결 내의 프래그먼트가 삭제되고 있음을 나타낼 수 있습니다. Wirshark 필터는 SCTP 스트림의 차이를 식별하는 데 도움이 됩니다.

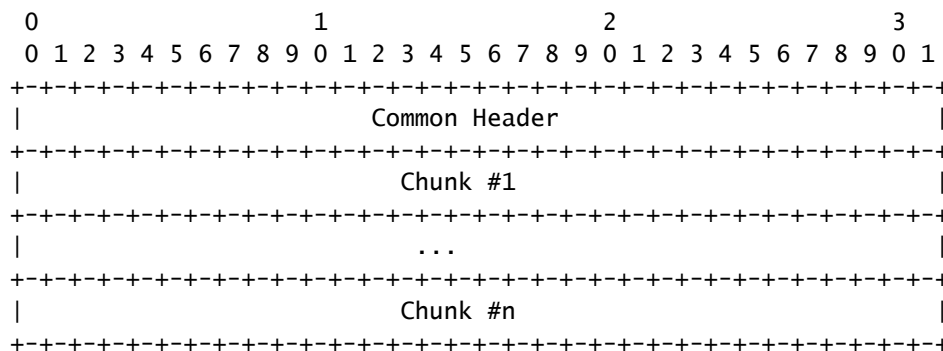
sctp.sack_gap_block_start or sctp.sack_gap_block_end

SCTP 청크 번들링

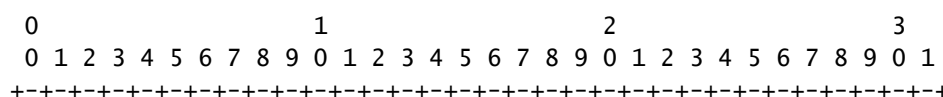
INIT, INIT ACK 및 SHUTDOWN COMPLETE 청크를 제외한 여러 청크를 최대 MTU 크기까지 하나의 SCTP 패킷으로 번들로 묶을 수 있습니다.

An SCTP packet is composed of a common header and chunks. A chunk contains either control information or user data.

The SCTP packet format is shown below:



각 SCTP 데이터 청크의 청크 길이는 각 데이터 청크 내에 나열됩니다.




```
[mme]ASR5500-2(config)# port ethernet 1/10
#exit
vlan 200
no shutdown
bind interface int1/10_slmme mme_ctx
#exit
vlan 201
no shutdown
bind interface int1/10_src mme_ctx
#exit
#exit
port ethernet 1/11
no shutdown
vlan 198
no shutdown
#exit
vlan 200
no shutdown
bind interface int1/11_slmme mme_ctx
#exit
vlan 201
no shutdown
bind interface int1/11_src mme_ctx
#exit
```

S1AP UE 무선 기능 IE 크기

MME 서비스 구성에서, S1AP UE Radio Capability IE 메시지 크기들이 구성된다. 기본값은 9000바이트입니다.

```
[context_name]host_name(config-mme-service)# s1-mme ue-radio-cap size 9000
```

사례 연구

다음은 구성된 SCTP 최대 MTU 크기에 맞게 SCTP 프래그먼트를 생성하는 프래그먼트화된 초기 컨텍스트 설정 요청/UE 기능 정보 메시지의 예입니다.

가입자는 SCTP 프래그먼트된 초기 컨텍스트 설정 요청 메시지 전송 후 전송 라우터에서 MME로 전송되는 ICMP 메시지 "프래그먼트화가 필요함"을 추적합니다.

No.	Time	Source	Destination	Info	Protocol	Stream identifier	Stream sequence number	Frame length on the wire
1	2024-10-18 06:45:46.481369410	MME	eNodeB	DATA (TSN=0) (Message Fragment)	SCTP	0x0001	11339	1522
2	2024-10-18 06:45:46.488853860	MME	eNodeB	DATA (TSN=1) (Message Fragment)	SCTP	0x0001	11339	1522
3	2024-10-18 06:45:46.488855090	MME	eNodeB	DATA (TSN=2) (Message Fragment)	SCTP	0x0001	11339	1522
4	2024-10-18 06:45:46.488856320	MME	eNodeB	DATA (TSN=3) (Message Fragment)	SCTP	0x0001	11339	1522
5	2024-10-18 06:45:46.488857560	MME	eNodeB	InitialContextSetupRequest, UECapabilityInformation, Paging	S1AP	0x0001,0x0000	11339,18839	1530
6	2024-10-18 06:45:46.489096060	Transport Router	MME	Destination unreachable (Fragmentation needed)	ICMP			82

프레임 5에서는 여러 SCTP 패킷(2)이 하나의 IP 패킷 아래에 함께 클러스터링됩니다.

```

> Frame 5: 1530 bytes on wire (12240 bits), 1530 bytes captured (12240 bits)
> Ethernet II, Src: Cisco_, Dst: Cisco_
> MultiProtocol Label Switching Header, Label:
> Internet Protocol Version 4, Src: MME, Dst: eNodeB
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
> S1 Application Protocol
> Stream Control Transmission Protocol
> S1 Application Protocol

```

첫 번째 데이터 청크는 E-Bit 정보 요소의 1개로 표시된 것처럼 프래그먼트된 메시지의 마지막 세그먼트입니다.

```

> Frame 5: 1530 bytes on wire (12240 bits), 1530 bytes captured (12240 bits)
> Ethernet II, Src: Cisco_, Dst: Cisco_
> MultiProtocol Label Switching Header, Label:
> Internet Protocol Version 4, Src: MME, Dst: eNodeB
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
  Source port: 36412
  Destination port: 36412
  Verification tag: 0xbe183285
  [Association index: 0]
  Checksum: 0xfb290f84 [unverified]
  [Checksum Status: Unverified]
  DATA chunk (ordered, last segment, TSN: 4, SID: 1, SSN: 11339, PPID: 18, payload length: 1367 bytes)
    > Chunk type: DATA (0)
    > Chunk flags: 0x01
      .... 0... = I-Bit: Possibly delay SACK
      .... .0.. = U-Bit: Ordered delivery
      .... ..0. = B-Bit: Subsequent segment
      .... ...1 = E-Bit: Last segment
    Chunk length: 1383
    Transmission sequence number (relative): 4
    Transmission sequence number (absolute): 3957018401
    Stream identifier: 0x0001
    Stream sequence number: 11339
    Payload protocol identifier: S1 Application Protocol (S1AP) (18)
    > Reassembled SCTP Fragments (7175 bytes, 5 fragments):
      Chunk padding: 00
  > S1 Application Protocol
  > Stream Control Transmission Protocol
  > S1 Application Protocol

```

B-Bit 및 E-Bit 정보 요소가 1로 표시된 것처럼 두 번째 데이터 청크는 프래그먼트된 메시지의 일부가 아닙니다.

```

> Frame 5: 1530 bytes on wire (12240 bits), 1530 bytes captured (12240 bits)
> Ethernet II, Src: Cisco_66:8c:90, Dst: Cisco_a1:d0:e3
> MultiProtocol Label Switching Header, Label:
> Internet Protocol Version 4, Src: MME, Dst: eNodeB
> Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
> S1 Application Protocol
v Stream Control Transmission Protocol
  v DATA chunk (ordered, complete segment, TSN: 5, SID: 0, SSN: 18839, PPID: 18, payload length: 73 bytes)
    > Chunk type: DATA (0)
    v Chunk flags: 0x03
      .... 0... = I-Bit: Possibly delay SACK
      .... .0.. = U-Bit: Ordered delivery
      .... ..1. = B-Bit: First segment
      .... ...1 = E-Bit: Last segment
    Chunk length: 89
    Transmission sequence number (relative): 5
    Transmission sequence number (absolute): 3957018402
    Stream identifier: 0x0000
    Stream sequence number: 18839
    Payload protocol identifier: S1 Application Protocol (S1AP) (18)
    Chunk padding: 000000
  > S1 Application Protocol

```

첫 번째 SCTP 데이터 청크의 길이는 1383바이트입니다. 두 번째 SCTP 데이터 청크의 길이는 89바이트이므로 각 개별 SCTP 패킷이 구성된 SCTP-Max-MTU-Size인 1500바이트를 초과하지 않습니다.

```

  > Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
    Source port: 36412
    Destination port: 36412
    Verification tag: 0xbe183285
    [Association index: 0]
    Checksum: 0xfb290f84 [unverified]
    [Checksum Status: Unverified]
  > DATA chunk (ordered, last segment, TSN: 4, SID: 1, SSN: 11339, PPID: 18, payload length: 1367 bytes)
    > Chunk type: DATA (0)
    > Chunk flags: 0x01
    Chunk length: 1383
    Transmission sequence number (relative): 4
    Transmission sequence number (absolute): 3957018401
    Stream identifier: 0x0001
    Stream sequence number: 11339
    Payload protocol identifier: S1 Application Protocol (S1AP) (18)
    > Reassembled SCTP Fragments (7175 bytes, 5 fragments):
      Chunk padding: 00
  > S1 Application Protocol
  > Stream Control Transmission Protocol
    > DATA chunk (ordered, complete segment, TSN: 5, SID: 0, SSN: 18839, PPID: 18, payload length: 73 bytes)
      > Chunk type: DATA (0)
      > Chunk flags: 0x03
        .... 0... = I-Bit: Possibly delay SACK
        .... .0.. = U-Bit: Ordered delivery
        .... ..1. = B-Bit: First segment
        .... ...1 = E-Bit: Last segment
      Chunk length: 89
      Transmission sequence number (relative): 5
      Transmission sequence number (absolute): 3957018402
      Stream identifier: 0x0000
      Stream sequence number: 18839
      Payload protocol identifier: S1 Application Protocol (S1AP) (18)
      Chunk padding: 000000
  > S1 Application Protocol

```

SCTP 패킷과 IP 헤더를 포함한 결과 IP 데이터그램의 총 크기가 구성된 IP MTU 크기인 2000보다 작기 때문에, 이러한 SCTP 청크는 MME의 IP 스택 레벨에서 한 IP 패킷 내에 그룹화됩니다.

솔루션

S1AP UE Radio Capability IE 메시지 크기는 컨피그레이션에서 기본값 9000바이트로 허용됩니다. 구성된 SCTP 최대 MTU 크기인 1500보다 작은 레벨에서 이러한 메시지를 전달하려면 SCTP 레이아웃에서 단편화가 발생해야 합니다.

sctp-max-mtu-size가 1500이면 전송된 모든 SCTP 패킷이 1500바이트를 초과하지 않음을 의미합니다.

IP 인터페이스 MTU 크기가 2000이면 모든 IP 패킷이 2000바이트를 초과할 수 없습니다.

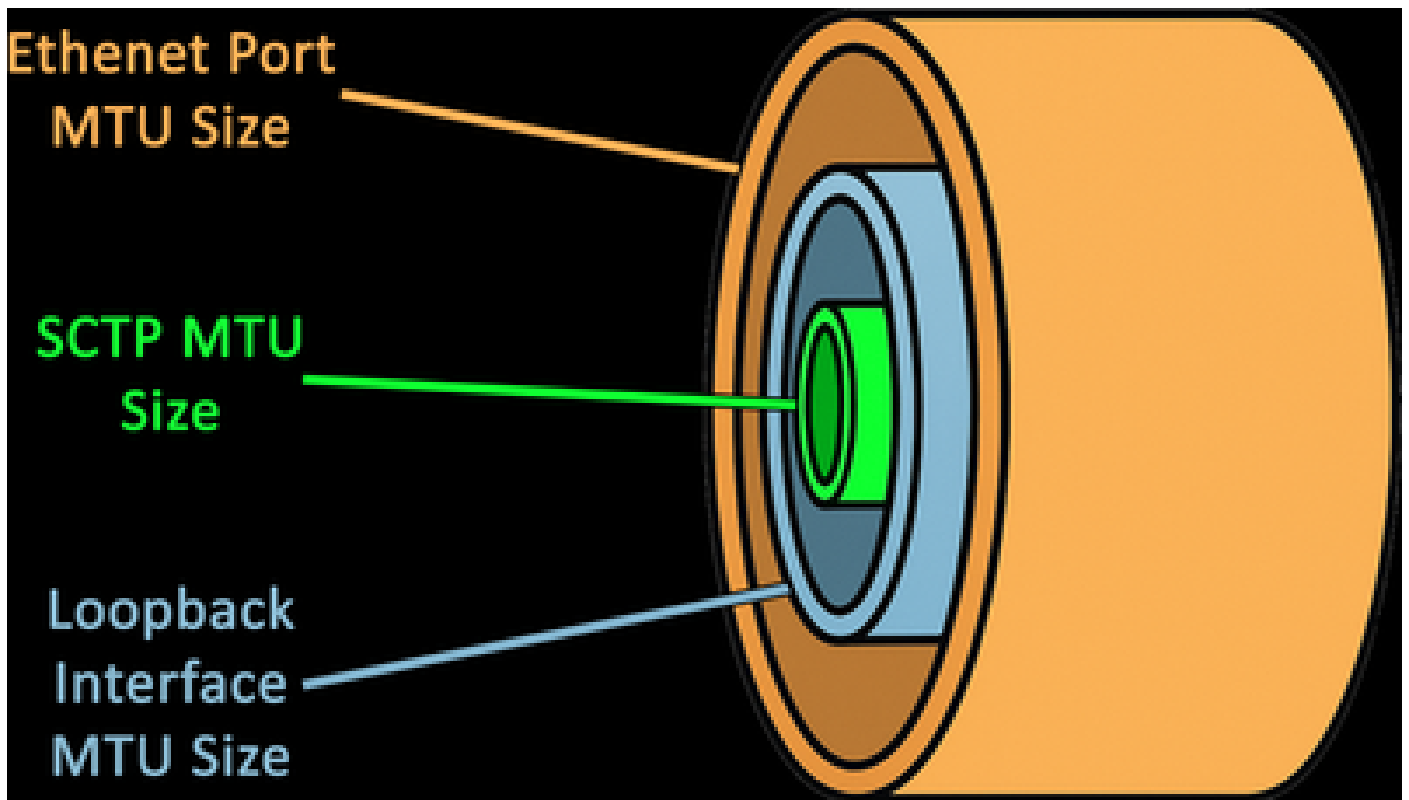
하나의 IP 패킷에는 여러 SCTP 패킷이 있을 수 있고 각 SCTP 패킷에는 여러 청크가 있을 수 있습니다. 개별 SCTP 패킷 크기가 SCTP MTU 크기에 부합하고 함께 결합된 모든 SCTP 패킷의 총 크기가 IP MTU 크기에 부합하면 노드는 예상대로 작동합니다.

다음과 같은 경우 노드 내에서 패킷 삭제는 발생하지 않습니다.

- 패킷 추적 프레임 내의 SCTP 청크의 총 크기가 SCTP-Param-Template에서 구성된 SCTP-

Max-MTU-Size 값보다 작으며

- SCTP PDU + IP 헤더의 총 값이 노드에서 구성된 인터페이스 MTU 크기보다 작습니다.

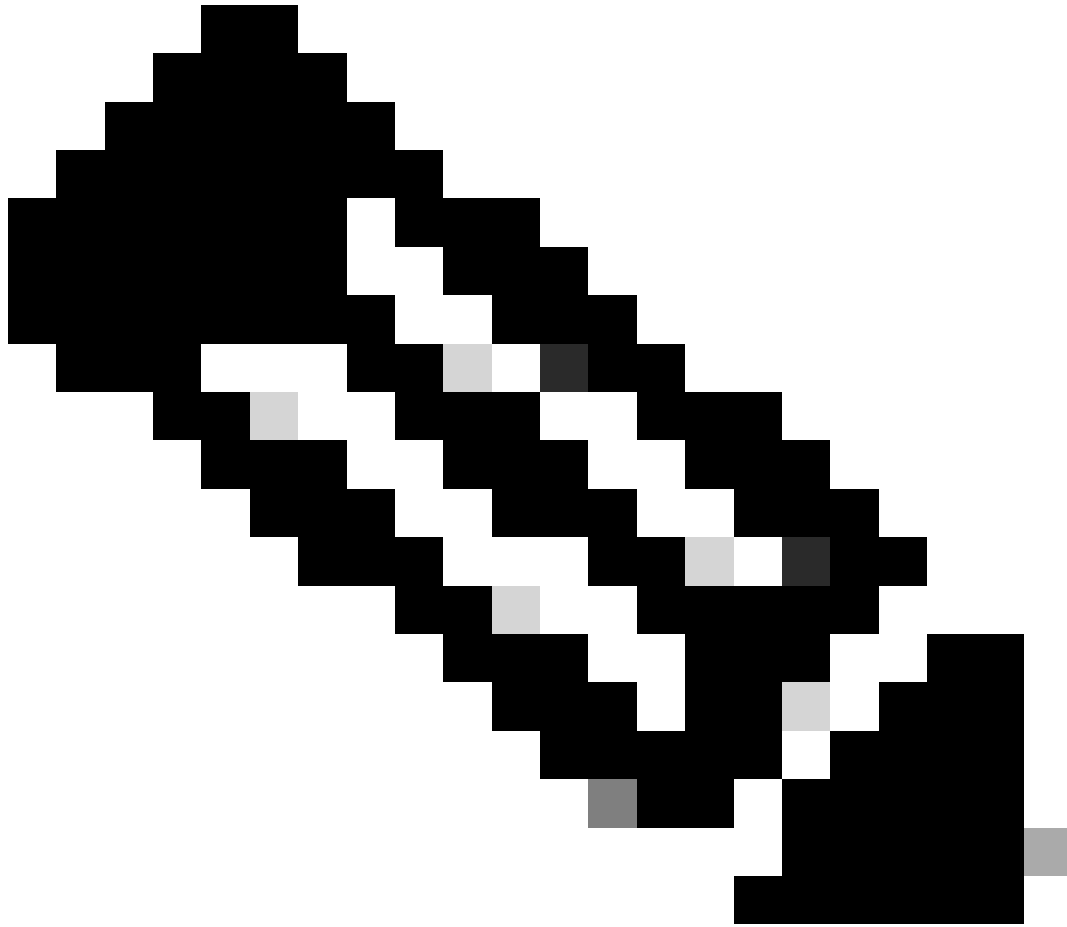


이 사례 연구에서는 전송 라우터에 대한 조사 결과 전송 라우터의 IP MTU 크기가 1500인 것으로 나타났습니다. 그 사이의 전송 노드는 MTU가 1500이므로 전송 노드의 IP 인터페이스에 의해 패킷이 삭제되어 전송 라우터가 "Destination Unreachable"이라는 메시지를 MME에 전송하도록 촉구했습니다.

삭제 해결을 위한 해결 방법

해결 #1: SCTP 최대 MTU 크기 감소

sctp-max-mtu-size를 더 낮은 값으로 구성하여 SCTP MTU 크기를 줄입니다.



참고: sctp-max-mtu-size를 낮출 때는 sctp-start-mtu-size가 sctp-max-mtu-size보다 작거나 같은 값으로 구성되어야 합니다.

예: sctp-param-template S1_MME_SCTP를 수정합니다(sctp-start-mtu-size from 1500 to 1460).

해결 #2: 전송 노드 MTU 크기를 1500보다 크게 증가

관련 정보

- [RFC 4960 스트림 제어 전송 프로토콜](#)
- [MME 관리 가이드, StarOS 릴리스 21.28 장: UE 무선 기능 IE 크기](#)
- [명령줄 인터페이스 참조, 모드 E - F, StarOS 릴리스 21.28 장: 이더넷 인터페이스 컨피그레이션 모드 명령 IP MTU 크기](#)
- [명령줄 인터페이스 참조, 모드 E - F, StarOS, 장: 이더넷 인터페이스 컨피그레이션 모드 명령:](#)

ip.mtu

- SCTP 매개변수 템플릿 컨피그레이션 모드 명령: sctp-max-mtu-size
- Cisco TechNote - StarOS MTU 인터페이스, APN 및 로컬 가입자 구성
- SCTP 및 MTU SR 697666400(UE Idle to Active mode not working)(MME에서 서비스 요청 디코딩 오류가 표시됨) 논의 SR

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.