

مزلحلا طاقسإ تاي لمع ءاطخأ فاشك تسأ MTU ىصقألا SCTP مزجحب ةقلعتملا اهحالصإو

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[ةيظشت](#)

[SCTP ةمزح ةمزح عي مزجت](#)

[مزجحلل ديذجت ىلع رثؤت يتلا ةئيهتلا تاي لمع](#)

[مزجحلل SCTP-Param-Template SCTP MTU](#)

[MME قاي سلا تئيرثيا ةمزح او نيوك](#)

[ذفنملا تئيرثيا ةكبشلا \(MTU\) لقنللا ىصقألا دحلل ةدجو مزج](#)

[IE مزجح ةئيكما ىكل سالا S1APUE](#)

[ةلحلا ةسارد](#)

[لحللا](#)

[طوق سالا تالاح لحلل ةليدب لولح](#)

[SCTP لوكوتورب ربع \(MTU\) لقنللا ىصقألا دحلل ةدجو مزجحلل ىصقألا دحلل لىلقن: 1 # لحللا](#)

[1500 نم رثكأ ىلا MTU لقنللا ةدقع مزجح ةدايزب مق: تئيكما لحللا](#)

[ةلص تاذ تامولعم](#)

ةمدقملا

ةي فيك و Cisco MME في لاصتالا تاعومجم ةئزجت و SCTP ةئزجت تاي لآ دنتسملا اذه فص ي
مزلحلا طاقسإ تاي لمع ىلع عي مزجتلا و ةئزجتلا ريثأت.

ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال.

ةمدختسملا تانوكملا

ةي لالتلا ةي داملا تانوكملا و جماربلا تارادصإ ىلا دنتسملا اذه في ةدراولا تامولعملا دنتست

- 21.28.m18 رادصإلا، QVPC-SI جم انرب

ةصاخ ةي لمعم ةئيب في ةدوجوملا ةزهجألا نم دنتسملا اذه في ةدراولا تامولعملا عاشنإ مت

تنالك اذا. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتمل ريثاتلل كمهف نم دكأتف، ليغشتال ديقتك كبش

ةيساسا تامولعم

ةكبش قوف لمعي قووثوم لقن لوكتورب وه (SCTP) ثبالا يف مكحتلل لاسرالا لوكتورب دحلا ةدحو مجح عم قفاوتت شيحب تانايبلا ةئزجتب موقي نا نكمي و IP. لثم ةلصتم ريغ مزح يف ةددعتمل مدختسمل لئاسر عيمجتو هفاشتكا مت يذلا راسملل (MTU) لقنلل يصقألا تالاح ةجالعمل نيقتقيرط دنتسمل اذه مدقي. لتكلا عيمجت مادختساب ةدحاو SCTP ةمزح راسملل (MTU) لقنلل يصقألا دحلا ةدحو دويق ببسب ثدحت يتال مزحلا طاقسا

امب، ةمزحلا طاقسا تاي لمع حيضوتل ةليسوك عيمجتلاو ةئزجتلا تايلا ةلالا ةسارد ضرعت SCTP مجح نيوكتب ببسب نم الدب، Cisco MME جراخ ثدحت يتال مزحلا طاقسا تاي لمع كلذ يف Max MTU.

ةداعاو ةئزجتلا) 6.9 رادصالا (ثبالا يف مكحتلل لاسرالا لوكتورب) RFC 4960 راي عمل اقفو (عيمجتلا):

ةلاسر مجح ناك اذا مدختسم ةلاسر ةئزجت اهيلع بجي، ةئزجتلا معدت ةياهن ةطقن تنالك اذا" MTU مجح ةرداصل SCTP ةمزح مجح زواجت يف ببستي اهلاسرلا متيس يتال مدختسمل لايلا.

ةدحاو SCTP ةمزح يف ةددعتمل SCTP تانايب تاعومجم عيمجت نكمي، كلذلى ةفاضلا ابو SCTP ةمزح كلذ يف امب، جتانال IP تانايب ططخمل يلامجال مچحل نوكي نا بجي. ةرداص لىل MTU راسم نيوكتب متي، MME لىل. يلالا راسملل MTU يواسي وأ كلذ نم لقأ، IP سوؤرو مزل هذه ةجالعمل موقت يتال IP ةهجاو

ةيظشت

فرعم ةطساوب اهنم لك فيرعت متي، SCTP نارتقا يف ةددعتم تاقفدت كانه نوكي نا نكمي نكمي. ددحم SCTP قفدت نمض عزج لكل رمالا (SSN) قفدل لسلسلت مقرر فرعي. (SI) قفدل (TSN) لاسرالا لسلسلت مقرر فرعي. SCTP قفد سفن ةددعتمل لمعل تاسلج مدختست نا لملالاب SCTP نارتقا نمض عزج لكل بيترتلا

عزجال وه عزجال ناك اذا ام لىل E و B يلحق يف SCTP ةلومح تانايب طخ ريشي، هئزجت دنع يف رطلال عزجال وأ طسألا عزجال وأ يلالا

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+++++
|  Type = 0      | Reserved|U|B|E|      Length      |
+++++
|                               TSN                               |
+++++
|  Stream Identifier S      |  Stream Sequence Number n      |
+++++
|                               Payload Protocol Identifier      |
+++++
\

```

```

/                               User Data (seq n of Stream S)                               /
\                               \
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

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

وأراغب إلى اخذ ألقاس م ت ي هنا إلى قفد ل ل س ل س ت م ا ق ر أ ي ف ت ا و ج ف ل ر ي ش ت ن أ ن ك م ي
 S C T P : ت ا ق ف د ت ي ف ت ا و ج ف ل د ي د ح ت ي ل ع W i r s h a r k ت ا ح ش ر م د ع ا س ت ن أ ن ك م ي . ن ا ر ت ق ا ل ا

sctp.sack_gap_block_start or sctp.sack_gap_block_end

SCTP ة م ز ح ة م ز ح ع ي م ج ت

ل ق ن ل ل ي ص ق أ ل د ح ل ا ة د ح و م ج ح ي ت ح ة د ح ا و S C T P ة م ز ح ي ف ة د د ع ت م ت ا ع و م ج م ع ي م ج ت ن ك م ي
 : ة ل م ا ك ل S h u t d o w n و I n i t A c k و I N I T ت ا ع و م ج م ا ن ث ت س ا ب ، (M T U)

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

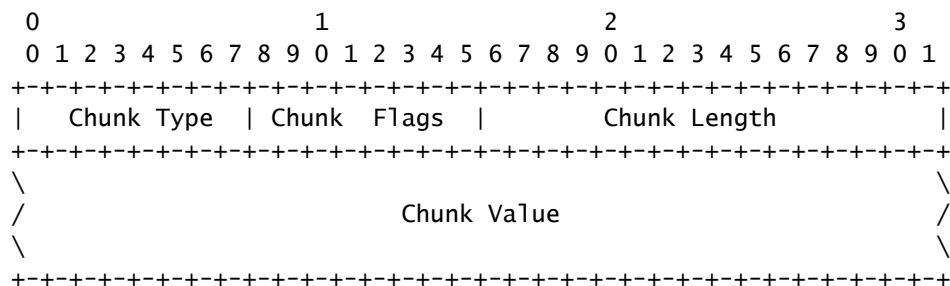
The SCTP packet format is shown below:

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Common Header                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Chunk #1                                   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               ...                                       |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               Chunk #n                                   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

تانايب ةومجم لك لخاد SCTP تانايب ةومجم لكل ةومجم لوط درس متي



مجم ل دي دحت ىل ع رثؤت ي ت ل ةئيه ت ل تاي ل م ع

مجم ل SCTP-Param-Template SCTP MTU

SCTP-max-mtu-size رايخ مادختساب SCTP-Max-MTU مجم نيوكت متي SCTP-Param-Template في مجم ل وه تي اب 1500. تي اب ل اب ه نيوكت متي ي ذل ، SCTP-start-mtu-size رايخ و او size MTU: ء د ب ل ي ضا ر ت ف ا ل SCTP Max MTU مجم و SCTP ي ضا ر ت ف ا ل

```

Exec > Global Configuration > SCTP Parameter Template Configuration
[Local]ASR5500-2# sctp-param-template template_name
[Local]ASR5500-2(sctp-param-template)# sctp-max-mtu-size 1500
[Local]ASR5500-2(sctp-param-template)# sctp-start-mtu-size 1500

```

MME قاي س ب SCTP-Param-Template ن ا ر ق ا متي ، MME ة م د خ ي ف

```

Exec > Global Configuration > Context Configuration > MME Service
[mme]ASR5500-2(config-mme-service)# associate sctp-param-template S1_MME_SCTP

```

MME قاي س ل ت ن ر ث ي ا ة ه ج ا و ني و ك ت

ب و غ ر م ل IP MTU مجم ع MME ة م د خ ل ة ط س ا و ب ا ه م ا د خ ت س ا متي ي ت ل ة ه ج ا و ل ني و ك ت متي (ي ضا ر ت ف ا ل وه 1500) تي اب ل اب

```

Exec > Global Configuration > MME Context Configuration
[mme]ASR5500-2(config-ctx)# interface int1/10_s1mme
[mme]ASR5500-2(config-if-eth)# ip address 10.5.203.195 255.255.255.254
[mme]ASR5500-2(config-if-eth)# ip mtu 2000
[mme]ASR5500-2(config-if-eth)# exit

```

ذفنم لل تنرثي إكبش ل (MTU) لقنل لصقأال دحلأ دحو مچ

قبطي يذلأ تنرثي إذفنم ب اذه MME قاي س طبر متي،ماعال نيوكتال عضو ي في (يضا رتفالا 1500):

```
[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
```

مچ IE ةردق يكلسال S1AP UE

S1AP UE يكلسالال ةردق لاب ةصاخال IE لئاسر ماحأ نيوكت متي، MME ةمدخ نيوكت ي في تياب 9000 يه ةيضا رتفالا ةميقلال:

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

ةلأال ةسارد

،أزجمال يلوأال قاي سال دادعإ مادختسإ/بلط ةردق لوح تامولعم ةلاسر رل ع لاثم ي لي امي فو، هن يوكت مت يذلأ Sctp Max MTU مچ ع ق فاوتت ل SCTP ءانجأ يهو.

MME وحن لقنلأ هجوم نم "ةبولطمال ةئجتال" ICMP ةلاسر عاجرا متي، كرتشمال بقعت ي في SCTP. ءانجم يمازلإ قاي س دادعإ بلط ةلاسر لاسرا دعب

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

عدح او IP ةمزح تحت اعم (2) ةددعت الم SCTP مزح عي مجت متي 5 راطإل ا في

```
> 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
```

1 ةمالعالب حضوم وه امك ،ةأزجم الم ةلاس رل ك لت نم ريخأل اعزل ا في تاناي بلل لىل وأل ةعومجم الم ة. ني نورث ك لإل ت بلل تامولول عم رصنع في

```
> 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
```

و B-Bit تامولول عم رصان عب حضوم وه امك ،ةأزجم ةلاس ر نم اعزج ةي ناثل تاناي بلل ةعومجم دعت ال 1 مقرب E-Bit:

```

> 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
▼ 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

```

تانايب ةومجم لوط غلب ي. لوطلاب تياب 1383 ىل عىلوالا SCTP تانايب ةومجم يوتحت
 م تيذلا SCTP-Max-MTU مجح ةيدرف SCTP ةمزح لك زواجتت ال لكذل ،تياب 89 ةيناثلا SCTP
 :تياب 1500 هنيوكت

```

  ▾ 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

```

رغصاً IP سوؤرو SCTP ةمزنح كلذيف امب ،جتانل IP تانايب ططخمل يللامجال مرجال نأل ارظن IP ةمزنح لخاد اعم هذه SCTP تاعومجم عيمجت متي ،هنيوكت مت يذال 2000 غالبال IP MTU مرجح نم MME لىل IP سدكم يوتسم يف ةدحاو

لحل

ةيضارتفال ةميقلل دنع نيوكتل يف S1AP UE Radio Capability IE لئاسر ماجحأب حمسي نم رغصاً يوتسم لىل لئاسرل هذه لمحل SCTP ةقبط يف ةئزتلل ثودح بجي .تيا 9000 1500 غلب يذلاو هنيوكت مت يذال SCTP Max MTU مرجح

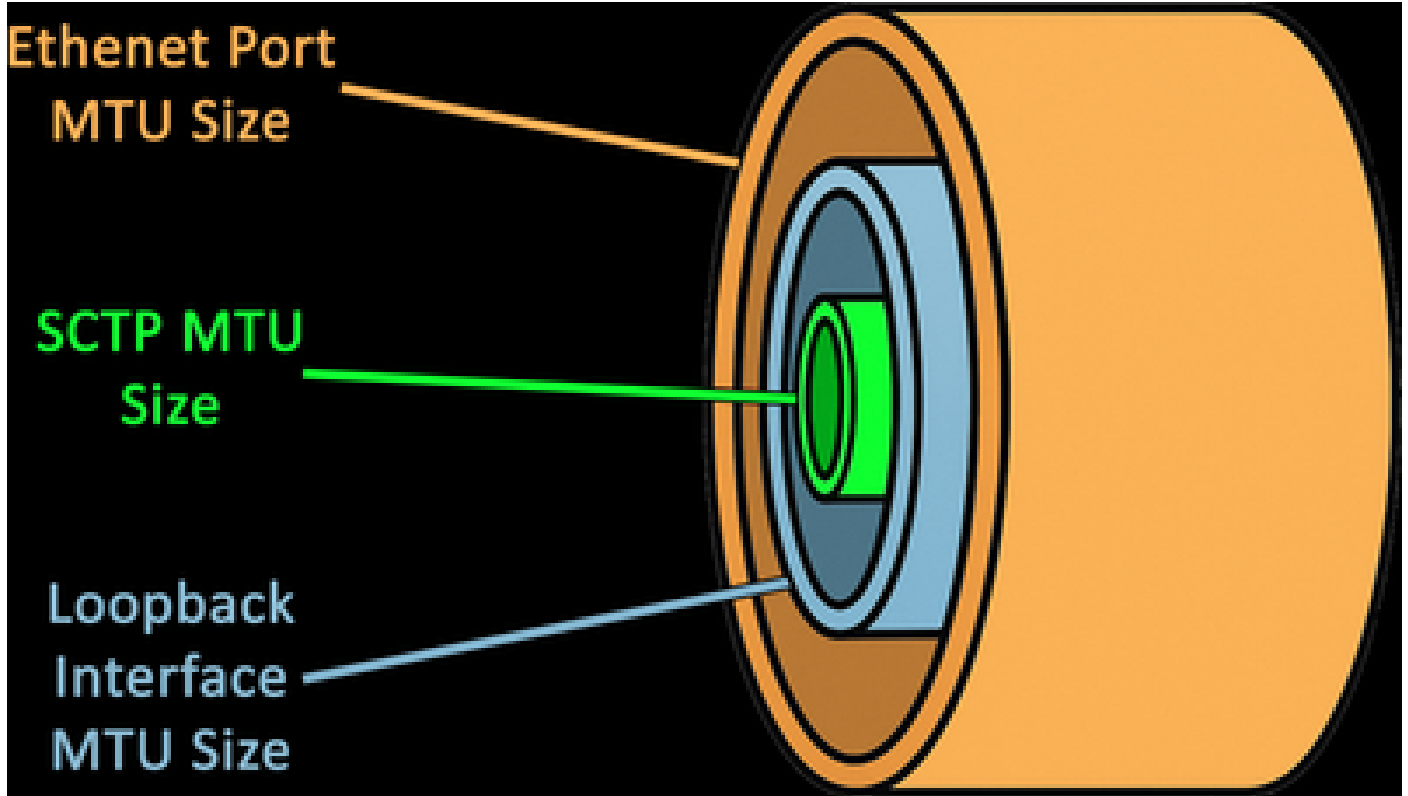
1500 زواجتت ال اهلاسرل متي SCTP ةمزنح يأ نأ 1500 نوكتي يذال SCTP-Max-MTU مرجح ينعي .تيا

زواجتت نأ نكمي ال هنا 2000 غلب يذال IP ةهاول (MTU) لقنلل لصقأال دحلل ةدحو مرجح ينعي .تيا 2000 IP ةمزنح ي

تاعومجم SCTP ةمزنح لكل نوكتي نأ نكمي وةدعت SCTP مزح ةدحاو IP ةمزنحل نوكتي نأ نكمي عيمجل يللامجال مرجحلاو SCTP MTU مرجح ب طبترم ةيدرفل SCTP ةمزنح مرجح نأ املاط .ةدعت مزح عقتوم وه امك فرصتت ةدقعل نإ ،IP MTU مرجح عم قفاوتي ةعمتجم SCTP مزح

إذا، ةدقعل لخد مزحل طاقسإ تايلمع ثدحت ال

- مت يتيلا ةميقل نم لقاً ةمزلح عبتت تاراطإ لخد Sctp تاعومجمل يلامجال مجحل نوكي و Sctp-Param-Template في Sctp-Max-MTU مجحل اهنوكت
- يلع اهنوكت مت يتيلا ةهجالل MTU مجح نم لقاً IP سار Sctp PDU ةميقل يلامجال ةدقعل.

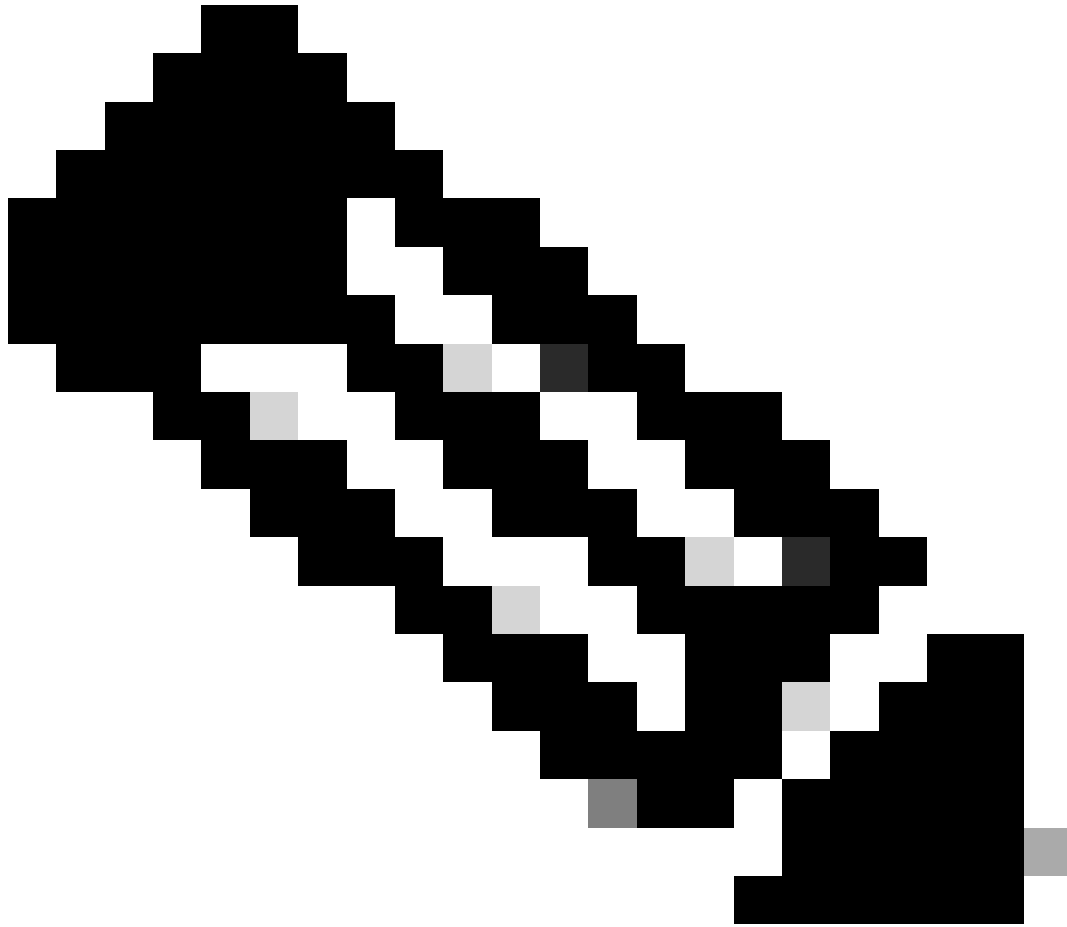


هيدل لقنللا هجوم نأ نع لقنللا هجوم في قيقحتلا فشك، انب صاخلا ةلاحلا ةسارد لاثم في ةطساوب مزحل طاقسإ مت، MTU 1500 اهل نيب امي في لقنللا ةدقع نأ امبو. IP MTU 1500 مجح ةهجالا" يلى ريشتم MME يلى ةلسر لاسر لقنللا هجوم نم بلطو، لقنللا ةدقع يلى IP ةهجالا "اهيلى لوصول رذعتي يتيلا".

طوقسلال تالاح لحل ةليدب لولح

ربع (MTU) لقنلل يصولال دحلا ةدحو مجحل يصولال دحلا ليلقت: 1 # لحل Sctp لوكوتورب

يرت ال يتح لقاً ميقل يلى Sctp-Max-MTU مجح نيوكت لالخد نم Sctp MTU مجح ليلقتب مق طاقسإ تايلمع.



ىل ع sctp-start-mtu مچح نيوكت نم اضيأ دكأت ، sctp-max-mtu مچح ضفخ دنع :ةظحال م
sctp-max-mtu مچح يواست وأ نم لقأ ةميقي .

، (1460 ىل 1500 نم sctp-start-mtu-size S1_mme_sctp sctp-param-template لي دعيت :لاثم

1500 نم رثكأ ىل MTU لقنلا ةدقع مچح ةدايزب مق :يناثلا لجال

ةلص تاذا تامولعم

- [RFC 4960 راي عمل اعم قفاوتملا ثبلا يف مكحتلل لاسرالا لوكوتورب](#)
- [مدختسملا ويدارلا ةردقل IE مچح :لصفلا ، StarOS نم 21.28 رادصلا ، MME ةرادا ليلد](#)
- [:لصفلا 21.28 رادصلا StarOS ليغشتلا ماطن ، E - F عاضوأل ، رماوأل رطس ةهجاو عجرم](#)
- [IP MTU size تنرثيالا ةهجاو نيوكت عضورم](#)
- [ةهجاو نيوكت عضورم اوأ :لصفلا ، StarOS ، E - F عاضوأل ، رماوأل رطس ةهجاو عجرم](#)

ip mtu: نت نرثيالا

- SCTP: sctp-max-mtu-size ةم لعم بلاق ني وكت عض ورم او
- Cisco TechNote - ةهچ او ني وكت APN، و StarOS MTU، نئي لجملا ني كرت ش ممل او
- SR 69766400 (UE لماخ) سق اني يذلا SR و SCTP شق اني يذلا SR (لمعي ال طشنلا عضولا يلا لماخ UE) (MME يلع رهظي يذلا ةمدخلا بلط ري فشت كف)

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت
م ل ا ع ل ا ا ح ن ا ع ي م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل آل ا ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ء ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا