

ةيلخادلل FirePOWER تالوحم تاعومجم نيوكت اهتحص نم ققحتلاو ةنمآلا

تايوتحملا

[ةمدقملا](#)

[ةيساسآلا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسآا تامولعم](#)

[مراظنلا ةينب يلع يوتسملا ةيلاع ةماع ةرظن](#)

[ةيلخادلل تالوحملا تايلمع يلع يوتسملا ةيلاع ةماع ةرظن](#)

[طاقتللا طاقنو ةمزحلا قفدت](#)

[Firepower 4100/9300 يلع ققحتلاو نيوكتلا](#)

[ذفنم ةانق ةهجو وأ ةيدام ةهجو يلع ةمزحلا طاقنتلا](#)

[ةيلخدل ةجوللا تامهجو يلع ةمزحلا طاقنتلا](#)

[قيبطتلا ذفانمو قيبطتلا يلع ةمزحلا طاقنتلا](#)

[ذفنم ةانق ةهجو وأ ةيدام ةهجو ةيعرف ةهجو يلع ةمزحلا طاقنتلا](#)

[مزحلا طاقنتلا ةيفصت لماع](#)

[Firepower 4100/9300 يلخادلل لوجملا طاقنتلا تافلعم عيمجت](#)

[يلخادلل لوجملا ةمزح طاقنتلا لئاسرامملا لصف أو ديدحت و تاداشرا](#)

[3100/4200 نمآلا ةيامحلا رادج يلع ققحتلاو نيوكتلا](#)

[ذفنم ةانق ةهجو وأ ةيدام ةهجو يلع ةمزحلا طاقنتلا](#)

[ذفنم ةانق ةهجو وأ ةيدام ةهجو ةيعرف ةهجو يلع ةمزحلا طاقنتلا](#)

[ةيلخادلل تامهجو يلع ةمزحلا طاقنتلا](#)

[مزحلا طاقنتلا ةيفصت لماع](#)

[نمآلا ةيامحلا رادج يلخادلل لوجملا طاقنتلا تافلعم عيمجت](#)

[يلخادلل لوجملا ةمزح طاقنتلا لئاسرامملا لصف أو ديدحت و تاداشرا](#)

[ةلصت اذ تامولعم](#)

ةمدقملا

حاتفم يلخاد Secure Firewall ل او، FirePOWER ل نم ققحتلاو ليكشتلا ةقيثو اذه فصي
ضبق يلع.

ةيساسآلا تابلطتملا

تابلطتملا

طاقنتلا ليلحتو ةيساسآلا جتنملا ةفرعم

عمدختسمل تانوكملا

صاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنم تنانك اذإ. (يضارتفا) حوسمم نيوكتب دنتسمل اذه يف عمدختسمل ةزهجال عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكاتف ، ليغشتلا ديقتك تبش

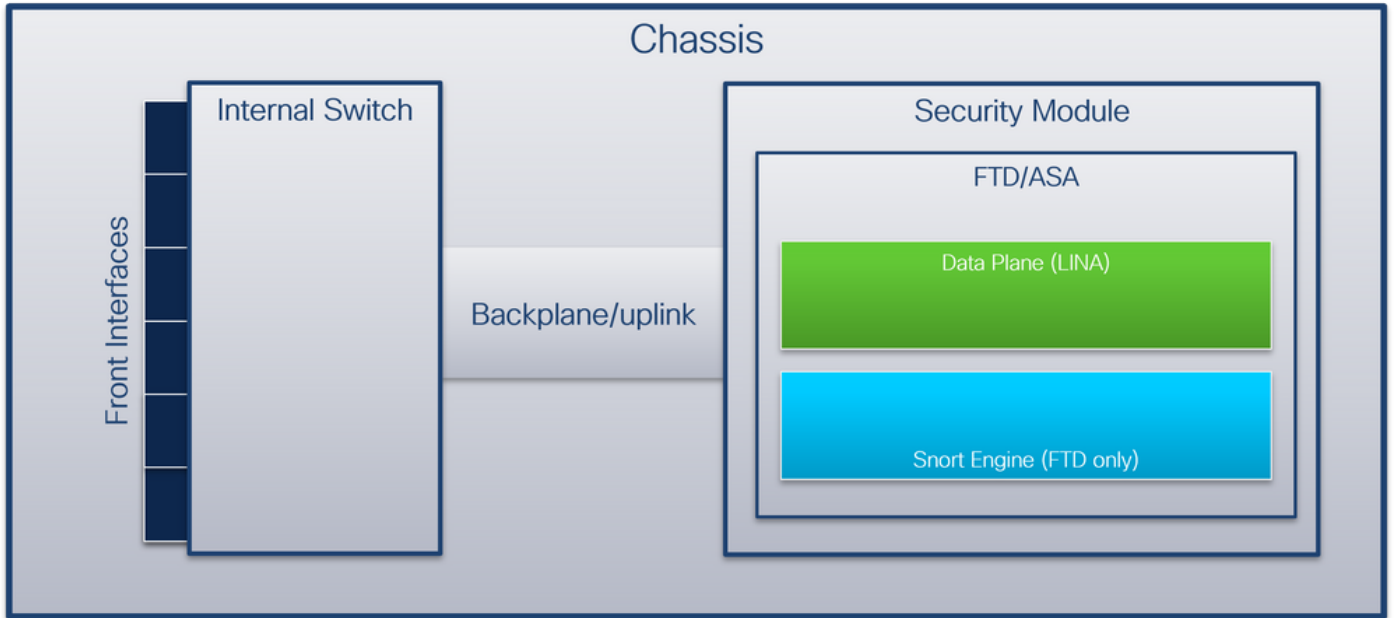
ةيلاتلا ةيدامل تانوكملا وجماربال تارادصلا دنتسمل اذه يف ةدراول تامولعمل دنتست

- Secure Firewall 31xx و 42xx
- Firepower 41xx
- Firepower 93xx
- Cisco نم 2.12.0.x (FXOS) نمال ليغشتلل لباقلا ليغشتلا ماظن
- Cisco 7.2.0.x، 7.4.1-172 نم (FTD) ةيامل رادج ديهت نع نمال عافدل
- Cisco 7.2.0.x، 7.4.1-172 نم (FMC) نمال ةيامل رادج ةرادك زكرم
- Cisco 9.18(1)x و 9.20(x) فكتلل لباقلا نامال زاغ
- Wireshark 3.6.7 (<https://www.wireshark.org/download.html>)

ةيساسا تامولعمل

ماظنلا ةينب يلع يوتسمل ةيلع ةماع ةرظن

نم ال ةيامل رادجو Firepower 4100/9300 ةينب روصت نكمي ، ةمزلال قفدت روظنم نم لكشلا اذه يف حضورم وه امك 3100/4200:



تانوكملا هذه لكهلا نمضتي

- ليصوت متي .سكعلاو قيبطتلا لىل ةكبشلا نم ةمزلال هيجوت ديعي - ليخادلا لوجملا ةكبشلا تادحو و اجمدملا ةهجال ةدحو لىل ةدوجوملا ةيامل ال تاهجال ليخادلا لوجملا تاهجال ةلثمأ .تالوجملا ، لاثملا لىبس لىل ، ةيخرال ةزهجال اب لاصتال او ةيخرال اينقت افيرعت تسيل "ةهجال" ن .كلذ لىل امو ، 2/4 تنرثي او ، 1/1 تنرثي يه ةيامل ال ةيخرال ةزهجال اب ةلصتال تاهجال لىل زيمتل همادختسلا متي ، دنتسمل اذه يف .ايوق

تالصلولا تاهجاو وأة فيفلخلا ءحوللا نم

- لوحملاب (SM) ءة طمنللا نامألا ءءو لصل ءة لءاء ءه جاو - ءلصلوا وأة فيفلخلا ءحوللا فيلءاءلا
- رورم ءكء راسم رفو ء 3100/4200 نمألا ءة طمنللا راءءل ءة لءاء ءه جاو - ءراءلا ءلصلو قءب طءلا ءلءاءلا لوحمللا نءب ءراءلا ءانا ب

ءلء ءالصلولا تاهجاو و FirePOWER 4100/9300 ءلء ءة فيفلخلا ءحوللا تاهجاو لوءءلا اءه ءضو ب ءراءلا ءة طمنللا راءءل 3100/4200:

ءة صنملا	ءاءءو ءء نامألا ءة طمنللا ءموءءملا	ءحوللا تاهجاو ءالصلولا/ءة فيفلخلا	لءلصلو ءاهجاو ءراءلا	ءاهجاو قءب طءلا ءة نءب ءملا
Firepower 4100 (ءانءءءاب) Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	رفو ءم رءء	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	رفو ءم رءء	Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	رفو ءم رءء	Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1 Internal-Data0/0 Internal-Data0/1
Secure Firewall 3100	1	SM1: in_data_uplink1	in_mgmt_uplink1	Internal-Data0/1 ءراءلا 1/1


```
udld disable
no shutdown
```

متي و. قيبطت اللى طببرلا لسري نأ تلمعت ساو يلخاد حات فم لبا تلخدا اضيأ VN-tag ال
ايودي اهرييغت نكمي الو ماظنلا ةطساوب ايئاقلت اهنيوكت

قيبطت اللى لخدني. قيبطت اللى عم VN-tag ةمالعو ذفنم لبا ةصاخ ال VLAN ةمالع ةكراشم مت
نم طبرملتسي ام دنع. ةمزح لك في VN-tags تامالعو و جورخ ال ةهجاوب ةصاخ ال VLAN تامالعو
ةقاطب نراق جورخ ال ارقى حات فم لبا، نراق ةيفللخ ال ةحول اللى عل يلخاد حات فم لبا قيبطت ال
ةقاطب ال VN- و ةقاطب VLAN ءانيم لدرجي، نراق جورخ ال او قيبطت ال نيعي، VN-tag ال و VLAN
ةكبش اللى طببرلا لسري و.

Secure Firewall 3100/4200

لبق نم ذفنم لبا ةصاخ ال VLAN ةكبش ةمالعو مادختسا متي، Firepower 4100/9300 في امك
ةهجاو فيرعتل يلخاد ال لوجم ال

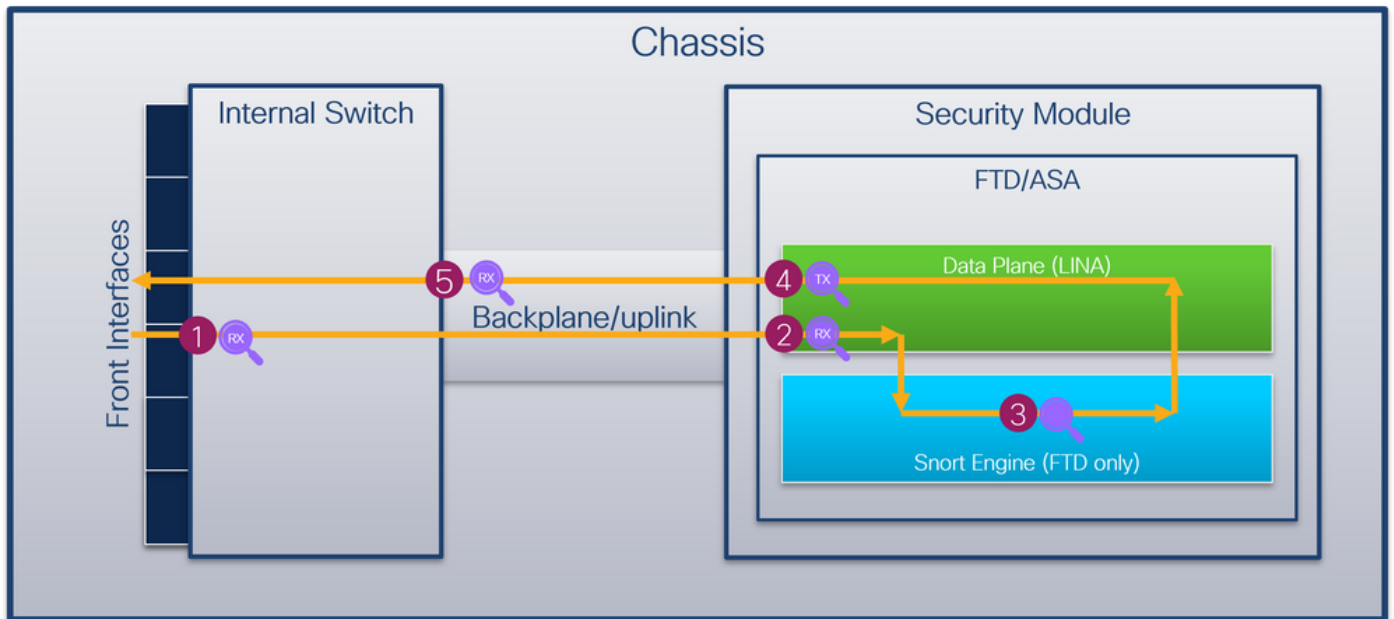
VLAN تامالعو قيبطت اللى لخدني. قيبطت اللى عم ذفنم لبا ةصاخ ال VLAN ةمالع ةكراشم مت
لعل يلخاد حات فم لبا قيبطت اللى نم طبرملتسي ام دنع. ةمزح لك في جورخ ال ةهجاوب ةصاخ ال
ءانيم لدرجي، نراق جورخ ال نيعي، ةقاطب VLAN نراق جورخ ال ارقى حات فم لبا، نراق ةلصول
ةكبش اللى طببرلا لسري و، ةقاطب VLAN.

طاقات اللى ةمزح ال قفدت

3100 نم ال ةي امحل رادجو و Firepower 4100/9300

لوجم ال تاهاو اللى ةمزح ال Secure Firewall 3100 Firewalls و Firepower 4100/9300 نم لك طقت لي
يلخاد ال.

قيبطت اللى لخدني اللى لخدني ةمزح ال راسم اللى ةمزح ال طاقن ال طاقن لكش ال اذو حضوي



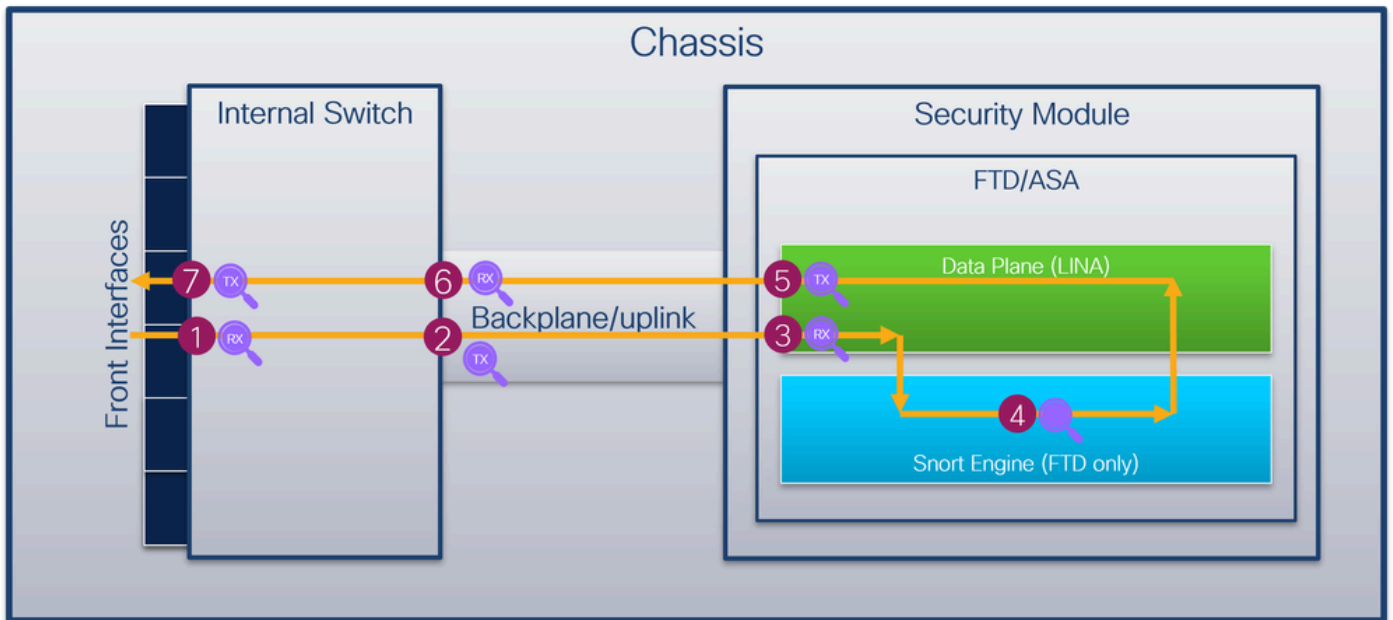
يه طاقتلالا طاقن:

1. قلمصتم ةهجاو يآ يه ةيمامألا ةهجاو. ةيلخادلا ةيمامألا لوحملا ةهجاو ةهجاو طاقتلا ةطقن. تالوحملا لثم ريظنلا ةزهجأب.
2. تانايبلا يوتسم ةهجاو لخدم طاقتلا ةطقن.
3. طروشلا طاقتلا ةطقن.
4. تانايبلا يوتسم ةهجاو جرم طاقتلا ةطقن.
5. ةحوللا وأ ليصوتلا ةهجاو موقت. لخدم طاقتلا ةطقن وأ ةيلخاد ةيلفلخ ليصوت ةحول. قيبتلاب يلخادلا لوحملا ليصوتب ةيلفلخلا.

وأ ةكبشلا نم ملتسي طبلا طقف اذه. ضبق يلع نراق لخدم طقف يلخاد حاتفملا دناسي موعدم ريغ جورخلا مزح طاقتلا. ضبق يلع تنك عيطتسي قيبتلا ASA/FTD ل نام.

Secure Firewall 4200

اذه حضوي. يلخادلا لوحملا تاهجاو يلع 4200 Firewalls نمألا ةياملحلا راج معد ةمزح طاقتلا قيبتلاو لكيهلا لخاد ةمزحلا راسم يلع ةمزحلا طاقتلا طاقن لكشلا:



يه طاقتلالا طاقن:

1. قلمصتم ةهجاو يآ يه ةيمامألا ةهجاو. ةيلخادلا ةيمامألا لوحملا ةهجاو ةهجاو طاقتلا ةطقن. تالوحملا لثم ريظنلا ةزهجأب.
2. يلخادلا لوحملا ةيلفلخلا ةحوللا ةهجاو جرم طاقتلا ةطقن.
3. تانايبلا يوتسم ةهجاو لخدم طاقتلا ةطقن.
4. طروشلا طاقتلا ةطقن.
5. تانايبلا يوتسم ةهجاو جرم طاقتلا ةطقن.
6. ةحوللا وأ ليصوتلا ةهجاو موقت. لخدم طاقتلا ةطقن وأ ةيلخاد ةيلفلخ ليصوت ةحول. قيبتلاب يلخادلا لوحملا ليصوتب ةيلفلخلا.
7. ةيلخادلا ةيمامألا لوحملا ةهجاو ةهجاو جرم طاقتلا ةطقن.

جورخلاو لوخدلا نم الك - هاجتالا ةيئانث طاقتلالا تايلمع ايرايخا يلخادلا لوحملا معدني هاجتالا لخدملا ي ف طبر يلخاد حاتفملا ضبق يلع، يضا رتفا لكش.

FirePOWER 4100/9300 نم ققحتلالا ونيوكتلا

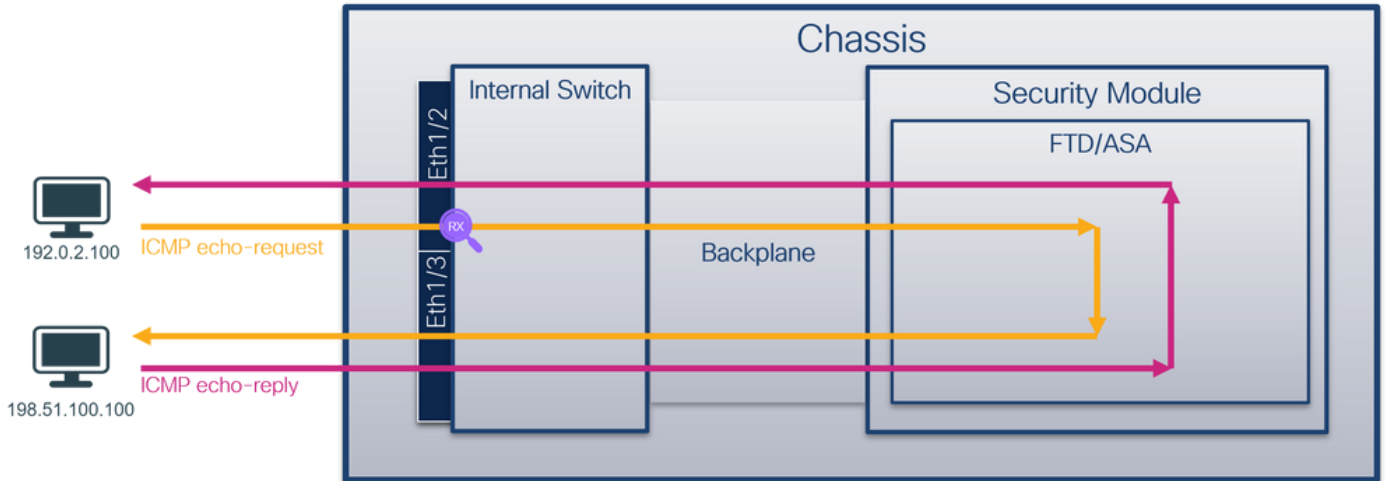
ىلع مزحل طاققتلا > تاودألا ي Firepower 4100/9300 يلىخادلا لوجملا طاققتلا ونيوكت نكمي FXOS ليغشتلا ماظنل (CLI) رمأوالا رطس ةهجاو ي قاطنلا ةمزح طاققتلا ي ف وأ FCM. FXOS Cisco لىه ريدم ونيوكت لىلد عجار ةمزحل طاققتلا تاراخي فصوى لىل لوصحلل Cisco Firepower 4100/9300 رمأوالا رطس ةهجاو ونيوكت لىلد وأ FXOS Firepower 4100/9300 ةمزحل طاققتلا مسقلا، اءال صاوا عااخال فاشكتسا لىل صفا، FXOS.

Firepower 4100/9300 تالوجم طاققتلالا عئاشلا مادختسالا تالاج تاهو يرانيسلا هذه ي طغت ةلىلخادلا.

ذفنم ةانق ةهجاو وأ ةيدام ةهجاو لىل ةمزحل طاققتلا

ةهجاو وأ 1/2 تىنرثي ةهجاو لىل هتحص نم ققحتلالا ةمزح طاققتلا ونيوكتل CLI و FCM مدختسا PortChannel1. ةيداملا اءاعالا تاهجاو عيمج ديدحت نم دكا، ذفنملا ةانق ةهجاو ةلج ي ف.

طاققتلالا طاقنو، ةمزحل قفدت، طاطخملا

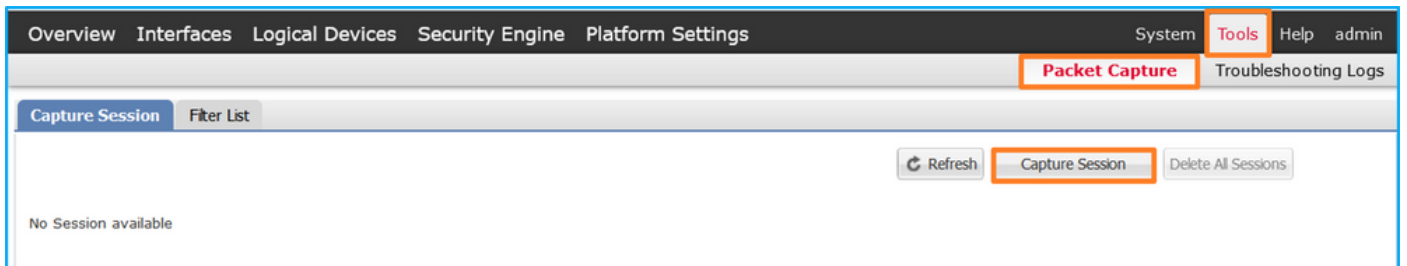


نيوكتلا

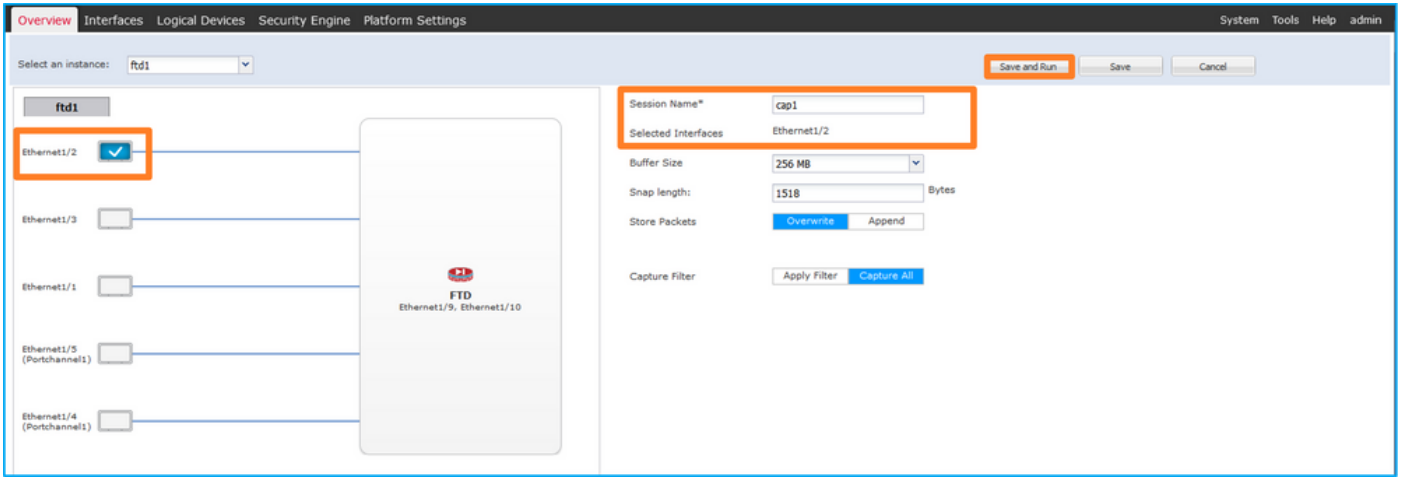
FCM

PortChannel1: و 1/2 تىنرثي نراق لىل طبر لكشي نأ FCM لىل steps اذه تىزنأ:

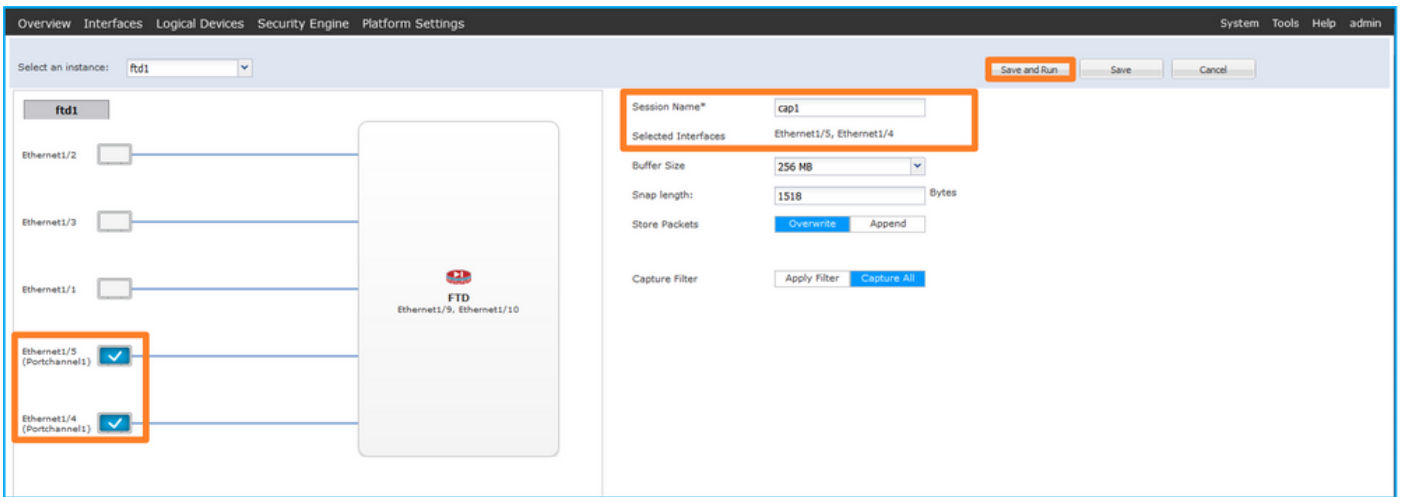
1. ةديج طاققتلا لمع ةسلىج عااشنال طاققتلالا ةسلىج > مزحل طاققتلا > تاودأ مدختسا.



2. طيشنتل لغشو ظفح رقناو ةسلىجلا مسا ريفوتب مقو، Ethernet1/2 ةهجاو لىل دح: طاققتلالا



3. طافح ةق طقو مسإ ةسلجلا تدوز ،نراق ي عي بط وضع لك دح ،نراق ةانق اذا ام ةلاح ي ف .
 طاق تلالا طشن ي نأ لغشو :



م Fxos (CLI) رم اوألا رطس ةه جاو

PortChannel1: وأ 1/2 تي نرثا نراق يلع طبر لك شي نأ FXOS CLI يلع steps اذه تزج نأ

1. قي بطتال فرعمو قي بطتال عون في رعت :

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

App Name	Identifier	Slot	ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No

2. اهئاضعأ تاهجاو فيرعتب مق ،ذفنملا ةانق ةهجاو ةلحي في:

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
<output skipped>
```

```
firepower(fxos)#
```

```
show port-channel summary
```

```
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
  Channel
-----
1      Po1(SU)    Eth       LACP      Eth1/4(P)  Eth1/5(P)
```

3. طاقتل ةسلج ءاشن |:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
create session cap1
```

```
firepower /packet-capture/session* #
```

```
create phy-port Eth1/2
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app ftd
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app-identifier ftd1
```

```
firepower /packet-capture/session/phy-port* #
```

up

```
firepower /packet-capture/session* #
```

```
enable
```

```
firepower /packet-capture/session* #
```

```
commit
```

```
firepower /packet-capture/session #
```

وضع ههجاو لكل لصفنم طاقنم لنيوكت متي، ذفنم لانا ق تاهجاو:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
create session cap1
```

```
firepower /packet-capture/session* #
```

```
create phy-port Eth1/4
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app ftd
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app-identifier ftd1
```

```
firepower /packet-capture/session/phy-port* #
```

```
up
```

```
firepower /packet-capture/session* #
```

```
create phy-port Eth1/5
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app ftd
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app-identifier ftd1
```

```
firepower /packet-capture/session/phy-port* #
```

```
up
```

```
firepower /packet-capture/session* #
```

```
enable
```

```
firepower /packet-capture/session* #
```

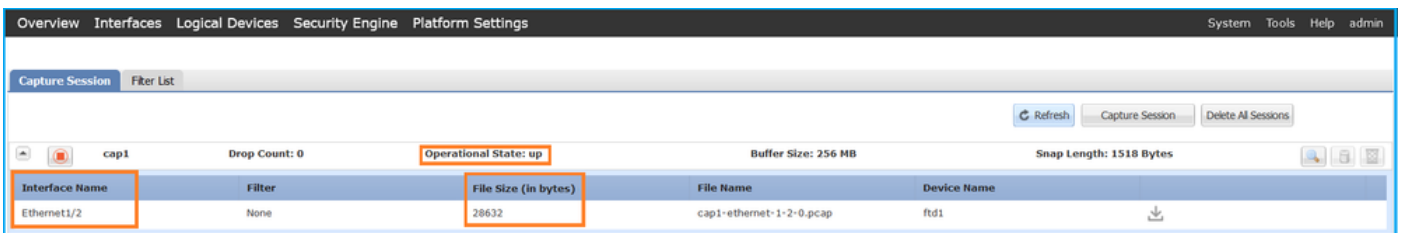
```
commit
```

```
firepower /packet-capture/session #
```

ق قحت ل

FCM

فلم ل مجح ة داي ز نم و ل يغش ل دي ق ل يغش ل ة ل ا ح ن أ ن م د ك أ ت و ، ة ه ج اول ا م سا ن م ق قحت (ت ي ا ب ل ا ب):



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	28632	cap1-ethernet-1-2-0.pcap	ftd1

PortChannel1 م ة ل ا ح ن أ ن م د ك أ ت و ، ة ه ج اول ا م سا ن م ق قحت ل



Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	ftd1
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1

ق قحت ل م جح ة داي ز نم و ل يغش ل دي ق ل يغش ل ة ل ا ح ن أ ن م د ك أ ت و ، ة ه ج اول ا م سا ن م ق قحت ل

ق قحت ل م جح ة داي ز نم و ل يغش ل دي ق ل يغش ل ة ل ا ح ن أ ن م د ك أ ت و ، ة ه ج اول ا م سا ن م ق قحت ل

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
show session cap1
```


Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

slot Id: 1

Port Id: 2

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

Pcapsize: 75136 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

1/5: تنرثي|و 1/4 تنرثي|ءاضعألا تاهجاوع م 1 ذفنملا ةانق

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 4

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap

Pcapsize: 310276 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 5

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-5-0.pcap

Pcapsize: 160 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

طاقات لال تافلم عي مچت

Firepower 4100/9300 ي لخال دل ل و ح مل طاق تال تافلم عي مچت م س ق ل ي ف تا و ط خ ل ا ع ا ر ج ا ب م ق

طاقات لال فلم ل ي ل ح ت

ة م ز ح ل ا د ح 1/2 ت ن ر ث ي ا ل طاق تال لال فلم ح ت ف ل م ز ح ل ا طاق تال تافلم ئ ر ا ق ق ي ب ط ت م د خ ت س ا ة ي س ا س ا ل طاق ن ل ا ص ح ف و ي ل و ا ل ا

1. تارم 2 اه ضرع و ة م ز ح ل ك طاق تال م ت ي . طوق ICMP Echo-Request م ز ح طاق تال م ت ي .
2. ة م ا ل ع ن و د ب ي ل ل ص ا ل ا ة م ز ح ل ا س ا ر .
3. 1/2 ت ي ن ر ث ا ن ر ا ق ل خ د م ل ن ي ع ي ن ا 102 ة ق ا ط ب VLAN ا ن ي م ي ف ا ض ا ي ل خ ا د ح ا ت ف م ل ل خ د ي .
4. ة ي ف ا ض ا V N ة م ا ل ع ي ل خ ا د ل ا ح ا ت ف م ل ل خ د ي .

The screenshot displays a network traffic capture analysis tool interface. The top section shows a list of captured packets, with the first packet selected. The packet details are shown in a table with columns for No., Time, Source, Destination, Protocol, Length, IP ID, P TTL, and Info. The selected packet is an ICMP Echo (ping) request from 192.0.2.100 to 198.51.100.100, with IP ID 0x9dec (40428) and P TTL 64. The info column indicates 'id=0x001a, seq=7/1792, ttl=64 (no response found)'. Below the table, the packet details are expanded, showing the Ethernet II header, VLAN-Tag, 802.1Q Virtual LAN header, and Internet Protocol Version 4 header. The Ethernet II header shows source MAC 08:00:0e:00:00:00 and destination MAC 08:00:0e:00:00:00. The VLAN-Tag shows priority 0 and DEI 0. The 802.1Q header shows priority 0 and DEI 0. The IP header shows source 192.0.2.100 and destination 198.51.100.100. The right side of the screenshot shows the raw packet data in hexadecimal and ASCII.

ة ي س ا س ا ل طاق ن ل ا ص ح ف و ة ي ن ا ث ل ا ة م ز ح ل ا د ح

1. تارم 2 اه ضرع و ة م ز ح ل ك طاق تال م ت ي . طوق ICMP Echo-Request م ز ح طاق تال م ت ي .

2. VLAN عمالع نودب يلصلأا ةمزحلا سار.

3. 1/2 تيئرثا نراق لخدملا نيغي نأ 102 ةقاطب VLAN ءانيم يفاضل يلخاد حاتفملا لخدي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x00dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	108	0x00dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x0e00 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x0e00 (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0xf920 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
6	2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0xf920 (40736)	64	Echo (ping) request id=0x001a, seq=9/2304, ttl=64 (no response found)
7	2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0xf92d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
8	2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0xf92d (40749)	64	Echo (ping) request id=0x001a, seq=10/2560, ttl=64 (no response found)
9	2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	0xf988 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
10	2022-07-13 06:24:02.381074999	192.0.2.100	198.51.100.100	ICMP	102	0xf988 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127689	192.0.2.100	198.51.100.100	ICMP	108	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
18	2022-07-13 06:24:06.477129899	192.0.2.100	198.51.100.100	ICMP	102	0xa1e9 (41449)	64	Echo (ping) request id=0x001a, seq=15/3840, ttl=64 (no response found)
19	2022-07-13 06:24:07.501293141	192.0.2.100	198.51.100.100	ICMP	108	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
28	2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801)	64	Echo (ping) request id=0x001a, seq=20/5120, ttl=64 (no response found)
29	2022-07-13 06:24:12.618610222	192.0.2.100	198.51.100.100	ICMP	108	0xa3dc (41948)	64	Echo (ping) request id=0x001a, seq=21/5376, ttl=64 (no response found)

```

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:db:b9:77:0e)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
0000 ..... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...P V...f
0010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ..E..T...@...
0020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 @...d...3dd...N...d
0030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 11 ..b...z/...
0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 ..c...l...
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 ..d...!#$%&'()*+
0060 32 33 34 35 36 37 ..-./:01234567
    
```

طاقنلا صحفو يلوألا ةمزحلا دح 1. PortChannel وضع تاهجا اول طاقنلا تافلح حتفا ةيساسلا

1. تارم 2 اهضرعو ةمزح لك طاقنلا متي. طقف ICMP Echo-Request مزح طاقنلا متي.
2. VLAN عمالع نودب يلصلأا ةمزحلا سار.
3. نراق لخدملا نيغي نأ 1001 ةقاطب VLAN يفاضل يلخاد حاتفملا لخدي PortChannel1.
4. ةيفاضل VN ةمالع يلخادلا حاتفملا لخدي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
2	2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	0x322e (12846)	64	Echo (ping) request id=0x002d, seq=245/62720, ttl=64 (no response found)
3	2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
4	2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9 (12985)	64	Echo (ping) request id=0x002d, seq=246/62976, ttl=64 (no response found)
5	2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
6	2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8 (13016)	64	Echo (ping) request id=0x002d, seq=247/63232, ttl=64 (no response found)
7	2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
8	2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	0x3373 (13171)	64	Echo (ping) request id=0x002d, seq=248/63488, ttl=64 (no response found)
9	2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
10	2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64	Echo (ping) request id=0x002d, seq=249/63744, ttl=64 (no response found)
11	2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
12	2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de (13534)	64	Echo (ping) request id=0x002d, seq=250/64000, ttl=64 (no response found)
13	2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
14	2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c (13644)	64	Echo (ping) request id=0x002d, seq=251/64256, ttl=64 (no response found)
15	2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
16	2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602 (13826)	64	Echo (ping) request id=0x002d, seq=252/64512, ttl=64 (no response found)
17	2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
18	2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed (14061)	64	Echo (ping) request id=0x002d, seq=253/64768, ttl=64 (no response found)
19	2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5 (14293)	64	Echo (ping) request id=0x002d, seq=254/65024, ttl=64 (no response found)

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_3, id 0
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)
VN-Tag
1..... = Direction: From Bridge
.0..... = Pointer: vif_id
..00 0000 0101 0100 ..... = Destination: 84
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... 0000 0000 0000 = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
0000 ..... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0011 1110 1001 = ID: 1001
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
0000 a2 76 f2 00 00 25 00 50 56 9d e8 be 89 26 80 54 v...P V...&T
0010 00 00 81 00 03 e9 08 00 45 00 00 54 32 2e 40 00 ..... E...T2.@
0020 40 01 1b 7f c0 00 02 64 c6 33 64 64 08 00 1e d6 @...d...3dd...
0030 00 2d 00 f5 a6 a2 ed 62 00 00 00 00 7a 2f 0b 00 ..b...z/...
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b ..c...l...
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ..d...!#$%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ..-./:01234567
    
```


ةيساسأل طاقنل صحنو ةينائل ةمزل دح:

1. تارم 2 اهضرعو ةمزل لك طاقنل متي .طقف ICMP Echo-Request مزح طاقنل متي .
2. ةمالع نودب يلصلأل ةمزل سار .
3. نراق لخدملا نيعي نأ 1001 ةقاطب VLAN يفاضل انيم يلخاد حاتفملا لخددي PortChannel1.

The image shows a network capture in Wireshark. The top part is a packet list showing ICMP Echo (ping) requests from 192.0.2.100 to 198.51.100.100. The bottom part is a packet details pane for the selected packet, showing the 802.1Q Virtual LAN configuration. The configuration includes:

- Priority: Best Effort (default) (0)
- DEI: Ineligible
- ID: 1001
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
- Internet Control Message Protocol

حرنل

نيترم دحاو تقوي ةمزل لك لوحنل طقتلي ،ةيمامأ ةهجاو لىل ةمزل طاقنل نيوكت دنع:

- ةمالع لخددي دعب .
- (VN) ةيرهظال ةصاخلل ةكبشلا ةمالع لخددي دعب .

ةصاخلل VLAN ةمالع جاردا نم ةقحال ةلحرم يي VN ةمالع جاردا متي ،تايللمعلا بيترت يي VLAN انيملا عم طبرلا نم ركبأ ةقاطب VN لىل عم طبرلا ،دربم طاقنل لىل يي ،امهم .ذفنم لىل ةقاطب .

ةمهمل لودجل اذه صخللي:

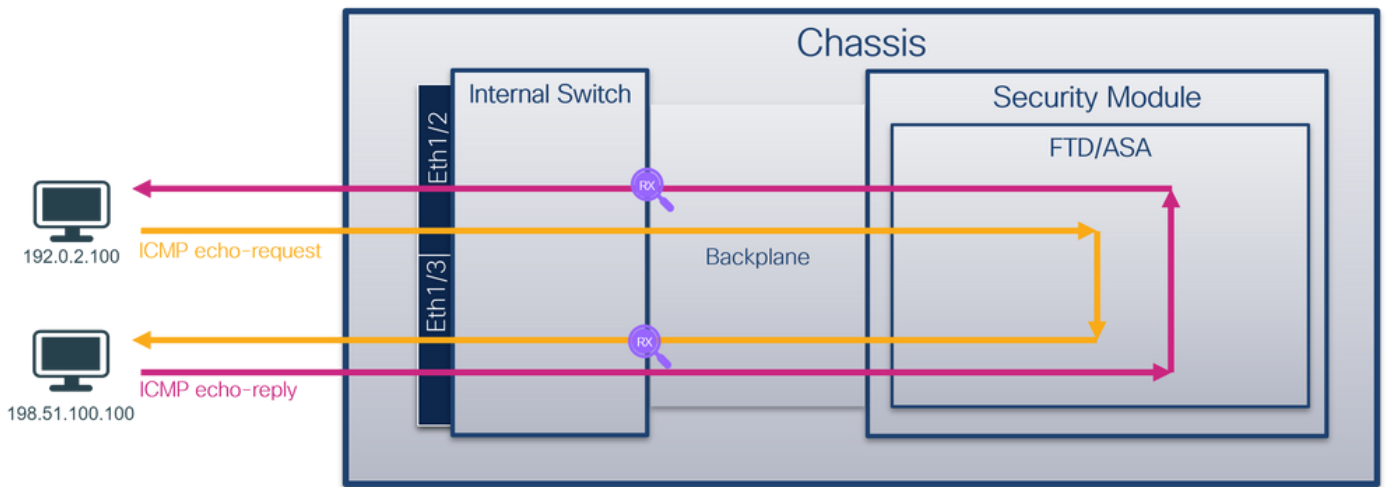
ةمهمل	ةطقن طاقنل لىل	انيم يلخاد ضبق يي VLAN طبر	هاجتا	اهيلع لىل وسملا رورملا ةكرح
ةمزل طاقنل نيوكت هتحنص نم ققحنل لىل ةهجاو لىل Ethernet1/2	Ethernet1/2	102	لخدم طاقف	نم ICMP لىل للىل 192.0.2.100 للىل 198.51.100.100
ةمزل طاقنل نيوكت ةهجاو لىل	Ethernet1/4 Ethernet1/5	1001	لخدم طاقف	نم ICMP لىل للىل 192.0.2.100

PortChannel1 هتحص نم ققحتل او تاهجاو مادختساب Ethernet1/4 ءاضعأل و Ethernet1/5				198.51.100.100 فيضملا
--	--	--	--	-----------------------

ةيفللخلاة حولللا تاهجاو ىلع ةمزحل طاقتللا

ةيفللخلاة حولللا تاهجاو ىلع هتحص نم ققحتل او ةمزح طاقتللا نيوكتل CLI و FCM مدختسأ

طاقتللا طاقنو، ةمزحل قفدت، طاطملا

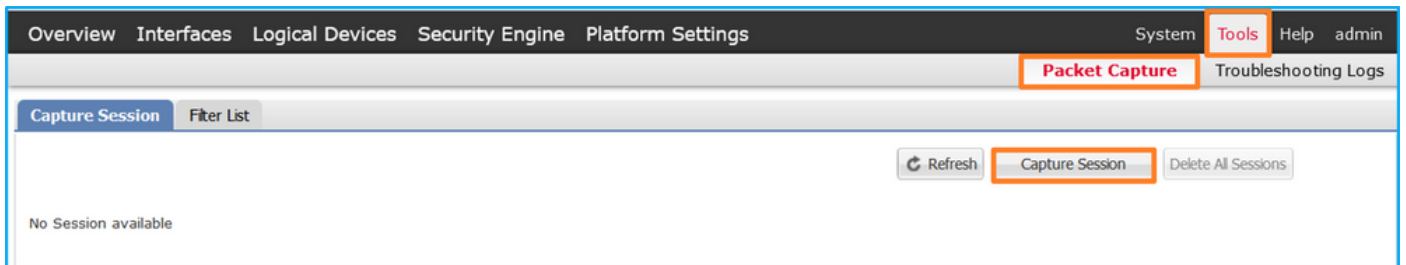


نيوكتللا

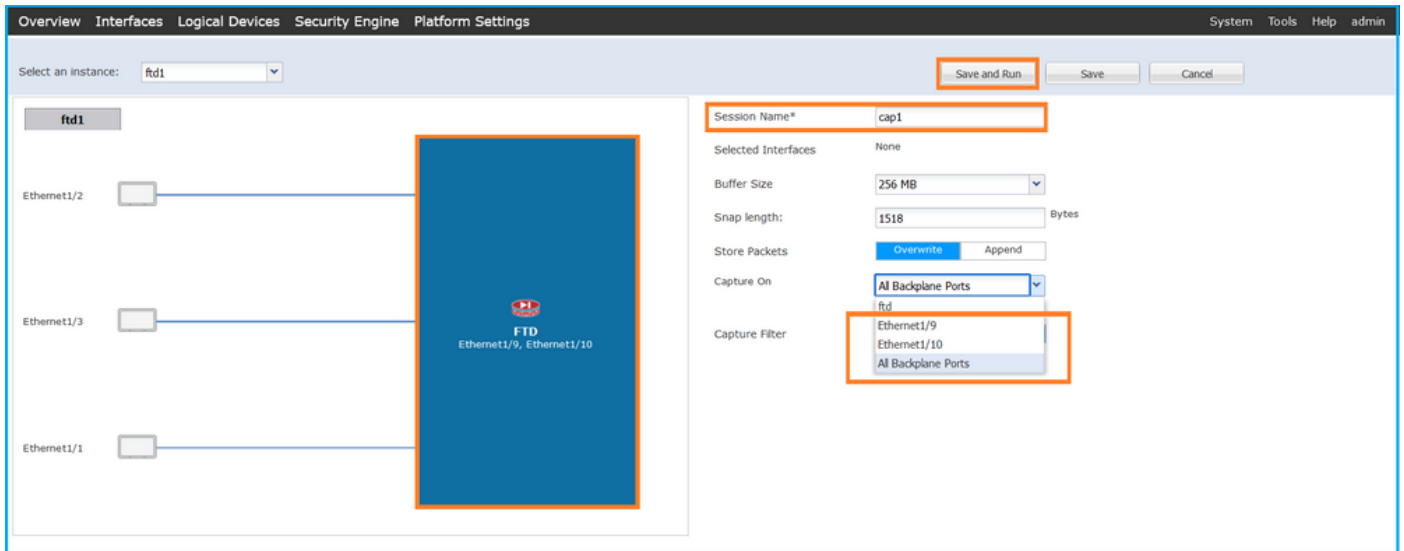
FCM

ةيفللخلاة حولللا نراق ىلع طبر لكشې نأ FCM ىلع steps اذه تزجنأ

ةيدج طاقتللا لمع ةسلج ءاشنأل طاقتللا ةسلج > مزحل طاقتللا > تاودأ مدختسأ 1.



ذفانم عيمج مث، قيبطتللا دح، ةيفللخلاة حولللا تاهجاو عيمج ىلع مزحل طاقتللا
ةحولللا ءهجاو رتخأ، كلذ نم الدب. ةلدسنملا ءمئاقلا ىلع طاقتللا نم ةيفللخلاة حولللا
و Ethernet1/9 ةيفللخلاة حولللا تاهجاو رفوتت، ءالخال هذه في. ءددملا ةيفللخلاة
طاقتللا طيشنتل ليغشتو ظفح ىلع رقن او ةسلجلا مسا لخدأ. Ethernet1/10



رماوأل رطس ةهجاو (CLI) نم Fxos

تاهاجاو ىلع مزحلا طاقتلا نيوكتل FXOS ل (CLI) رماوأل رطس ةهجاو ىلع تاوطخل هذه عارجاب مق ةيفلخل ءحولل:

1. قيبطتل فرعمو قيبطتل عون فيرعت:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82	Native No

2. طاقتلا ةسلج ءاشنإ:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
create session cap1
```

```
firepower /packet-capture/session* #
create phy-port Eth1/9

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/10

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

ققحتلا

FCM

فلملا مچح ةدايز نمو لئغشتلا دي ق لئغشتلا ةلاح نأ نم دكأتو ،ةهأولا مسأ نم ققحت
(تياابلأ):

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/10	None	194352	cap1-ethernet-1-10-0.pcap	ftd1
Ethernet1/9	None	286368	cap1-ethernet-1-9-0.pcap	ftd1

قماواأل رطس ةهجاو نم Fxos (CLI)

قماطنلا ةمزح طماقتلا يف طماقتلالا لىصافت نم ققحتلالا

<#root>

firepower#

scope packet-capture

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 10

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-10-0.pcap

Pcapsize: 1017424 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-9-0.pcap

Pcapsize: 1557432 bytes

Filter:
Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

طاقات الالات افلم عي مجت

Firepower 4100/9300 ي لخدال ل وحمال طاقات الالات افلم عي مجت مسقلا يف تاوطلخال اءارجاب مق

طاقات الالات فلم ليلحت

نم رثكأ دوجو ةلاح يف .طاقات الالات افلم حتفل مزحل طاقات الالات افلم ئراق قيبطت مدختسأ هذه يف .ةيفلخ ةحول ةهجاو لكل طاقات الالات افلم عي مجحتف نم دكأت ،ةيفلخ ةحول ةهجاو 1/9 تيئرثا نراق ةيفلخال ةحولل يلع طبرللا تطلقتلا ،ةلاحال

ةيساسال طاقنال صحتفو ،ةيناثلاو اولوال مزحلادح

1. ةرم 2 اهراهظا ICMP يدص بلط ةمزح لك طاقات الالات متي .
2. ةمالع نودب يلصلال ةمزحلا سار .
3. 1/3 تيئرثا نراق جرحملا ني عي نا 103 ةقاطب VLAN اءانيم يفاضل ي لخدال حاتفملا لخددي .
4. ةيفاضا VN ةمالع ي لخدال حاتفملا لخددي .

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found)
2	2022-07-14 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (reply in 3)
3	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64


```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 0000... .. = Destination: 0
  ... .. = Looped: No
  ... .. = Reserved: 0
  ... .. = Version: 0
  ... .. = Source: 10
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
  000... .. = Priority: Best Effort (default) (0)
  ...0... .. = DEI: Ineligible
  ... 0000 0110 0111 = ID: 103
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
  
```

هذه هي أساسيات طاقن ال صرح و، ع بارل او ة ثلاث ال مزحل ا دح:

1. ةرم 2 هراهظ او ICMP ىدص ىلع در لك طاقن ال متي .
2. ةمالع نودب ىلصألا ةمزحل ا سآر .
3. 1/2 تىنرث ا نراق جرحم ل نىعي نأ 102 ةقاطب VLAN ءانيم ىفاضا ىلخاد حاتفم ل ا لخدى .
4. ةىفاضا VN ةمالع ىلخاد ل حاتفم ل ا لخدى .

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-07-14 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22928)	64	Echo (ping) request id=0x0001, seq=15/3840, ttl=64 (no response found)
2	2022-07-14 20:20:36.514117394	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
3	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64


```

> Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  0... .. = Direction: To Bridge
  .0... .. = Pointer: vif_id
  ..00 0000 0000 0000... .. = Destination: 0
  ... .. = Looped: No
  ... .. = Reserved: 0
  ... .. = Version: 0
  ... .. = Source: 10
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
  000... .. = Priority: Best Effort (default) (0)
  ...0... .. = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
  Internet Control Message Protocol
  
```

حرج ل

دحاو تقوي ف ةم زح لك لوحم ل طقت ل، في ف ل يوت سم ةه جاو ل ع ةم زح طاق ل نيوكت دن ع ل ع ق ي ب ط ل ل ب ت د د ح ل ع ف ل ل ب ن و ك ي ن أ ط ب ر ي ل خ ا د ح ا ت ف م ل م ل ت س ي ، ة ل ا ح ل ه ذ ه ي ف . ن ي ت ر م ن أ ن ر ا ق ج ر خ م ل ة ق ا ط ب ن ي ع ي V L A N ل V N . ل ا و ة ق ا ط ب V L A N ء ا ن ي م ل ا ع م ة ي ط م ن ة د ح و ة ي ن م أ ل ب ل ط م ز ح ي ف V L A N 103 ة م ا ل ع ف ر ع ت . ة ك ب ش ل ل ي ل ط ب ر ل ل س ر ي ن أ ل م ع ت س ي ي ل خ ا د ل ك ي ه ل I C M P E C H O د ر م ز ح ي ف V L A N 102 ة م ا ل ع ف ر ع ت ا م ن ي ب ، ج ر خ م ة ه ج ا و ك 1/3 ت ن ر ث ي إ ل I C M P ي د ص ة ق ا ط ب V L A N ة ي ل خ ا د ل ا ة ه ج ا و ل ا و ة ق ا ط ب V N ل ي ل خ ا د ح ا ت ف م ل ل ي ز ي . ج ر خ م ة ه ج ا و ك 1/2 ت ن ر ث ي إ ل ة . ة ك ب ش ل ل ي ل ت ل س ر أ ن و ك ي ط ب ر ل ل ن أ ل ب ق .

ة م ه م ل ل و د ج ل ا ذ ه ص خ ل ي :

ة م ه م ل	ة ط ق ن ط ا ق ت ل ل ا	ء ا ن ي م ي ل خ ا د ص ب ق ي ف V L A N ط ب ر	ه ا ج ت ا	ه ي ل ع ي ل و ت س م ل ر و ر م ل ا ة ك ر ح
م ز ح ل ا ت ا ط ق ل ن ي و ك ت ة ح و ل ل ا ت ا ه ج ا و ي ل ع ا ه ن م ق ق ح ت ل ل ا و ة ي ف ل خ ل ا	ت ا ه ج ا و ة ح و ل ل ا ة ي ف ل خ ل ا	102 103	ل خ د م ط ق ف	ن م I C M P ي د ص ت ا ب ل ط ي ل ل 192.0.2.100 ف ي ض م ل ا 198.51.100.100 ف ي ض م ل ا ن م I C M P E C H O د و د ر ف ي ض م ل ا ي ل ل 198.51.100.100 192.0.2.100

ق ي ب ط ل ل ذ ف ا ن م و ق ي ب ط ل ل ي ل ع ة م ز ح ل ا ط ا ق ت ل ل

ة ف ا ض إ ل ا ب ة ي ف ل خ ل ا ة ح و ل ل ا ت ا ه ج ا و ي ل ع ا م ئ ا د ق ي ب ط ل ل ا و ا ق ي ب ط ل ل ا ذ ف ا ن م م ز ح ن ي و ك ت م ت ي ق ي ب ط ل ل ا ط ا ق ت ل ل ه ا ج ت ا د ي د ح ت ب م د خ ت س م ل ا م ا ق ا ذ ا ة ي م ا م أ ل ا ت ا ه ج ا و ل ا ي ل ع ك ل ذ ي ل ل .

م ا د خ ت س ا ي ت ل ا ح س ا س أ ل ا ي ف د ج و ت :

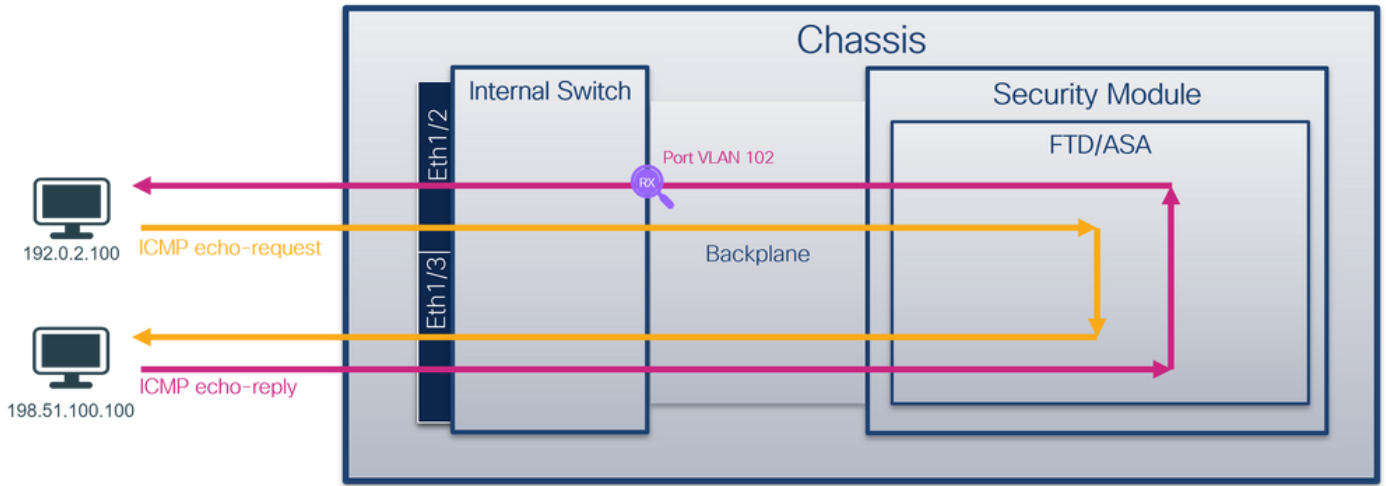
- ة ي م ا م أ ة ه ج ا و ك ر ت ت ي ت ل ل م ز ح ل ل ة ي ف ل خ ل ا ة ح و ل ل ا ت ا ه ج ا و ي ل ع م ز ح ل ا ط ا ق ت ل ل ن ي و ك ت ب م ق ة ي ف ل خ ل ا ة ح و ل ل ا ة ه ج ا و ي ل ع م ز ح ل ا ط ا ق ت ل ل ن ي و ك ت ب م ق ، ل ا ث م ل ل ي ب س ي ل ع . ة ن ي ع م Ethernet1/2 ة ه ج ا و ك ر ت ت ي ت ل ل م ز ح ل ل Ethernet1/9 .
- ة ي ف ل خ ل ا ة ح و ل ل ا ت ا ه ج ا و ة ن ي ع م ة ي م ا م أ ة ه ج ا و ي ل ع ة ن م ا ز ت م ل م ز ح ل ا ط ا ق ت ل ل ن ي و ك ت ب م ق ، ل ا ث م ل ل ي ب س ي ل ع Ethernet1/2 ة ه ج ا و ي ل ع ن م ا ز ت م ل م ز ح ل ا ط ا ق ت ل ل ن ي و ك ت ب م ق ، ل ا ث م ل ل ي ب س ي ل ع Ethernet1/2 ة ه ج ا و ك ر ت ت ي ت ل ل م ز ح ل ل Ethernet1/9 ة ي ف ل خ ل ا ة ح و ل ل ا ة ه ج ا و

م ا د خ ت س ا ل ا ت ا ل ا ح ن م ا ل ك م س ق ل ا ا ذ ه ي ط غ ي .

1 ة م ه م ل ل

ة ي ف ل خ ل ا ة ح و ل ل ا ة ه ج ا و ي ل ع ه ت ح ص ن م ق ق ح ت ل ل ا و ة م ز ح ط ا ق ت ل ل ن ي و ك ت ل C L I و F C M م د خ ت س أ ي ف . ج ر خ م ة ه ج ا و ك Ethernet1/2 ق ي ب ط ل ل ا ذ ف ن م د ي د ح ت ا ه ل ج أ ن م م ت ي ي ت ل ل م ز ح ل ا ط ا ق ت ل ل م ت ي I C M P د و د ر ط ا ق ت ل ل م ت ي ، ة ل ا ح ل ه ذ ه

طاقات الال طاقنو، مزلال قفدت، طاطم ال

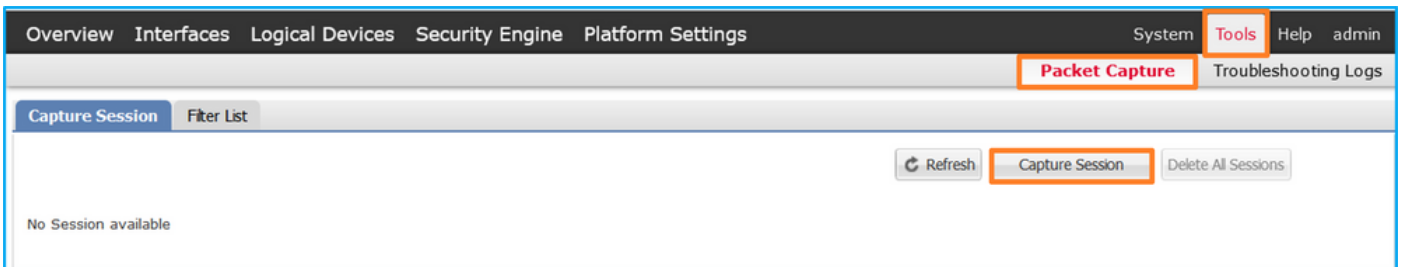


نيوكتال

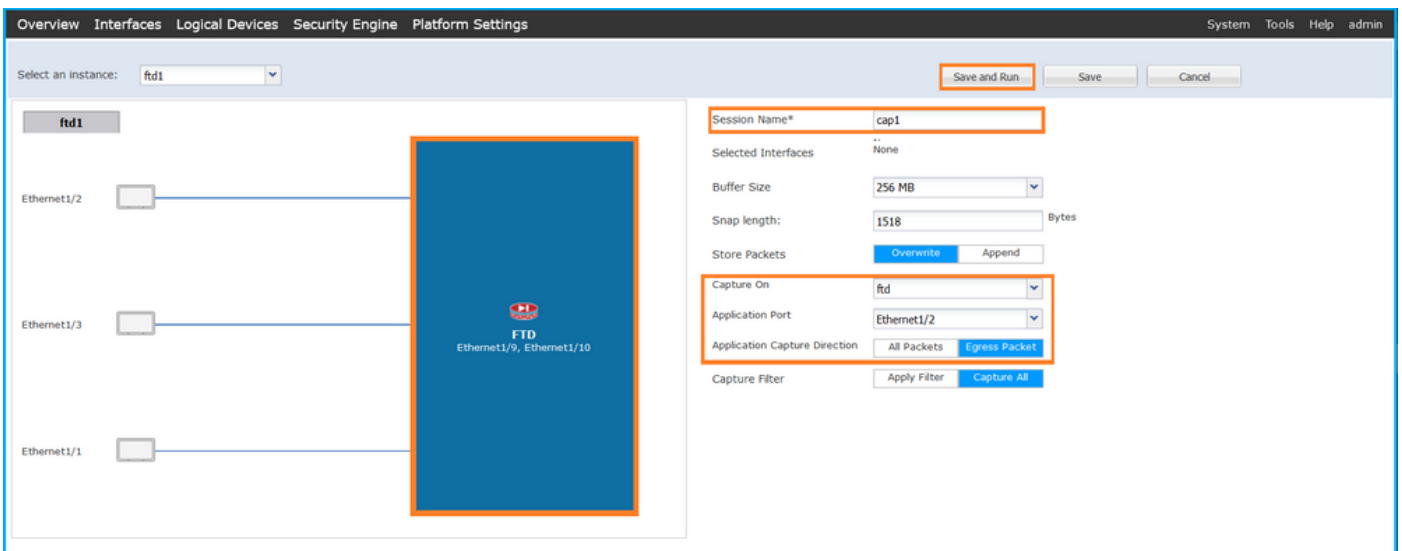
FCM

قبيطت ال ذفنم و FTD قبيطت ال على مزل طاقت ال نيوكتال FCM على تاوطخل ال هذه عارجاب مق Ethernet1/2:

1. ةديج طاقت ال لمع ةسلج عاشن ال طاقت الال ةسلج > مزلال طاقت ال > تاودأ مدختسأ.



2. يف جرم ةمزل دحو قبيطت ال ذفنم ةلدسنم ال ةمئال ال يف Ethernet1/2، قبيطت ال دحو طيشنتل ليغشت و ظفح على رقن او ةسلج ال مسا لخدأ. قبيطت ال طاقت ال حاجت ال طاقت الال:



رم اوأال رطس ةهجاو (CLI) نم Fxos

تاهجاو ىلع مزحلا طاقتلا نيوكتل ل FXOS ل (CLI) رم اوأال رطس ةهجاو ىلع تاوطخل هذه عارجاب مق ةيفلخل ءحوللل:

1. قيبطتل فرعمو قيبطتل عون فيرعت:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1						
1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No	

2. طاقتلا ةسلج ءاشن:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
create session cap1
```

```
firepower /packet-capture/session* #
```

```
create app-port 1 112 Ethernet1/2 ftd
```

```
firepower /packet-capture/session/app-port* #
```

```
set app-identifier ftd1
```

```
firepower /packet-capture/session/app-port* #
```

```
set filter ""
```

```
firepower /packet-capture/session/app-port* #
```

```
set subinterface 0
```

```
firepower /packet-capture/session/app-port* #
```

```
up
```

```
firepower /packet-capture/session* #
```

```
commit
```

```
firepower /packet-capture/session #
```

ققحتلا

FCM

فلمل مجح ةدايز نم وليغشتلا دي ق ليغشتلا ةلاح نأ نم دكأتو، ةهجاوالمسا نم ققحت (تيبابل):

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2 - Ethernet1/10	None	576	cap1-vethernet-1175.pcap	ftd1
Ethernet1/2 - Ethernet1/9	None	4360	cap1-vethernet-1036.pcap	ftd1

رم اوالم رطس ةهجاو (CLI) نم Fxos

ق:اطنللا ةمزح طاقتللا يف طاقتللالا ليصافات نم ققحتلا

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Application ports involved in Packet Capture:

slot Id: 1

Link Name: 112

Port Name: Ethernet1/2

App Name: ftd
Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap

Pcapsize: 53640 bytes

Vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

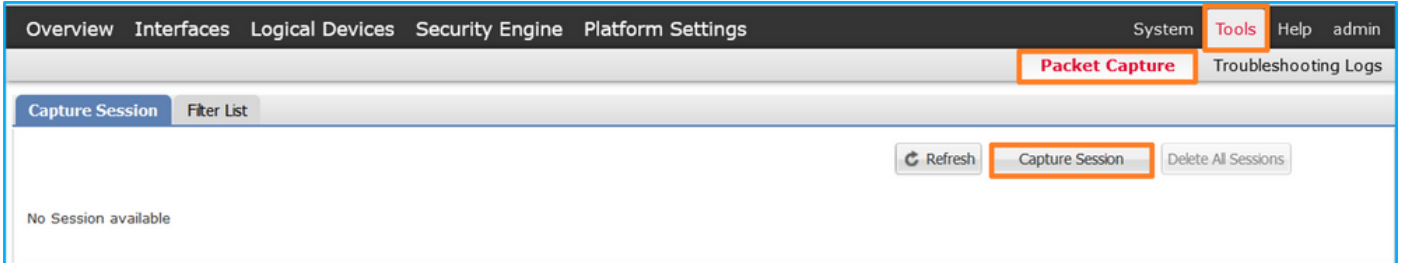
Eq Port Id: 10

نيوكتال

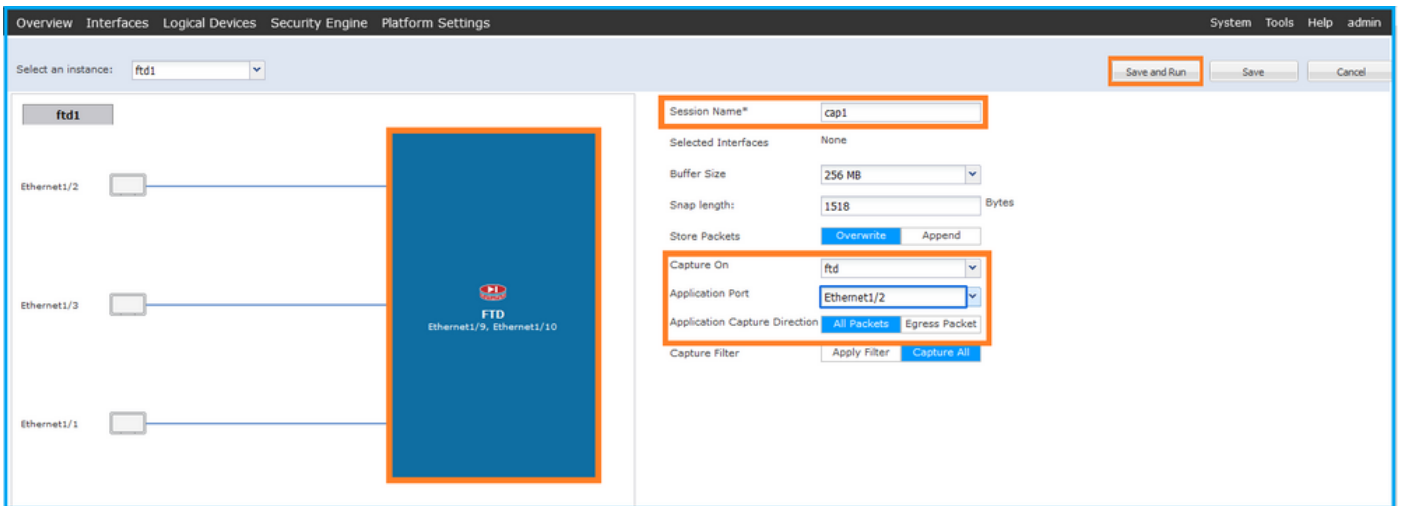
FCM

قيبطت ال ذفنم و FTD قيبطت يلع ةمزنح طاقنال نيوكتال FCM يلع تاوطلال هذه ءارجاب مق Ethernet1/2:

ةديج طاقنال لمع ةسلج ءاشنال طاقنال ال ةسلج > مزحل طاقنال > تاودأ مدختسأ 1.



مزحل ءيمج ددو قيبطت ال ذفنم ةلدسنم ال ةمئاق ال ي ف 1/2 تنرثي، FTD قيبطت ددح 2. طيشننل ليغش و ظفح يلع رقناو ةسلج ال مسا لخدأ. قيبطت ال طاقنال ءاجت ي ف طاقنال ال:



نم Fxos (CLI) رماوال رطس ةهجو

تاهاجو يلع مزحل طاقنال نيوكتال FXOS ل (CLI) رماوال رطس ةهجو يلع تاوطلال هذه ءارجاب مق ةيفلل ءحولل:

قيبطت ال فرعمو قيبطت ال عون فيرعت 1.

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1						
1	Enabled	Online		7.2.0.82	7.2.0.82	Native	No

طاق ت ل ة س ل ج ء ا ش ن ا . 2.

```

<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create session cap1

firepower /packet-capture/session* #
create phy-port eth1/2

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
exit

firepower /packet-capture/session* #
create app-port 1 link12 Ethernet1/2 ftd

firepower /packet-capture/session/app-port* #
set app-identifier ftd1

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session # commit

```

ق ق ح ت ل ا

FCM

فلمل مچج ةدايز نم وليغش التال دي ق ليغش التال ةلاح نأ نم دكأتو، ةهجاوالمسا نم ققحت (تياابلاب):

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	95040	cap1-ethernet-1-2-0.pcap	fd1
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	fd1
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	fd1

رم اوالم رطس ةهجاو (CLI) نم Fxos

قاطن الم مزح طاق التال ي ف طاق التال ل ل ي صافات نم ققحت التال

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

```
Session Mem Usage: 256 MB
```

```
Session Pcap Snap Len: 1518 Bytes
```

```
Error Code: 0
```

```
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
slot Id: 1
```

Port Id: 2

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

Pcapsize: 410444 bytes

Filter:

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

Application ports involved in Packet Capture:

Slot Id: 1

Link Name: link12

Port Name: Ethernet1/2

App Name: ftd

Sub Interface: 0

Application Instance Identifier: ftd1

Application ports resolved to:

Name: vnic1

Eq Slot Id: 1

Eq Port Id: 9

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap

Pcapsize: 128400 bytes

Vlan: 102

Filter:

Name: vnic2

Eq Slot Id: 1

Eq Port Id: 10

Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap

Pcapsize: 2656 bytes

Vlan: 102

Filter:

طاقات الالاف لم عيمجت

Firepower 4100/9300 يلاخل الالاف لم عيمجت مسقلا يف تاوطلال اارجاب مق

طاقات الالاف لم ليلحت

ةحول تاهاولة لاه يف . طاقات الالاف لم حتفل مزحلا طاقات الالاف لم ئراق قيبطت مدختسأ،
ةالال هذه يف . ةيفلخ ةحول ةهجال لكل طاقات الالاف لم عيمجت حتف نم دكأت، ةددعتم ةيفلخ
1/9 تيئرثا نراق ةيفلخال ةحوللا لعل طبرلا تطقتلا

ةيساس الالاف لم ققحتو، لوالا ةمزحلا ددحو، 1/2 تيئرثا ةهجال طاقات الالاف لم حتفا

1. تارم 2 اهضرعو ةمزح لك طاقات الالاف لم . طقف ICMP لصد بلط مزح طاقات الالاف لم .
2. VLAN ةمالع نودب لصلال ةمزحلا سار .
3. 1/2 تيئرثا نراق لخدمل لاه يف نأ 102 ةقابط VLAN لاه يف لخال حااتفملا لخدل .
4. ةيفاضا VN ةمالع لخال حااتفملا لخدل .

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266930	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:22.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

```

VN-Tag
1..... = Direction: From Bridge
.0..... = Pointer: vif_id
..00 0000 0000 1010 ..... = Destination: 10
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... 0000 0000 0000 = Source: 0
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000..... = Priority: Best Effort (default) (0)
..0..... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X...w..P V.....&
0010 00 00 81 00 00 66 08 00 45 00 00 54 c0 09 40 00f...E...T...@
0020 40 01 8d a3 c0 00 02 64 c6 33 64 04 08 00 8d 7c @...-d-3dd...|
0030 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00b.....
0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b!*"#\$%&'()*+
0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,...-/0123 4567

دع: ةي ساسأل طاقنلأ صرحو ةيناثلأ ةمزلأ دح

1. تارم 2 اهضرعو ةمزلأ لك طاقنلأ متي. طاق ICMP يدص بلط مزح طاقنلأ متي.
2. ةمالع ونودب يلصلأ ةمزلأ سار.
3. 1/2 تي نرثا نراق لخدمل نيعي نأ 102 ةقاطب VLAN ءانيم يفاضا يلخاد حتافلم لخد.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266930	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:22.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
24	2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) request id=0x0013, seq=11/2816, ttl=64 (no response found)
25	2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
26	2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) request id=0x0013, seq=12/3072, ttl=64 (no response found)
27	2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
28	2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) request id=0x0013, seq=13/3328, ttl=64 (no response found)
29	2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) request id=0x0013, seq=14/3584, ttl=64 (no response found)

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000..... = Priority: Best Effort (default) (0)
..0..... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X...w..P V.....f
0010 08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00E...T...@
0020 02 64 c6 33 64 04 08 00 8d 7c 00 13 00 01 f2 b9 e7d-3dd...|
0030 e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 11b.....
0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31!*\$%&'()*+,-./01
0060 32 33 34 35 36 37 ,...-/0123 4567

طاقنلأ نم ققحتو، ةيناثلأو لوالأ مزحلأ ددحو، 1/9 تي نرثا ةهجال طاقنلأ فلم حتاف ةي ساسأل:

1. ةرم 2 هراهطاو ICMP يدص لعل در لك طاقنلأ متي.
2. ةمالع ونودب يلصلأ ةمزلأ سار.

- 1/2 تينترث اراق جرحم ل نيعي نأ 102 قاطب VLAN ءاني م يفاضل يلخاد حاتفم ل لخد ي.
- ة يفاضل VN ةم ال ع يلخاد ل حاتفم ل لخد ي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Seq	TTL	Seq	TTL
1	2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply	id=0x0013, seq=1/256, ttl=64		
2	2022-08-01 11:33:19.071514882	198.51.100.100	192.0.2.100	ICMP	108	0x4f27 (20263)	64	Echo (ping) reply	id=0x0013, seq=1/256, ttl=64		
3	2022-08-01 11:33:20.072677302	198.51.100.100	192.0.2.100	ICMP	108	0x4ff0 (20472)	64	Echo (ping) reply	id=0x0013, seq=2/512, ttl=64		
4	2022-08-01 11:33:20.072679384	198.51.100.100	192.0.2.100	ICMP	108	0x4ffb (20475)	64	Echo (ping) reply	id=0x0013, seq=2/512, ttl=64		
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply	id=0x0013, seq=3/768, ttl=64		
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply	id=0x0013, seq=3/768, ttl=64		
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64		
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply	id=0x0013, seq=4/1024, ttl=64		
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64		
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply	id=0x0013, seq=5/1280, ttl=64		
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64		
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply	id=0x0013, seq=6/1536, ttl=64		
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64		
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply	id=0x0013, seq=7/1792, ttl=64		
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64		
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64		
17	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply	id=0x0013, seq=9/2304, ttl=64		
18	2022-08-01 11:33:27.154400198	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	64	Echo (ping) reply	id=0x0013, seq=9/2304, ttl=64		
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64		
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64		
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply	id=0x0013, seq=11/2816, ttl=64		
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply	id=0x0013, seq=11/2816, ttl=64		
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply	id=0x0013, seq=12/3072, ttl=64		
24	2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply	id=0x0013, seq=12/3072, ttl=64		
25	2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply	id=0x0013, seq=13/3328, ttl=64		
26	2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply	id=0x0013, seq=13/3328, ttl=64		
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply	id=0x0013, seq=14/3584, ttl=64		
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply	id=0x0013, seq=14/3584, ttl=64		
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply	id=0x0013, seq=15/3840, ttl=64		

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0 Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)		0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 ..PV...X...w...&... 0010 00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00f...E...TO... 0020 40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c @->3dd...d... 0030 00 13 00 01 f2 b9 e7 62 00 00 00 cb 7f 06 00b..... 0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b 0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ...!# \$%&'()*+... 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,./:0123 4567
VN-Tag 0... .. = Direction: To Bridge 0... .. = Pointer: vif_id ..00 0000 0000 0000 .. = Destination: 0 .. = Looped: No .. = Reserved: 0 .. = Version: 0 .. 0000 0000 1010 = Source: 10 Type: 802.1Q Virtual LAN (0x8100)		
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102 000... .. = Priority: Best Effort (default) (0) ...0 .. = DEI: Ineligible ... 0000 0110 0110 = ID: 102 Type: IPv4 (0x0800)		
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 Internet Control Message Protocol		

حرش ل

مزرح يتحتف نيوك ت متيسف ، قيبطت ل طاق ت ل اجات ي مزرح ل عي م رايخ ل اديحت مت اذ ا
 ة يمام ال ا ه ج اول ا ل ع طاق ت ل : 1/2 تنرث ي ا د ح م ل ا ق ي ب ط ت ل ا ب ن ي ت ط ب ت ر م ن ي ت ن م ا ز ت م
 ة د ح م ل ا ة ي ف ل خ ل ل ا ح و ل ل ا ت ا ه ج ا و ل ع طاق ت ل ا و 1/2 تنرث ي ا

ن ي ت ر م د ح ا و ت ق و ي ف ة م ز ح ل ك ل و ح م ل ا ط ق ت ل ي ، ة ي م ا م ا ة ه ج ا و ل ع ة م ز ح طاق ت ل ا ن ي و ك ت د ن ع

- Port VLAN ة م ال ع ل ا خ د ا د ع ب .
- (VN) ة ي ر ه ا ط ل ا ة ص ا خ ل ا ة ك ب ش ل ا ة م ال ع ل ا خ د ا د ع ب .

ة ص ا خ ل ا VLAN ة م ال ع ج ا ر د ا ن م ة ق ح ال ة ل ح ر م ي ف VN ة م ال ع ج ا ر د ا م ت ي ، ت ا ي ل م ع ل ا ب ي ت ر ت ي ف
 ع م ط ب ر ل ا ن م ر ك ب م ة قاطب VN ل ا ع م ط ب ر ل ا ر ه ط ي ، طاق ت ل ا ل ا ف ل م ي ف ن ك ل و . ذ ف ن م ل ا ب
 ا ي د ص ت ا ب ل ط م ز ح ي ف 102 VLAN ة م ال ع ف ر ع ت ، ل ا ث م ل ا ا ذ ه ي ف . ة قاطب VLAN ء ا ن ي م ل ا
 ل خ د م ة ه ج ا و ك 1/2 تنرث ي ا ل ا

د ح ا و ت ق و ي ف ة م ز ح ل ك ل و ح م ل ا ط ق ت ل ي ، ي ف ل خ ي و ت س م ة ه ج ا و ل ع ة م ز ح طاق ت ل ا ن ي و ك ت د ن ع
 ة د ح و ة ي ن م ا ل ا ل ع ق ي ب ط ت ل ا ب ت د د ح ل ع ل ا ب ن و ك ي ن ا ط ب ر ي ل خ د ا ح ا ت ف م ل ا م ل ت س ي . ن ي ت ر م
 ن ر ا ق ج ر ح م ل ا ة قاطب VLAN ء ا ن ي م ل ا ن ي ع ي . ة قاطب VLAN ل ا و ة قاطب VLAN ء ا ن ي م ل ا ع م ة ي ط م ن
 VLAN ة م ال ع ف ر ع ت ، ل ا ث م ل ا ا ذ ه ي ف . ة ك ب ش ل ا ل ا ط ب ر ل ا ل س ر ي ن ا ل م ع ت س ي ي ل خ د ل ك ي ه ل ا ن ا
 ج ر ح م ة ه ج ا و ك 1/2 تنرث ي ا ل ا ICMP ECHO ل ع د و ر ل ا م ز ح ي ف 102

ن و ك ي ط ب ر ل ا ن ا ل ب ق ة قاطب VLAN ة ي ل خ د ا ل ا ه ج ا و ل ا و ة قاطب VN ل ا ي ل خ د ا ح ا ت ف م ل ا ل ي ز ي
 ة ك ب ش ل ا ل ا ل س ر ا

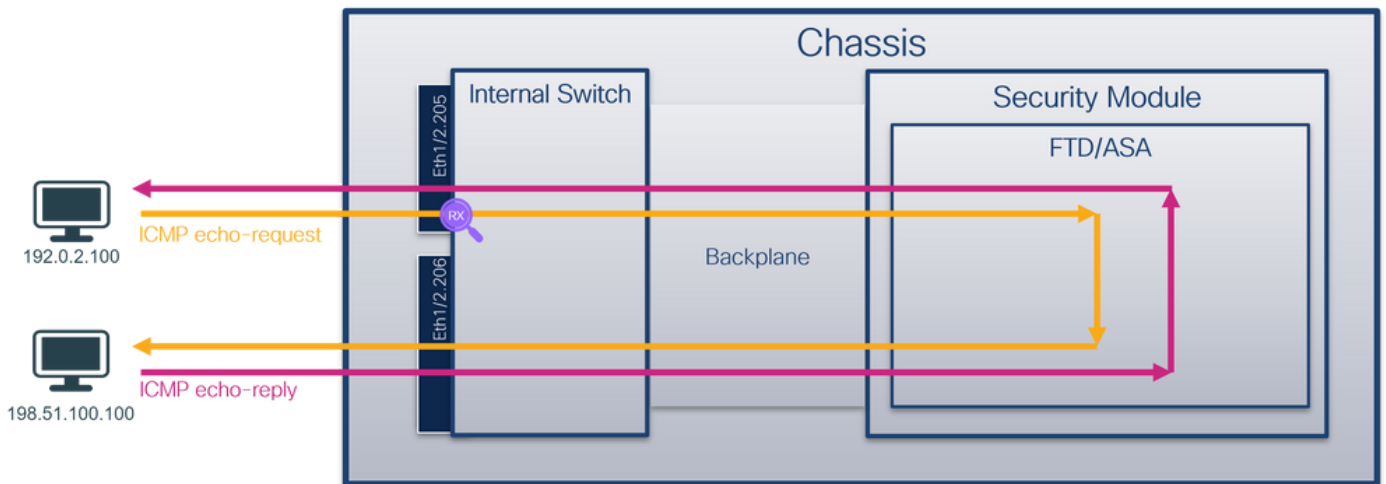
ة م م ل ل و د ج ل ا ا ذ ه ص خ ل ي

ةمهمل	ةطقن طاقتلال	ءانيم يلخاد في VLAN طبر ضبق	هاجتإ	ىلوتسملا رورملا ةكرح اهيلع
تايلمع نيوكت ققحتلاو طاقتلال تنرثيإ يلع اهنم قېبطلال ذفنمل 1/2 قېبطلالو	تاهجاو ةحوللا ةيفللخا	102	لخدم طقف	نم ICMP ECHO دودر ىلإ 198.51.100.100 فيضملا 192.0.2.100 فيضملا
	ةهجاو 1/2 تنرثيإ	102	لخدم طقف	نم ICMP يدص تابلط ىلإ 192.0.2.100 فيضملا 198.51.100.100 فيضملا

ذفنم ةانق ةهجاو وأ ةيدام ةهجاو ل ةيعرف ةهجاو يلع ةمزحلال طاقتلال

ةيعرفلال ةهجاو ل يلع هتحص نم ققحتلاو ةمزحلال طاقتلال نيوكتل CLI و FCM مدختسأ
CLI و FCM ذفنم ل ةيعرفلال ةانقلل PortChannel1.207 ةيعرفلال ةهجاو ل وأ Ethernet1/2.205
عضو في FTD قېبطلال طقف ةمومدم ةيعرفلال تاهجاو ل يلع طاقتلال ةيعرفلال تاهجاو ل
PortChannel1.207 و Ethernet1/2.205 يلع ةمزحلال طاقتلال نيوكت مت ، ةلالح هذه في . ةيواحلا

طاقتلال طاقنو ، ةمزحلال قفدت ، ططخملا

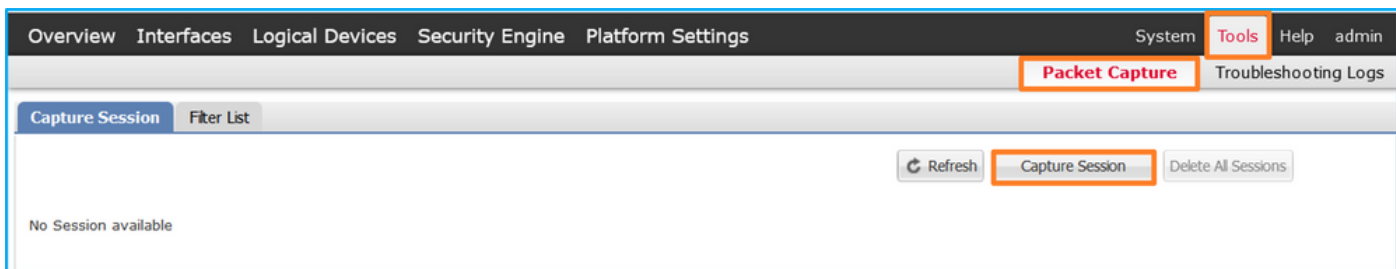


نيوكتل

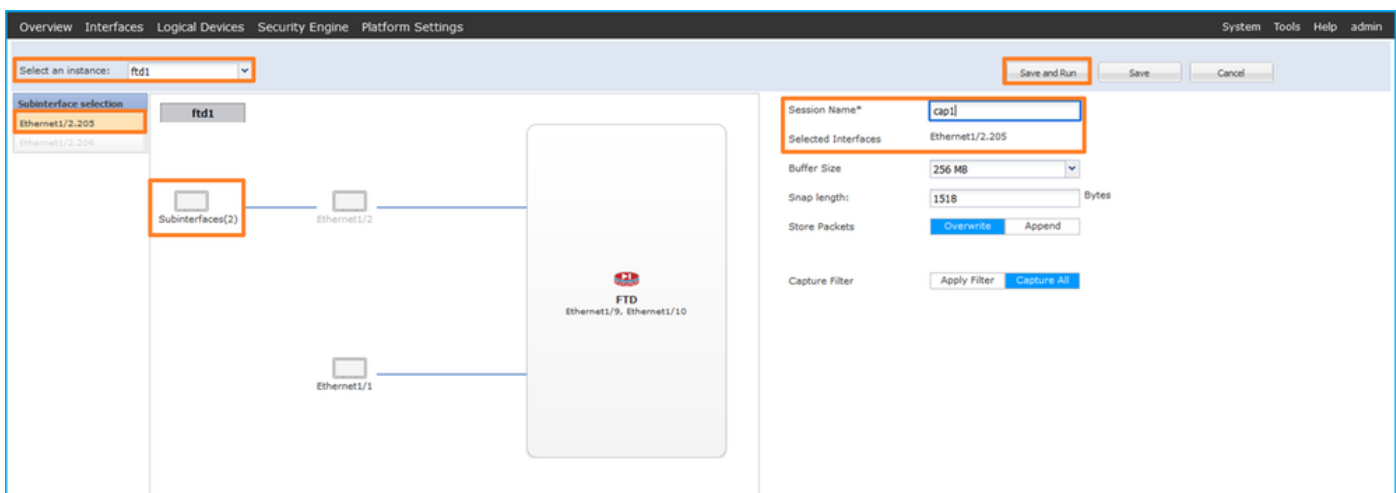
FCM

قېبطلال ذفنم و FTD قېبطلال يلع ةمزحلال طاقتلال نيوكتل FCM يلع تاوطخلال هذه ءارجاب مق
Ethernet1/2:

ةيديج طاقتلال لمع ةسلج ءاشنال طاقتلال ةسلج > مزحلال طاقتلال > تاودأ مدختسأ 1.



2. مرسا ريفوتب مقو، 1/2.205 ت نرثي اية عرفال ة هجاو او، دح م ال ftd1 ق ي ب ط ت ال ل ي م دح. دح:
طاقات الال طي ش ن ت ل ل ي غ ش ت و ظ ف ح ق و ف ر ق ن و، ة س ل ل ج:



3. ن م ا ط خ ال ا ح ح ص ت ف ر ع م ب ب س ب، ذ ف ن م ال ا ن ق ل ة ي ع ر ف ال ة ه ج ا و ال ا ح ي ف. ف
ل ع ط ا ق ت ال ال ن ي و ك ت ل FXOS CLI م د خ ت س ا. FCM ي ف ي ئ ر م ر ي غ [CSCvq33119](#) subinterfaces
ذ ف ن م ال ا ن ق ل ة ي ع ر ف ال ت ا ه ج ا و ال

ر م ا و ال ر ط س ة ه ج ا و (CLI) ن م Fxos

ل ع م ز ح ط ا ق ت ال ال ن ي و ك ت ل FXOS ل (CLI) ر م ا و ال ر ط س ة ه ج ا و ل ع ت ا و ط خ ال ه ذ ه ا ر ج ا ب م ق
Ethernet1/2.205 و PortChannel1.207 ة ي ع ر ف ال ت ا ه ج ا و ال

1. ق ي ب ط ت ال ف ر ع م و ق ي ب ط ت ال ع و ن ف ي ر ع ت:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

App Name	Identifier	Slot	ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1							
ftd	1	ftd2	1	Enabled	Online	7.2.0.82	7.2.0.82	Container
ftd				Enabled	Online	7.2.0.82	7.2.0.82	Container

2. اهئاضعأ تاهجاو فيرعتب مق ،ذفنملا ةانق ةهجاو ةلحي في:

```
<#root>
```

```
firepower#
```

```
connect fxos
```

```
<output skipped>
```

```
firepower(fxos)#
```

```
show port-channel summary
```

```
Flags: D - Down          P - Up in port-channel (members)
       I - Individual    H - Hot-standby (LACP only)
       s - Suspended     r - Module-removed
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
Group Port-      Type      Protocol  Member Ports
  Channel
-----
1     Po1(SU)    Eth       LACP      Eth1/3(P)  Eth1/3(P)
```

3. طاقتل ةسلج ءاشن |:

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
create session cap1
```

```
firepower /packet-capture/session* #
```

```
create phy-port Eth1/2
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app ftd
```

```
firepower /packet-capture/session/phy-port* #
```

```
set app-identifier ftd1
```

```
firepower /packet-capture/session/phy-port* #
```

```
set subinterface 205

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #
```

ذفنملا ةانق يف وضع ةهجاو لكل ةمزح طاقتلا عاشنإب مق ،ةيعرفلا ءانيملا ةانق تاهجاو:

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create filter vlan207

firepower /packet-capture/filter* #
set ovlan 207

firepower /packet-capture/filter* #
up

firepower /packet-capture* #
create session cap1

firepower /packet-capture/session*
create phy-port Eth1/3

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1
```

```

firepower /packet-capture/session/phy-port* #
set subinterface 207

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
create phy-port Eth1/4

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set subinterface 207

firepower /packet-capture/session/phy-port* #
up

firepower /packet-capture/session* #
enable

firepower /packet-capture/session* #
commit

firepower /packet-capture/session #

```

ققحتلا

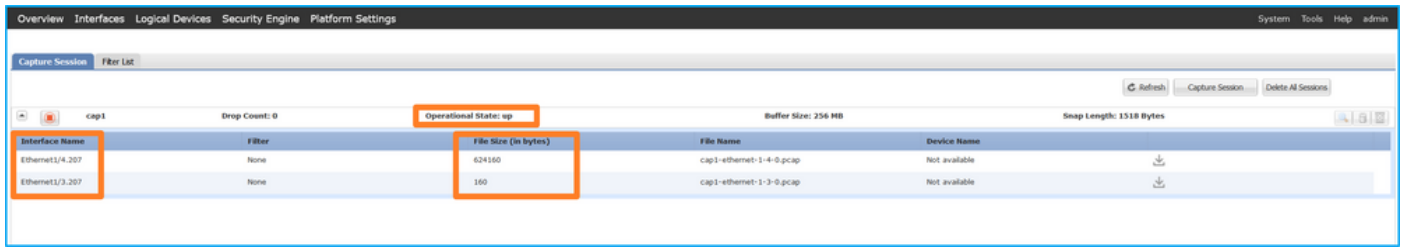
FCM

فلمل مجح ةدايز نم وليغشتلا دي ق ليغشتلا ةلاح نأ نم دكأتو ، ةهجاولا مسانم ققحت (تياجالاب):

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2_205	None	233992	cap1-ethernet-1-2-0.pcap	ftd1

اضيأ ةيئرم FXOS CLI لىع اهنوك ت مت يتلا ذفنملا ةانقل ةي عرفلا ةهجاولا طاقتلانوك

اهريحت نكمي ال، كلذ عمو، FCM ىلع



رم اوأل رطس ةهجاو نم Fxos (CLI)

ق اطنلا ةمزح طاقنلا يف طاقنلا لاي صافات نم ققحتلا

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
show session cap1
```

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
```

```
Session: 1
```

```
Admin State: Enabled
```

```
Oper State: Up
```

```
Oper State Reason: Active
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

```
Session Mem Usage: 256 MB
```

```
Session Pcap Snap Len: 1518 Bytes
```

```
Error Code: 0
```

```
Drop Count: 0
```

Physical ports involved in Packet Capture:

```
Slot Id: 1
```

```
Port Id: 2
```

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

Pcapsize: 9324 bytes

Filter:

Sub Interface: 205

Application Instance Identifier: ftd1

Application Name: ftd

1/4: تنرثي أو 1/3: تنرثي إاضعألأ تاهج او عم 1 ذفنملا ةانق

<#root>

firepower#

scope packet-capture

firepower /packet-capture # show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes

Config Fail Reason:

Append Flag: Overwrite

Session Mem Usage: 256 MB

Session Pcap Snap Len: 1518 Bytes

Error Code: 0

Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 3

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-3-0.pcap

Pcapsize: 160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

Slot Id: 1

Port Id: 4

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-4-0.pcap

Pcapsize: 624160 bytes

Filter:

Sub Interface: 207

Application Instance Identifier: ftd1

Application Name: ftd

طاقات الالات افلم عي مجت

Firepower 4100/9300. يلد ادل ل و ح م ال طاقات ال افلم عي مجت م س ق ل ا ي ف تا و ط خ ال ا ر ج ا ب م ق

طاقات الالات فلم ل ل ح ت

ص ح ف و ل و ال اة م ز ح ل ا د ح . طاقات الالات فلم ح ت ف ل م ز ح ل ا طاقات ال افلم عي مجت م س ق ل ا ي ف تا و ط خ ال ا ر ج ا ب م ق م د خ ت س اة س ا س ال ا طاقات ال :

1. تارم 2 اهض ر وة م ز ح ل ك طاقات ال م ت ي . ط ق ف ICMP ي د ص ب ل ط م ز ح طاقات ال م ت ي .

2. VLAN 205 إلى صالمة زارة ووتحى.

3. 1/2 نراق لخدملا نى عى نأ 102 قاطب VLAN ءانى م يفاضل يلخاد حاتفملا لخدى.

4. ةىفاضل VN ةمالع يلخادل حاتفملا لخدى.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9ff8 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9ff8 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

> Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

```

0000  a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54  .V...P V.....
0010  00 00 81 00 00 66 81 00 00 c0 08 00 45 00 00 54  ..-T-t @-@-@-@-
0020  95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64  t@ @-@-@-d 3dd
0030  08 00 08 95 00 22 00 01 88 73 be 62 00 00 00 00  s-b.....
0040  d9 9d 00 00 00 00 00 11 12 13 14 15 16 17  .....
0050  18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27  ..... !"#%&'
0060  28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37  (*+,-./ 01234567
  
```

4

```

1. .... = Direction: From Bridge
..0. .... = Pointer: vif_id
..00 0000 0101 0100 .... = Destination: 84
.....0. .... = Looped: No
.....0. .... = Reserved: 0
.....0000 0000 0000 = Version: 0
.....0000 0000 0000 = Source: 0
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

ةىساسال طاقنلا صرحو ةىناتلا ةمزحلل دح:

1. تارم 2 اهضرعو ةمزح لك طاقنلا مئى طقف ICMP ىدص مل طاقنلا مئى.

2. VLAN ةمالع ىلصالمة زارة ووتحى.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9ff8 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
24	2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9ff8 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)

```

0000  a2 76 f2 00 00 1b 00 50 56 9d e8 be 81 00 00 cd  .V...P V.....
0010  08 00 45 00 00 54 95 74 40 00 01 b8 38 c0 00 02 64  c-@-@-@-@-@-@-
0020  02 64 c6 33 64 64 08 00 08 95 00 22 00 01 88 73  d-3dd-@-@-@-@-
0030  be 62 00 00 00 00 00 09 d9 9d 00 00 00 00 00 11  b.....
0040  12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21  ..... |
0050  22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31  "###"()*+,-./01
0060  32 33 34 35 36 37  .....
  
```

2

```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
000. .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
... 0000 1100 1101 = ID: 205
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

حاتفملا طاقن صرحو لىلوالا ةمزحلل دح. PortChannel1.207 ل طاقنلالا تافملا نال حاتفملا

1. تارم 2 اهضرو ةمزح لك طاقنلا متي . طقف ICMP يدص بلط مزح طاقنلا متي .
2. ةمالع ىلع ىلصلأا ةمزحلا سار يوتحي .
3. نراق لخدملا نيعي نأ 1001 ةقاطب VLAN يفاضل انايم يلخاد حاتفملا لخدي PortChannel1.
4. ةيفاضل VN ةمالع يلخادلا حاتفملا لخدي .

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found)
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found)
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found)
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found)
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found)
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found)
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found)
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found)
9	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found)
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found)
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found)
12	2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found)
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found)
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found)
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found)
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found)
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found)
18	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found)
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found)
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found)
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found)
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found)
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found)
24	2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found)
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found)
26	2022-08-04 08:18:24.578900087	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found)
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request id=0x007b, seq=13/3328, ttl=255 (no response found)

Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

```

VNI-Tag
1 ..... = Direction: From Bridge
. .... = Pointer: vif_id
..00000011101 ..... = Destination: 61
..... = Looped: No
..... = Reserved: 0
..... = Version: 0
..... = Source: 0
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001
000 ..... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0011 1110 1001 = ID: 1001
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
000 ..... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0000 1100 1111 = ID: 207
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
Internet Control Message Protocol
  
```

ةيساسأل طاقنلا صحفو ةيناثلا ةمزحلا دح:

1. تارم 2 اهضرو ةمزح لك طاقنلا متي . طقف ICMP يدص بلط مزح طاقنلا متي .
2. ةمالع ىلع ىلصلأا ةمزحلا سار يوتحي .

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found)
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request id=0x007b, seq=0/0, ttl=255 (no response found)
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found)
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request id=0x007b, seq=1/256, ttl=255 (no response found)
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found)
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request id=0x007b, seq=2/512, ttl=255 (no response found)
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found)
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request id=0x007b, seq=3/768, ttl=255 (no response found)
9	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found)
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request id=0x007b, seq=4/1024, ttl=255 (no response found)
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found)
12	2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request id=0x007b, seq=5/1280, ttl=255 (no response found)
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found)
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request id=0x007b, seq=6/1536, ttl=255 (no response found)
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found)
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request id=0x007b, seq=7/1792, ttl=255 (no response found)
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found)
18	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request id=0x007b, seq=8/2048, ttl=255 (no response found)
19	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found)
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request id=0x007b, seq=9/2304, ttl=255 (no response found)
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found)
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request id=0x007b, seq=10/2560, ttl=255 (no response found)
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found)
24	2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request id=0x007b, seq=11/2816, ttl=255 (no response found)
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found)
26	2022-08-04 08:18:24.578900087	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request id=0x007b, seq=12/3072, ttl=255 (no response found)
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request id=0x007b, seq=13/3328, ttl=255 (no response found)

Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture_u0_3, id 0
Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207
000 ..... = Priority: Best Effort (default) (0)
...0 ..... = DEI: Ineligible
... 0000 1100 1111 = ID: 207
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102
Internet Control Message Protocol
  
```

حرج ل

نيترم دحاو تقوي ف ةم زح لك لوحم ل طقت لي، ةي مام أ ةه جاو يلع ةم زح طاق تال نيوك ت دنع

- ةم ل Port VLAN ةم ل ل اء اء ب
- ةم ل (VN) ةم ل ةص اء ل ةك ب ةم ل ل اء اء ب

ةص اء ل VLAN ةم ل ل ج اء اء ن م ةق ح ال ةل ح ر م ي ف VN ةم ل ل ج اء اء م تي، تا ي ل م ل ل ب ي ت ر ت ي ف م ط ب ر ل ل ن م ر ك ب م ةق اء ب VN ل ل م ط ب ر ل ل ر ه ظ ي، ط اء ت ل ل ال ف ل م ي ف ن ك ل و. ذ ف ن م ل ل ب، ط اء ت ل ل ال تا ف ل م ي ف، ةي ةر ف ل ل تا ه ج اء ال ةل ح ي ف، ك ل ذ ي ل ل ة ف اء اء ب. ةق اء ب VLAN ةم ل ل ل، ذ ف ن م ل ل ز ي ي م ت ةم ل ل ل ع ل ع ةي ن اء ةم زح لك ي و ت ح ت ال

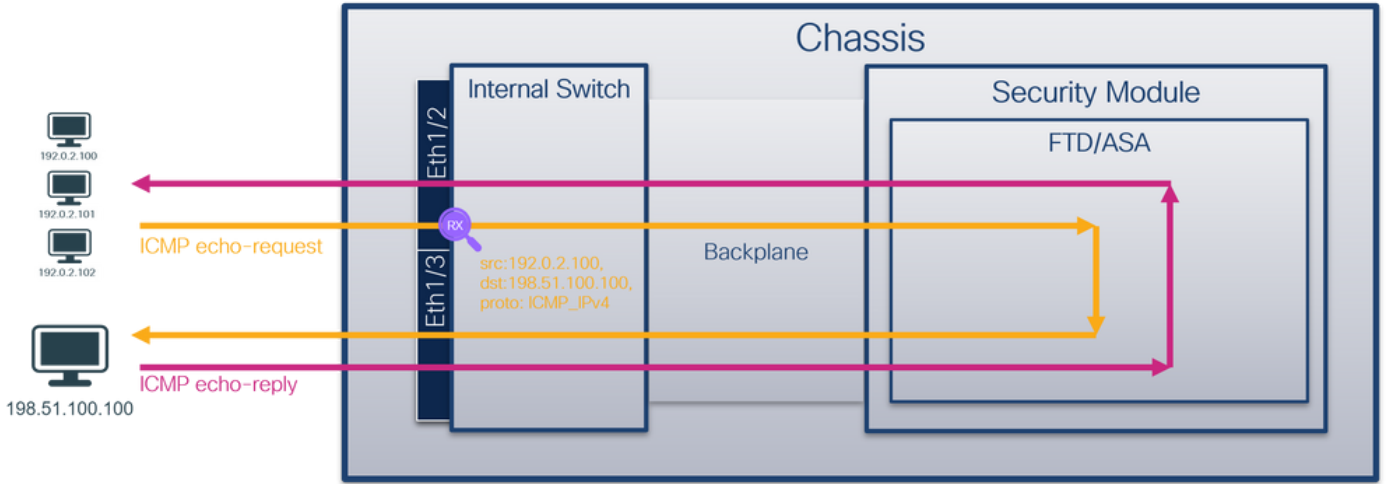
ةم م ل ل ل وء ج ل ل اء ه ص ل ل

ةم م ل ل	ةق ن ط اء ت ل ل ال	ء اء ي م ي ل ل اء اء ي ف VLAN ط ب ر ص ب ق	ه اء اء اء	ي ل و ت س م ل ر و ر م ل ل ةك ر ح اء ي ل ل ع
ةم زح ط اء ت ل ل نيوك ت ه ت ح ص ن م ق ق ح ت ل ل و ةي ةر ف ل ل ةه ج اء ال ي ل ل Ethernet1/2.205	Ethernet1/2.205	102	ل ل ل ل ل ط ق ف	ن م ICMP يء ص تا ب ل ل ط ي ل ل 192.0.2.100 ف ي ص م ل ل 198.51.100.100 ف ي ص م ل ل
ط اء ت ل ل نيوك ت ب م ق ن م ق ق ح ت ل ل و ةم زح ةه ج اء ال ي ل ل ه ت ح ص ةه ج اء ال PortChannel1 ةي ةر ف ل ل تا ه ج اء م اء خ ت س اء ب و Ethernet1/3 ةم ل ل Ethernet1/4	1/3 ت ن ر ث ي اء Ethernet1/4	1001	ل ل ل ل ل ط ق ف	ن م ICMP يء ص تا ب ل ل ط ة ف اء ص ت س ال 192.168.207.100 192.168.207.102

م زح ل ط اء ت ل ل ةي ف ص ت ل م اء ع

1/2 ت ن ر ث ي اء ةه ج اء ال ي ل ل ه ت ح ص ن م ق ق ح ت ل ل و ةم زح ط اء ت ل ل نيوك ت ل CLI و FCM مء خ ت س اء ح ش ر م م اء خ ت س اء ب

ط اء ت ل ل ال ط اء ن و، ةم زح ل ل ق فء ت، ط اء خ م ل ل

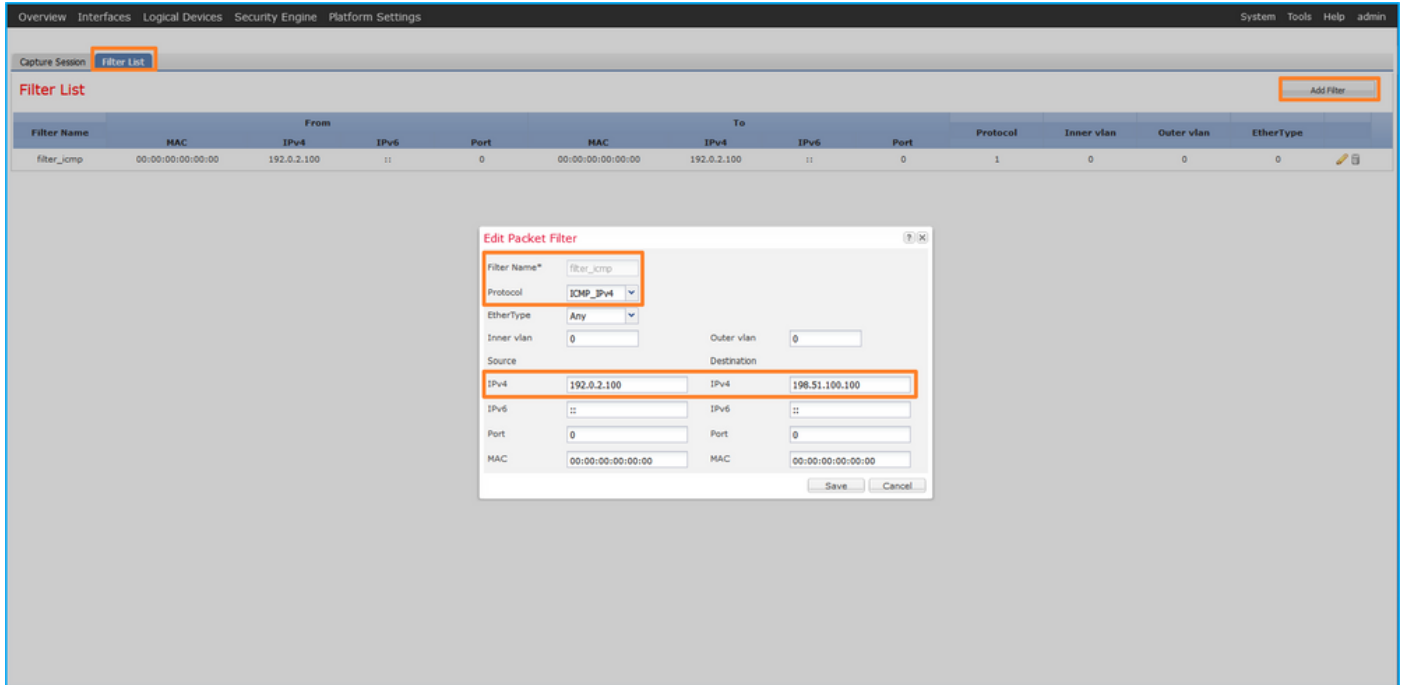


نيوكتالا

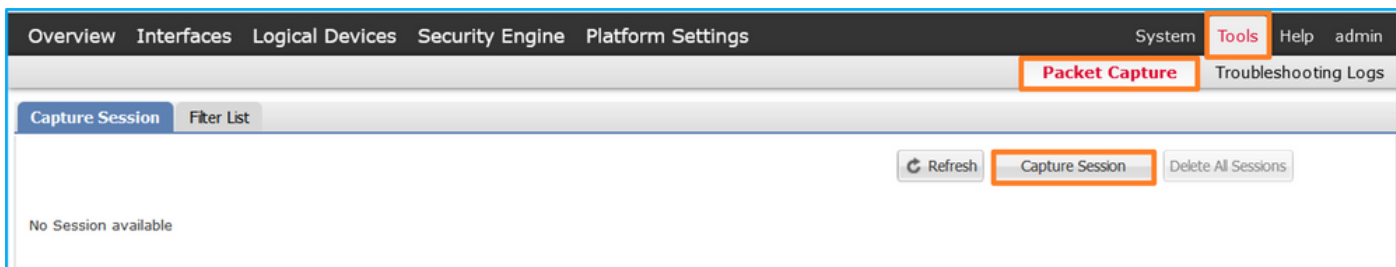
FCM

نم ICMP يدص بل ط مزل طاق تلالا ةي فرصت لماع نيوكتال FCM لىل ع تاوطلال هذه عارجاب مق ةهجاو لىل ع مزل طاق تلالا لىل ع هق يبططو 198.51.100.100 فيضم لىل ا 192.0.2.100 فيضم لىل ا 1/2 ت نرثي ا:

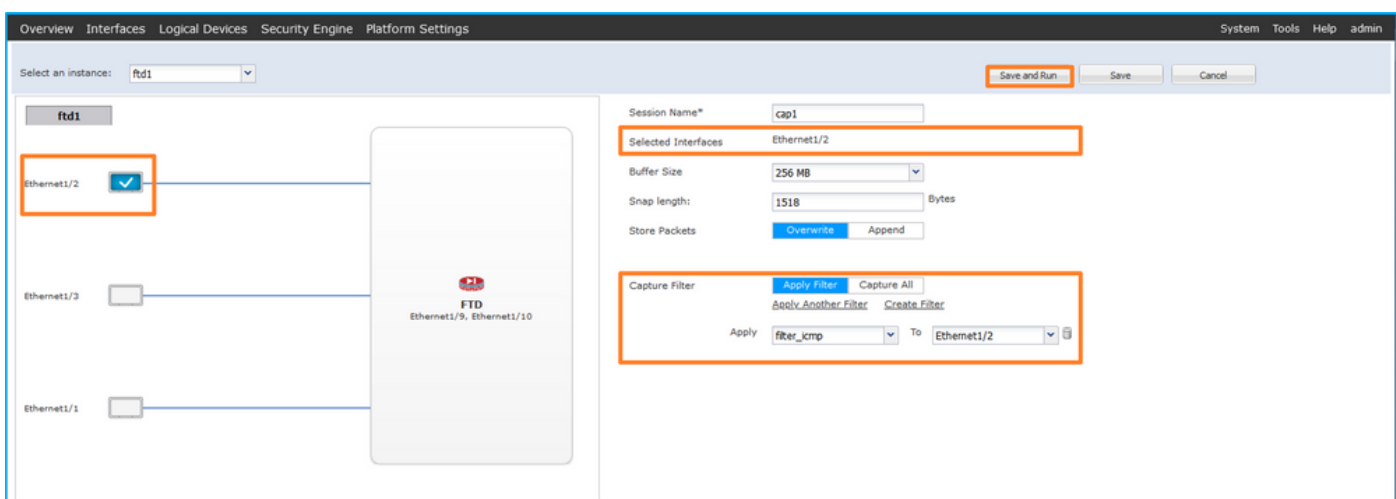
1. حشرم عاشن ا حشرم ة فاضا > تاحشرم لىل عمئاق > مزل طاق تلالا > تاودا مدختسا ا طاق تلالا.
2. طافح ةق طوطو IPv4 ةي اغ ، IPv4 ردصم ، لوكوتورب ، مس ا حشرم لىل تنيع :



3. ةديج طاق تلالا لمع ةسلج عاشن ا طاق تلالا ةسلج > مزل طاق تلالا > تاودا مدختسا ا:



4. نأ لغشو ظرفح ةق طوق و حشرم طاق تلالا تقب ط ،مسإ ةس لجالا تدوز ، 1/2 تي نرثإ دح .
طاق تلالا طش ني :



رم اوألا رطس ةه او نم Fxos (CLI)

تاه او يلع مزحلا طاق تلالا ني وك تال FXOS ل (CLI) رم اوألا رطس ةه او يلع تاوطلخا هذ ءارج اب مق ةي فلخا ءحوللا :

1. قيب طتلا فرعمو قيب طتلا عون في رعت :

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

App Name	Identifier	Slot	ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82	Native	No

2. في IP لوكوتورب مقرر دح .
1. وه ICMP لوكوتورب مقرر نوكي ، ةالجالا هذ في . <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>

3. طاقات لاسلج ءاشنإ:

```
<#root>
firepower#
scope packet-capture

firepower /packet-capture #
create filter filter_icmp

firepower /packet-capture/filter* #
set destip 198.51.100.100

firepower /packet-capture/filter* #
set protocol 1

firepower /packet-capture/filter* #
set srcip 192.0.2.100

firepower /packet-capture/filter* #
exit

firepower /packet-capture* #
create session cap1

firepower /packet-capture/session* #
create phy-port Ethernet1/2

firepower /packet-capture/session/phy-port* #
set app ftd

firepower /packet-capture/session/phy-port* #
set app-identifier ftd1

firepower /packet-capture/session/phy-port* #
set filter filter_icmp

firepower /packet-capture/session/phy-port* #
exit

firepower /packet-capture/session* #
```

```
enable
```

```
firepower /packet-capture/session* #
```

```
commit
```

```
firepower /packet-capture/session #
```

ققحتلا

FCM

فلملا مجح ةدايز نم وليغشتلا دي ق ليغشتلا ةلاح نأ نم دكأتو، ةهجاولا مسا نم ققحت (تيابلاب):

Filter Name	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType
filter_icmp	00:00:00:00:00:00	192.0.2.100	::	0	00:00:00:00:00:00	198.51.100.100	::	0	1	0	0	0

يف دي زي (تيابلاب) مجح دربملا، عفترم عضو ةيلمعلا تنمض، حشرم لا، مسا نراقلا تققد لمع ةسلج طاقتلا > طبر طاقتلا > تادأ:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	ftd1

م Fxos (CLI) رمأوالا رطس ةهجاو

قاطنلا ةمزح طاقتلا يف طاقتلا ليصافت نم ققحتلا

```
<#root>
```

```
firepower#
```

```
scope packet-capture
```

```
firepower /packet-capture #
```

```
show filter detail
```

Configure a filter for packet capture:

```
Name: filter_icmp
```

```
Protocol: 1
```


Ivlan: 0
Ovlan: 0

Src Ip: 192.0.2.100

Dest Ip: 198.51.100.100

Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0
Src Ipv6: ::
Dest Ipv6: ::

firepower /packet-capture #

show session cap1

Traffic Monitoring Session:

Packet Capture Session Name: cap1

Session: 1

Admin State: Enabled

Oper State: Up

Oper State Reason: Active

Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
Session Pcap Snap Len: 1518 Bytes
Error Code: 0
Drop Count: 0

Physical ports involved in Packet Capture:

Slot Id: 1

Port Id: 2

Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap

Pcapsize: 213784 bytes

Filter: filter_icmp

Sub Interface: 0

Application Instance Identifier: ftd1

Application Name: ftd

طاقات لال تافل م عي مجت

Firepower 4100/9300. ي ل خ اد ل ل و ح م ل ط ا ق ت ل ل ت ا ف ل م ع ي م ج ت م س ق ل ا ي ف ت ا و ط خ ل ل ا ع ا ر ج ا ب م ق

طاقات لال فلم ل ل ح ت

ص ح ف و ل و ا ل ا م ز ح ل ا د ح . ط ا ق ت ل ل ا ل ا ف ل م ح ت ف ل م ز ح ل ا ط ا ق ت ل ل ت ا ف ل م ئ ر ا ق ق ي ب ط ت م د خ ت س ا ح ا ت ف م ل ط ا ق ن

1. ت ا ر م 2 ا ه ض ر ع و م ز ح ل ك ط ا ق ت ل ل م ت ي . ط ق ف I C M P ي د ص ب ل ط م ز ح ط ا ق ت ل ل م ت ي .
2. م ا ل ع ن و د ب ي ل ص ا ل ا م ز ح ل س ا ر .
3. 1/2 ت ي ن ر ث ا ن ر ا ق ل خ د م ل ن ي ع ي ن ا 102 ق ا ط ب V L A N ا ن ي م ي ف ا ض ا ي ل خ ا د ح ا ت ف م ل ل خ د ي .
4. م ا ل ع ي ل خ ا د ل ح ا ت ف م ل ل خ د ي .

The screenshot displays a network traffic capture tool interface. The top section shows a list of captured packets, with the first packet (No. 1) highlighted. The packet details show it is an ICMP Echo (ping) request from source 192.0.2.100 to destination 198.51.100.100. The packet length is 108 bytes, and the IP ID is 0x0012 (18). The IP TTL is 64. The packet info shows it is an Echo (ping) request with id=0x0018, seq=349/23809, and ttl=64.

The bottom section shows a detailed view of the packet structure, with the following fields highlighted:

- 4: VII-Tag (Type: 802.1Q Virtual LAN (0x8100))
- 3: 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102 (Type: IPv4 (0x0800))
- 2: Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 (Internet Control Message Protocol)

ح ا ت ف م ل ط ا ق ن ص ح ف و ، م ا ن ا ث ل ا م ز ح ل ل د ح :

1. ت ا ر م 2 ا ه ض ر ع و م ز ح ل ك ط ا ق ت ل ل م ت ي . ط ق ف I C M P ي د ص ب ل ط م ز ح ط ا ق ت ل ل م ت ي .

2. VLAN مآل ع نوب ي لصلأ ةمزل سآر.

3. 1/2 تي نرثا نراق لخدمال ني عي نأ 102 قاطب VLAN ءاني م يفاض ي لخداحات فمالم لخد ي.

The image shows a Wireshark packet capture. The top pane displays a list of 20 packets, all of which are ICMP Echo (ping) requests from source IP 192.0.2.100 to destination IP 198.51.100.100. The packet details pane is expanded to show the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (ICMP Echo (ping) request) layers. A red box highlights the ICMP Echo (ping) request layer, and a yellow box highlights the Internet Protocol Version 4 layer. The packet bytes pane shows the raw data of the packet.

حرضال

نېترم دحاو تقو ي ف ةمزل لك لو حمال طقت لي، ةي مامأ ةه جاو لي ع ةمزل طاقتل ني وك ت دن ع

- Port VLAN ةمآل ع لخدإ دعب .
- (VN) ةي ره اظلال ةصاخلا ةكبشلا ةمآل ع لخدإ دعب .

ةصاخلا VLAN ةمآل ع جاردا نم ةقحال ةلحرم ي ف VN ةمآل ع جاردا متي، تا ي لمع ال بي ت رت ي ف عم طبرل نم ركبم ةقاطب VN ل عم طبرل ره ظي، طاقتل ال ف لم ي ف نكلو . ذف نم ل باب ةقاطب VLAN ءاني مالا .

هآجتا ي ف حشرم ال قباطت ي تل مزل طاقتل متي طقف طاقتل حشرم ق ي ب طت متي ام دن ع لخدمال .

ةمهمال لودجال اذه صخل ي:

ةمهمال	ةطقن طاقتل ال	ءاني م ي لخداحات ي ف VLAN طبر ضبق	هآجتا	ةي ف صت لماع مدختسمال	رورم ال ةكرح اهي ل ع ي لوتسمال
طاقتل ني وك ت ققحت لاو ةمزل هت حص نم لماع مادختساب ي ل ع ةي ف صت ةي مامأ ال هجاو ال Ethernet1/2	Ethernet1/2	102	لخدمال طقف	ICMP: لو كوت وربال ردصم ال: 192.0.2.100 ةه جولا: 198.51.100.100	نم ICMP ي دص تا بل ط 192.0.2.100 ف ي ضم ال ف ي ضم ال ي ل 198.51.100.100


```
firepower /packet-capture/session #
```

```
disable
```

```
firepower /packet-capture/session* #
```

```
commit
```

```
firepower /packet-capture/session #
```

```
up
```

```
firepower /packet-capture #
```

```
show session cap1 detail
```

```
Traffic Monitoring Session:
```

```
Packet Capture Session Name:
```

```
cap1
```

```
Session: 1
```

```
Admin State: Disabled
```

```
Oper State: Down
```

```
Oper State Reason: Admin Disable
```

```
Config Success: Yes
```

```
Config Fail Reason:
```

```
Append Flag: Overwrite
```

```
Session Mem Usage: 256 MB
```

```
Session Pcap Snap Len: 1518 Bytes
```

```
Error Code: 0
```

```
Drop Count: 0
```

```
Physical ports involved in Packet Capture:
```

```
Slot Id: 1
```

```
Port Id: 2
```

```
Pcapfile:
```

```
/workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
```

```
Pcapsize: 115744 bytes
```

```
Filter:
```

```
Sub Interface: 0
```

```
Application Instance Identifier: ftd1
```

```
Application Name: ftd
```

2. local-mgmt: رمألا قاطن نم طاقتلالا فلم ليمحت.

```
<#root>
```

```
firepower#
```

```
connect local-mgmt
```

```
firepower(local-mgmt)#
```

```
copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ?
```

```
ftp:          Dest File URI
http:         Dest File URI
https:        Dest File URI
scp:          Dest File URI
sftp:         Dest File URI
tftp:         Dest File URI
usbdrive:     Dest File URI
volatile:     Dest File URI
workspace:    Dest File URI
```

```
firepower(local-mgmt)#
```

```
copy /packet-capture/session-1/cap1-ethernet-1-2-0.pcap ftp://ftpuser@10.10.10.1/cap1-ethernet-1-2-0.pca
```

```
Password:
```

وضع ههجاو لكل طاقتل الال فلم خسنا ،ذفنملا ةانق تاهجاو ةلاح يف

يلخادلا لوجملا ةمزح طاقتل الال تاسرامملا لصف او ديدحتو تاداشرا

Firepower 4100/9300 ييلخادلا لوجملا طاقتل الال ةقلعتملا دويقل او تاداشرالا يلع لوصحلل
و Cisco Firepower 4100/9300 FXOS Chassis Manager لك يههلا ريديم نيوكت ليلد يلع جرا
فاشكتسا لصفلا ، Cisco Firepower 4100/9300 FXOS رم او الال رطس ههجاو نيوكت ليلد
مزلحلا طاقتل الال مسقلا ، اهلص او اعاطخ الال

TAC: تالاح يف مزلحلا طاقتل الال مادختسا يلع ةدنتسملا تاسرامملا لصف او ةمئاق يه هه

- دويقل او ةيههيجوتل الال ةدابملا ب ةيارد يلع نك
- طاقتل الال تافل م لك ليلحتو ةانق م الال ةانق و وضع تاهجاو لك يلع مزلحلا طاقتل الال
- طاقتل الال ةيفصت لم اوع مادختسا
- حشرم طاقتل الال تلكتش ام دنع ناو نع طبرل الال يلع NAT ريثا ت رابتع الال يف تعضو
- ةميقل الال نع ههفالتخ ةلاح يف راطل الال مزلح ددحي يذال len باذننا ليلقت او ةدايزب مق
مزلحلا نم ديازتم ددع رصق الال مزلحلا نع جتنني . تياب 1518 غلبت يتل الال ةيضرارتف الال
سكع الال س كع الال ةطقتل لم الال
- ةجالح الال بسح تقوؤم الال نزلح مزلح طبزب مق
- لوصول الال درجم ب . FXOS او FCM نم رم او الال رطس ههجاو يلع طاقس الال ددع ب ةيارد يلع نك
طاقس الال دادع دادع دادزي ، تقوؤم الال نزلح مزلح دح يلع
- اذه VN. ةمالع نودب طقف مزلح الال ضرع ل Wireshark يلع !vntag ةيفصت الال لماع مادختسا
درجم طاقتل الال طبر ةيما مال الال ههجاو الال يف طبر VN-tagged يف فخ ي ن ا ديفم
- كلذ ديفي . طقف ةي درف تاراطل الال ضرع ل Wireshark يلع &1frame.number حشرم مادختسا
ةيفلخ الال ةحول الال ههجاو ةمزح طاقتل الال تافل م يف ةرركم الال مزلح الال افخ ي

- نيولتال دعاوق يضارتفا لكش ب Wireshark قبطي، TCP لثم تالوكوتورب ةلاح يف
 يلخادلا لوحمل طاقتل ةلاح يف. ةفلتخم ناولأب ةني عم طورشب مزحلل ضرعت يتل
 اهيلع ةمالع عوضوو ةمزحلل نيولت نكمي، طاقتلال تافل م يف مزحلل راركت ب بسب
 مق م ث، حشرم أ تقب طو ةمزحلل طاقتل تافل م ليح تب تمق اذ. ةئطاخ ةبجوم ةقيرطب
 كلذ نم ال دب فل ملل حت فاو ديدج فلم ل ة ضرورم مزحلل ري دصت ب

3100/4200 نمآل ةي امحلل رادج يلع ققحتل او نيوكتل

نمآل ةي امحلل رادج يلع يلخادلا لوحمل طاقتل نيوكت متي، Firepower 4100/9300 س كع يلعو
 راخي ددحي ثي ح، capture <name> switch رمأل ربع قيبطتلل رماو ا رطس ةهجاو يلع 3100/4200
 يلخادلا لوحمل يلع طاقتلال تاي لمع نيوكت مت هنأ لوحمل

ل: لوحمل راخي عم capture رمأل وه اذه

<#root>

```
> capture cap_sw switch
```

?

```
buffer          Configure size of capture buffer, default is 256MB
ethernet-type   Capture Ethernet packets of a particular type, default is IP
interface       Capture packets on a specific interface
ivlan           Inner Vlan
match           Capture packets based on match criteria
ovlan           Outer Vlan
packet-length   Configure maximum length to save from each packet, default is
                64 bytes
real-time       Display captured packets in real-time. Warning: using this
                option with a slow console connection may result in an
                excessive amount of non-displayed packets due to performance
                limitations.
stop            Stop packet capture
trace           Trace the captured packets
type            Capture packets based on a particular type
<cr>
```

يلي امك يه ةمزحلل طاقتل نيوكتل ةماعل تاوطلل:

1. نراق لخدم تنيع:

تاهجاو عامسأ ديدحت مدختس ملل نكمي. لوخدلا ةهجاو مسا لوحمل طاقتل نيوكت لبقي
 ةرادال تاهجاو وأ ةيلخادلا تالصولا وأ تانايلل

<#root>

```
>
```

```
capture capsw switch interface ?
```

Available interfaces to listen:

```
in_data_uplink1 Capture packets on internal data uplink1 interface
```

```
in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
inside           Name of interface Ethernet1/1.205

management      Name of interface Management1/1
```

مل ام ،لخدم ةميققلا .هاتإلا ةيئانث طاقتلالا تايلمع 4200 زارط نمألا ةيامحلل رادج معددي
كلذ فالخ نيغي:

```
<#root>
```

```
>
```

```
capture capi switch interface inside direction
```

```
both      To capture switch bi-directional traffic
egress    To capture switch egressing traffic
ingress   To capture switch ingressing traffic
```

ليصوت ةهجاو 2و ةيلخاد تانايب 2 ىلع 4245 نمألا ةيامحلل رادج يوتحي ،كلذ ىلا ةفاضلإابو
ةيرادإ:

```
<#root>
```

```
>
```

```
capture capsw switch interface
```

```
eventing      Name of interface Management1/2
in_data_uplink1  Capture packets on internal data uplink1 interface
in_data_uplink2  Capture packets on internal data uplink2 interface
in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
in_mgmt_uplink2  Capture packets on internal mgmt uplink2 interface
management      Name of interface Management1/1
```

2. تنرثيإ عون رايق ميقدحت . IP. وه يضا رتفال EtherType .تنرثيإلا راطإل EtherType ددح
EtherType عون:

```
<#root>
```

```
>
```

```
capture capsw switch interface inside ethernet-type ?
```

```
802.1Q
<0-65535> Ethernet type
arp
ip
```



```
ip6
pppoed
pppoes
rarp
sgt
vlan
```

3. قباطتلا ريياعم قباطت طاقتلالا راخ ددحي .ةقباطملا طورش ددح

```
<#root>
```

```
>
```

```
capture capsw switch interface inside match ?
```

```
<0-255> Enter protocol number (0 - 255)
```

```
ah
eigrp
esp
gre
icmp
icmp6
igmp
igrp
ip
ipinip
ipsec
mac      Mac-address filter
nos
ospf
pcp
pim
pptp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. كلذىلإ امو ةمزحلا لوطوت قؤملا نزملا مجح لثم ىرخألا ةيرايتخالا تاملعمل ددح.

5. طاقتلالا طشنى فاقىإ حاتفم <name> no capture رمالا .طاقتلالا نيكمتب مق

```
<#root>
```

```
>
```

```
capture capsw switch interface inside match ip
```

```
>
```

```
no capture capsw switch stop
```

6. طاقوتلالا لېصافات نم ققحت:

- ةطشنو لېغشلتا دي ق لېغشلتا ةلاح تناكو، ةيرادإلا ةلاحلا نيكمت مت
- Packet Capture File Size دي زي.
- يرفص ريغ `show capture <cap_name>` جارخا ي ةطقتلما مزحلا ددع.
- دلجملا ي ف اياقلا ةطقتلما مزحلا ظفح متي. راسملا ل PCAPFILE فلم طاقوتلا /mnt/disk0/packet-capture/.
- طورش يلع ءانب اياق طاقوتلالا تا حشرم ءاشناب جم انربلا موق ي. طاقوتلالا فورظ طاقوتلالا.

```
<#root>
```

```
>
```

```
show capture capsw
```

```
27 packet captured on disk using switch capture
```

```
Reading of capture file from disk is not supported
```

```
>
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
Session:             1
Admin State:        enabled
Oper State:         up
```

```
Oper State Reason: Active
```

```
Config Success:     yes
Config Fail Reason:
Append Flag:        overwrite
Session Mem Usage:  256
Session Pcap Snap Len: 1518
Error Code:         0
Drop Count:         0
```

```
Total Physical ports involved in Packet Capture: 1
```

```
Physical port:
```

```
Slot Id:            1
Port Id:            1
```

```
Pcapfile:           /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
```


Oper State Reason: Session_Admin_Shut

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 24
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

طاقات الة افلم عي مجت مسقلا يف ةدوجوملا تاوطخلا ءارجاب مق . طاقات الة افلم عي مجت 8. نم الة يلخادلا ةيامحلا راج لوجم .

ىلع يلخادلا لوجملا طاقات الة نيوكت معدى ال ، نم الة ةيامحلا راج جم انرب نم 7.4 رادصل الة يف طاقات الة نيوكت نكمي ، ثدح الة ارادصل الة او 9.18(1) رادصل الة ASA جم انرب ةلاح يف FMC و FDM . ثدح الة ارادصل الة او ASDM 7.18.1.x رادصل الة يف ةيلخادلا الة لوجملا .

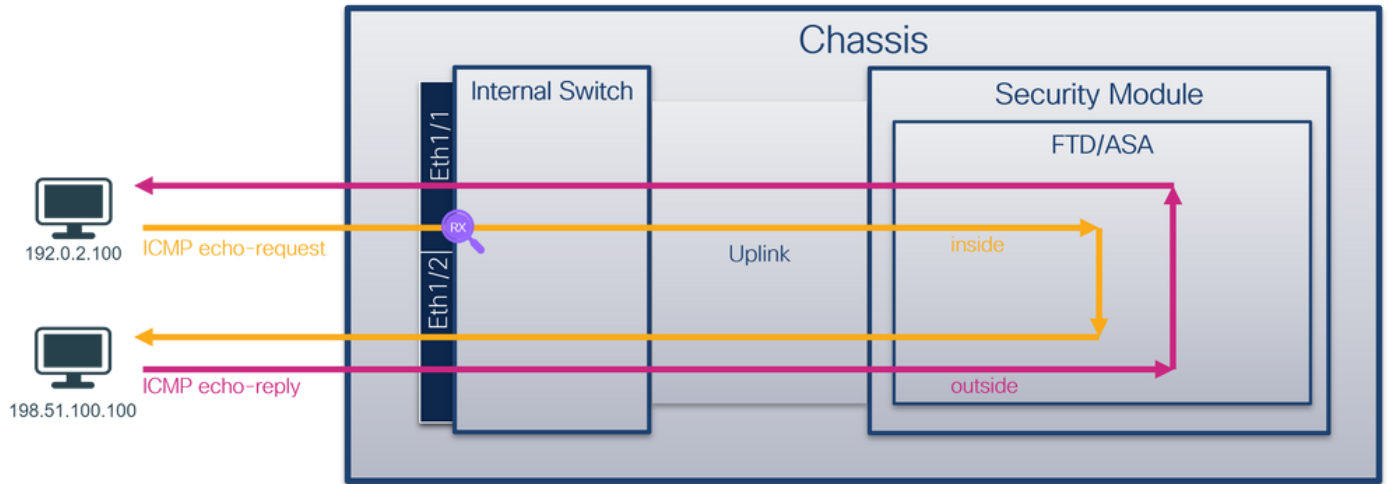
Secure Firewall الة لوجم طاقات الة ءاشل ماخذتس الة الة اح تاو يرانيسل الة هذه ي طغت ةيلخادلا 3100/4200 .

ذفنم ةانق ةهجاو و اةي دام ةهجاو ىلع ةمزح الة طاقات الة

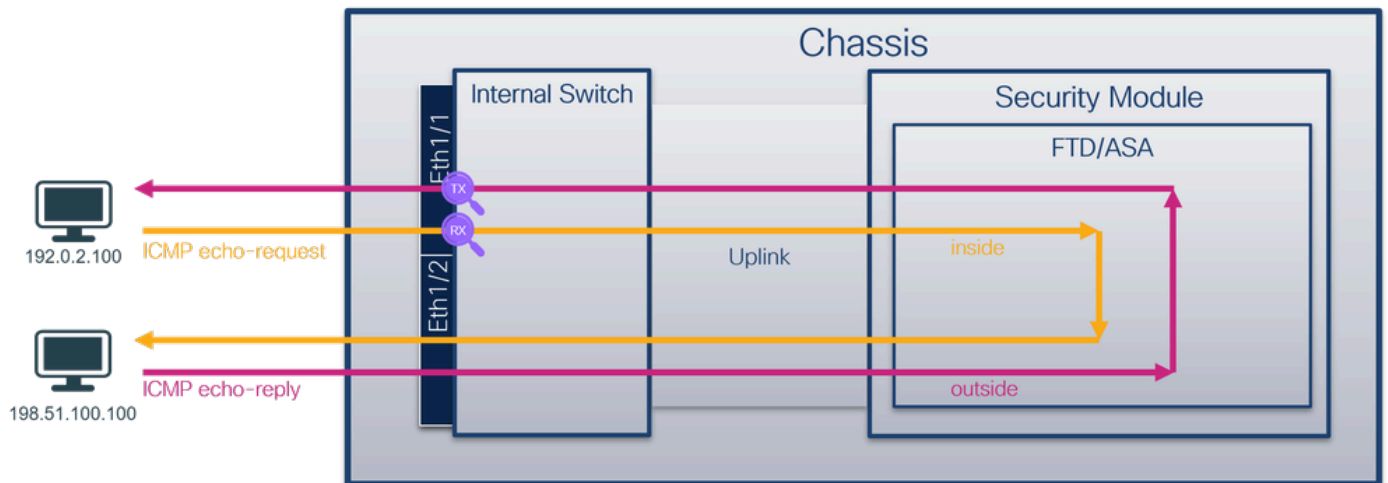
و 1/1 تنرثي ةهجاو ىلع هتحص نم ققحتل او ةمزح طاقات الة نيوكت الة ASA CLI و FTD مدختس ا لخدلا اب مسال نيتهجاو الة لك لمحت و . PortChannel1 ةهجاو

طاقات الة لوجم ، ةمزح الة قفدت ، طاطخملا

3100 نمآلآ ةياملال رادج:



هإتالآ ةيئانث تاعومجمب دوزملا 4200 زارط نمآلآ ةياملال رادج:



نيوكتلا

Port-channel1 و 1/1 تيئرثا نراق ىلع طبرلكشي نأ فTD CLI و ASA ىلع steps اذه تزجنا

مسالال نم ققحت 1.

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Port-channel1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

طاقات لاسلكية 2.

```
<#root>
```

```
>
```

```
capture capsw switch interface inside
```

طاقات لاسلكية هي جوت Secure Firewall 4200 مع دي:

```
<#root>
```

```
> capture capsw switch interface inside direction ?
```

```
both To capture switch bi-directional traffic  
egress To capture switch egressing traffic  
ingress To capture switch ingressing traffic
```

```
> capture capsw switch interface inside direction both
```

3. طاقات لاسلكية تنكم:

```
<#root>
```

```
> no capture capsw switch stop
```

ققحت لاسلكية

نم دكأت. فرع م لاسلكية حفت فو لي غش ت لاسلكية راد لاسلكية طاقات لاسلكية م س لاسلكية نم ققحت
ي: ر ف ص ري غ ا ه ط ا ق ت ل ل م ت ي ت ل ل م ز ح ل ا د د ع ن أ و ت ي ا ب ل ا ب Pcapsize م ي ق د ا ي ز

```
<#root>
```

>

show capture capsw detail

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up

Oper State Reason: Active

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 12653
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

79 packets captured on disk using switch capture

Reading of capture file from disk is not supported

Secure Firewall 4200:

<#root>

>

show cap capsw detail

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up

Oper State Reason: Active

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 0

Direction: both

Drop: disable
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0

Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

33 packet captured on disk using switch capture

Reading of capture file from disk is not supported

أعضاء ألتاهج او عيمج ىلع طاق تلالال نيوك ت متي ، 1 Port-channel ةلأح ي في

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up

Oper State Reason: Active

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

slot Id: 1
Port Id: 4

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 28824

Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

Slot Id: 1

Port Id: 3

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap
Pcapsize: 18399

Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

show رمألا لال خ نم fxos local-mgmt رمأ يف port ملة ان قلا وضع تاهجاو نم ققحتلا نكمي
portchannel summary:

```
<#root>
```

```
>
```

```
connect fxos
```

```
...  
firewall#
```

```
connect local-mgmt
```

```
firewall(local-mgmt)#
```

```
show portchannel summary
```

```
Flags: D - Down          P - Up in port-channel (members)  
I - Individual H - Hot-standby (LACP only)  
s - Suspended  r - Module-removed  
S - Switched   R - Routed  
U - Up (port-channel)  
M - Not in use. Min-links not met
```

```
-----  
Group Port-      Type      Protocol  Member Ports  
  Channel  
-----  
1      Po1(U)      Eth       LACP      Eth1/3(P)  Eth1/4(P)
```

```
LACP KeepAlive Timer:
```

```
-----  
Channel PeerKeepAliveTimerFast  
-----  
1      Po1(U)      False
```

```
Cluster LACP Status:
```

```
-----  
Channel ClusterSpanned ClusterDetach ClusterUnitID ClusterSysID  
-----  
1      Po1(U)      False      False      0          clust
```

قاي سلا ةلا ح يف connect fxos admin رمألا ليغش تب مق، ASA لىل FXOS لىل لوصول
ةرادلا قاي س يف رمألا ليغش تب مق، ددعت مل

طاقات لال تافل م عي مجت

يلخ ادلا ةي امحلا رادج لوح م طاقات لال تافل م عي مجت مس قلا يف ةدوج و مل تاوطلخا اراج مق
نمألا.

طاقات لال فلم ليلحت

1/1. تنرثي إكبش ل طاقات لال اتافلم حتفل مزحلا طاقات لال اتافلم ئراق قيبطت مدختسا
 لولأا ةمزحلا دح. 3100 نمألا ةيامحل راج لىل مزحلا طاقات لال ليلحت متي، لاثملا اذف
 ةيساسألا طاقنلا صحفو:

1. طقف ICMP يدص بلط مزح طاقات لال متي.
2. ةمالع نودب لىل صألا ةمزحلا سار.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39482)	64	Echo (ping) request id=0x0034, seq=2/512, ttl=64 (no res
3	2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39590)	64	Echo (ping) request id=0x0034, seq=3/768, ttl=64 (no res
4	2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39678)	64	Echo (ping) request id=0x0034, seq=4/1024, ttl=64 (no re
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no re
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no re
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no re
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no re
9	2022-08-07 19:50:14.932804	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no re
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no r
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no r
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no r
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no r
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9ef6 (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no r
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no r
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40932)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no r
17	2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no r
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 Internet Control Message Protocol

```

0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00 ...4...P V....E-
0010 00 54 9a 10 40 00 40 01 b3 9c c0 02 64 c6 33 ..T:@:....d:3
0020 64 64 08 00 c6 91 00 34 00 01 61 17 f0 62 00 00 dd...X-5..MM-b-
0030 00 00 18 ec 08 00 00 00 00 00 10 11 12 13 14 15 .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 55 55 55 55 67UUUU
    
```

طاقنلا صحفو لولأا ةمزحلا دح. 1. PortChannel وضع تاهجاول طاقات لال اتافلم حتفا
 ةيساسألا:

1. طقف ICMP يدص بلط مزح طاقات لال متي.
2. ةمالع نودب لىل صألا ةمزحلا سار.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c)
 Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
 Internet Control Message Protocol

```

0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00 ...4...P V....E-
0010 00 54 92 96 40 00 40 01 bb 1b c0 00 02 64 c6 33 ..T:@:....d:3
0020 64 64 08 00 58 a8 00 35 00 01 4d 23 f0 62 00 00 dd...X-5..MM-b-
0030 00 00 0e c8 04 00 00 00 00 00 10 11 12 13 14 15 .....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .....!#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,-./012345
0060 36 37 55 55 55 55 67UUUU
    
```

حرشللا

Ethernet1/1 وأ PortChannel1 تاهجاول لىل لوحمل طاقات لال نيوكت متي

ةمهمل لودجلا اذف صخلى:

اهيلع ىلوتسملا رورملا ةكرح	هاجتا	ملاع ةيفصت يلخاد	ةطقن طاقتلالا	ةمهملا
نم ICMP ىدص تابلط ىلإ 192.0.2.100 فيضملا 198.51.100.100 فيضملا	* لخدم طقف	None	Ethernet1/1	ةمزح طاقتلالا نيوكت ىلج هتحص نم ققحتلاو Ethernet1/1 ةهجاو
نم ICMP ىدص تابلط ىلإ 192.0.2.100 فيضملا 198.51.100.100 فيضملا	* لخدم طقف	None	1/3 تنرثيلا Ethernet1/4	ىلج ةمزح طاقتلالا نيوكت PortChannel1 ةهجاو وضعلا تاهجاو مادختساب Ethernet1/3 و Ethernet1/4

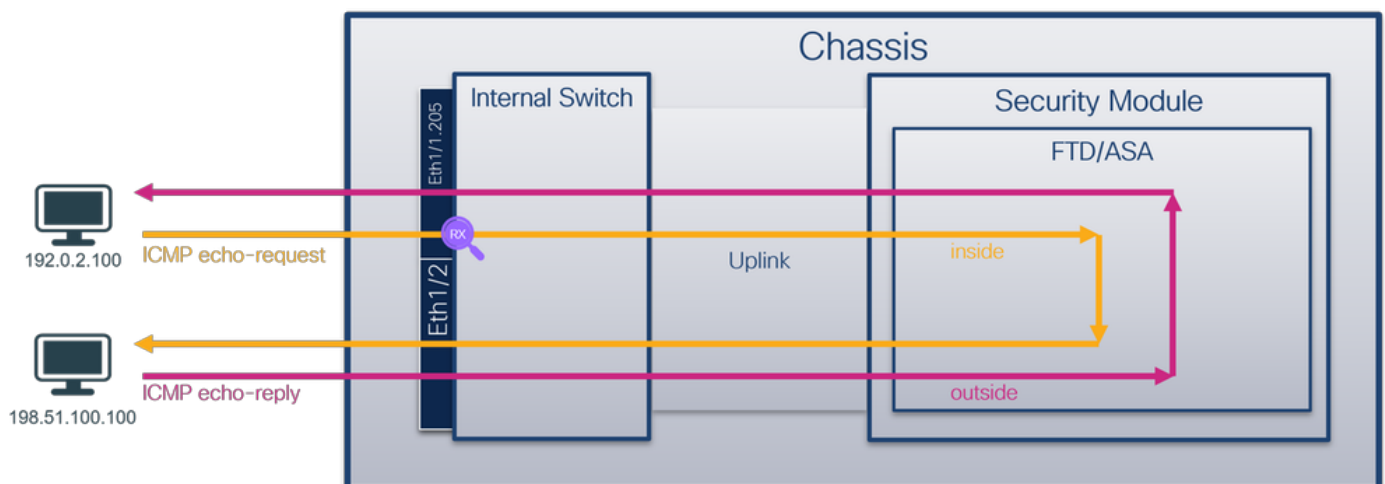
(لوخدلا) هاجتالا ةيئانث طاقتلالا تايلمع 4200 نمآلا ةيماحلا راج معدى، 3100 سكه ىلج * (جورخلاو).

ذفنم ةانق ةهجاو و ةيدام ةهجاو ةي عرف ةهجاو ىلج ةمزحلا طاقتلالا

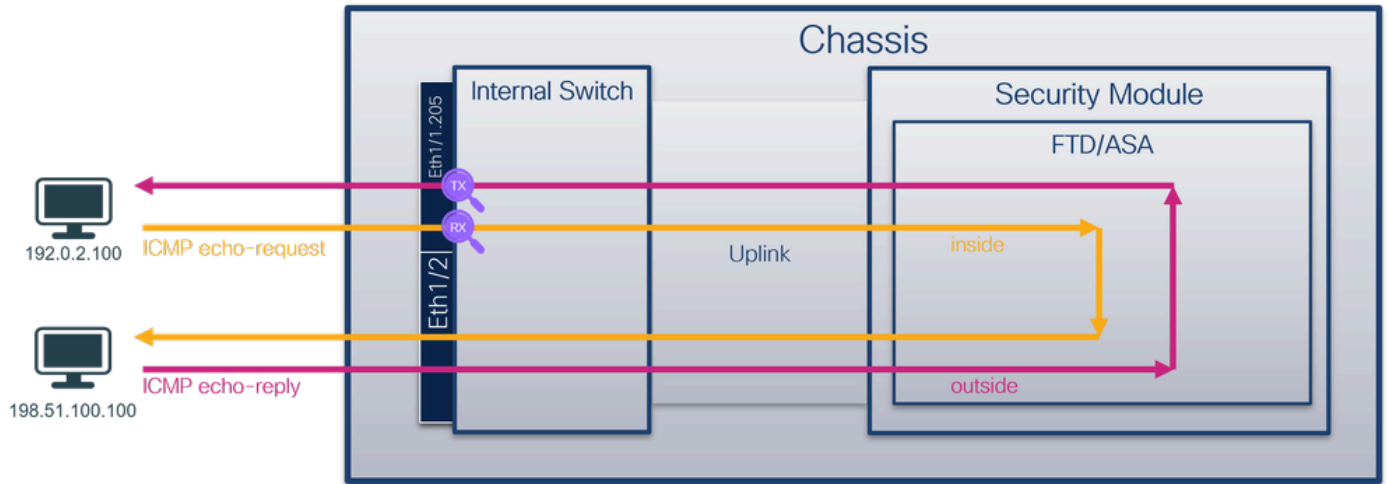
نم ققحتلاو ةمزح طاقتلالا نيوكتل ASA و FTD عون نم (CLI) رم اوألا رطس ةهجاو مدختسا تاهجاو الك يوتحت. PortChannel1.205 و Ethernet1/1.205 ةي عرفلا تاهجاو ىلج هتحص لخدلا م سالا ىلج ةي عرفلا.

طاقتلالا طاقنو، ةمزحلا قفدت، طمخمل

3100 نمآلا ةيماحلا راج:



4200 زارط نمآلا ةيماحلا راج:



نيوكتالا

Port-channel1 و 1/1 تي نرتا نراق يلع طبر لكشي نأ FTD CLI و ASA يلع steps اذه تزجنا

1. م ساللا نم ققحت:

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Port-channel1.205	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

2. طاقتلا ةسلج ءاشن:

```
<#root>
```

>

```
capture capsw switch interface inside
```

طاقات لالال هي جوت Secure Firewall 4200 م عدي

<#root>

```
> capture capsw switch interface inside direction ?
```

```
both To capture switch bi-directional traffic
egress To capture switch egressing traffic
ingress To capture switch ingressing traffic
```

```
> capture capsw switch interface inside direction both
```

3. طاقات لالال ة سلج ني ك مت ب م ق .

<#root>

```
> no capture capsw switch stop
```

ققحت لال

نأ ن م دكأت . فرع م لاولا ة تحت فول لي غ ش تل او ة راد لال ة لاج و طاقات لالال ة سلج م سا ن م ق قحت
ار فص سيل اه طاقات لال م ت ي تل م زحل لاد د ن أو ت ي اب ل اب دادزت PCAPSIZE ة م ي ق :

<#root>

>

```
show capture capsw detail
```

Packet Capture info

```
Name:                capsw

Session:             1

Admin State:         enabled

Oper State:          up

Oper State Reason:   Active
```

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap

Pcapsize: 6360

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0

Ivlan: 0

Ovlan: 205

Src Ip: 0.0.0.0

Dest Ip: 0.0.0.0

Src Ipv6: ::

Dest Ipv6: ::

Src MAC: 00:00:00:00:00:00

Dest MAC: 00:00:00:00:00:00

Src Port: 0

Dest Port: 0

Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

46 packets captured on disk using switch capture

Reading of capture file from disk is not supported

نراقب الـ VLAN=205 في جراح VLAN عم حشرم تقلخ، الـ هذه في

عـيـمـجـ الـ VLAN=205 في فصـتـ لـمـاعـ مـادـخـتـسـابـ طـاقـتـالـاـ نـيـوكـتـ مـتـيـ Port-channel1 الـ في
عـاضـعـالـ تـاهـجـاو:

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw
Session: 1
Admin State: enabled
Oper State: up

Oper State Reason: Active

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

slot Id: 1
Port Id: 4
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap
Pcapsize: 23442
Filter: capsw-1-4

Packet Capture Filter Info

Name: capsw-1-4
Protocol: 0
Ivlan: 0
Ovlan: 205
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00

Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Physical port:

slot Id: 1

Port Id: 3

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap

Pcapsize: 5600

Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3

Protocol: 0

Ivlan: 0

Ovlan: 205

Src Ip: 0.0.0.0

Dest Ip: 0.0.0.0

Src Ipv6: ::

Dest Ipv6: ::

Src MAC: 00:00:00:00:00:00

Dest MAC: 00:00:00:00:00:00

Src Port: 0

Dest Port: 0

Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

show رمأل لال خ نم fxos local-mgmt رمأ ي ف port ملة ان ق ل و ض ع تاه ج او نم ق ق ح ت ل ن ك م ي
portchannel summary:

<#root>

>

connect fxos

...

firewall#

connect local-mgmt

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
5	2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64	Echo (ping) request id=0x0037, seq=5/1280, ttl=64 (no res
6	2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64	Echo (ping) request id=0x0037, seq=6/1536, ttl=64 (no res
7	2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64	Echo (ping) request id=0x0037, seq=7/1792, ttl=64 (no res
8	2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64	Echo (ping) request id=0x0037, seq=8/2048, ttl=64 (no res
9	2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64	Echo (ping) request id=0x0037, seq=9/2304, ttl=64 (no res
10	2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64	Echo (ping) request id=0x0037, seq=10/2560, ttl=64 (no res
11	2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64	Echo (ping) request id=0x0037, seq=11/2816, ttl=64 (no res
12	2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64	Echo (ping) request id=0x0037, seq=12/3072, ttl=64 (no res
13	2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64	Echo (ping) request id=0x0037, seq=13/3328, ttl=64 (no res
14	2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64	Echo (ping) request id=0x0037, seq=14/3584, ttl=64 (no res
15	2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64	Echo (ping) request id=0x0037, seq=15/3840, ttl=64 (no res
16	2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64	Echo (ping) request id=0x0037, seq=16/4096, ttl=64 (no res
17	2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64	Echo (ping) request id=0x0037, seq=17/4352, ttl=64 (no res
18	2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64	Echo (ping) request id=0x0037, seq=18/4608, ttl=64 (no res

<p>Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)</p> <p>Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)</p> <p>802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205</p> <p>000. = Priority: Best Effort (default) (0)</p> <p>...0 = DEI: Ineligible</p> <p>... 0000 1100 1101 = ID: 205</p> <p>Type: IPv4 (0x0800)</p> <p>Trailer: 55555555</p> <p>Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100</p> <p>Internet Control Message Protocol</p>		<pre> 0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 81 00 00 cd ...4...P V..... 0010 08 00 45 00 00 54 41 1f 40 00 40 01 0c 8e c0 00 ..E..TA..@..... 0020 02 64 c6 33 64 64 08 00 06 67 00 37 00 01 b0 2c ..d:3dd...g:7... 0030 f0 62 00 00 00 00 8e fe 03 00 00 00 00 10 11 ..b..... 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 ..:.....! 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "##\$%&'()*+,-./01 0060 32 33 34 35 36 37 55 55 55 55 234567UU UU </pre>
---	--	---

طاقن ال صرحف وى لوالا ةمزلح ددح .PortChannel1 وضع تاهجاول طاقن الال تافل م ح تافا ةى ساسال:

1. طقف ICMP ى دص بل ط مزح طاقن الال م تي .
2. ةمالع ىلع ىلصلال ةمزلح لسأر يوتحي .

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	0x411f (16671)	64	Echo (ping) request id=0x0037, seq=1/256, ttl=64 (no res
2	2022-08-07 21:21:02.609418	192.0.2.100	198.51.100.100	ICMP	106	0x413a (16698)	64	Echo (ping) request id=0x0037, seq=2/512, ttl=64 (no res
3	2022-08-07 21:21:03.610671	192.0.2.100	198.51.100.100	ICMP	106	0x421a (16922)	64	Echo (ping) request id=0x0037, seq=3/768, ttl=64 (no res
4	2022-08-07 21:21:04.609160	192.0.2.100	198.51.100.100	ICMP	106	0x426c (17004)	64	Echo (ping) request id=0x0037, seq=4/1024, ttl=64 (no res
5	2022-08-07 21:21:05.609409	192.0.2.100	198.51.100.100	ICMP	106	0x4310 (17168)	64	Echo (ping) request id=0x0037, seq=5/1280, ttl=64 (no res
6	2022-08-07 21:21:06.611847	192.0.2.100	198.51.100.100	ICMP	106	0x43df (17375)	64	Echo (ping) request id=0x0037, seq=6/1536, ttl=64 (no res
7	2022-08-07 21:21:07.616688	192.0.2.100	198.51.100.100	ICMP	106	0x44d3 (17619)	64	Echo (ping) request id=0x0037, seq=7/1792, ttl=64 (no res
8	2022-08-07 21:21:08.618023	192.0.2.100	198.51.100.100	ICMP	106	0x4518 (17688)	64	Echo (ping) request id=0x0037, seq=8/2048, ttl=64 (no res
9	2022-08-07 21:21:09.619326	192.0.2.100	198.51.100.100	ICMP	106	0x453d (17725)	64	Echo (ping) request id=0x0037, seq=9/2304, ttl=64 (no res
10	2022-08-07 21:21:10.616696	192.0.2.100	198.51.100.100	ICMP	106	0x462b (17963)	64	Echo (ping) request id=0x0037, seq=10/2560, ttl=64 (no res
11	2022-08-07 21:21:11.621629	192.0.2.100	198.51.100.100	ICMP	106	0x4707 (18183)	64	Echo (ping) request id=0x0037, seq=11/2816, ttl=64 (no res
12	2022-08-07 21:21:12.619309	192.0.2.100	198.51.100.100	ICMP	106	0x474b (18251)	64	Echo (ping) request id=0x0037, seq=12/3072, ttl=64 (no res
13	2022-08-07 21:21:13.620168	192.0.2.100	198.51.100.100	ICMP	106	0x4781 (18305)	64	Echo (ping) request id=0x0037, seq=13/3328, ttl=64 (no res
14	2022-08-07 21:21:14.623169	192.0.2.100	198.51.100.100	ICMP	106	0x4858 (18520)	64	Echo (ping) request id=0x0037, seq=14/3584, ttl=64 (no res
15	2022-08-07 21:21:15.622497	192.0.2.100	198.51.100.100	ICMP	106	0x4909 (18697)	64	Echo (ping) request id=0x0037, seq=15/3840, ttl=64 (no res
16	2022-08-07 21:21:16.626226	192.0.2.100	198.51.100.100	ICMP	106	0x490b (18699)	64	Echo (ping) request id=0x0037, seq=16/4096, ttl=64 (no res
17	2022-08-07 21:21:17.629363	192.0.2.100	198.51.100.100	ICMP	106	0x4932 (18738)	64	Echo (ping) request id=0x0037, seq=17/4352, ttl=64 (no res
18	2022-08-07 21:21:18.626651	192.0.2.100	198.51.100.100	ICMP	106	0x4a05 (18949)	64	Echo (ping) request id=0x0037, seq=18/4608, ttl=64 (no res

<p>Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 bits)</p> <p>Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14)</p> <p>802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205</p> <p>000. = Priority: Best Effort (default) (0)</p> <p>...0 = DEI: Ineligible</p> <p>... 0000 1100 1101 = ID: 205</p> <p>Type: IPv4 (0x0800)</p> <p>Trailer: 55555555</p> <p>Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100</p> <p>Internet Control Message Protocol</p>		<pre> 0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 81 00 00 cd ...4...P V..... 0010 08 00 45 00 00 54 41 1f 40 00 40 01 0c 8e c0 00 ..E..TA..@..... 0020 02 64 c6 33 64 64 08 00 06 67 00 37 00 01 b0 2c ..d:3dd...g:7... 0030 f0 62 00 00 00 00 8e fe 03 00 00 00 00 10 11 ..b..... 0040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 ..:.....! 0050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "##\$%&'()*+,-./01 0060 32 33 34 35 36 37 55 55 55 55 234567UU UU </pre>
---	--	---

ح رشل

Ethernet1/1.205 ةى عرفال تاهجاولا ىلع لو حمال طاقن الال نى وكت م تي PortChannel1 و ةى جراخال VLAN ةكبش عم قباطتي ةى فصت لماع مادختساب

ةمهمل لودجال اذه صخلى:

ةمهمل	طاقن الال	لماع ةى فصت ىلخاد	هاجتا	ىلوت سمال رورمال ةك رح اه ىلع
-------	-----------	-------------------	-------	-------------------------------

ق قحتل او ة مزح طاق تال ني وكت ة ه اوالا ل ع ه تحص ن م ة ي عرفال Ethernet1/1.205	Ethernet1/1	ة ك ب ش VLAN ة ي ج را خ ل ا 205	ل خ دم * ط ق ف	ن م ICMP ي دص ت ا ب ل ط ل ا 192.0.2.100 في ضم ل ا 198.51.100.100 في ضم ل ا
ة مزح طاق تال ني وكت ب م ق ل ع ه تحص ن م ق قحتل او ة ي عرفال ة ه اوالا م ا د خ ت س ا ب PortChannel1.205 و Ethernet1/3 ا ض ع ا ل ا ت ا ه ا و ل ا Ethernet1/4	1/3 ت ن ر ث ي ا Ethernet1/4	ة ك ب ش VLAN ة ي ج را خ ل ا 205	ل خ دم * ط ق ف	ن م ICMP ي دص ت ا ب ل ط ل ا 192.0.2.100 في ضم ل ا 198.51.100.100 في ضم ل ا

(لو خ دل ا) ه ا ج ت ا ل ا ة ي ئ ا ن ث طاق تال ا ل ا ت ا ي ل م ع 4200 ن م ا ل ا ة ي ا م ح ل ا ر ا د ج م ع د ي ، 3100 س ك ع ل ع *
(ج و ر خ ل ا و).

ة ي ل خ ا د ل ا ت ا ه ا و ل ا ل ع ة مزح ل ا طاق تال

ن ي ت ي ل خ ا د ن ي ت ه ج ا و ل ع 3100 ن م ا ل ا ة ي ا م ح ل ا ر ا د ج ي و ت ح ي :

- in_data_uplink1 - ل ي ل خ ا د ل ا ل و ح م ل ا ب ق ي ب ط ت ل ل ل ي ص و ت ب م و ق ي -
- in_mgmt_uplink1 - ة ه ا و ل ا ل ا ل ا ص ت ا ل ا ص ص خ م ة مزح ر ا س م ر ف و ي - sftunnel م س ا ب ا ض ي ا ف و ر ع م ل ا ، ة ر ا د ا ل ا ل ا ص ت ا و ا ، ة ر ا د ا ل ا
FMC و FTD ن ي ب .

ة ي ل خ ا د ت ا ه ا و ل ا 4 ل ا ل ا ل ص ي ا م ل ع 4200 ن م ا ل ا ة ي ا م ح ل ا ر ا د ج ي و ت ح ي :

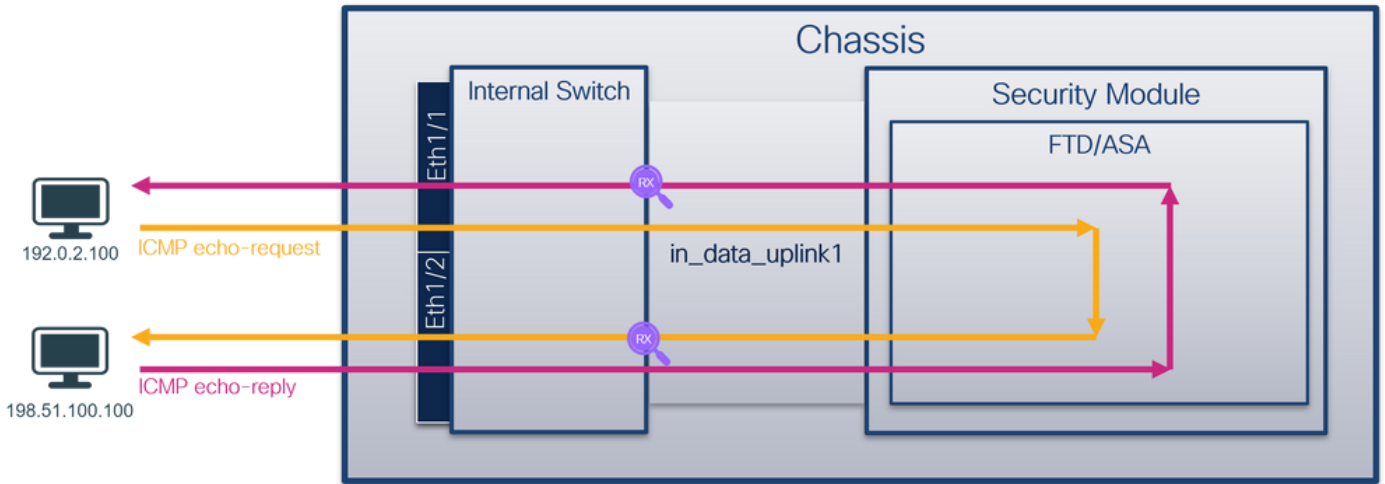
- in_data_uplink1 gin_data_uplink2 (4245 ط ق ف) - م و ق ت - ة ي ب ط ت ل ل ل ي ص و ت ب ت ا ه ا و ل ا ه ذ ه م و ق ت -
2. ت ا ل ا ص و ل ا ت ا ه ا و ل ا و ر ب ع ل ا م ح ا ل ا ة ن ز ا و م م ز ح ل ا ن و ك ت ، 4245 ة ل ا ح ي ف . ل ي ل خ ا د ل ا ل و ح م ل ا ب
- in_mgmt_uplink1 gin_mgmt_uplink2 - م و ق ت - ة ه ا و ل ا ل ا ص ص خ م ة مزح ر a s m ر ف و ت -
ن ي ب ، sftunnel م س ا ب ا ض ي ا ف و ر ع م ل ا ، ة ر a د ا ل ا ل ا ص ت a و a ، ة R a D a l a ة ه a و ل a ل ا S S H ل ث م ، ة R a D a l a
FMC و FTD . ة R a D a l a ي ت ه a و L 4200 ن M a l a ة ي a M ح l a R a D ج M ع D ي .

1 ة م ه م ل ا

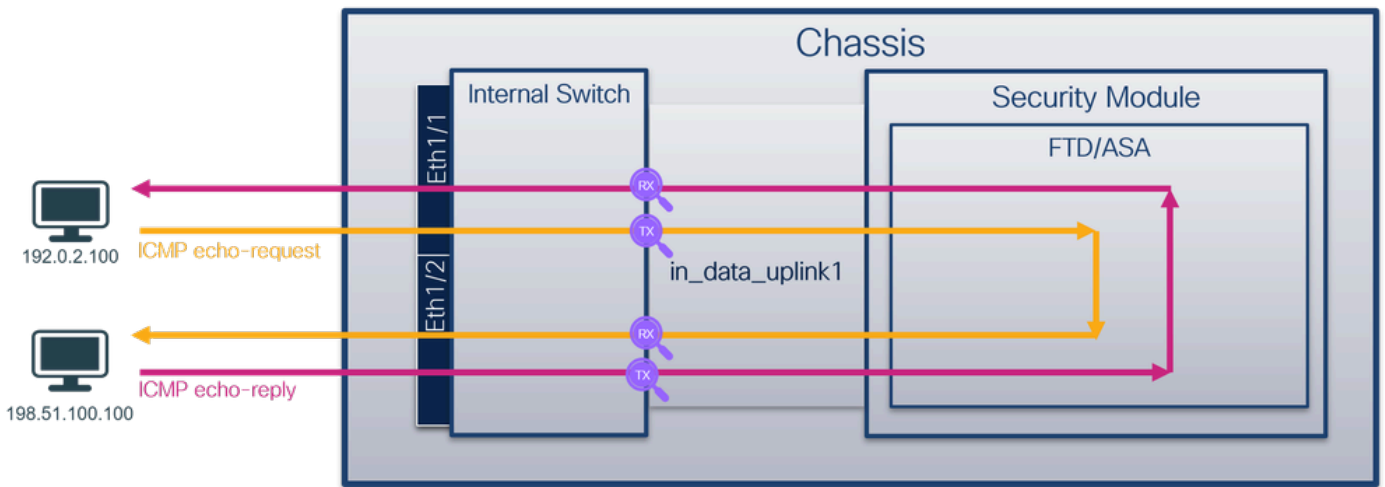
ة ل ص و ل ا ة ه ا و ل ا ل ع ه تحص ن م ق قحتل او ة مزح طاق تال ني وكت ل ASA CLI و FTD م د خ ت س ا
في_data_uplink1.

طاق تال ا ل ا طاق ن و ، ة مزح ل ا ق ف د ت ، ط ا ط خ م ل ا

3100 ن م ا ل ا ة ي ا م ح ل ا ر ا د ج :



4200: زارط نم آلا ةي امحل رادج



ني وكتلا

in_data_uplink1: نراق يلع طاقتل طبر لكشي نأ FTD CLI و ASA يلع steps اذه تزجنأ

1. طاقتل ةسلج عاشنإ:

```
<#root>
```

```
>
```

```
capture capsw switch interface in_data_uplink1
```

طاقتل الال هي جوت Secure Firewall 4200 م عدي

```
<#root>
```

```
> capture capsw switch interface in_data_uplink1 direction ?
```

both To capture switch bi-directional traffic
egress To capture switch egressing traffic

ingress To capture switch ingress traffic

```
> capture capsw switch interface in_data_uplink1 direction both
```

2. إرسال طاقته الال تنكمم:

<#root>

```
> no capture capsw switch stop
```

ققحتال

نأ نم دكأت. فرع مل او هج اول اة تحت فو لي غش تل او ة راد ال اة لاج و طاقته الال ة سلج مسا نم ققحت
ارفض س سل اه طاقته الال م ت ي تل مزحلل ددع ن أو ت ي اب لاب دادزت PCAPSIZE ة مي ق

<#root>

>

```
show capture capsw detail
```

Packet Capture info

Name: capsw

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

Config Success: yes

Config Fail Reason:

Append Flag: overwrite

Session Mem Usage: 256

Session Pcap Snap Len: 1518

Error Code: 0

Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

slot Id: 1

Port Id: 18

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap

Pcapsize: 7704

Filter: capsw-1-18

Packet Capture Filter Info

Name: capsw-1-18
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

66 packets captured on disk using switch capture

Reading of capture file from disk is not supported

هه او وهو 18 يلخاد فرعم مادختساب هه اولو لىل ع طاقتل عاشن متي، لال هذه في
في show portManager switch status رمال ضرعي. 3130 نمال اهي امحل رادج لىل ع in_data_uplink1
هه اولو تافرعم fxos local-mgmt shell رمال:

<#root>

>

connect fxos

...

firewall#

connect local-mgmt

firewall(local-mgmt)#

show portmanager switch status

Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up

0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

قايس الة لاج في connect fxos admin رمال لئغشتب مق، ASA لى لى FXOS لى لوصول لة رادل قايس في رمال اذ لئغشتب مق، ددعت مال

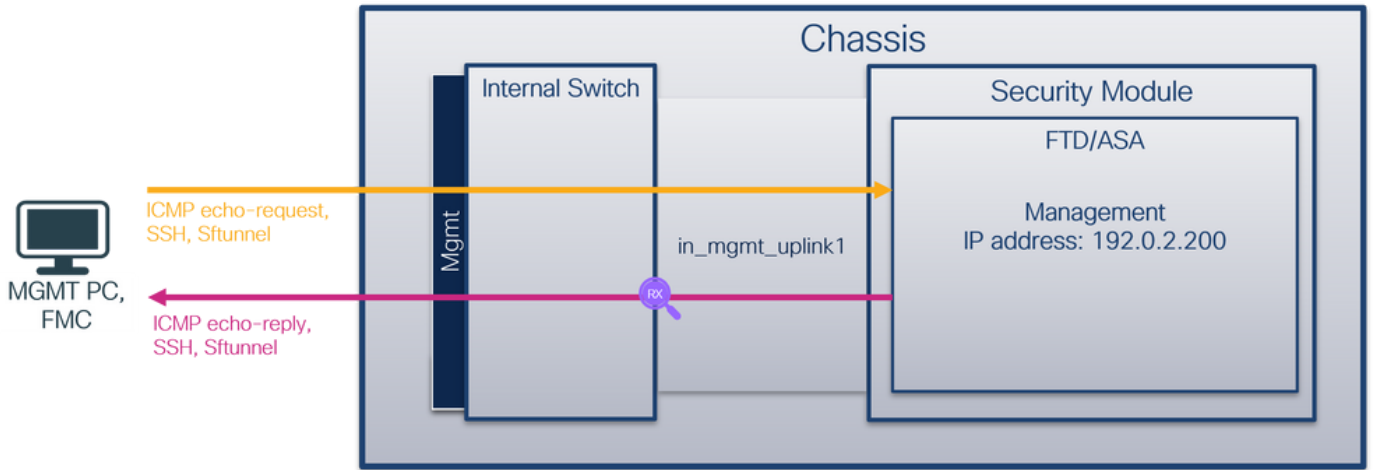
طاقات الة تافل م عي م ح ت

يلخ ادلة لة م ح الة راج ل و ح م طاقات الة تافل م عي م ح ت م س ق الة في ة د و ج و م الة تا و ط خ الة ا ر ج اب مق ن م الة

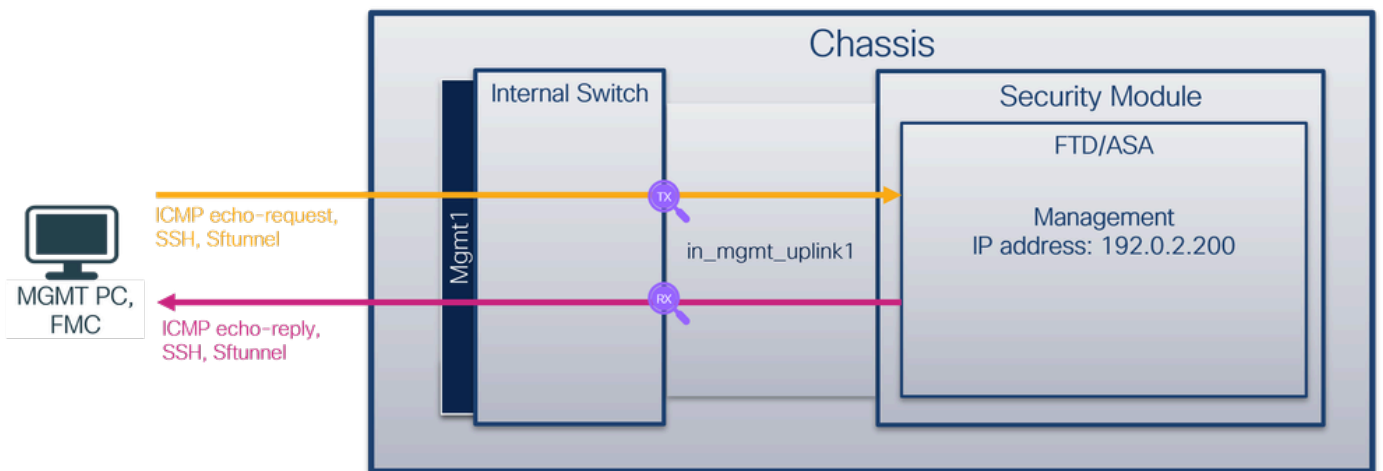
طاقات الة فلم لئ ل ح ت

ة ه ج اولل طاقات الة تافل م ح ت فلم م ح الة طاقات الة تافل م ئراق قئ ب ط ت م د خ ت س ا 3100 ن م الة لة م ح الة راج لى لى م ح الة طاقات الة لئ ل ح ت م تئ، ل ا ث م الة اذ لى في .data_uplink1 في

للى لى م ح و ICMP لى ص ب ل ط طاقات الة م تئ، ل ا ح الة هذ لى في - ح ا ت ف م الة ة ط ق ن م ق ق ح ت لى لى ل و ح م الة لى قئ ب ط ت الة ن م ة ل س ر م الة م ح الة لى هذ لى د ا د ت ر الة



4200 زارط نمآلآ ةي امحلآ رادج:



نيوكتلآ

in_mgmt_uplink1: ف نراق ىل ع طاقتلآ طبر لكشي نأ FTD CLI و ASA ىل ع steps اذه تزجنأ

1. طاقتلآ ةسلج عاشنإ:

```
<#root>
```

```
>
```

```
capture capsw switch interface in_mgmt_uplink1
```

طاقتلآ الآ هي جوت Secure Firewall 4200 معدي

```
<#root>
```

```
> capture capsw switch interface in_mgmt_uplink1 direction ?
```

both To capture switch bi-directional traffic
egress To capture switch egressing traffic
ingress To capture switch ingressing traffic

0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset
0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

قاي سلا ة ل ا ح ي ف . connect fxos admin ر م أ ل ا ل ي غ ش ت ب م ق ، ASA ل ع FXOS ل ل ا ل و ص و ل ل ة ر ا د ا ل ا ق ا ي س ي ف ر م أ ل ا ا ذ ه ل ي غ ش ت ب م ق ، د د ع ت م ل ا

ط ا ق ت ل ل ا ل ا ت ا ف ل م ع ي م ح ت

ي ل خ ا د ل ا ة ي ا م ح ل ا ر ا د ج ل و ح م ط ا ق ت ل ل ا ت ا ف ل م ع ي م ح ت م س ق ل ا ي ف ة د و ج و م ل ا ت ا و ط خ ل ا ذ ي ف ن ت ن م أ ل ا

ط ا ق ت ل ل ا ل ا ف ل م ل ي ل ح ت

in_mgmt_uplink1. ة ه ا و ل ط ا ق ت ل ل ا ل ا ت ا ف ل م ح ت ف ل م ح ل ا ط ا ق ت ل ل ا ت ا ف ل م ئ ر ا ق ق ي ب ط ت م د خ ت س أ 3100 ن م أ ل ا ة ي ا م ح ل ا ر ا د ج ل ع م ح ل ا ط ا ق ت ل ل ا ل ي ل ح ت م ت ي ، ل ا ث م ل ا ا ذ ه ي ف

ة ر ا د ا ل ا ب ص ا خ ل ا IP ن ا و ن ع ن م م ح ل ا ض ر ع م ت ي ط ر ف ة ل ا ح ل ا ه ذ ه ي ف - ح ا ت ف م ل ا ة ط ق ن ن م ق ق ح ت م ح ل ا ي ه ه ذ ه . ICMP echo و Sftunnel و SSH ل و ك و ت و ر ب ل ع د ر ل ا م ح ي ه ة ل ث م أ ل ا . 192.0.2.200 ي ل خ ا د ل ا ل و ح م ل ا ل ا ل خ ن م ة ك ب ش ل ا ل ل ق ي ب ط ت ل ا ة ر ا د ا ة ه ا و ن م ة ل س ر م ل ا

(جورنالو).

مزحل طاقتلل ةيفصت لماع

اهب متي يتللا ةقيرطال س فنن ب يلخادلل لومللا ةمزح طاقتلل ةيفصت لماع نيوكت متي لماع نيوكتل ةقباطملاو تنرثيلا عون تاراخي مدختسا. تانايبلا يوتسم نيوكتل ةيفصتلل.

نيوكتلل

ةمزح طاقتلل نيوكتل FTD و ASA ل (CLI) رم اوأل رطس ةهجاو يلل ع تاوطخلل هذه ءارجاب مق ةهجاو يلل ع 198.51.100.100 فيضملل نم ICMP مزح و ARP تارايل قباطي حشرم مادختساب 1/1 تنرثيلا:

1. م سالل نم ققحت:

```
<#root>
```

```
>
```

```
show nameif
```

Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

2. ARP و ICMP ل طاقتلل ةسلج ءاشنل:

```
<#root>
```

```
>
```

```
capture capsw switch interface inside ethernet-type arp
```

```
<#root>
```

```
> capture capsw switch interface inside match icmp 198.51.100.100
```

ققحتلل

0x0806 و يرشع 2054 ه EtherType ةمقي ق. ةيفصتلل لماع و طاقتلل ةسلج مسا نم ققحت يرشع يسايس ف:

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 0

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0

Ethertype: 2054

Total Physical breakout ports involved in Packet Capture: 0

0 packet captured on disk using switch capture

Reading of capture file from disk is not supported

ICMP: وه 1 IP لوكوتورب. ICMP ةيفصت نم ققحتلا وه اذه

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1
Admin State: disabled
Oper State: down
Oper State Reason: Session_Admin_Shut
Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize: 0

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 1

Ivlan: 0
Ovlan: 0

Src Ip: 198.51.100.100

```
Dest Ip:          0.0.0.0
Src Ipv6:         ::
Dest Ipv6:        ::
Src MAC:          00:00:00:00:00:00
Dest MAC:         00:00:00:00:00:00
Src Port:         0
Dest Port:        0
Ethertype:        0
```

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

نم آلا ةي امحلل رادجل يلخادلا ل وحملا طاقتل اتافل م عي مجت

اضي انكمي، FTD لىل ع. يلخادلا ل وحملا طاقتل اتافل م عي مجت ل FTD CLI و ASA مدختسأ لال خ نم اهل ل لوصول انكمي يتل اتاهول لىل CLI ل copy رمأل ربع طاقتل الال فلم ري دصت ات. اصي خشتل و اتاناي بل اتاهول

FMC نم هل يزنت و ري بخلل عضو في /ngfw/var/common لىل فلم ال خسن انكمي، كلذ نم ال دب فلم ال ل يزنت رايل لال خ نم

ءاضع ال اتاهول عي مجت نم مزحلل طاقتل اتافل م عي مجت نم صت ذفنم ال ةانق اتاهول ةلا ح في

ASA

ASA CLI لىل دربم طاقتل اتافل م يلخاد عمجي نأ قوف steps اذه تزجنأ

1. طاقتل الال فاقيل:

```
<#root>
```

```
asa#
```

```
capture capsw switch stop
```

2. طاقتل الال فلم مسا طحال و طاقتل الال ةسلج فاقيل نم ققحت.

```
<#root>
```

```
asa#
```

```
show capture capsw detail
```

Packet Capture info

Name: capsw

Session: 1

Admin State: disabled

Oper State: down

Oper State Reason: Session_Admin_Shut

Config Success: yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code: 0
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1
Port Id: 1

Pcapfile:

/mnt/disk0/packet-capture/

sess-1-capsw-ethernet-1-1-0.pcap

Pcapsize: 139826
Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1
Protocol: 0
Ivlan: 0
Ovlan: 0
Src Ip: 0.0.0.0
Dest Ip: 0.0.0.0
Src Ipv6: ::
Dest Ipv6: ::
Src MAC: 00:00:00:00:00:00
Dest MAC: 00:00:00:00:00:00
Src Port: 0
Dest Port: 0
Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

3. اديعب تاهجوى لى فلملا ري دصت ل CLI copy رم ال مدختسأ .

<#root>

asa#

copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?

```
cluster:      Copy to cluster: file system
disk0:        Copy to disk0: file system
disk1:        Copy to disk1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
smb:          Copy to smb: file system
startup-config Copy to startup configuration
system:       Copy to system: file system
tftp:         Copy to tftp: file system
```

asa#

copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/

Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?

Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?

Copy in progress...C

139826 bytes copied in 0.532 secs

م اظن Firepower Threat Defense (FTD)

رم اوأل رطس ةه جاو ىل ع ةي لخ ادل ل و ح م ل ط ا ق ت ل ا ف ل م ع ي م ج ت ل ا و ط خ ل ا ه ذ ه ا ر ج ا ب م ق ت ا ص ي خ ش ت ل ا و ا ت ا ن ا ي ب ل ا ت ا ه ج ا و ر ب ع ا ه ي ل ل و و ص و ل ا ن ك م ي ي ت ل ا م د ا و خ ل ا ى ل ا ه خ س ن و F T D ي ف

1. ي ص ي خ ش ت ل ا C L I ى ل ل ا ق ت ن ا ل ا .

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Click 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>

enable

Password:

<-- Enter

firepower#

2. طاقنلالا فاقيا:

```
<#root>
```

```
firepower#
```

```
capture capi switch stop
```

3. طاقنلالا فلم مسا طحالو طاقنلالا ةسلج فاقيا نم ققحت:

```
<#root>
```

```
firepower#
```

```
show capture capsw detail
```

```
Packet Capture info
```

```
Name:                capsw
```

```
Session:             1
```

```
Admin State:        disabled
```

```
Oper State:         down
```

```
Oper State Reason:  Session_Admin_Shut
```

```
Config Success:     yes
```

```
Config Fail Reason:
```

```
Append Flag:        overwrite
```

```
Session Mem Usage:  256
```

```
Session Pcap Snap Len: 1518
```

```
Error Code:         0
```

```
Drop Count:         0
```

```
Total Physical ports involved in Packet Capture: 1
```

```
Physical port:
```

```
Slot Id:            1
```

```
Port Id:            1
```

```
Pcapfile:
```

```
/mnt/disk0/packet-capture/
```

```
sess-1-capsw-ethernet-1-1-0.pcap
```

```
Pcapsize:           139826
```

```
Filter:             capsw-1-1
```

Packet Capture Filter Info

```
Name:          capsw-1-1
Protocol:      0
Ivlan:        0
Ovlan:        0
Src Ip:        0.0.0.0
Dest Ip:       0.0.0.0
Src Ipv6:      ::
Dest Ipv6:     ::
Src MAC:       00:00:00:00:00:00
Dest MAC:      00:00:00:00:00:00
Src Port:      0
Dest Port:     0
Ethertype:    0
```

Total Physical breakout ports involved in Packet Capture: 0

886 packets captured on disk using switch capture

Reading of capture file from disk is not supported

4. ةديعب تاهجو لىل فلمل ري دصت ل CLI copy رمأل مدختسأ .

```
<#root>
```

```
firepower#
```

```
copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
```

```
cluster:      Copy to cluster: file system
disk0:        Copy to disk0: file system
disk1:        Copy to disk1: file system
flash:        Copy to flash: file system
ftp:          Copy to ftp: file system
running-config Update (merge with) current system configuration
scp:          Copy to scp: file system
smb:          Copy to smb: file system
startup-config Copy to startup configuration
system:       Copy to system: file system
tftp:         Copy to tftp: file system
```

```
firepower#
```

```
copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
```

```
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
```

```
Copy in progress...C
```

```
139826 bytes copied in 0.532 secs
```

فلمل ليزنت راخ لالخ نم FMC نم طاقتلال تافل عيمحتل تاوطخل هذه عارجاب مق

1. طاقتلال فاقلي:

<#root>

>

capture capsw switch stop

لماكلا طاقتلالا فلم راسمو فلملا مسا ظحالو طاقتلالا ةسلج فاقيا نم ققحت 2.

<#root>

>

show capture capsw detail

Packet Capture info

Name: capsw

Session: 1

Admin State: disabled

Oper State: down

Oper State Reason: Session_Admin_Shut

Config Success: yes

Config Fail Reason:

Append Flag: overwrite

Session Mem Usage: 256

Session Pcap Snap Len: 1518

Error Code: 0

Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

Slot Id: 1

Port Id: 1

Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap

Pcapsize: 139826

Filter: capsw-1-1

Packet Capture Filter Info

Name: capsw-1-1

Protocol: 0

Ivlan: 0

Ovlan: 0

Src Ip: 0.0.0.0


```
Dest Ip:          0.0.0.0
Src Ipv6:         ::
Dest Ipv6:        ::
Src MAC:          00:00:00:00:00:00
Dest MAC:         00:00:00:00:00:00
Src Port:         0
Dest Port:        0
Ethertype:        0
```

Total Physical breakout ports involved in Packet Capture: 0
886 packets captured on disk using switch capture
Reading of capture file from disk is not supported

3. رذجال عضو لى لقتنا وري بخلال عضو لى لقتنا:

```
<#root>
```

```
>
```

```
expert
```

```
admin@firepower:~$
```

```
sudo su
```

```
root@firepower:/home/admin
```

4. لى لقتنا لال فلم خسننا:

```
<#root>
```

```
root@KSEC-FPR3100-1:/home/admin
```

```
cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap /ngfw/var/common/
```

```
root@KSEC-FPR3100-1:/home/admin
```

```
ls -l /ngfw/var/common/sess*
```

```
-rwxr-xr-x 1 root admin 139826 Aug  7 20:14
```

```
/ngfw/var/common/sess-1-capsw-ethernet-1-1-0.pcap
```

```
-rwxr-xr-x 1 root admin    24 Aug  6 21:58 /ngfw/var/common/sess-1-capsw-ethernet-1-3-0.pcap
```

5. فلم لى لىزنت > ةزهجال رتخأ، FMC فى:

ةرادإلا قايس يف طقف in_mgmt_uplink1

TAC تالاح يف مزحلا طاقنلا مادختسا إىلا ةدنتسما تاسرامملا لضفا ةمئاق يه هذه

- دووقلاو ةيهيجوتلا ئدابملا بة ياردى لىع نك
- طاقنلا ةيفصت لماع مادختسا
- حشرم طاقنلا تلكش ام دنع ناو نع طبرلا لىع NAT ريثأت رابتعالا يف تعضو
- ةميقلا نع هفالتخا ةلاح يف ، راطإلا مجح دحت يىتلا ةمزحلا لوط لىلقن وأ ةدايزب مق ةطقنلما مزحلا نم ديازتم ددع رصقألا مجحلا نع جتنى . تياب 1518 ةيضا رتفالا سكالاب سكالو
- ةجالحا بسح تقوؤملا نزخملا مجح طبضب مق
- درجمب . show cap <cap_name> detail رمألا تاجرخم يف طاقنلا ددعب ةياردى لىع نك . طاقنلا دادع دادع دادع ، تقوؤملا نزخملا مجح دح لىلا لوصول

ةلص تاذا مولىعم

- [Firepower 4100/9300 يف رماوأل رطس ةهجاو نيوكت ةلدأ](#)
- [Cisco نم 3100 نمأل ةيماحلا رادج لىغشت ادب لىلد](#)
- [Cisco Firepower 4100/9300 FXOS رماوأل عجرم](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل