

ةيلخادلإ FirePOWER تالوحه تاعومجم نيوكت  
اـهـتـحـصـ نـمـ قـقـحـتـلـاـوـ ةـنـمـ آلـاـ

تایوتیم

مدودة

قىسىم اولا تابلىطتىمىلا

تاتل طتملا

## ةمدختس ملاتانوكمل

قیس اس اتامولعمر

**ماظنلا قينب ىلعا ىوتسملا ىلداع قماع قرطن**

قرطاجي ملائكة يحيى وحملات اسلامية قديمة

## طاقة الـ مـزـحـلـاـ قـفـدـت

Firepower 4100/9300 نیوکوتلا قوقحت لاو یلع

**ذفنم قانق ٥٥جاو وأ ٦٥جاو يلع ٦٥مزحل طاقتلا**

**قىفل خلا ۋە حوللا تاھجاوىلىع قمىز خلا طاقلى**

**قىب طتلا ذفانمو قىب طتلا يلىع ۋەزىللا طاقتلا**

**ذفنم ۋانق ۋەجىۋەل دام ۋەجىۋەل قىيىرۇن ئەمچىكلىق ۋەجىۋەل ئەمچىكلىق**

## مژحل لام او فیصله طاقت

**Firepower 4100/9300 يلخادل لوحمل ا طاقتل ا تافلم عيمجت**

**يُخلِّصُ الْجَنَاحَ الْمُلْكَ لِلْمُؤْمِنِينَ إِذَا دَعَا إِلَيْهِ وَتَرَدَّدَ**

3100/4200 نمآلا قيامحلا رادجىلۇر ققحتلار نېوكتىلا

ذفنم ۋانق ۋەجىءەن دام ۋەجىءەنلىق ۋەزىلە ئەملىكىلا طاقىتلى

ةيكلخ ادلات اهجاولايلىع قمىزجلا طاقتلا

مزيلا طاقتلا ئيفصت لىمادع

نمآلا ڦيامحل را راجل یلخ ادل لوحمل طاقتلا تافلم عيمجت

يـلـخـادـلـا لـوـحـمـلـا قـمـزـحـ طـاقـتـلـا لـاـ تـاسـرـامـمـلـا لـضـفـأـوـدـيـدـحـتـوـتـادـاشـراـ

علم و اذ تاذ ام قلص

# مدقّم

LITERATURE

as you do | I am so | full of | love for | you || || You are

## ةمـدـخـتـسـمـلـا تـانـوـكـمـلـا

ةـصـاخـ ةـيـلـمـعـ ةـئـيـبـ يـفـ ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـمـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـدـرـاـوـلـا تـامـوـلـعـمـلـا عـاـشـنـا مـتـ تـنـاـكـ اـذـاـ .(يـضـارـتـفـا) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،لـيـغـشـتـلـا دـيـقـ لـكـنـكـبـشـ

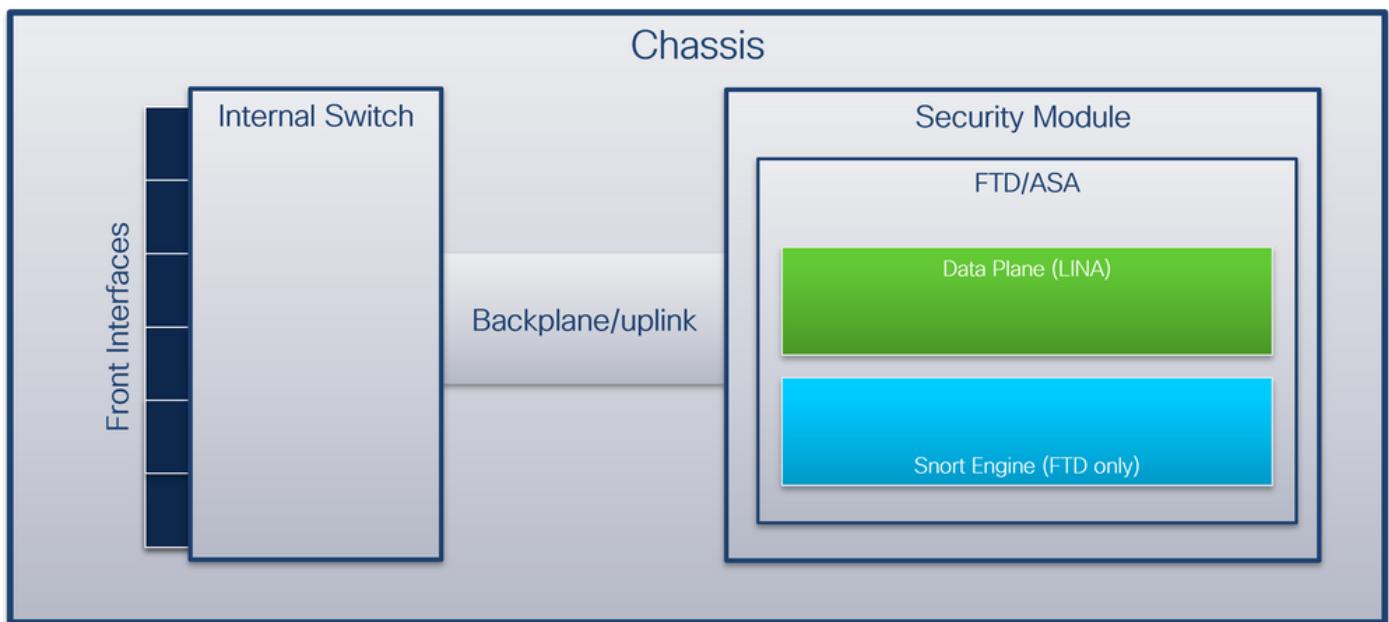
ةـيـلـاتـلـا ةـيـدـاـمـلـا تـانـوـكـمـلـا وـجـمـارـبـلـا تـارـادـصـاـىـلـا دـنـتـسـمـلـا اـذـهـ يـفـ ةـدـرـاـوـلـا تـامـوـلـعـمـلـا دـنـتـسـتـ

- Secure Firewall 31xx و 42xx
- Firepower 41xx
- Firepower 93xx
- نـمـ Cisco FXOS 2.12.0.x (FXOS) نـمـ Cisco FTD 7.2.0.x، 7.4.1-172
- نـمـ Cisco FMC 7.2.0.x، 7.4.1-172
- فـيـكـتـلـلـ لـبـاـقـلـا نـامـأـلـا زـاهـجـ (ASA) 9.18(1)x و 9.20(x)
- Wireshark 3.6.7 (<https://www.wireshark.org/download.html>)

## ةـيـسـاسـأـ تـامـوـلـعـمـ

### ماـظـنـلـا ةـيـنـبـ يـلـعـ يـوـتـسـمـلـا ةـيـلـاعـ ةـمـاـعـ ةـرـظـنـ

نـمـآـلـا ةـيـاـمـحـلـا رـاـدـجـوـ 4100/9300 Firepower ةـيـنـبـ روـصـتـ نـكـمـيـ ،ةـمـزـحـلـا قـفـدـتـ روـظـنـمـ نـمـ 3100/4200:



تـانـوـكـمـلـا هـذـهـ لـكـيـهـلـا نـمـضـتـيـ:

- ليـصـوتـ مـتـيـ .سـكـعـلـاوـ قـيـبـطـتـلـا يـلـا ةـكـبـشـلـا نـمـ ةـمـزـحـلـا هـيـجـوـتـ دـيـعـيـ - يـلـخـادـلـا لـوـحـمـلـا ةـكـبـشـلـا تـادـحـوـ وـأـ ةـجـمـدـمـلـا ةـهـجـاـوـلـا ةـدـحـوـ يـلـعـ ةـدـوـجـوـمـلـا ةـيـمـامـأـلـا تـاهـجـاـوـلـا يـلـخـادـلـا لـوـحـمـلـا تـاهـجـاـوـلـا ةـلـثـمـأـ .تـالـوـحـمـلـا، لـلـاثـمـلـا لـيـبـسـ يـلـعـ، ةـيـجـرـاـخـلـا ةـزـهـجـأـلـا لـاـصـتـالـا وـةـيـجـرـاـخـلـا ةـيـنـقـتـ اـفـيـرـعـتـ تـسـيـلـ "ةـهـبـجـلـا" نـإـ .كـلـذـ يـلـا اـمـوـ، 2/4 تـنـرـثـيـاـوـ، 1/1 تـنـرـثـيـاـيـهـ ةـيـمـامـأـلـا ةـيـجـرـاـخـلـا ةـزـهـجـأـلـا لـمـاـصـتـمـلـا تـاهـجـاـوـلـا زـيـيـمـتـلـ ـمـتـيـ ، دـنـتـسـمـلـا اـذـهـ يـفـ .ايـوـقـ

تالصوّل ا تاهج او و ا ئي فلخلا ئحوللا نم.

- لوجه ملاب (SM) ئي طمنلا نامألا ئدحولصت ئيلخاد ئههجا - ئلصوّل او ئي فلخلا ئحوللا يلخادلا.
- روم ئكرح راسم رفوت 3100/4200 نمآللا ئي امحلا رادجل ئيرصح ئيلخاد ئههجا - ئرادإلا ئلصوقي بطبتل او يلخادلا ئوحمللا نيب ئرادإلا تانايىب.

ىلع تالصوّل ا تاهج او و ا ئي فلخلا ئحوللا تاهج او لودجلا اذه حضوي ئلوج 3100/4200 نمآللا ئي امحلا رادجل:

ئصنملا	تادح و ددع نامألا ئي طمنلا ئموعدملا	ئحوللا تاهج او تالصوّل او ئي فلخلا	ليصوت تاهج او ئرادإلا	تاهج او قى بطبتل ئنيعمللا
Firepower 4100 (غانثتساب) Firepower 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	رفوتم رىغ	Internal-Data0/0 Internal-Data0/1
Firepower 4110/4112	1	Ethernet1/9	رفوتم رىغ	Internal-Data0/0 Internal-Data0/1
Firepower 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet1/11 Ethernet1/12 SM3: Ethernet1/13 Ethernet1/14	رفوتم رىغ	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 1 ئرادإلا

Secure Firewall 4200	1	SM1: in_data_uplink1		Internal-Data0/1
		SM1: in_data_uplink2 (4245 طقف)	in_mgmt_uplink1 in_mgmt_uplink2	Internal-Data0/2 (4245 طقف) ةرادل 1/1 ةرادل 1/2

وأًدحول كل ئيكلخ ليصوت ئحول تاھج او عم Secure Firewall Firepower 4100/9300 تادھولوا ئل ع ئدوجوملا تاقىب طتل او يلخادلا لوحملما موقى، تانايىب لىصوت تاھج او عم 4245 2. تاھج اولار بىع تانايىبلا رورم ئكىرچ لامحأ ئنزاومب ئيطنمنلا.

- تي بثت اهي ف متي يتلا ةدحولا - يلصنلا مداخلا وأ نامألا كرحم وأ ئي طمنلا نامألا ةدحو.
  - نامأ تادحو 3 لىا لصي ام Firepower 9300 معدي ASA وأ FTD لثم تاقيب طن.
  - تاقيب طتللا يف تالصو لا تاهج او وأ ئيف لخلا ةحوللا عامسأ - ئني عمللا قي بطللا ةهجاو.
  - FTD ASA وأ لثم

لخادلا تاهجاوـلا نـم قـقـحتـلـل show interface detail رـمـأـلـا مـدـخـتـسـأـ

<#root>

7

```
show interface detail | grep Interface
```

Interface Internal-Control0/0 "ha\_ctl\_nlp\_int\_tap", is up, line protocol is up  
Control Point Interface States:

Interface number is 6

Interface config status is active  
Interface state is active

Interface Internal-Data0/0 "", is up, line protocol is up

## Control Point Interface States:

```
Interface number is 2  
Interface config status is active  
Interface state is active
```

Interface Internal-Data0/1 "", is up, line protocol is up

## Control Point Interface States:

```
Interface number is 3  
Interface config status is active  
Interface state is active
```

Interface Internal-Data0/2 "nlp int tap" is up, line protocol is up

Control Point Interface States:

```
Interface number is 4  
Interface config status is active  
Interface state is active
```

Interface state is active  
Interface Internal-Data0/3 "cc1\_ha\_pnp\_int\_tap" is up, line protocol is up

## Interface Internal-Data0/3 CCI\_M Control Point Interface States:

3) Point Interface station  
Interface number is E

```

Interface config status is active
Interface state is active
Interface Internal-Data0/4 "cmi_mgmt_int_tap", is up, line protocol is up
Control Point Interface States:
    Interface number is 7
    Interface config status is active
    Interface state is active
Interface Port-channel6.666 "", is up, line protocol is up
Interface Ethernet1/1 "diagnostic", is up, line protocol is up
Control Point Interface States:
    Interface number is 8
    Interface config status is active
    Interface state is active

```

## ةيلخادلأا تالوحملا تايملع ىلع ىوتسملا ةيلاع ٰماع ٰرظن

Firepower 4100/9300

ذفنمل VLAN ٰماع وأ، ٰهجاول VLAN ٰماع يلخادلأا لوحملأا مدخلتسى، ٰيجوت ٰداعإ رارق ٰذاختال و ٰيرهاظ ٰكبش ٰماع و (VN-tag).

ٰهجاوف يرعتل يلخادلأا لبقل نم ذفنملاب ٰصاخلا VLAN ٰكبش ٰماع مادختسإ متى ٰماع نيوكت متى .يماماً نراق ىلع يتأي نأ طبر لخدم لك لخاد ٰقاطب VLAN لا حاتفملأا لخدن VLAN ٰماعلا ٰميق نم ققحتلا نكمي .ايودي اهرييغت نكمي الوماظنلا ٰطساوب ايئاقلت رمأ يف fxos shell:

```

<#root>
firepower#
connect fxos

...
firepower(fxos)#
show run int e1/2

!Command: show running-config interface Ethernet1/2
!Time: Tue Jul 12 22:32:11 2022

version 5.0(3)N2(4.120)

interface Ethernet1/2
description U: Uplink
no lldp transmit
no lldp receive
no cdp enable
switchport mode dot1q-tunnel

switchport trunk native vlan 102

speed 1000
duplex full

```

ud1d disable  
no shutdown

متيو. قيبرتلا ىلا طبرلا لسرى نأ تلمعتساو يلخاد حاتفملاب تلخداً اضيأ VN-tag ىلا ايودى اهرييغت نكمى الوماظنلا ةطساوب ايناقلت اهنويكت.

قيبرتلا لخددي. قيبرتلا عم VN-tag ڈفندملاب ڈصالخا VLAN ڈمالع ڈكراشم متت نم طبرملتسى امدنع. ڈمزح لك يف تامالع وجورخلا ڈهجاوب ڈصالخا VLAN تامالع ڈقاطب نراق جرخملارقى حاتفملانراق ڈيفلخلا ڈحوللا ىلع يلخاد حاتفملاب قيبرتلا VLAN ىلا و ڈقاطب VLAN ئانيملادرجي، نراق جرخملارقى بطبتلانىعي، لجا و VN-tag، ڈكبشللا ىلا طبرلا لسرىو.

## Secure Firewall 3100/4200

لبق نم ڈفندملاب ڈصالخا VLAN ڈكبش ڈمالع مادختسما متى، Firepower 4100/9300 يف امك ڈجاجاو فيرعتل يلخادلاروحملانىعى.

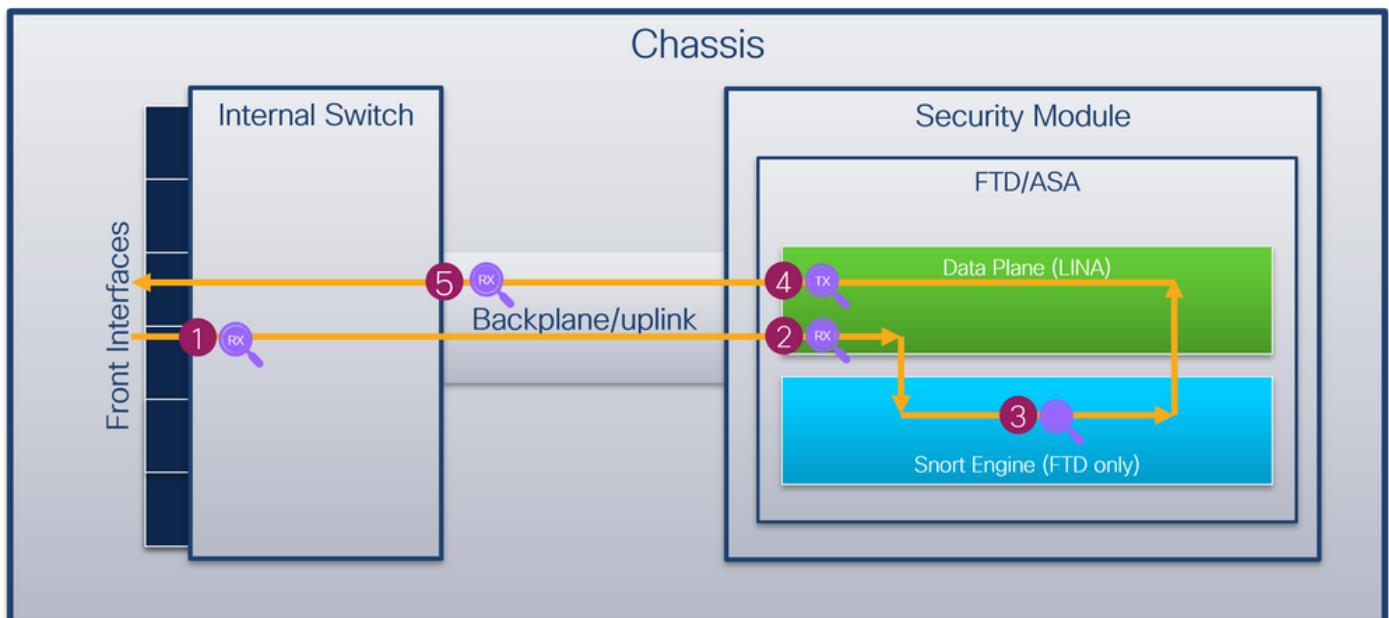
تامالع قيبرتلا لخددي. قيبرتلا عم ڈفندملاب ڈصالخا VLAN ڈمالع ڈكراشم متت ىلع يلخاد حاتفملاب قيبرتلا نم طبرملتسى امدنع. ڈمزح لك يف جورخلا ڈهجاوب ڈصالخا ئانيملادرجي، نراق جرخملانىعي، ڈقاطب VLAN نراق جرخملارقى حاتفملانراق ڈلصولىا VLAN ىلا طبرلا لسرىو، ڈقاطب.

## طاقتللا طاقنون ڈمزحلا

### Firepower 4100/9300 ئاماچلا رادجو 3100

لروحملاتاهجاو ىلع ڈمزحلا Secure Firewall 3100 Firewalls Firepower 4100/9300 نم لك طقتلى يلخادلاروحملانىعى.

قيبرتلاو لكىهلاراخاد ڈمزحلا راسمه ىلع ڈمزحلا طاقتلا طاقنون لكشلا ادھ حضوى:



یہ طاقت لا طاقد

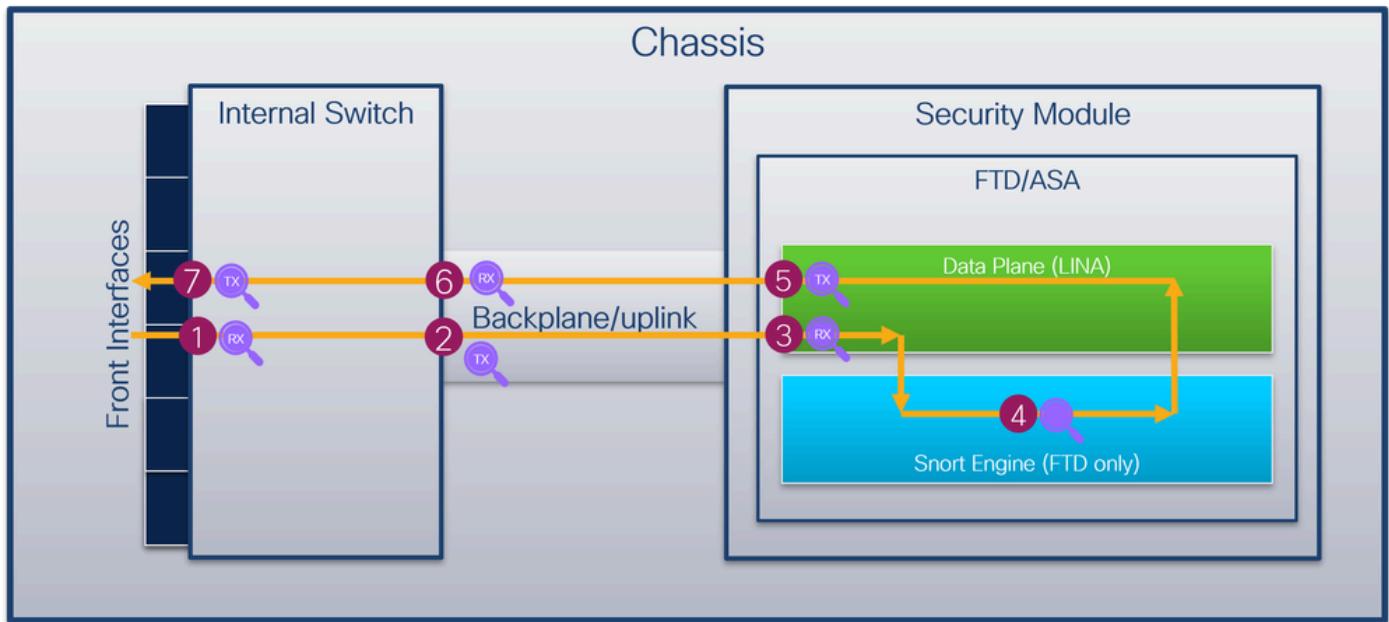
١. ٦. ٥. ٤. ٣. ٢.

٦. ٥. ٤. ٣. ٢. ١.

وأكبسلا نم ملتسى طبرلا طقف اذه . ضبق ىلع نراق لخدم طقف يلخاد حاتفمل دناسى . موعدم ريغ جورخلا مزح طاقتلا . ضبق ىلع تنك عي طتسى قي بطبت ASA/FTD لا نم

## Secure Firewall 4200

اده حضوي .يـلـخـادـلـا لـوـحـمـلـا تـاهـجـاـوـىـلـعـ 4200 Firewalls نـمـآـلـا ئـيـامـحـلـا رـادـجـمـعـدـ ئـمـزـحـ طـاـقـتـلـا  
قـيـبـطـتـلـاـوـلـكـيـهـلـا لـخـادـ ئـمـزـحـلـا رـاسـمـىـلـعـ ئـمـزـحـلـا طـاـقـتـلـا طـاـقـنـلـكـشـلـا



## یہ طاقت لا طاون:

1. ٠لصلتم ٠هـجـاوـيـأـ يـهـ ٠يـمـامـأـلـاـ لـوحـمـلـاـ ٠هـجـاوـ ٠هـجـ طـاقـتـلـاـ ٠طـقـنـ. ٠يـلـخـادـلـاـ ٠يـمـامـأـلـاـ لـوحـمـلـاـ ٠هـجـاوـ ٠هـجـ اوـ طـاقـتـلـاـ ٠طـقـنـ.  
٠تـالـوـحـمـلـاـ لـثـمـ رـيـظـنـلـاـ ٠زـهـجـأـبـ.
2. ٠يـلـخـادـلـاـ لـوحـمـلـلـ ٠يـفـلـخـلـاـ ٠حـوـلـلـاـ ٠هـجـاوـ جـرـخـ طـاقـتـلـاـ ٠طـقـنـ.
3. ٠تـانـاـيـبـلـاـ ٠وـتـسـمـ ٠هـجـاوـ لـخـدـمـ طـاقـتـلـاـ ٠طـقـنـ.
4. ٠طـرـوـشـلـاـ طـاقـتـلـاـ ٠طـقـنـ
5. ٠تـانـاـيـبـلـاـ ٠وـتـسـمـ ٠هـجـاوـ جـرـخـ طـاقـتـلـاـ ٠طـقـنـ.
6. ٠حـوـلـلـاـ وـأـ ٠لـيـصـوـتـلـاـ ٠هـجـاوـ مـوقـتـ. ٠لـخـدـمـ طـاقـتـلـاـ ٠طـقـنـ وـأـ ٠يـلـخـادـلـاـ ٠يـفـلـخـ لـيـصـوـتـ ٠حـوـلـ.
7. ٠قـيـبـطـاطـلـابـ ٠يـلـخـادـلـاـ لـوحـمـلـاـ ٠لـيـصـوـتـبـ ٠يـفـلـخـلـاـ  
٠يـلـخـادـلـاـ ٠يـمـامـأـلـاـ لـوحـمـلـاـ ٠هـجـاوـ ٠هـجـ اوـ طـاقـتـلـاـ ٠طـقـنـ.

جورخل او لوح دلا نم الک - هاجت إلا ۀیئان ث طاقت لالا تایلمع ای رایتخا یلخ ادلار لوح ملا مع دی.  
هاجت ای ف طبر یلخ ادحات فمل ا ضبق یلع، یض ارتفا لکش ب.

# نم ققحتل او نيوكتلـا FirePOWER 4100/9300

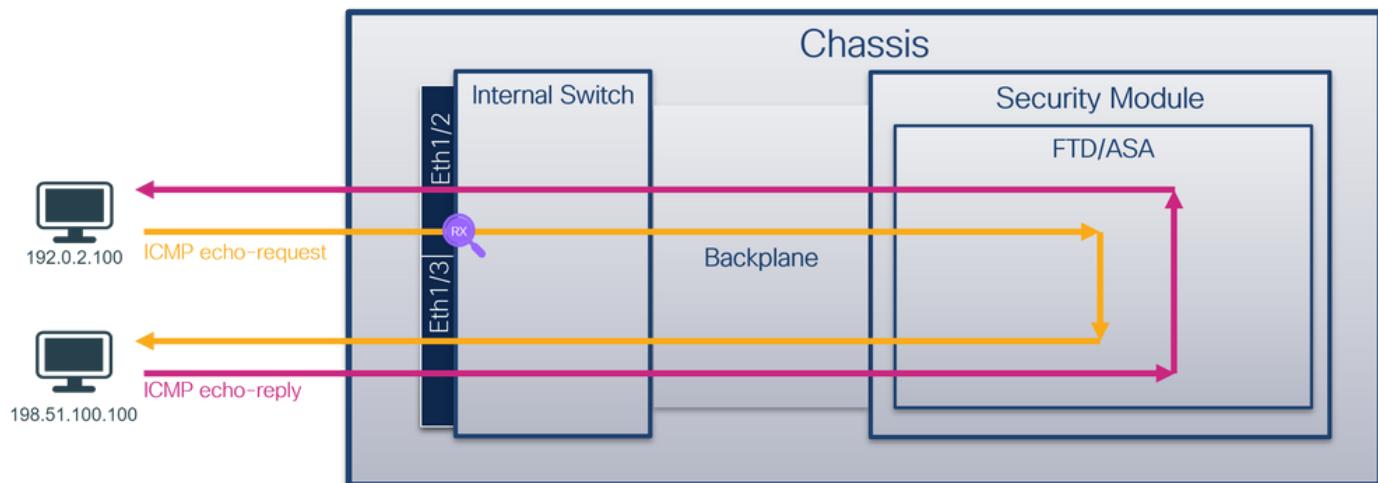
ىلع مزحـلا طاقتـلا > تاوـدـلا يـف Firepower 4100/9300 يـلـخـادـلا لـوـحـمـلا طـاقـتـلا نـيـوـكـتـ نـكـمـيـ FXOSـ.ـ لـيـغـشـتـلا مـاـظـنـلـ (CLI) رـمـاـوـلـا رـطـسـ ةـهـجـاـوـيـف قـاطـنـلـا ةـمـزـحـ طـاقـتـلا يـفـ وـأـ FCMـ.ـ لـكـيـهـ رـيـدـمـ نـيـوـكـتـ لـيـلـدـ عـجـارـ ةـمـزـحـ طـاقـتـلا تـارـايـخـ فـصـوـلـعـ لـوـصـحـلـلـ Ciscoـ Firepower 4100/9300ـ FXOSـ Ciscoـ Firepower 4100/9300ـ FXOSـ.ـ ةـمـزـحـلا طـاقـتـلا مـسـقـلـاـ،ـ اـهـحـالـصـ اوـعـاطـخـاـلـاـ فـاشـكـتـسـأـ لـصـفـلـاـ.

تـالـوـحـمـ طـاقـتـلـاـ عـئـاشـلـاـ مـاـدـخـتـسـاـلـاـ تـالـاحـ تـاهـوـيـرـانـيـسـلـاـ هـذـهـ يـطـغـتـ FXOSـ.ـ

## ذـفـنـمـ ةـانـقـ ةـهـجـاـوـ وـأـ ةـيـدـامـ ةـهـجـاـوـ ئـلـعـ ةـمـزـحـلاـ طـاقـتـلاـ

ةـهـجـاـوـ وـأـ 1/2ـ تـنـرـثـيـاـ ةـهـجـاـوـ ئـلـعـ هـتـحـصـ نـمـ قـقـحـتـلـاـوـ ةـمـزـحـ طـاقـتـلاـ نـيـوـكـتـلـ FCMـ وـ CLIـ مـدـخـتـسـأـ.ـ ةـيـدـامـلـاـ ءـاضـعـأـلـاـ تـاهـجـاـوـعـيـمـجـ دـيـدـحـتـ نـمـ دـكـأـنـ،ـ ذـفـنـمـلـاـ ةـانـقـ ةـهـجـاـوـ ةـلـاحـ يـفـ PortChannel1ـ.

طـاقـتـلـاـ طـاقـنـوـ،ـ ةـمـزـحـلاـ قـفـدـتـ،ـ طـطـخـمـلـاـ



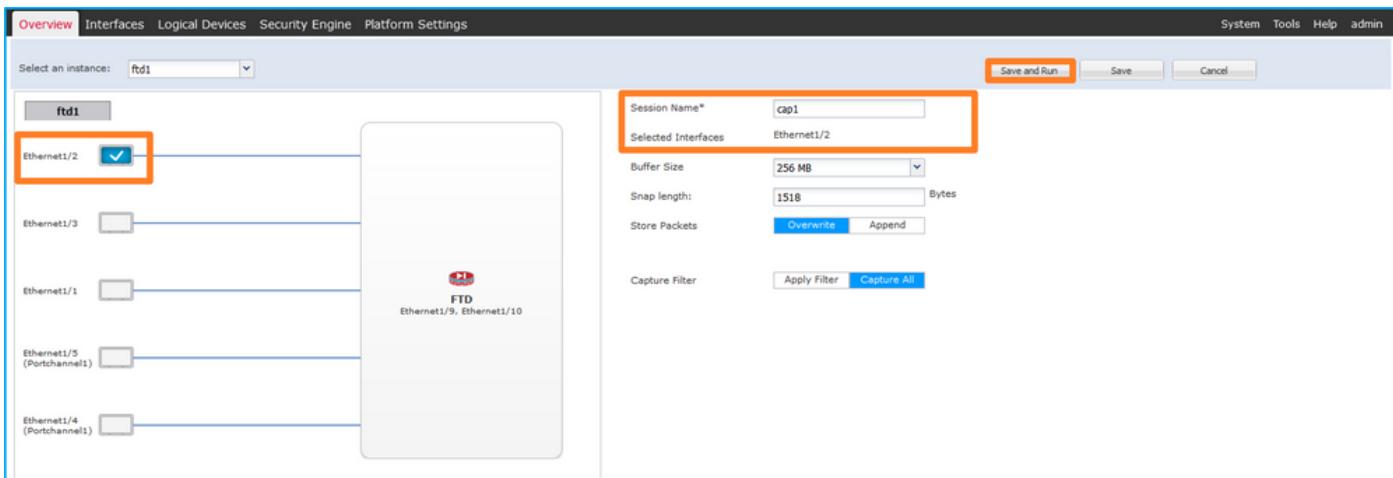
نيـوـكـتـلـاـ

FCM

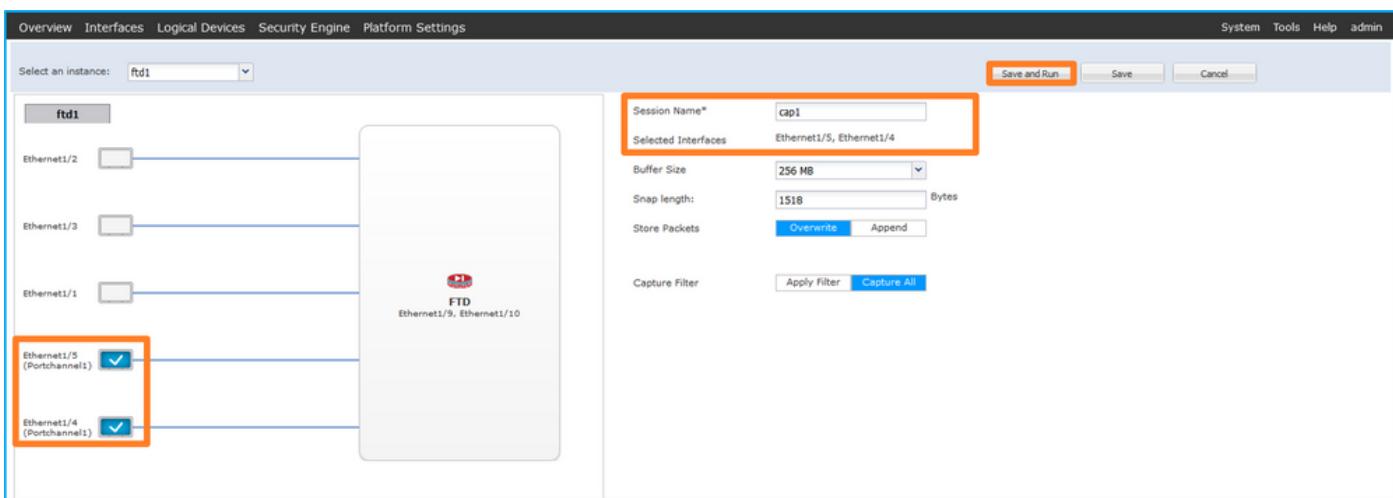
1/2ـ تـيـنـرـثـاـ نـرـاقـ ئـلـعـ طـبـرـلـكـشـيـ نـأـ FCMـ ئـلـعـ stepsـ اـذـهـ تـزـجـنـأـ:

1ـ دـيـدـجـ طـاقـتـلـاـ لـمـعـ ةـسـلـجـ عـاشـنـاـلـ طـاقـتـلـاـ طـاقـتـلـاـ > مـزـحـلاـ طـاقـتـلـاـ > تـاوـدـلاـ يـفـ مـدـخـتـسـأـ.

2ـ طـيـشـنـتـلـ لـغـشـ وـظـفـحـ رـقـنـاـوـ ةـسـلـجـلـاـ مـسـاـ رـيـفـوـتـبـ مـقـوـ،ـ ةـهـجـاـوـلـاـ دـدـحـ طـاقـتـلـاـ:



ظفح ظق طق طو مس ا سل جلا ت دوز ، نراق يعي بط وضع لك ددح ، نراق ظانق اذا ام ظلاح يف  
3. ظا قتل الـ ا طشنـي نـأ لـغـشـو:



## نرم افزار CLI (Command Line Interface) چیست؟

وأ 1/2 تينرثا نراق ىلع طبر لکشی نأ FXOS CLI ىلع steps اذه تزجن PortChannel1:

1: قىب طتلا فرعون و قىب طتلا عون فى رع.

<#root>

firepower#

## SCOPE SSA

firepower /ssa #

**show app-instance**

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

اهىاضعأ تاهج او فيرعتب مق ، ذفنمل ا ةانق ةهج او ئلاح يف .2.

```
<#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| ةسنج 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 ظهوج او لكل لصفنم طاقتلا نويوكت متى ،ذفنملأا ةانق تاهج اول:

**<#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 #

```

## ققحتل

### FCM

فلملأا مجح ةدایز نم ولیغشتلا دیق ليغشتلا ةلاح نأ نم دكأتو، و هجأولأا مسا نم ققحت (تیابلاب):

Overview Interfaces Logical Devices Security Engine Platform Settings					System Tools Help admin	
Capture Session		Filter List				
cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB	Snap Length: 1518 Bytes		
<b>Interface Name</b>	<b>Filter</b>	<b>File Size (in bytes)</b>	<b>File Name</b>	<b>Device Name</b>		
Ethernet1/2	None	28632	cap1-ethernet-1-2-0.pcap	ftd1		

PortChannel1 و Ethernet1/4 و Ethernet1/5 عاضعألا تاهجأو عPortChannel1:

Overview Interfaces Logical Devices Security Engine Platform Settings					System Tools Help admin	
Capture Session		Filter List				
cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB	Snap Length: 1518 Bytes		
<b>Interface Name</b>	<b>Filter</b>	<b>File Size (in bytes)</b>	<b>File Name</b>	<b>Device Name</b>		
Ethernet1/5	None	160	cap1-ethernet-1-5-0.pcap	ftd1		
Ethernet1/4	None	85000	cap1-ethernet-1-4-0.pcap	ftd1		

و فرجأو (CLI) Fxos نم رمأوألا رطس ةهجاو

قطلنلا ةمزح طاقتلا يف طاقتلala ليصافت نم ققحتل:

```
<#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: ذفنمل اةانق 1 ذفناج او 1/4 تنرثي اءاضع ألا تاهج او عم 1 تنرثي او 1/4:

<#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

## طاقتل الا تافلم عي مجت

يلخادلا لوحمل ا طاقتلا تافلم عي مجت مسقلما يف تاوطلخا عارجاب مق Firepower 4100/9300.

## طاقتل الا فلم لي لح

ةمزحلا ددح 1/2. تنرثيال طاقتل الا فلم حتفل مزحلا طاقتلا تافلم ئراق قي ب طت مدخلتسا: ئيساس ال طاقنلا صحفو ىلوا

تارم 2 اه ضرع و ةمزح لك طاقتلا متى . طقف ICMP Echo-Request مزح طاقتلا متى.

2. ةمزحلا نودب يلص ال ةمزحلا سأر VLAN.

3. تينرثا نراق لخدملا نوعي نأ 102 ئقاطب VLAN ءانيم يف اضي يلخاد حاتفمل ا لخددي.

4. ةمزحلا يلخادلا حاتفمل ا لخددي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info	
1	2022-07-13 06:23:58.28508930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64	Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
2	2022-07-13 06:23:58.28508938	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64	Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
3	2022-07-13 06:23:59.30904886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64	Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
4	2022-07-13 06:23:59.30919373	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64	Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
5	2022-07-13 06:24:00.33305419	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (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	0x9f20 (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	0x9f2d (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	0x9f2d (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	0x9f80 (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	0x9f80 (40840)	64	Echo (ping) request	id=0x001a, seq=11/2816, ttl=64 (no response found!)
11	2022-07-13 06:24:02.40519941	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 06:24:06.477127687	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 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1fe (41462)	64	Echo (ping) request	id=0x001a, seq=16/4096, ttl=64 (no response found!)
20	2022-07-13 06:24:07.501293403	192.0.2.100	198.51.100.100	ICMP	102	0xa1fe (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 06:24:10.573118146	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 06:24:11.597086670	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 06:24:12.621061022	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 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  
.... .... .... 0... .... .... .... = Reserved: 0  
.... .... .... ..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

00000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X--w-P V--&-  
00100 00 00 81 00 66 00 45 00 00 54 0d ec 40 00 .....f-E-T-@  
00200 40 01 af c0 00 02 64 c6 33 64 64 00 00 4e a2 @...-d-3dd-N  
00300 00 1a 00 07 f4 64 ce 62 00 00 00 20 a2 07 00 .....d-b-  
00400 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b .....!# \$%)\*+  
00500 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ,./0123 4567  
00600 2c 2d 2e 2f 30 31 32 33 34 35 36 37

## ةيسياس ال طاقنلا صحفو ئيناثلا ةمزحلا ددح:

تارم 2 اه ضرع و ةمزح لك طاقتلا متى . طقف ICMP Echo-Request مزح طاقتلا متى.

2. ظالع نودب يلصألا ظالع VLAN.  
 3. تينرثا نراق لخدملا نوعي نأ 102 ظاطب VLAN ءانيم يفاضا يلخاد حاتفمل لخددي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.28508930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
2	2022-07-13 06:23:58.28508930	192.0.2.100	198.51.100.100	ICMP	102	0x9dec (40428)	64 Echo (ping) request	id=0x001a, seq=7/1792, ttl=64 (no response found!)
3	2022-07-13 06:23:59.30904886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
4	2022-07-13 06:23:59.30919931	192.0.2.100	198.51.100.100	ICMP	102	0x9ed0 (40656)	64 Echo (ping) request	id=0x001a, seq=8/2048, ttl=64 (no response found!)
5	2022-07-13 06:24:00.33305419	192.0.2.100	198.51.100.100	ICMP	108	0x9f20 (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	0x9f20 (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	0x9f20 (40736)	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	0x9f2d (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	0x9fb8 (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	0x9fb8 (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 06:24:04.429153583	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 06:24:06.477127687	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 06:24:07.501291314	192.0.2.100	198.51.100.100	ICMP	108	0xa1fe (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	0xa1fe (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 06:24:11.597086627	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 06:24:12.621061022	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_uw_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) (816 bytes on wire (64.568 ms), 816 bytes captured (64.568 ms) on interface capture_uw_1, id 0)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
00. .... .... .... = Priority: Best Effort (default) (0)
..0. .... .... .... = DEI: Ineligible
.... 0000 0110 0100 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol

طاقنلا صحفو لـ 102 ظالع VLAN وضع تاهج اول طاقنلا PortChannel1. تاهج اول طاقنلا PortChannel1. ئيساس ظالع VLAN.

- تارم 2 اهضرع و ظالع لـ 102 ظالع VLAN طاقنلا متي. طقف ظالع ICMP Echo-Request.
1. ظالع VLAN.
  2. ظالع VLAN.
  3. ظالع VLAN.
  4. ظالع VN.

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 (nc)
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 (nc)
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 (nc)
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 (nc)
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 (nc)
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 (nc)
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 (nc)
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 (nc)
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 (nc)
10	2022-08-05 23:07:35.883479199	192.0.2.100	198.51.100.100	ICMP	102	0x3427 (13351)	64 Echo (ping) request	id=0x002d, seq=249/63744, ttl=64 (nc)
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 (nc)
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 (nc)
13	2022-08-05 23:07:37.913777111	192.0.2.100	198.51.100.100	ICMP	108	0x354c (13644)	64 Echo (ping) request	id=0x002d, seq=251/64256, ttl=64 (nc)
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 (nc)
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 (nc)
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 (nc)
17	2022-08-05 23:07:39.9378178128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed (14061)	64 Echo (ping) request	id=0x002d, seq=253/64768, ttl=64 (nc)
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 (nc)
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 (nc)

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_uw_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) (864 bytes on wire (68.88 ms), 864 bytes captured (68.88 ms) on interface capture_uw_3, id 0)
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
00. .... .... .... = 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

دح ةيـنـاـثـلـاـ صـحـفـوـ ةـيـنـاـسـأـلـاـ طـاقـنـلـاـ

1. ICMP Echo-Request مزح طاقتـلـاـ مـتـيـ طـقـفـ.
2. VLAN نـوـدـبـ يـلـصـأـلـاـ مـزـحـلـاـ سـأـرـ.
3. VLAN يـفـاصـإـ عـانـيـمـ يـلـخـادـ حـاتـفـمـلـاـ لـخـدـيـ PortChannel1.

حرشـلـاـ

دنـيـوـكـتـ دـحـ اوـ تـقـوـيـفـ مـزـحـ لـكـ لـوـحـمـلـاـ طـقـتـلـيـ ،ـيـمـامـاـ مـهـجـاوـىـلـعـ مـزـحـ طـاقـتـلـاـ نـيـوـكـتـ

- VLAN مـالـعـ لـاخـدـاـ دـعـبـ Port VLAN.
- (VN) مـاـظـلـاـ ةـصـاخـلـاـ ةـكـبـشـلـاـ مـالـعـ لـاخـدـاـ دـعـبـ.

VLAN مـالـعـ جـارـدـاـ نـمـ ةـقـحـالـ ةـلـحـرمـ يـفـ VN مـالـعـ جـارـدـاـ مـتـيـ ،ـتـايـلـمـعـلـاـ بـيـتـرـتـ يـفـ عـانـيـمـلـاـ عـمـ طـبـرـلـاـ نـمـ رـكـبـأـ ةـقـاطـبـ VLN لـاـ عـمـ طـبـرـلـاـ ،ـدـرـبـمـ طـاقـتـلـاـ يـفـ ،ـاـمـهـمـ .ـذـفـنـمـلـاـ بـقـاطـبـ.

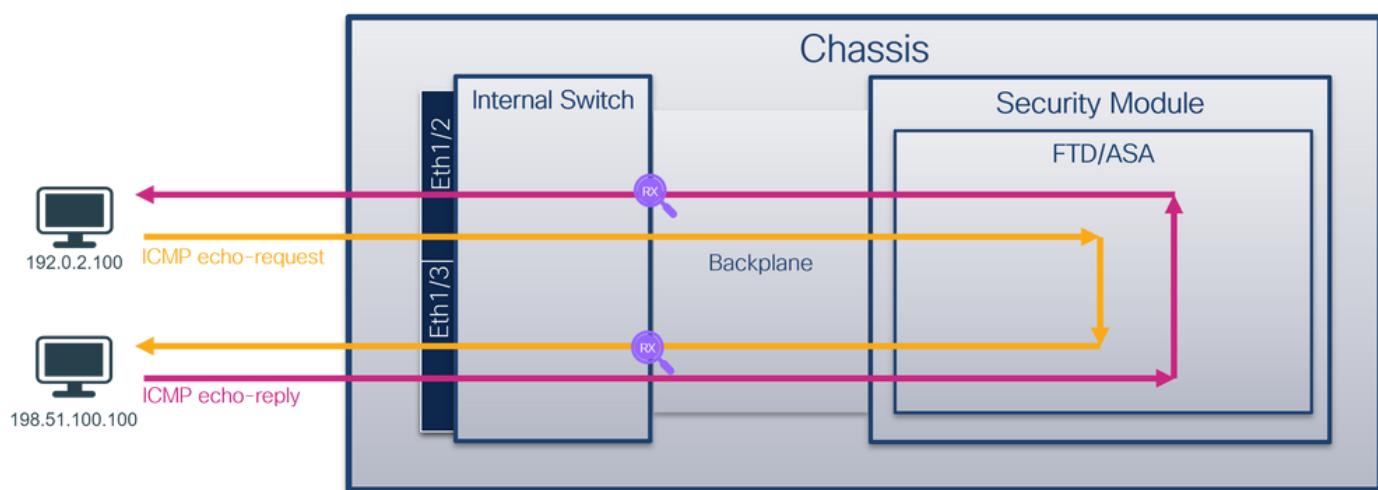
مـهـمـمـلـاـ لـوـدـجـلـاـ اـذـهـ صـخـلـيـ:

مـهـمـمـلـاـ	طـقـنـ طـاقـتـلـلـاـ	ضـبـقـ يـفـ VLAN طـبـرـ	هـاجـتـاـ	اهـيلـعـ ىـلـوـتـسـمـلـاـ رـورـمـلـاـ ةـكـرـحـ
مـزـحـ طـاقـتـلـاـ نـيـوـكـتـ ٥ تـحـصـ نـمـ قـقـحـتـلـاـ وـهـجـاوـىـلـعـ Ethernet1/2	Ethernet1/2	102	لـخـدـمـ طـقـفـ	نـمـ ICMP ئـدـصـ تـابـلـطـ ىـلـاـ 192.0.2.100 فـيـضـمـلـاـ 198.51.100.100
مـزـحـ طـاقـتـلـاـ نـيـوـكـتـ ٥ هـجـاوـىـلـعـ	Ethernet1/4 Ethernet1/5	1001	لـخـدـمـ طـقـفـ	نـمـ ICMP ئـدـصـ تـابـلـطـ ىـلـاـ 192.0.2.100 فـيـضـمـلـاـ

PortChannel1 وتحص نم ققحتلوا تاهج او مادختس اب عاصع ألا Ethernet1/4 و Ethernet1/5				فيفيضم ملا 198.51.100.100
---	--	--	--	---------------------------

ةيفلخلا ٩حوللا تاهج او لع ٩مزحلا طاقتلا

ةيفلخلا ٩حوللا تاهج او لع ٩تحص نم ققحتلوا ٩مزح طاقتلا نيوكتل FCM و مدخلتسا طاقتلala طاقن و ٩مزحلا قفت ، ططخملا



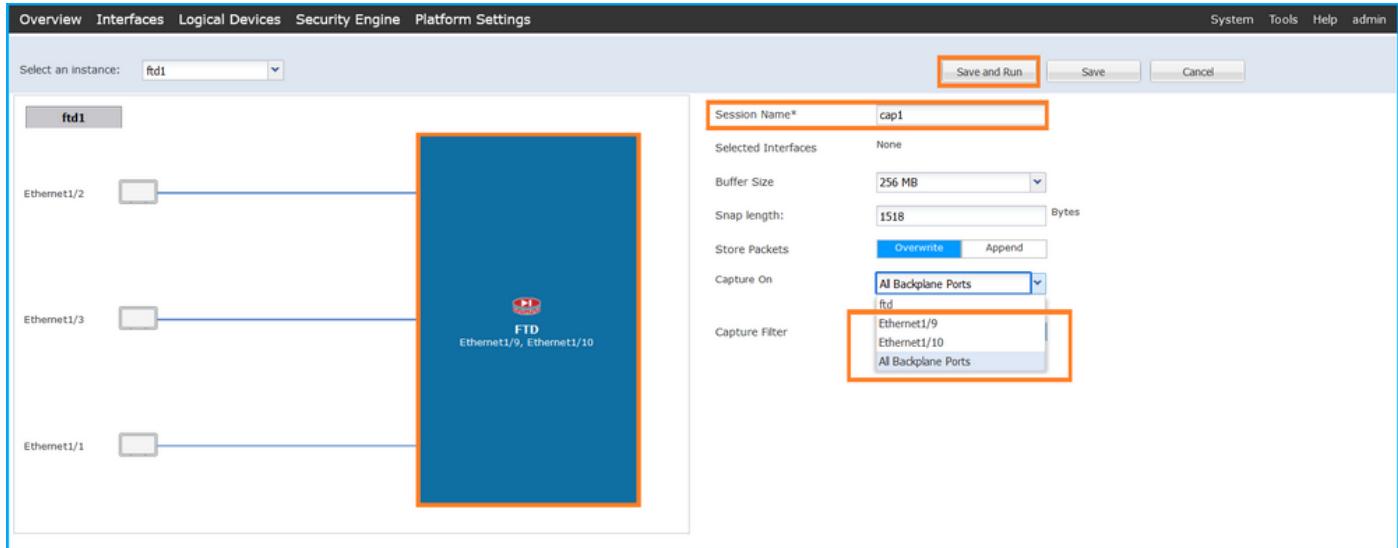
نيوكتل

FCM

ةيفلخلا ٩حوللا نراق لع طبر لکشی نأ FCM لع steps اذه تزجنأ:

ةديج طاقتلا لم مع ٩سلج عاشنال طاقتلala ٩سلج > ٩مزحلا طاقتلا > ناودأ مدخلتسا.

ذفانم عيمج مث ، قيبطتل ددح ، ةيفلخلا ٩حوللا تاهج او عيمج لع ٩مزحلا طاقتلal 2. ٩حوللا ٩هج او رتخأ ، كلذ نم الدب . ٩لسنملا ٩مئاقلا لع طاقتلala نم ةيفلخلا ٩حوللا و ٩Ethernet1/9 ةيفلخلا ٩حوللا تاهج او رفووت ، ٩لاحلا هذه يف . ٩ددحملا ةيفلخلا طاقتلala طيشنتل ليغشت و ظفح لع رقن او ٩سلجلا مسا لخدأ .



## واده ج او رطس (CLI) FXOS نم او اولا

تاهج او لىع مزحلا طاقتلا نيوكتل FXOS (CLI) رم او اولا رطس او هجلا تاوطخلا هذه عارجاب مق ئيفلخلا ۋە حوللا:

1. قىبىطتلا فرعمو قىبىطتلا عون فيرعت:

```
<#root>
```

```
firepower#
scope ssa
```

```
firepower /ssa#
```

```
show app-instance
```

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

2. طاقتلا ئاسلىج ئاشن:

```
<#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 #
```

ققحتل

FCM

فلملا مجح ةدايز نموليغشتلا ديق ليغشتلا ةلاح نأ نم دكأتو، ةهجاولامسا نم ققحت (تيلاباب):

Overview    Interfaces    Logical Devices    Security Engine    Platform Settings						System    Tools    Help    admin		
Capture Session		Filter List						
						Refresh	Capture Session	Delete All Sessions
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				

وهجاً رطس اولاً (CLI) Fxos نم ( ) اوألا رطس اولاً

قاطنلا ةمزح طاقتلا يف طاقتلا لاصافت نم ققحتل:

```
<#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

## طاقتل الا تافلم عيمجت

يلخادلا لوحمل ا طاقتلا تافلم عيمجت مسقل اي ف تاوطلخا عارجاب مق Firepower 4100/9300.

## طاقتل الا فلم ليلح

نم رثكأ دوجو ةلاح يف .طاقتل الا تافلم حتفل مزحل ا طاقتلا تافلم ئراق قيبطت مدخلتساً ذهه يف .ةيفلخ ٽحول ٽهجاول كل طاقتل الا تافلم عيمج حتف نم دكأت ،ةيفلخ ٽحول ٽهجاوت ٩/١ تينرثا نراق ئيفلخلا ٽحوللا ىلع طبرلا تطبقتلا ،ةلاحلا

ةيساسألا طاقنلا صحفو ،ةيناثلاو ىلوا مزحل ا ددح:

1. ةرم 2 اهراهظاو ICMP يدص بلط ةمزح لك طاقتلا مت ي.
2. ٽمالع نودب يلصألا ٽمزحل ا سأر VLAN.
3. ٤٣ تينرثا نراق جرخل ا نيعي نأ 103 ٽقااطب VLAN عانيم يفاضا يلخاد حاتفمل ا لخددي.
4. ةيفاضا ٽمالع يلخادلا حاتفمل ا لخددي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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	0xcc2c (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	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778810	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562042888	198.51.100.100	192.0.2.100	ICMP	108	0xcc4c (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xcc4c (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
13	2022-07-14 20:20:39.585670943	192.0.2.100	198.51.100.100	ICMP	108	0xcc4c (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
15	2022-07-14 20:20:39.585678455	198.51.100.100	192.0.2.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657798067	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

## ةيسيس اسألا طاقنلا صحفو، عبارل او ظلال مزحلا دح:

1. هرم 2 هراه ظاو ICMP يدىص لىلع در لك طاقتلا متى.

2. ڈم الاع نوب يلىص الـ VLAN.

3. تين رثا نراق جرخملما نيعي نأ 102 ڈقاطپ عانيم يفاضا يلىخاد حاتفملال خدي.

4. ڈم الاع يلىخادلما حاتفملال خدي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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	0xcc2c (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	0xcc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (no response found!)
6	2022-07-14 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23040)	64	Echo (ping) request id=0x0001, seq=16/4096, ttl=64 (reply in 7)
7	2022-07-14 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
8	2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64 (request in 6)
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778130	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23223)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562042888	198.51.100.100	192.0.2.100	ICMP	108	0xcccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
12	2022-07-14 20:20:38.562050333	198.51.100.100	192.0.2.100	ICMP	108	0xcccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64 (request in 10)
13	2022-07-14 20:20:39.585670943	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (no response found!)
14	2022-07-14 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0x5b46 (23366)	64	Echo (ping) request id=0x0001, seq=18/4608, ttl=64 (reply in 15)
15	2022-07-14 20:20:39.585678455	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
16	2022-07-14 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64 (request in 14)
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (no response found!)
18	2022-07-14 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=19/4864, ttl=64 (reply in 19)
19	2022-07-14 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
20	2022-07-14 20:20:40.610181944	198.51.100.100	192.0.2.100	ICMP	108	0xccd8 (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64 (request in 18)
21	2022-07-14 20:20:41.633805153	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (no response found!)
22	2022-07-14 20:20:41.633806997	192.0.2.100	198.51.100.100	ICMP	108	0x5b7e (23422)	64	Echo (ping) request id=0x0001, seq=20/5120, ttl=64 (reply in 23)
23	2022-07-14 20:20:41.634084102	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
24	2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64 (request in 22)
25	2022-07-14 20:20:42.657709988	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (no response found!)
26	2022-07-14 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23536)	64	Echo (ping) request id=0x0001, seq=21/5376, ttl=64 (reply in 27)
27	2022-07-14 20:20:42.657798067	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
28	2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64 (request in 26)
29	2022-07-14 20:20:43.681736697	192.0.2.100	198.51.100.100	ICMP	108	0x5c52 (23634)	64	Echo (ping) request id=0x0001, seq=22/5632, ttl=64 (no response found!)

# حرب

دح او تقويف ةمزح لك لوحمل ا طقتلي ،يفلخ ئوتسم ةهجاولع ةمزح طاقتلا نېوكت دناع  
ىلعل قييىبتتلاب ب تدح لعفلاب نوكىي نأ طبر يلىخاد حاتفمل ا ملتسي ،ةلاحلا ھذه يف .نىيترم  
نأ نراق جرخمل ا ۋقااطب نىعي VLAN ل او ۋقااطب عانيملا عم ئيىطمن ةدحو ئينمآل  
بلط مزح يف VLAN 103 ئممالع فرعت .ةكبسلا لىلا طبرلا لسرىي نأ لممعتسى يلىخاد لكىيەلا  
ICMP ECHO در مزح يف VLAN 102 ئممالع فرعت امنىيپ ،جرخم ةهجاوك 1/3 تىنرثىإلا ICMP ئدص  
ۋقااطب VLAN ئيلخادلا ةهجاول او ۋقااطب VN ل او ۋقااطب VN ل يلىخاد حاتفمل ا ليزي .جرخم ةهجاوك 1/2 تىنرثىإلا  
ةكبسلا لىلا تلسرا نوكىي طبرلا نأ لباق.

## ڦمڻا لودجل اذه صخلی:

اهىل عىلوك سملار رورملا ئەكىح	هاجتايىض بقىف VLAN طبىرى	ءانىيم يېلىخاد	طقن طاقىتلالا	ةممەملە
نەم ICMP تابلىقىمىسىمىنىڭ ىلى 192.0.2.100 فەيپەمىلار نەم ICMP ECHO دودرلىقىمىسىمىنىڭ ىلى 198.51.100.100 فەيپەمىلار	لەخىدىم طقىف	102 103	تاهجىاو ةحوللىا ةيىفلخلىا	مۇزىقىلىقلىك نېرىكىت عەلەمەتلىك ئەنەم قىچتىلما لەخىدىم طقىف

قىيىب طتلا ذفانم و قىيىب طتلا ىلע ۋەمىزحلا طاقتلا

فاض الاب ئي فلخلا ـ حوللا تاهجاویل عامیاد قیب طتللا و اقیب طتللا ذفانم مرح نیوکت متی  
قیب طتللا طاقتلا هاجتا دیدحتب مدخلتسملما ماق اذا ئیمام الیا تاهجاویل عالیل کلذیل.

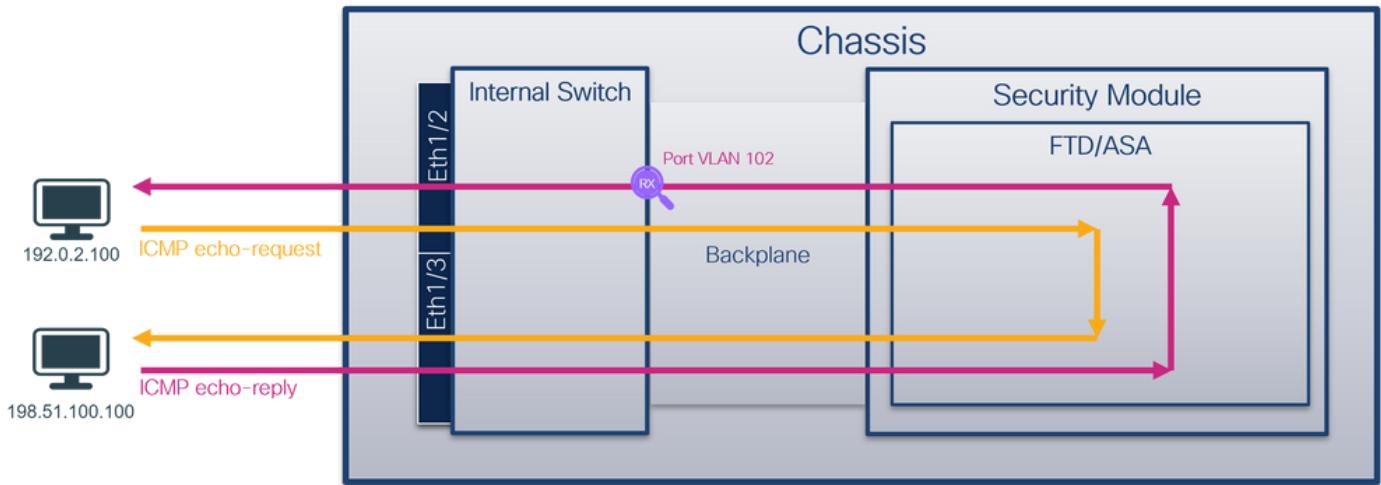
## مادختسإ يتلاح ساسألا يف دجوت

- ةيماماً ٥هج او كرتت يتلا مزحلل ئيفلخلالا ٤حوللا تاهجاو ىلع مزحلالا طاقتلا نيوكتب مق ئيفلخلالا ٤هج او ىلع مزحلالا طاقتلا نيوكتب مق ، لاثملالا ليبس ىلع . ةنيعム Ethernet1/9 ٥هج او كرتت يتلا مزحلل Ethernet1/2.
  - ئيفلخلالا ٤حوللا تاهجاو و ةنيعム ةيماماً ٥هج او ىلع نمازتملا مزحلالا طاقتلا نيوكتب مق ىلع و ٥هج او ىلع نمازتملا مزحلالا طاقتلا نيوكتب مق ، لاثملالا ليبس ىلع ئيفلخلالا ٤هج او كرتت يتلا مزحلل Ethernet1/9 ٥هج او كرتت يتلا مزحلل Ethernet1/2.

مادختس الاتاچ نم الک مسقل اذه یطغی

موم ۱

طاقة لالا طاقن و، ظاهرلا قفت ، ططخمل



نيوكـتـلـا

FCM

قـيـبـطـتـلـاـ ذـفـنـمـ وـ FTDـ قـيـبـطـتـلـاـ ظـاهـرـلـاـ نـيـوـكـتـلـاـ FCMـ يـلـعـ تـاوـطـخـلـاـ هـذـهـ عـارـجـابـ مـقـ

Ethernet1/2:

1. دـيـدـجـ طـاقـتـلـاـ لـمـعـ ةـسـلـجـ عـاـشـنـإـلـ طـاقـتـلـاـ ةـسـلـجـ <ـ مـزـحـلـاـ طـاقـتـلـاـ >ـ تـاوـدـأـ مـدـخـتـسـأـ:

2. يـفـ جـرـخـمـ ظـاهـرـلـاـ ذـفـنـمـ ةـلـدـنـمـلـاـ ةـمـئـاـقـلـاـ يـفـ، قـيـبـطـتـلـاـ دـدـحـ طـيـشـنـتـلـ لـيـغـشـتـوـ ظـفـحـ يـلـعـ رـقـنـاـوـ ةـسـلـجـلـاـ مـسـاـ لـخـدـأـ. قـيـبـطـتـلـاـ طـاقـتـلـاـ هـاجـتـاـ طـاقـتـلـاـ:

## ن م (CLI) رم اوألا رطس ڦهنجاو Fxos

تاهج اویلع مزحل ا طاقتلا نیوکتل FXOS (CLI) رم اوألا رطس ڦهنجاویلع تاوطلخا هذه عارجاب مقیةی فلخل ڦحوللما:

1. قیب طتلما فرعمو قیب طتلما عون فیرعت:

```
<#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 ڦس لج ئاشن:

```
<#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 #

```

## ققحتل

### FCM

فلملا مجح ةدایز نم ولیغشتلا دیق ليغشتلا ئلاح نا نم دکأتو، ئەجأولامسا نم ققحت (تیابلاپ):

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

نم (CLI) رم اوللا رطس ئەج او

قاطنلا ئمزح طاقتلا يف طاقتلا لىصافت نم ققحتل:

```
<#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: l12

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

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

Pcapsize: 1824 bytes

vlan: 102

Filter:

طاقتل الا تافلم عي مجت

يلخادلا لوحمل ا طاقتلا تافلم عي مجت مسقلما يف تاوطلخا عارجاب مق Firepower 4100/9300.

طاقتل الا فلم لي لحت

ةحول تاهجاو ةلاح يف .طاقتل الا تافلم حتفل مزحللا طاقتلا تافلم ئرافق قيبطت مدخلتسا، ةلاحلا هذه يف .ةيفلخ ةحول ةهجاو لكل طاقتل الا تافلم عي مجت حتف نم دكأت ،ةددعتم ئيفلخ 1/9 تينرثا نراق ئيفلخلا ئحوللا لىع طبرلا تطبق تلا

ةيساسألا طاقنلا صحفو ،ةيناثلاو ئلولا مزحللا ددح

1. در لك طاقتل الا متي.

2. ةمالي نودب يلصألا ئمزحللا سأر VLAN.

3. 1/2 تينرثا نراق جرخمل ا نوعي نأ 102 ئقاطب VLAN ءانيم يفاضا يلخاد حاتفمل ا لخدي.

4. ئيفاضا ةمالي يلخادلا حاتفمل ا لخدي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 10:03:22.231237959	198.51.100.100	192.0.2.100	ICMP	108	1 0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	2 0x42f8 (17144)	64	Echo (ping) reply id=0x0012, seq=1/256, ttl=64
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	3 0x4305 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	4 0x43b3 (17331)	64	Echo (ping) reply id=0x0012, seq=2/512, ttl=64
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	5 0x445e (17502)	64	Echo (ping) reply id=0x0012, seq=3/768, ttl=64
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	6 0x445e (17502)	64	Echo (ping) reply id=0x0012, seq=3/768, ttl=64
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	7 0x4464 (17508)	64	Echo (ping) reply id=0x0012, seq=4/1024, ttl=64
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	8 0x4464 (17508)	64	Echo (ping) reply id=0x0012, seq=4/1024, ttl=64
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	9 0x44c3 (17603)	64	Echo (ping) reply id=0x0012, seq=5/1280, ttl=64
10	2022-08-01 10:03:26.282666161	198.51.100.100	192.0.2.100	ICMP	108	10 0x44c3 (17603)	64	Echo (ping) reply id=0x0012, seq=5/1280, ttl=64
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	11 0x44e7 (17639)	64	Echo (ping) reply id=0x0012, seq=6/1536, ttl=64
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	12 0x44e7 (17639)	64	Echo (ping) reply id=0x0012, seq=6/1536, ttl=64
13	2022-08-01 10:03:28.3386664677	198.51.100.100	192.0.2.100	ICMP	108	13 0x4550 (17744)	64	Echo (ping) reply id=0x0012, seq=7/1792, ttl=64
14	2022-08-01 10:03:28.338667153	198.51.100.100	192.0.2.100	ICMP	108	14 0x4550 (17744)	64	Echo (ping) reply id=0x0012, seq=7/1792, ttl=64
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	15 0x4553 (17747)	64	Echo (ping) reply id=0x0012, seq=8/2048, ttl=64
16	2022-08-01 10:03:29.354936786	198.51.100.100	192.0.2.100	ICMP	108	16 0x4553 (17747)	64	Echo (ping) reply id=0x0012, seq=8/2048, ttl=64
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	17 0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	18 0x4597 (17815)	64	Echo (ping) reply id=0x0012, seq=9/2304, ttl=64
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	19 0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	20 0x467a (18042)	64	Echo (ping) reply id=0x0012, seq=10/2560, ttl=64
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	21 0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	22 0x468a (18058)	64	Echo (ping) reply id=0x0012, seq=11/2816, ttl=64

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_w0_8, id 0	0000 00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 PV - X - w - 8 -
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)	0010 00 0a 81 00 00 66 00 00 45 00 00 54 42 f8 00 00 f - E - TB -
VN-Tag	0020 40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 90 04 @ J - 3dd - d -
0... .... .... .... .... = Direction: To Bridge	0030 00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 09 b -
.0... .... .... .... .... = Pointer: vif_id	0040 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b -
..00 0000 0000 0000 .... .... = Destination: 0	0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ... !# \$38`(*#
.... .... .... 0... .... .... = Reserved: 0	0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,,-./0123 4567
..... .... .... ..0... .... .... = Version: 0	
..... .... .... ..0000 0000 1010 = Source: 10	
Type: 802.1Q Virtual LAN (0x8100)	
802.1Q Virtual LAN, PRI: 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	

## حرب

ىدىص ICMP لىل نراق جىخملە 102 VLAN ئاقاطب Ethernet1/2 ئانىم عەم نوڭىي، ئەلا حلا ھەذە يەف درلە طېرىز.

## ڦمڻا لودجل اذه صخلی:

ىلولت سملار رورملا ئەكەن اھيلىع	ئاجتىا ضېقىيەت	ءانىم يېلىخاد VLAN طېرىز	طاقدىللا قاچقەلەنلا	ۋەنمەملا
نەم ICMP ECHO دودر ىلى 198.51.100.100 فييضملا نەم ICMP ECHO دودر ىلى 192.0.2.100 فييضملا	لەدمۇ طقف	102	تاهجاو قەحوللا قېفلەخلا	تايمۇ نېۋەت قىقەتلىلار طاقىتلەنلا تنرثىيە ئىلەن اھنم قىبەتلىلار ذەنەنمل قاچقەلەنلا 1/2

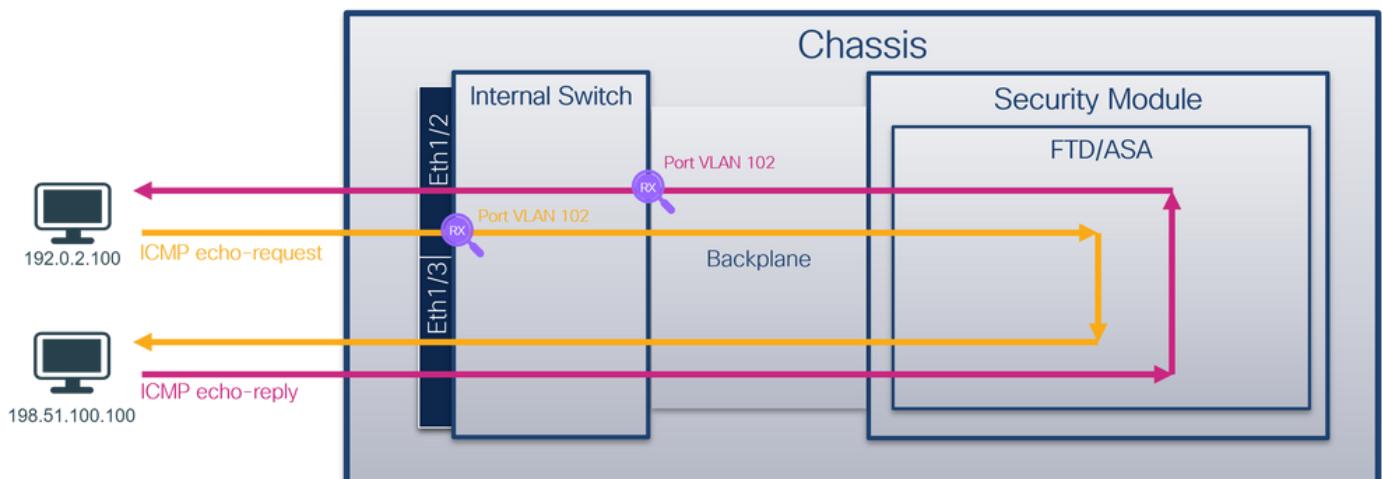
مهمة 2

ةيـفلـخـلـا ةـحـولـلـا ةـهـجـاـوـلـعـ هـتـحـصـ نـم قـقـحـتـلـا وـقـمـزـ طـاقـتـلـا نـيـوـكـتـلـا CـLـI وـFـCـM مـدـخـتـسـأـ Ethernet1/2.

یل ع نم از ت ملا مرح لا طاق ت لا نی و کت مت



طاقتل الا طاقن و، ةمنح لا قفت ، ططخملا

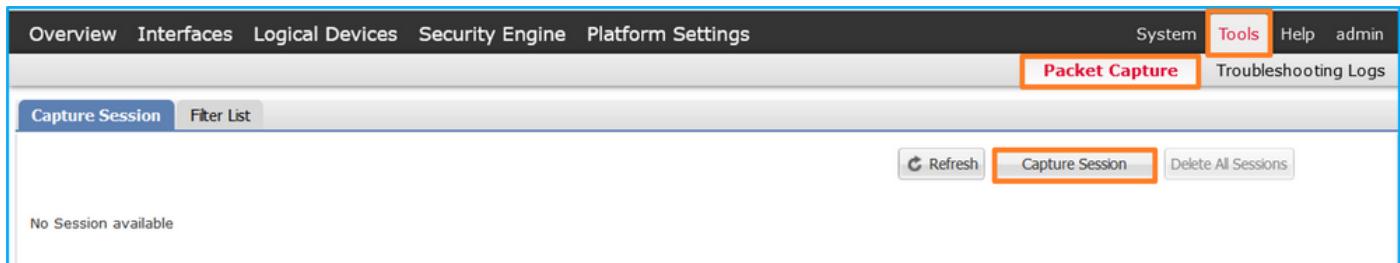


نيوكتلا

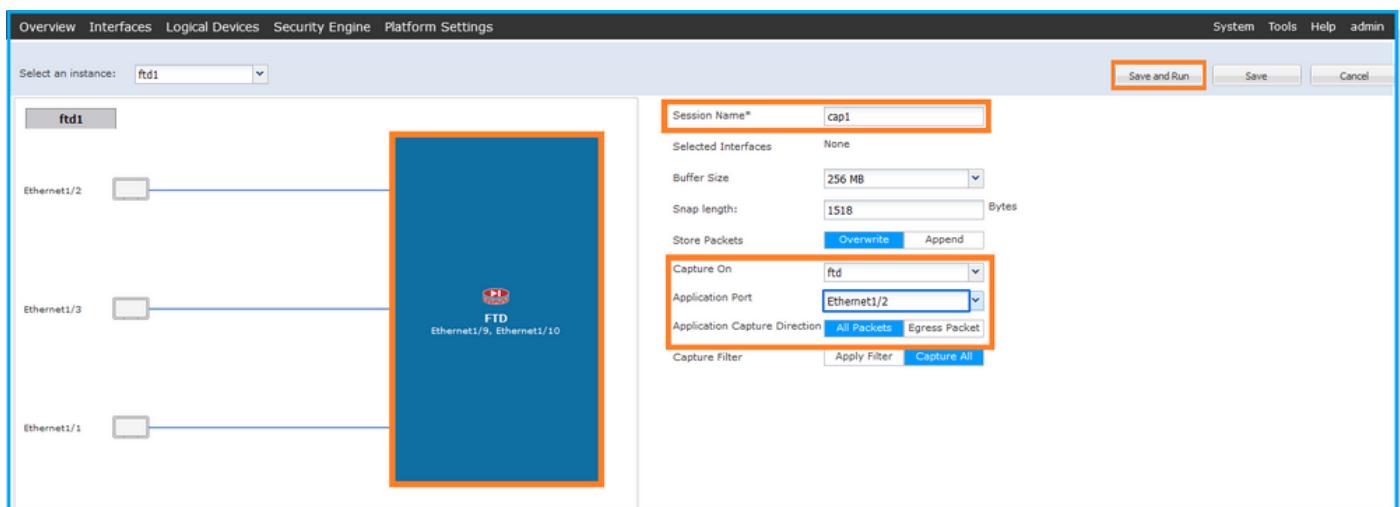
FCM

قىيىبىطتلا ذفندىم و FTD قىيىبىطت ئىلىع ئامزح طاقىتلا نيوكتل FCM ئىلىع تاوطخلا هذه عارجاب مق Ethernet1/2:

1. ئادىدج طاقىتلا لىمع ئاسلىج ئاشنال طاقىتلا ئاسلىج > مزحلا طاقىتلا > تاودا مىختسأ:



مزحلا عيمىج ددح و قىيىبىطتلا ذفندىم ئەلسەنملا ئامئاقلە يىف 1/2 تىنرەثىي، قىيىبىطت ددح. طېشىنتل لىيغىشتۇ ئەظفاح ئىلىع رقناو ئاسلىجلا مىسالىخ دا. قىيىبىطتلا طاقىتلا ھاجتاييف طاقىتلا:



FXOS نم (CLI) رماؤألا رطس ۋەجاو

تاهجاو ئىلىع مزحلا طاقىتلا نيوكتل FXOS (CLI) رماؤألا رطس ۋەجاو ئىلىع تاوطخلا هذه عارجاب مق ئەيەنلەخلا ۋەحوللا:

2. قىيىبىطتلا فرعمۇ قىيىبىطتلا عون فيرىعت:

```
<#root>
firepower#
scope ssa

firepower /ssa#
show app-instance
```

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

2. طاقتل اسلاج عاشن:

```
<#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
```

قوقحتل

## FCM

فلملأا مجح ةدایز نم ولیغشتلا دیق ليغشتلا ۃلاح نأ نم دكأت و، ۃهجاولما مسا نم ققحت (تیابلاب):

Capture Session					Filter List	System	Tools	Help	admin
cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB	Snap Length: 1518 Bytes					
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					

نم (CLI) رم اوألا رطس ۃھجاو

قاطنلأا ۃمزح طاقتلala يف طاقتلala ليصافت نم ققحتلأا:

```
<#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:

## طة قتل الـ اـ تـ اـ فـ لـ مـ عـ يـ مـ جـ تـ

Firepower 4100/9300. يلخادلا لوحملأا طاقتلا تافلم عيمجت مسقلأا يف تاوطلخلأا عارجإاب مق.

طاقت الا فلم ليحلت

ةحول تاهج او ئلخ يف . طاقتللا تافلم حتف مزحلا طاقتللا تافلم ئراق قىب طت مدخلتسا ، ئلخلا هذه يف . ئيفلخ ئحول ئهجاول كل طاقتللا تافلم عيجم حتف نم دكأت ، ئددعتم ئيفلخ تيئنرثا نراق ئيفلخلا ئحوللا ئلخ طبرلا تتطقىللا 1/9.

ءيىس اسألا طاقنلا نم ققحتو، ئيلوألا ۋەمىزلى دەجىو، 1/2 تىنرثىي ۋەھجى أول طاقتلالا فلم حىتفا:

- تارم 2 اهضرع و ةمزح لك طاقتلا متى . طقف ICMP يدص بـ لـ ط مـ زـ حـ طـ اـ قـ تـ لـ اـ مـ تـ يـ .
  2. ةـ مـ الـ عـ نـ وـ دـ بـ يـ لـ صـ أـ لـ اـ مـ زـ حـ لـ اـ سـ أـ رـ . VLAN.
  3. 1/2. تـ يـ نـ رـ ثـ اـ نـ رـ اـ قـ لـ خـ دـ مـ لـ اـ نـ يـ عـ يـ نـ اـ 102 ةـ قـ اـ طـ بـ عـ اـ نـ يـ مـ يـ فـ اـ ضـ اـ يـ لـ خـ اـ دـ حـ اـ تـ فـ مـ لـ اـ لـ خـ دـ يـ .
  4. ةـ يـ فـ اـ ضـ اـ VN ةـ مـ الـ عـ يـ لـ خـ اـ دـ لـ اـ حـ اـ تـ فـ مـ لـ اـ لـ خـ دـ يـ .

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL Info	
1	2022-08-01 11:33:19.078693081	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 11:33:19.078695347	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 11:33:19.072036625	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 11:33:21.073268372	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 11:33:23.075779989	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 11:33:24.081839494	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 11:33:28.177849755	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 11:33:29.201804760	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  
 .. 0000 0000 1010 .... .... .... = Destination: 10  
 .... .... 0. .... .... .... = Looped: No  
 .... .... . .... .... .... = Reserved: 0  
 .... .... ..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  
 ..... 0010 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

دح ڦمڻلا اٺلما ڦيئانو ڦاڻنلا طاقنلا سچف

- تارم 2 اهضرعو ۋەمىز لىك طاقىتلا مىتى. طقىف ICMP ئىدىص بىلەت مۇز طاقىتلا مىتى.
  2. ۋەمىز ئەنەجىن نووبىيە ئەنەجىن VLAN.
  3. 1/2 تىينرثا نرافق لىخىدىملا نېيغىي نأ 102 ۋەنىيەتلىك VLAN ئەنەجىن يەلخاد حات فەرمىلا لىخدى.

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	1 0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
2	2022-08-01 11:33:19.070695437	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	0xc00a (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
6	2022-08-01 11:33:20.072038899	192.0.2.100	198.51.100.100	ICMP	102	0xc00a (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	102	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 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc206 (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	0xc206 (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 11:33:24.081841186	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 11:33:26.129836272	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 11:33:27.153830281	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 11:33:29.0000048760	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 11:33:29.201806448	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 11:33:30.225837465	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!)

طاقنلا نم ققحتو، ةيناثل او لولأا مزحل ددحو، 1/9 تنرثي! ٰهـجـاـول طـاـقـتـلـالـا فـلـمـ حـتـفـاـ: ٰهـسـاسـأـلـا

3. 1/2. تينرث! نراق جرخملان ينعي نأ 102 VLAN عانيم يفاضا يلخاد حاتفملا لخددي.  
4. يفاضا VN ۋە مالع يلخادلا حاتفملا لخددي.

No.	Time	Source	Destination	Protocol	Length	# IP ID	# TTL Info	
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	0x4f10 (20475)	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	0x4ff0 (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 11:33:21.073915698	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 11:33:24.082407894	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	0x53ab (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	0x53ab (21414)	64 Echo (ping) reply	id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	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 11:33:28.178469864	198.51.100.100	192.0.2.100	ICMP	108	0x5451 (21651)	64 Echo (ping) reply	id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471818	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 11:33:29.202398087	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 11:33:30.226398756	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 11:33:31.250389791	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

حرشل

مزمحة يتحت فني وكت متي سف ، قي بطل طاقتلها هاجت ايف مزح لا عيمج رايخلا دي دحت مت اذا  
ةي مامألا ةهجاولا ىلع طاقتلا: 1/ ترنرثيا ددحملها قي بطلاب نيت طبترم نيت نمازتم  
ةددحملها ئيفلخلا ٤حوللا تاهجاو ىلع طاقتلا او 2/ ترنرثيا.

نیترم دح او تقویف ۀمزح لک لوحملأا طقتلی، ۀیمامأ ۀهجاویلع ۀمزح طاقتلا نیوکت دن ع

- ٤) مالع لاخدا دعب Port VLAN.
  - ٥) مالع لاخدا دعب VN.

دح او تقويف ةمزح لك لوحمل ا طقتلي ،يفلخ ىوتسم ٥٥ج او ىلع ةمزح طاقتلا نيوكت دنع  
ةدحو ةينمألا ىلع قيبطتلاب ب تدح لعفلاب نوكبي نأ طبر يلخاد حاتفملاب ملتسي .بنيترم  
نراق جحمل ا ٤قاطب VLAN عانيملاب نيعي .٤قاطب VLAN لاو ٤قاطب VLAN عانيملاب عم ئيطن  
ةمالع فرعت ،لاثملاب اذه يف .٤كبشلاب لىا طبرلا لسرى نأ لممعتسى يلخاد لكىهلا نأ  
VLAN .جرخم ٥هجانوک ١/٢ تونرثىإلا ICMP ECHO ىلع دورلاب مزح يف 102.

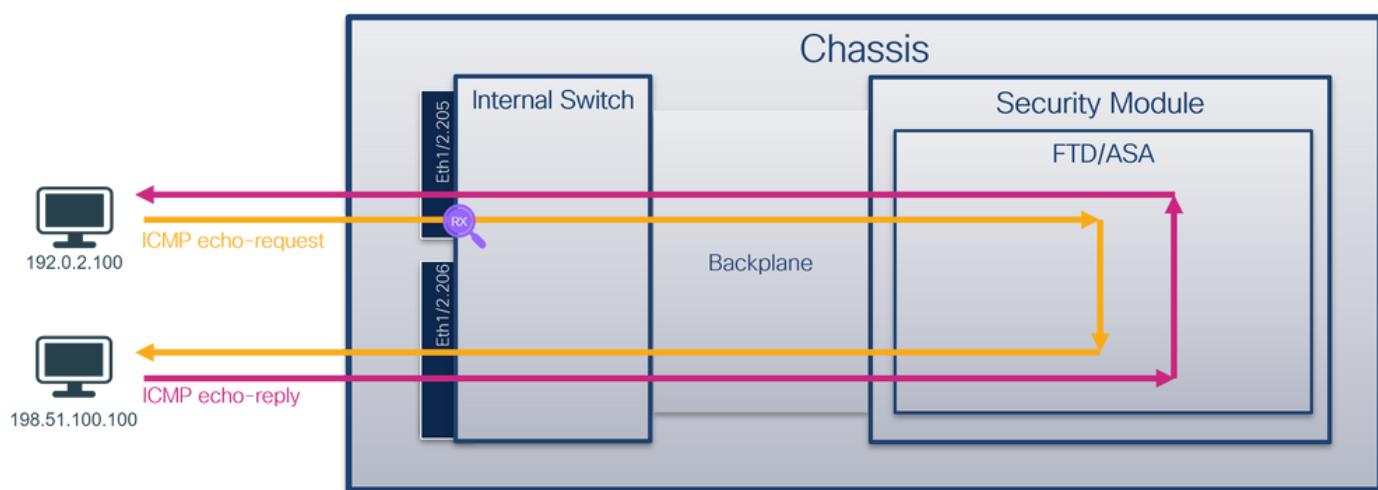
نوكى طبرلا نأ لبوق ققاطب VLAN ئىلخادلا ۋە جاول او ققاطب VN لى يلىخاد حاتفملا ليزي ۋە كېشىلما يلى تلسرا.

## لوجلا اذه صخلی مەممۇت:

ةممملا	ةطقن طاقتل الا	ءاني ميلخاد VLAN يف طبر ضبق	هاجتإ	ىلوتس ملا رورملا ةكرح اهيلع
تايلمع نيوكت ققحتل او طاقتل الا تنرثي ايلع اهنم قيبطتل ذفنمل او 1/2 قيبطتل او	تاهجاو ةحوللا ةيفلخلالا	102	لخدم طقف	نم ICMP ECHO دودر ىلإ 198.51.100.100 فيضم ملا 192.0.2.100 فيضم ملا
	ةهجاوا 1/2 تنرثي ا	102	لخدم طقف	نم ICMP ادىص تابلط ىلإ 192.0.2.100 فيضم ملا 198.51.100.100 فيضم ملا

## ذفنم ةانق ةهجاو وأ ئيدام ةهجاول ئيعرف ةهجاو ئيلع ةمزحلا طاقتلا

ئيعرفلا ةهجاول ئيلع هتحص نم ققحتل او ةمزح طاقتلا نيوكتل CLI و FCM مدخلتسا Ethernet1/2.205 و PortChannel1.207 CLI. FCM و ذفنملل ئيعرفلا ةانقلل PortChannel1.207 ئيعرفلا ةهجاول او FTD عضوي ف قيبطتل طقف ۋەمۇع دم ئيعرف دم ئيعرفلا تاهجاول او ئيعرفلا تاهجاول ئيلع ةمزح طاقتلا نيوكت مت، ئلاحلا هذه يف. ئيواحلما طاقتللا طاقن و، ةمزحلا قفت، ططخملا

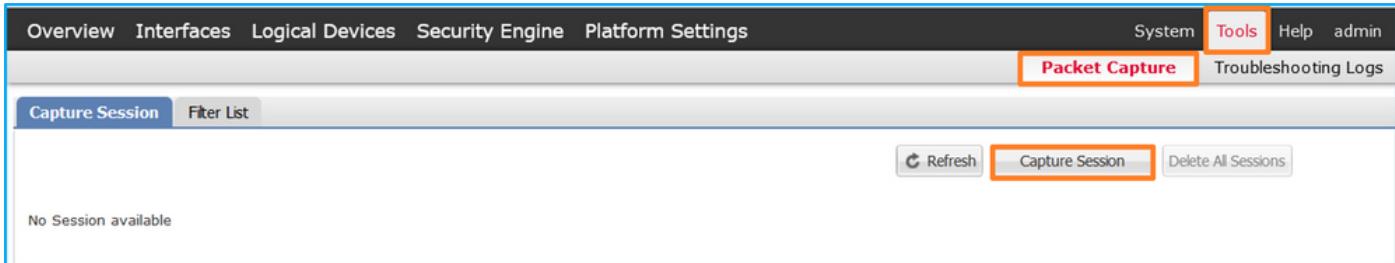


## نيوكتللا

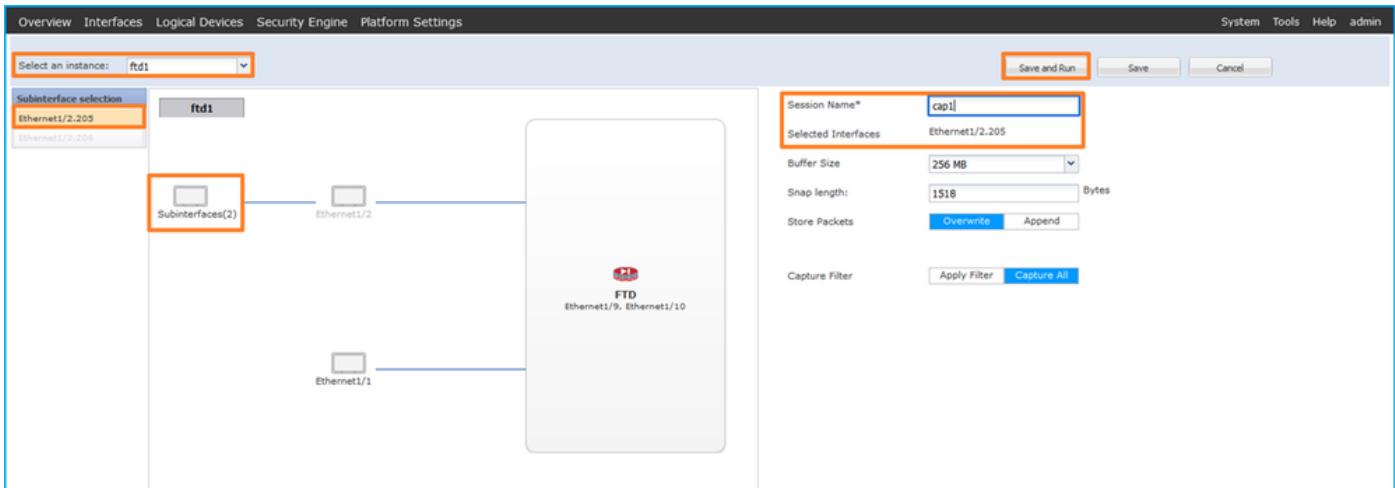
### FCM

قيبطتل ذفنم و FTD قيبطت ئيلع ةمزح طاقتلا نيوكتل FCM ئيلع تاوطخلارا هذه عارجاب مقت Ethernet1/2:

ةديج طاقتلا لمع ئاسلك ئاشنال طاقتللا ئاسلك > مزحلا طاقتلا > تاودأ مدخلتسا.



مسا ريفوتب مقو، 1/2.205 تنرثي اقيعرفلا ٰهـجـاـولـاـ اوـ، دـدـحـمـلـاـ ftd1ـ قـيـبـطـتـلـاـ ليـثـمـ دـدـحـ. طـاقـتـلـاـ طـيـشـنـتـلـ لـيـغـشـتـ وـظـفـحـ قـوـفـ رـقـنـاـ اوـ، ةـسـلـجـلـاـ:



3. Cisco نـمـ عـاطـخـأـلـاـ حـيـحـصـتـ فـرـعـمـ بـبـسـبـ، ذـفـنـمـلـاـ ٰهـاـنـقـلـ اـقـيـعـرـفـلـاـ ٰهـجـاـولـاـ ٰهـلـاـجـ يـفـ. [CSCvq33119](#) ىـلـعـ طـاقـتـلـاـ نـيـوـكـتـلـ FCMـ مـدـخـتـسـأـ. يـفـ يـئـرـمـ رـيـغـ FCMـ CLIـ مـدـخـتـسـأـ. ذـفـنـمـلـاـ ٰهـاـنـقـلـ اـقـيـعـرـفـلـاـ تـاهـجـاـولـاـ.

نـمـ (CLIـ)ـ Fxosـ رـمـاـوـأـلـاـ رـطـسـ ٰهـجـاـوـ

ىـلـعـ ٰهـمـزـحـ طـاقـتـلـاـ نـيـوـكـتـلـ FXOSـ (CLIـ)ـ لـ Jـ PortChannel1.207ـ وـ Ethernet1/2.205ـ رـمـاـوـأـلـاـ رـطـسـ ٰهـجـاـوـ ىـلـعـ تـاوـطـخـلـاـ هـذـهـ عـارـجـاـبـ مـقـ.

1. قـيـبـطـتـلـاـ فـرـعـمـ وـقـيـبـطـتـلـاـ عـونـ فـيـرـعـتـ:

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Version	Startup Version	Deploy Type
ftd	ftd1							
ftd	1	Enabled	Online	Enabled	7.2.0.82	7.2.0.82	7.2.0.82	Container No Container
ftd	ftd2	1	Enabled	Enabled	Online	7.2.0.82	7.2.0.82	Container Container

اهىاضعأ تاهج او فيرعتب مق ، ذفنمل ا ةانق ةهج او ئلاح يف .2.

```
<#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| ةسنج 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 #
```

ذفنمل ا ةانق يف وضع ٥هـج او لـكـل ٥ـمـزـح طـاـقـتـلـا ءـاشـنـابـ مـقـ، ٤ـيـعـرـفـلـا ءـانـيـمـلـا ةـانـقـ تـاهـجـاـوـلـ:

```
<#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 #

```

## ققحتل

### FCM

فلملا مجح ةدایز نم ولیغشتلا ديق ليغشتلا ةلاح نأ نم دكأت و، ةهجاولما مسا نم ققحت (تیابلاب):



اضيأ ةيئرم FXOS CLI ىلع اهنیوکت مت يتلما ذفنملما ۋانقل ئيعرفلا ةهجاولما طاقتلما نوکت

اهريحت نكمي ال ، كلذ عموم، لى ع FCM:

Interface Name	Filter	File Size (in Bytes)	File Name	Device Name
Ethernet1/4.207	None	624160	cap1-ethernet-1-4-0.pcap	Not available
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available

نم (CLI) Fxos رم اوألا رطس ڦڳاو

قاطنلا ڄمڙ طاقتلا یف طاقتلala ليصافت نم ققحتلما:

```
<#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 ذفنمل اةانق 1 تنرثي او 3 تنرثي | عاضع ألا تاهج اوعم 1 تنرثي او 3 تنرثي |

```
<#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
```

طاقتل الا تافلم عيمجت

يلخادلا لوحمل ا طاقتل الا تافلم عيمجت مسقل اي ف تاوطلخلا عارجاب مق Firepower 4100/9300.

طاقتل الا فلم ليلحت

صحف ويلوألا ۆمزحلا ددح . طاقتل الا فلم حتفل مزحلا طاقتل الا تافلم ئراق قيي بطت مدخلتسا ئيساسألا طاقنلا:

تارم 2 اهضرع و ۆمزح لك طاقتل الا متى . طقف ICMP ىدىص بلىط مزح طاقتل الا متى .

2. تارم 2 اهضرعو ۋە مزح لىك طاقىلما مىتى. طقىف ICMP ئىدىص بىلەت مزح طاقىلما مىتى.
3. تىنرە نراق لىدمىلا نىعى نأ 102 ۋە قاطب VLAN ئانىم يفاضا يلىخاد حاتفەملە لىخدى.
4. ۋە فاضا يلىخادلە حاتفەملە لىخدى.

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 07:22:08.229938829	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	0x9cc (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
10	2022-08-04 07:22:09.253946800	192.0.2.100	198.51.100.100	ICMP	102	0x9cc (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 07:22:13.3269898040	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 07:22:13.326990058	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 07:22:14.34194773	192.0.2.100	198.51.100.100	ICMP	112	0x9e64 (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	0x9e64 (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 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	112	0x9f08 (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	0x9f08 (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!)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	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)								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:76:f2:00:00:1b) [ethernet] [src=VMware_9d:e8:be dst=a2:76:f2:00:00:1b]								
<--> [ether] 0x0000 (VMware_9d:e8:be) > a2:76:f2:00:00:1b (a2:7								

- تارم 2 اهضر و ۆمزح لک طاقتلا متي. طقف ICMP ىدص بـلـط مـنـح طـاقـتـلا مـتـي.
1. ۆـمـالـع ىـلـع یـلـصـاـلـا سـأـرـيـوـتـحـيـ
  2. VLAN 207.
  3. نـرـاقـ لـخـدـمـلـا نـيـعـيـ نـأـ 1001 ۆـقـاطـبـ VLAN يـفـاضـاـ عـانـيـمـ يـلـخـادـ حـاتـفـمـلـا لـخـدـيـ
  4. PortChannel1.
4. یـفـاضـاـ ۆـمـالـع ىـلـخـادـلـا حـاتـفـمـلـا لـخـدـيـ

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 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) request	id=0x007b, seq=4/1024, ttl=255 (no response found!)
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
10	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
11	2022-08-04 08:18:24.575442569	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!)
12	2022-08-04 08:18:24.575443601	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!)
13	2022-08-04 08:18:24.575918119	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!)
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) request	id=0x007b, seq=4/1024, 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 08:18:24.576884055	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24741)	255 Echo (ping) request	id=0x007b, seq=7/1792, ttl=255 (no response found!)
18	2022-08-04 08:18:24.576884055	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24741)	255 Echo (ping) request	id=0x007b, seq=8/2048, ttl=255 (no response found!)
19	2022-08-04 08:18:24.576884055	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24742)	255 Echo (ping) request	id=0x007b, seq=8/2048, ttl=255 (no response found!)
20	2022-08-04 08:18:24.576884055	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24742)	255 Echo (ping) request	id=0x007b, seq=9/2304, ttl=255 (no response found!)
21	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24743)	255 Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
22	2022-08-04 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24743)	255 Echo (ping) request	id=0x007b, seq=10/2560, ttl=255 (no response found!)
23	2022-08-04 08:18:24.5778448781	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 08:18:24.578900043	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_w0_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)								
VN-Tag								
1 ..... = Direction: From Bridge								
.0..... = Pointer: vif_id								
..00 0000 0011 1101 = Destination: 61								
.....0... = Looped: No								
.....0.. = Reserved: 0								
.....0...0000 0000 = Version: 0								
Type: 802.1Q Virtual LAN (0x8100)								
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001								
000..... = Priority: Best Effort (default) (0)								
0...0.... = DEI: Ineligible								
....01 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...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								

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 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) request	id=0x007b, seq=4/1024, ttl=255 (no response found!)
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
10	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) request	id=0x007b, seq=5/1280, ttl=255 (no response found!)
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) request	id=0x007b, seq=6/1536, 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=7/1792, 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 08:18:24.576884055	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 08:18:24.576884055	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 08:18:24.577394328	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						

## حرشل

نیترم دح او تقویف ۋە مزح لىك لوحملۇ طوقتلىي، ئیماماً ۋە جاۋىلۇ ۋە مزح طاقتلۇ نیوكت دىن.

- ۋە مالۇ لاخدا دىعې Port VLAN.
- ئیرهاظلا ۋە ساخلا ۋە كېشلە ۋە مالۇ لاخدا دىعې (VN).

ۋە ساخلا VLAN ۋە مالۇ جاردا نم ۋە قىحال ئەلەرەم يىف VN ۋە مالۇ جاردا مىتى، تايىلمۇلۇ بىتىرىت يىف عەم طېرلە نم رکبم ۋە قاتپ ئەلە ئەلە فەلم يىف نىكلۇ و ۋە فەنملىپ، طاقتلالا تافلەم يىف، ئىعرفەلە تاھاچاولە ۋە لاح يىف، كەلذىلى ۋە فەاضەلاب. ۋە قاتپ VLAN ئانىملى، ۋە فەنملى زىيىمەت ۋە مالۇ ىلۇ ۋە مزح لىك يىوتىحتىت ئەل VLAN.

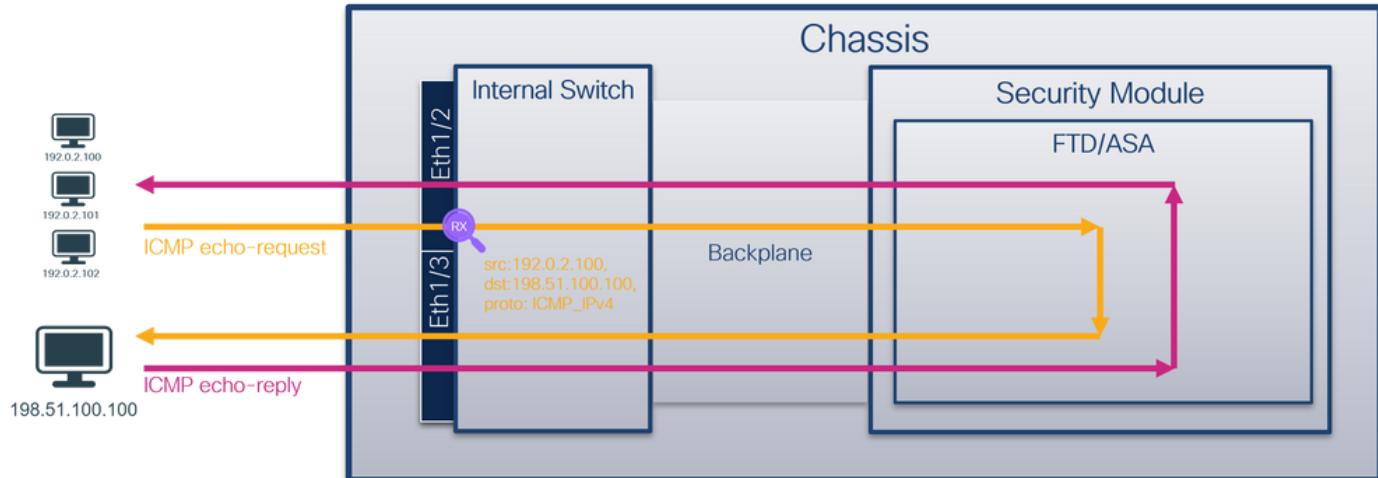
ۋە مەممەلە لودجلا اذە سەخلى:

ۋە مەممەلە	ۋە طقىن طاقتلالا	ئانىم يىلخاد VLAN طېرىضېق	ئاجتىھا	ىلۇتسەملى رورملا ۋە كەرە اھىلە
ۋە مزح طاقتلۇ نیوكت نم قىقەتلىلۇ ئىعرفەلە ۋە جاۋىلۇ Ethernet1/2.205	Ethernet1/2.205	102	لەخ دەم طقىف	نم ICMP ىدىص تابىلە ىلە 192.0.2.100 فييضمەلە 198.51.100.100
طاقتلۇ نیوكت بىمە نم قىقەتلىلۇ و ۋە مزح ۋە جاۋىلۇ ىلۇ ھەتھىچە ئىعرفەلە PortChannel1 تاھاچاوا مادختىسىپ و ۋە مادختىسىپ Ethernet1/3 و Ethernet1/4 Ethernet1/4	1/3 تىنرەتىي Ethernet1/4	1001	لەخ دەم طقىف	نم ICMP ىدىص تابىلە فەاضەتسال 192.168.207.100 192.168.207.102

## مزحلا طاقتلۇ ۋە فەصىت لە مەواع

1/2 تىنرەتىي ۋە جاۋىلۇ ھەتھىچە نم قىقەتلىلۇ و ۋە مزح طاقتلۇ نیوكتىل CLI و FCM و مەدختىسىپ حشرمادختىسىپ.

طاقتلالا طاقنۇ، ۋە مزحلا قىفتىت، طەطخەملى



نیوکتل

FCM

نم ICMP ىدص بـلـط مـزـحـل طـاقـتـلـا ئـيـفـصـت لـمـاع نـيـوـكـتـل FCM ىـلـع تـاوـطـخـلـا هـذـه عـارـجـاب مـقـةـجـا ىـلـع ئـمـزـحـلـا طـاقـتـلـا ىـلـع هـقـيـبـطـتـو 198.51.100.100 فـيـضـمـلـا ىـلـ 192.0.2.100 فـيـضـمـلـا 1/2: تـنـرـثـيـا:

1. حـشـرـم ءـاشـنـإـل حـشـرـم ئـفـاضـا > تـاحـشـرـمـلـا ئـمـئـاـق < مـزـحـلـا طـاقـتـلـا > تـاوـدـأ مـدـخـتـسـأ. طـاقـتـلـا.

2. ظـفـح ئـقـطـقـطـو IPv4 ئـيـاغـ، رـدـصـمـ، لـوـكـوـتـورـبـ، مـسـا حـشـرـمـلـا تـنـيـعـ:

The screenshot shows a "Filter List" table and a "Edit Packet Filter" dialog box. The table lists a single filter named "filter\_icmp" with the following details:

Filter Name	From MAC	From IPv4	From IPv6	Port	To MAC	To IPv4	To IPv6	Port	Protocol	Inner vlan	Outer vlan	EtherType
filter_icmp	00:00:00:00:00:00	192.0.2.100		11	0	00:00:00:00:00:00	192.0.2.100	11	0	1	0	0

The "Edit Packet Filter" dialog box shows the configuration for "filter\_icmp":

- Filter Name:** filter\_icmp
- Protocol:** ICMP\_IPv4
- EtherType:** Any
- Source:** IPv4: 192.0.2.100
- Destination:** IPv4: 198.51.100.100
- IPv6:** ::
- Port:** 0
- MAC:** 00:00:00:00:00:00

3. ئـدـيـدـج طـاقـتـلـا لـمـع ئـسـلـج ءـاشـنـإـل طـاقـتـلـا ئـسـلـج > تـاوـدـأ مـدـخـتـسـأ.

The screenshot shows the NetworkMiner application's main interface. At the top, there is a navigation bar with tabs: Overview, Interfaces, Logical Devices, Security Engine, Platform Settings, System, Tools (which is highlighted with a red box), Help, and admin. Below the navigation bar, there is a sub-navigation bar with tabs: Packet Capture (highlighted with a red box) and Troubleshooting Logs. The main content area has a title 'Capture Session' and a 'Filter List' button. At the bottom right of the content area, there are three buttons: 'Refresh' (with a circular arrow icon), 'Capture Session' (highlighted with a red box), and 'Delete All Sessions'. A message 'No Session available' is displayed at the bottom left.

نألغش و ظفح ظق طوح شرم طاقتل الا تقبط ، مسا ٤ سلجلة تدوز ، ١/٢ تينرث ددح طاقتل الا طشندي

The screenshot shows the FTD configuration interface. On the left, a network diagram displays four ports: Ethernet1/2 (selected), Ethernet1/3, Ethernet1/9, and Ethernet1/10. On the right, session configuration parameters are set: Session Name is 'gap1', Selected Interfaces is 'Ethernet1/2', Buffer Size is '256 MB', Snap length is '1518 Bytes', and Store Packets has 'Overwrite' selected. Below these, a 'Capture Filter' section is configured with 'Apply Filter' set to 'filter\_icmp' and 'To' set to 'Ethernet1/2'. The 'Save and Run' button is highlighted in orange.

## ن م Fxos (CLI) رم اول ا رطس، ٥٥ جاو

تاهج اویل ع مزحلا طاقتلا نیوکتل FXOS ل (CLI) رم اوألا رطس ٰهنجاویل ع تاوطلخا هذه عارجاب مق ٰهنجاویل ع تاوطلخا هذه عارجاب مق:

١- قیب طتل ا فرع و قیب طتل ا عون فی رعّت.

```
<#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. يف IP لوکوتورب مقر ددح <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>. 1. و ICMP لوکوتورب مقر نوکی، ۃاحلا ھذه يف.

### 3. طاقتل ا ةسلج عاشن|:

```
<#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 #

```

## ققحتل

### FCM

فلملا مجح ةدایز نم ولیغشتلا دیق ليغشتلا ئلاح نأ نم دكأت و، ؤهجاولما مسا نم ققحت (تیابلاب):

Capture Session													System Tools Help admin		
Filter List															
Filter List													Add Filter		
Filter Name	MAC	From IPv4	IPv6	Port	To MAC	From 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			

يـف دـيـزـيـ (ـتـيـابـلـابـ)ـ مجـحـ درـبـمـلـاـ عـفـتـرـمـ عـضـ وـ ؤـيـلـمـعـلـاـ تـنـمـضـ،ـ حـشـرـمـ لـاـ،ـ مـسـاـ نـرـاقـلـاـ تـقـقـدـ لـمـعـ ؤـسـلـجـ طـاقـتـلـاـ > طـبـرـ طـاقـتـلـاـ > تـاـوـدـأـ

Capture Session																System Tools Help admin		
Filter List																		
Filter List																Refresh Capture Session Delete All Sessions		
cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB	Snap Length: 1518 Bytes														
Interface Name	Filter	File Size (in bytes)	File Name	Device Name														
Ethernet1/2	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	fd1														

وـهـ رـمـاـوـأـلـاـ فـخـوسـ (ـCـLـIـ)ـ نـمـ

قـاطـنـلـاـ ؤـمـزـحـ طـاقـتـلـاـ يـفـ طـاقـتـلـاـ لـيـصـافـتـ نـمـ قـقـحـتـلـاـ:

<#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

## طة قتل الاتا فلم عي مجت

يـلخـادـلـا لـوـحـمـلـا طـاقـتـلـا تـافـلـم عـيـمـجـت مـسـقـلـا يـف تـاوـطـخـلـا عـارـجـابـ مـقـ

طاقت الا فلم ليـلـحـت

صحفویل والا ڦمزحلا ددح. طاقتلالا فلم حتفل مزحلا طاقتلا تافلم ئراق قیب طت مدختساً حاتفملما طاقن

- تارم 2 اهضرعو ةمزح لك طاقتلا متى .طقف ICMP ئىدص بلىط مزح طاقتلا متى.

  1. VLAN ئىماع نودب يىلصألا ةمزحلا سأر.
  2. 1/2 تىنرثا نراق لخدملان يىعي نأ 102 ئقاطب VLAN ئانىيم يفاضا يلىخاد حاتفملال خدي.
  3. ئيفاضا VN ئىماع يلىخادلا حاتفملال خدي.
  - 4.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info
1	2022-08-02 15:46:55.603277660	192.0.2.100	198.51.100.100	ICMP	108	0x0012 (18)	64 Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
2	2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18)	64 Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
3	2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64 Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
4	2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219)	64 Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
5	2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (459)	64 Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
6	2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459)	64 Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01de (470)	64 Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
8	2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01de (470)	64 Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64 Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153839	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64 Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64 Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64 Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162284	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64 Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64 Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64 Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64 Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64 Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64 Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791115192	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64 Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64 Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
<							
> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_uo_1, interface capture_uo_1, duration 0.000 seconds, capture size 108 bytes (864 bits)							
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)							
v VN-Tag							
1 .....	.....	= Direction: From Bridge				0000 58 97 bd b9 77 0e 50	X -w -P V -&
0.....	.....	= Pointer: vif_id				0010 00 00 81 00 00 66 08 00	....f E-T @-
.00 0000 0000 1010 .....	.....	= Destination: 10				0020 40 01 4d 9b c0 00 02 64	@M-d-3dd-g
.....	.....	= Looped: No				0030 00 18 01 5d e2 46 e9 62	...]-F-b .....
.....	.....	= Reserved: 0				0040 00 00 00 00 10 11 12 13	.....
.....	.....	= Version: 0				0050 1c 1d 1e 1f 20 21 22 23	!# \$&`)*+
.....	.....	= Source: 0				0060 2c 2d 2e 2f 30 31 32 33	,-,0123 4567
Type: 802.1Q Virtual LAN (0x8100)							
v 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							
2							

تارم 2 اهض، وع، و مزح لک طاق، تلا متی. طق، ف ICMP یدص، بلط مزح طاق، تلا متی.

2. ةمالمع نودب يلصألا ةمزحلا سأر.  
 3. تينرثا نراق لخدملا نوعي نأ 102 ئقاطب VLAN ءانيم يفاضا يلخاد حاتفملال خدي.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
2	2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012 (18)	64	Echo (ping) request id=0x0018, seq=349/23809, ttl=64 (no r
3	2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
4	2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db (219)	64	Echo (ping) request id=0x0018, seq=350/24065, ttl=64 (no r
5	2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
6	2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb (459)	64	Echo (ping) request id=0x0018, seq=351/24321, ttl=64 (no r
7	2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
8	2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6 (470)	64	Echo (ping) request id=0x0018, seq=352/24577, ttl=64 (no r
9	2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
10	2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (500)	64	Echo (ping) request id=0x0018, seq=353/24833, ttl=64 (no r
11	2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
12	2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (505)	64	Echo (ping) request id=0x0018, seq=354/25089, ttl=64 (no r
13	2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
14	2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (622)	64	Echo (ping) request id=0x0018, seq=355/25345, ttl=64 (no r
15	2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
16	2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (700)	64	Echo (ping) request id=0x0018, seq=356/25601, ttl=64 (no r
17	2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
18	2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (815)	64	Echo (ping) request id=0x0018, seq=357/25857, ttl=64 (no r
19	2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r
20	2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1039)	64	Echo (ping) request id=0x0018, seq=358/26113, ttl=64 (no r

حرشلا

نيرتم دح او تقويف ةمزح لك لوحمل ا طقتلي، ئيمامأ ٥ج او لمع ةمزح طاقتلا نيوكت دناع

- ةمالمع لاخدا دعب Port VLAN.
- ئيرهاظلا ةصالخا ئكبشلا ةكبشلا ةصالخا دعب (VN).

ةصالخا VLAN ةمالمع جاردا نم ٥قحال ٥لحرم يف VN ةمالمع جاردا متي، تايلىمعلاب يترتت يف عم طبرلا نم ركبم ٥قاطب VN لىع مطبرلا رهظي، طاقتلا رهظي، طاقتلا فلم يف نكلو. ٥فنملاب ٥قاطب VLAN ءانيم.

هاجتا يف حشرمل ا قباطت يتلا مزحلا طاقتلا متي طقف طاقتلا حشرم قيبطت متي امدنع لخدملا.

ةمممل ا لودجل ا اذه صخل:

ةمممل ا	ةطقن طاقتلا	ءانيم يلخاد VLAN يف طبر ضبق	هاجتا	ةيفصت لماع مدخلتسملالا	رورمل ا ئكرح اهيلع ئلولتسملالا
طاقتلا نيوكت ٥قحال او ةمزح تتحص نم لمع مادرختسلا ا ٥لعي ٥يفصت ئيمامألا ٥ج اولما Ethernet1/2	Ethernet1/2	102	لخدم طقف	لوكوتوربلا ICMP: 192.0.2.100: 198.51.100.100	نم ICMP ىدص تابلط 192.0.2.100 فيضملالا فيضملا ا 198.51.100.100

# يـلـخـادـلـا لـوـحـمـلـا طـاقـتـلـا تـافـلـم عـيـمـجـتـ

FCM

درـبـم طـاقـتـلـا حـاتـفـم يـلـخـادـعـمـجـي نـأ لـعـ فـمـيـلـا FCM اـذـهـ تـزـجـنـأ

1. طـشـنـلـا طـاقـتـلـا فـاقـيـإـلـا لـمـعـلـا ظـسـلـجـ لـيـطـعـتـ رـزـىـلـعـ رـقـنـا.

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	34700	cap1-ethernet-1-2-0.pcap	ftd1

2. - لـيـغـشـتـلـا ةـلـاحـ لـطـعـتـ نـمـ دـكـأـتـ:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	218828	cap1-ethernet-1-2-0.pcap	ftd1

3. طـاقـتـلـا فـلـمـ لـيـزـنـتـ لـيـزـنـتـ قـوـفـ رـقـنـا.

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2	None	218828	cap1-ethernet-1-2-0.pcap	ftd1

وضع ةـهـجـاـوـ لـكـلـ ـوـطـخـلـا هـذـهـ رـرـكـ ،ـذـفـنـمـلـا ةـانـقـ تـاهـجـاـوـ ةـلـاحـ يـفـ.

نم (CLI) FXOS رـمـاـوـأـلـاـ رـطـسـ ةـهـجـاـوـ

طـاقـتـلـا تـافـلـمـ عـيـمـجـتـ (CLI) FXOS رـمـاـوـأـلـاـ رـطـسـ ةـهـجـاـوـ ئـلـعـ تـاوـطـخـلـا هـذـهـ عـارـجـاـبـ مـقـ:

1. طـشـنـلـا طـاقـتـلـا فـاقـيـاـ:

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

firepower /packet-capture #
scope session cap1
```

```
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. لم ينجح ملف ftd1.pcap في إنشاء قاعدة بيانات.

```

<#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.pcap

Password:

```

وضع ٰهـجـاـوـلـكـلـ طـاـقـتـلـاـ فـلـمـ خـسـنـاـ ،ـذـفـنـمـلـاـ ـةـاـنـقـ تـاهـجـاـوـلـاحـ يـفـ.

## يـلـخـادـلـاـ لـوـحـمـلـاـ ـةـمـزـحـ طـاـقـتـلـاـ تـاسـرـامـمـلـاـ لـضـفـأـوـ دـيـدـحـتـوـ تـادـاشـرـاـ

يـلـخـادـلـاـ لـوـحـمـلـاـ طـاـقـتـلـاـ دـوـيـقـلـاـوـ تـادـاشـرـالـاـ ىـلـعـ لـوـصـحـلـلـ Firepower 4100/9300 Cisco Firepower 4100/9300 FXOS Chassis Manager وأـفـاـشـكـتـسـأـ لـصـفـلـاـ Cisco Firepower 4100/9300 FXOS، مـزـحـلـاـ طـاـقـتـلـاـ مـسـقـلـاـ ،ـاهـحـالـصـإـوـ عـاطـخـأـلـاـ.

تـالـاحـ يـفـ مـزـحـلـاـ طـاـقـتـلـاـ مـاـدـخـتـسـاـ ىـلـإـ ـةـدـنـتـسـمـلـاـ تـاسـرـامـمـلـاـ لـضـفـأـ ـةـمـئـاـقـ يـهـ ـهـ ذـهـ TAC:

- دـوـيـقـلـاـوـ ـةـيـهـيـجـوـتـلـاـ ـىـدـاـبـمـلـاـبـ ـةـيـارـدـ ـىـلـعـ نـكـ.
- طـاـقـتـلـاـ تـافـلـمـ لـكـ لـيـلـحـتـوـ ـعـانـيـمـلـاـ ـةـاـنـقـلـاـ ـوـضـعـ ـتـاهـجـاـوـلـكـ ـىـلـعـ مـزـحـلـاـ طـقـتـلـاـ.
- طـاـقـتـلـاـ ـةـيـفـصـتـلـمـاـعـ مـاـدـخـتـسـاـ.
- حـشـرـمـ طـاـقـتـلـاـ تـلـكـشـ اـمـدـنـعـ نـاـوـنـعـ طـبـرـلـاـ ـىـلـعـ NATـ رـيـثـأـتـ رـابـتـعـاـلـاـ ـيـفـ تـعـضـوـ.
- ـةـمـيـقـلـاـ نـعـ هـفـاـلـتـخـاـ ـةـلـاحـ يـفـ رـاـطـاـلـاـ مـجـحـ دـدـحـيـ يـذـلـاـ lenـ بـاـذـجـنـاـ لـيـلـقـتـ وـأـ ـةـدـايـزـبـ مـقـ.
- مـزـحـلـاـ نـمـ دـيـاـزـتـمـ دـدـعـ رـصـقـأـلـاـ مـجـحـلـاـ نـعـ جـتـنـيـ .ـتـيـابـ 1518ـ غـلـبـتـ يـتـلـاـ ـةـيـضـاـرـتـفـاـلـاـ سـكـعـلـاـبـ سـكـعـلـاـوـ طـقـتـلـمـلـاـ.
- ـةـجـاـحـلـاـ بـسـحـ تـقـفـمـلـاـ نـزـخـمـلـاـ مـجـحـ طـبـضـبـ مـقـ.
- لـوـصـولـاـ دـرـجـمـبـ FCMـ وـأـ FXOSـ نـمـ رـمـاـوـأـلـاـ رـطـسـ ـةـهـجـاـوـ ـىـلـعـ طـاـقـسـإـلـاـ دـدـعـبـ ـةـيـارـدـ ـىـلـعـ نـكـ.
- طـاـقـسـإـلـاـ دـادـعـ دـادـزـيـ ،ـتـقـفـمـلـاـ نـزـخـمـلـاـ مـجـحـ دـحـ ـىـلـاـ.
- اـذـهـ VNـ ـةـمـاـلـعـ نـوـدـبـ طـقـفـ مـزـحـلـاـ ضـرـعـلـ Wiresharkـ ـىـلـعـ !vntagـ ـةـيـفـصـتـلـاـ لـمـاـعـ مـدـخـتـسـأـ.
- درـبـمـ طـاـقـتـلـاـ طـبـرـ ـةـيـمـاـمـأـلـاـ ـةـهـجـاـوـلـاـ ـيـفـ طـبـرـ VN-taggedـ ـيـفـخـيـ نـأـ ـدـيـفـمـ.
- كلـذـ دـيـفـيـ .ـطـقـفـ ـةـيـدـرـفـ تـارـاـطـاـ ضـرـعـلـ Wiresharkـ ـىـلـعـ frame.number&1ـ ـحـشـرـمـ مـدـخـتـسـأـ.
- ـةـيـفـلـخـلـاـ ـةـحـوـلـلـاـ ـةـهـجـاـوـ ـةـمـزـحـ طـاـقـتـلـاـ تـافـلـمـ يـفـ ـةـرـكـمـلـاـ مـزـحـلـاـ ـعـافـخـاـ ـيـفـ.

- نیولتلار داعوق يضارتفا لکشپ Wireshark قبطي، لثم تالوكوتورب ئلاح يف يلخادلا لوحملار طاقتلار ئلاح يف. ئفلت خم ناولأب ئنديعم طورشپ مزحلا ضرعت يتلا اهيلع ئماملا عضوو مزحلا نيولت نكمي، طاقتلارلا تافلم يف مزحلا راركت ببساب مق مث، حشرم يأ تقبطو مزحلا طاقتلارلا تافلم ليلىحتب تمدق اذا. ئطاخ ئبجوم ئقيرطب كلذ نم الدب ديدجلا فلملا حتفاو ديدج فلم لىإ ئضورعلملا مزحلا ريدصتب.

## 3100/4200 نمآلار ئامحلارا راجىل ع ققحتلار نيوكتلار

نمآلار ئامحلارا راجىل ع يلخادلا لوحملار طاقتلار نيوكت متي، Firepower 4100/9300، سكع ئيلع رايخ ددحي ثيچ capture <name> switch، رمألا ربع قىبطة تلا رمألا رطس ئهه جاولىع يلخادلا لوحملار ئامحلارا راجىل ع ققحتلار ئايلىم ئوكت مت هنأ لوحملار.

لوحملارا رايخ ع رمألا و اوذه capture:

```
<#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>
```

يلىپ امك يه مزحلا طاقتلار نيوكتل ئاماعلارا تاوطخلار:

1. نراق لخدمنىع:

تاهجاو ئامسأ ديدحت مدخلتسىملل نكمي. لوحملارا مسالا طاقتلار نيوكت لبقي: ئارادىلا تاهجاو وأ ئيلخادلا تالصوّلار وأ تانايبلارا:

```
<#root>
>
capture caps_w 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 ۋەمىقلا .ئاجتىلا ئىانىڭ طاقىتلەلا تايلىمۇ 4200 زارت نەم آلا ئىامحلا رادج مۇعدىي: كىلذ فالخ نىعىي:

```

<#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

```

لىصوت ئەجاو 2 و ئىلخاد تانايىب 2 ئىل 4245 نەم آلا ئىامحلا رادج يوتحىي ،كىلذىلى ئەفاضەلاب و ئىرادا:

```

<#root>

>

capture capswh 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

```

تنرثىياعون رايىخ مېق ددھت .IP وە يىضارتىلا راطىل EtherType .تنرثىيالا راطىل EtherType: عون EtherType:

```

<#root>

>

capture capswh switch interface inside ethernet-type ?

802.1Q
<0-65535>  Ethernet type
arp
ip

```

ip6  
pppoed  
pppoes  
rarp  
sgt  
vlan

3: قباطل رییاعم قباط طاقتلا رایخ ددھی. قباطملا طورش ددھ.

```
<#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. كل ذى امو قمنح لوطو تقؤمل نزخمل ممح لثم يرخألا ةيراي تخالا تامملع ملا ددج.  
5. طاقتلالا طشنى فاققى حاتفم no capture <name> رمألا طاقتلالا نيكمنتب مق.

```
<#root>

>

capture capswh switch interface inside match ip

>

no capture capswh switch stop
```

## 6. طاقتل الـ LiCap افت نم ققحت:

- ةطشنول يغشتلا ديق ليغشتلا ةلاح تناكو، ةيرادالا ةلاحلا نيكمت مت.
- Packet Capture File Size ديزى.
- يرفص رieg show capture <cap\_name> جارخا يف ةطقتملا مزحلا ددع.
- دلجملا يف ايئاقلت ةطقتملا مزحلا ظفح متى .راسملل PCAPFILE فلم طاقتلala /mnt/disk0/packet-capture/.
- طورش ىلع عانب ايلآ طاقتل الـ LiCap اتاجشرم عاشناب جمانربلا موقى .طاقتل الـ LiCap طاقتل الـ LiCap.

```
<#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
```

```
Pcapsize: 18838  
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
```

7. ةجاجلإا دنع طاقتل الافاقي:

```
<#root>  
>  
capture capsw switch stop  
>  
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: 24
Filter: caps-w-1-1
```

```
Packet Capture Filter Info
Name: caps-w-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
```

طاقة لـ ASA تـ اـ فـ لـ مـ عـ يـ مجـ تـ مـ سـ قـ لـ اـ يـ فـ ةـ دـ وـ جـ وـ مـ لـ اـ تـ اوـ طـ خـ لـ اـ عـ اـ جـ اـ بـ مـ قـ . طـ اـ قـ تـ لـ اـ تـ اـ فـ لـ مـ عـ يـ مجـ تـ . نـ مـ آـ لـ اـ يـ لـ خـ اـ دـ لـ اـ ةـ يـ اـ مـ حـ لـ اـ رـ اـ دـ لـ جـ لـ وـ حـ مـ

يـ لـ عـ يـ لـ خـ اـ دـ لـ اـ لـ وـ حـ مـ لـ اـ طـ اـ قـ تـ لـ اـ نـ يـ وـ كـ تـ مـ عـ دـ يـ اـ لـ ، نـ مـ آـ لـ اـ ةـ يـ اـ مـ حـ لـ اـ رـ اـ دـ لـ جـ مـ اـ نـ رـ بـ نـ مـ 7.4 رـ اـ دـ صـ إـ لـ اـ يـ فـ طـ اـ قـ تـ لـ اـ نـ يـ وـ كـ تـ نـ كـ مـ يـ ، ثـ دـ حـ أـ لـ اـ تـ اـ رـ اـ دـ صـ إـ لـ اـ اوـ (1)9.18 رـ اـ دـ صـ إـ لـ اـ جـ مـ اـ نـ رـ بـ ظـ لـ اـ حـ يـ فـ . FMC وـ أـ FDM . ثـ دـ حـ أـ لـ اـ تـ اـ رـ اـ دـ صـ إـ لـ اـ اوـ x.18.1 ASDM تـ اـ رـ اـ دـ صـ إـ لـ اـ يـ فـ ةـ يـ لـ خـ اـ دـ لـ اـ تـ الـ وـ حـ مـ لـ اـ

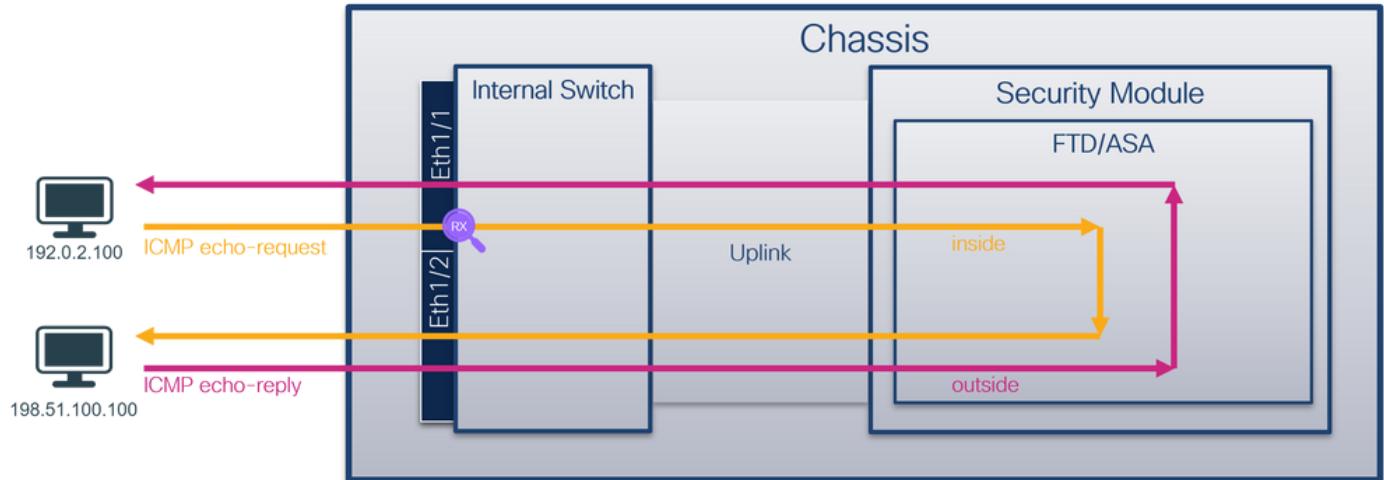
تـ الـ وـ حـ مـ طـ اـ قـ تـ لـ اـ عـ ئـ اـ شـ لـ اـ مـ اـ دـ خـ تـ سـ اـ لـ اـ تـ الـ اـ حـ تـ اـ هـ وـ يـ رـ اـ نـ يـ سـ لـ اـ هـ ذـ هـ يـ طـ غـ تـ . ةـ يـ لـ خـ اـ دـ لـ اـ

ذـ فـ نـ مـ ةـ اـ نـ قـ ةـ هـ جـ اـ وـ اـ ةـ يـ دـ اـ مـ ةـ هـ جـ اـ وـ اـ ةـ مـ زـ حـ لـ اـ طـ اـ قـ تـ لـ اـ

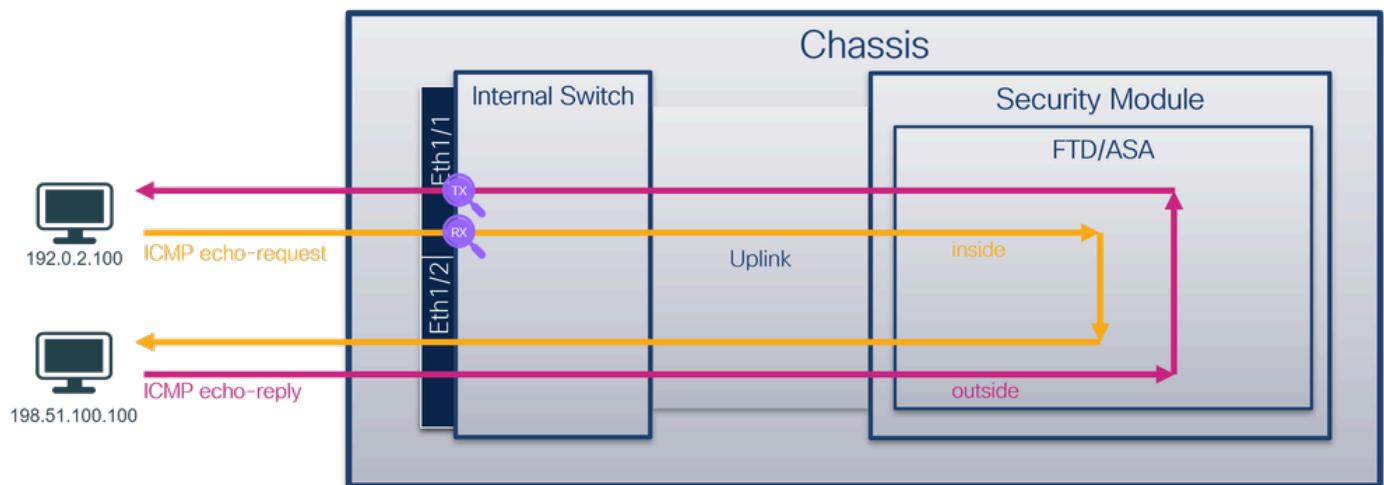
وـ اـ 1/1 تـ نـ رـ ثـ يـ اـ ةـ هـ جـ اـ وـ اـ لـ عـ 5 تـ حـ صـ نـ مـ قـ قـ حـ تـ لـ اـ وـ اـ مـ زـ حـ طـ اـ قـ تـ لـ اـ نـ يـ وـ كـ تـ لـ اـ FTD ASA CLI وـ اـ مـ دـ خـ تـ سـ اـ لـ خـ اـ دـ لـ اـ بـ مـ سـ اـ لـ اـ نـ يـ تـ هـ جـ اـ وـ اـ لـ اـ لـ كـ لـ مـ حـ تـ وـ . PortChannel1

طاقة لـ ASA تـ اـ قـ نـ وـ ، ةـ مـ زـ حـ لـ اـ قـ فـ دـ تـ ، طـ طـ خـ مـ لـ اـ

نـمـآـلـاـ ةـيـامـحـلـاـ رـادـجـ:



هـاجـتـإـلـاـ ةـيـائـانـثـ تـاعـوـمـجـمـبـ دـوـزـمـلـاـ 4200ـ زـارـطـ نـمـآـلـاـ ةـيـامـحـلـاـ رـادـجـ:



نـيـوـكـتـلـاـ

وـأـ 1/1ـ تـيـنـرـثـاـ نـرـاقـىـلـعـ طـبـرـلـكـشـيـ نـأـ ASAـ ىـلـعـ stepsـ اـذـهـ تـزـجـنـاـ:

مسـالـاـ نـمـ قـقـحـتـ 1ـ:

```
<#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

```

طاقتل إلة سلح عاشنإ 2.

```

<#root>
>
capture caps w switch interface inside

```

: طاقتل إلة هيجوت Secure Firewall 4200 معدي

```

<#root>
> capture caps w switch interface inside direction ?
both To capture switch bi-directional traffic
egress To capture switch egressing traffic
ingress To capture switch ingressing traffic

> capture caps w switch interface inside direction both

```

3. تنك م سلح طاقتل إلة:

```

<#root>
> no capture caps w switch stop

```

ققحتلإا

نم دكأت . فرعمل او ةهجاولإا ةحتفول يغشتل او ةراديل ا ةلاح و طاقتل إلة سلح مسا نم ققحت يرفص ريغ اه طاقتلإا مت يتلا مزحلا ددع نأوتي ابلاب ةميق ةدايز :

```
<#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 caps w detail
```

Packet Capture info

```
Name: caps w
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-caps w-ethernet-1-1-0.pcap
Pcapsize: 0
```

```
Direction: both
```

```
Drop: disable
Filter: caps w-1-1
```

```
Packet Capture Filter Info
Name: caps w-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

:عاصٌعُّا تاھج او عي مج ىل ع طا قتل الـا نـي وـكـت مـتـي ، 1، ةـلـاحـيـفـ:

<#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:           caps-w-1-4
```

Packet Capture Filter Info

Name:	caps-w-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:           caps-w-1-3
```

Packet Capture Filter Info

Name:	caps-w-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

رمألا لالخ نم show portchannel summary: ققحتل ا نكمي رمألا يف fxos local-mgmt وضع تاهج او نم

```
<#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
```

قايسلا ٽلاح يف FXOS ىلع ASA ىلإ لوصولل connect fxos admin. رمألا ليغشت بمق، ٽرادإلا قايس يف رمألا ليغشت بمق، ددعتملا.

طاقتل الـ اـ تـ اـ فـ لـ مـ عـ يـ مجـ تـ

يلخادلا ٽيامحلـا رـادـجـ لـوـحـمـ طـاقـتـلـاـ تـافـلـمـ عـيـمـجـتـ مـسـقـلـاـ يـفـ ٽـدـوـجـوـمـلـاـ تـاوـطـخـلـاـ عـارـجـابـ مـقـ نـمـ آـلـاـ.

## طاقتل الا فلم ليحلت

1/ تنرثي اوكبشن طاقتل الا تافلم حتفل مزحلا طاقتل اتافلم ئراق قىبطة مدخلتسا ئل والا ئمزحلا ددج 3100 نمآل ائامحلا رادج يلىع مزحلا طاقتل لىحلت متي ،لاثمل اذه يف ئيساساً طاقنلا صحفو:

1. طقف ICMP ئدص بلىط مزح طاقتل امتى.

2. ئممالع نودب يلىصاً ئمزحلا سأر VLAN.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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	0x9a3a (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 res)
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0xb910 (39696)	64 Echo (ping) request	id=0x0034, seq=5/1280, ttl=64 (no res)
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0xb934 (39732)	64 Echo (ping) request	id=0x0034, seq=6/1536, ttl=64 (no res)
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0xb983 (39811)	64 Echo (ping) request	id=0x0034, seq=7/1792, ttl=64 (no res)
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0xb98b (39819)	64 Echo (ping) request	id=0x0034, seq=8/2048, ttl=64 (no res)
9	2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64 Echo (ping) request	id=0x0034, seq=9/2304, ttl=64 (no res)
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 res)
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0xd9d8 (40296)	64 Echo (ping) request	id=0x0034, seq=11/2816, ttl=64 (no res)
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ed6 (40429)	64 Echo (ping) request	id=0x0034, seq=12/3072, ttl=64 (no res)
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 res)
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64 Echo (ping) request	id=0x0034, seq=14/3584, ttl=64 (no res)
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 res)
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9f64 (40932)	64 Echo (ping) request	id=0x0034, seq=16/4096, ttl=64 (no res)
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 res)
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 res)

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 00 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...4...a...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 55 67UUUU

طاقنلا صحفو ئل والا ئمزحلا ددج. وضع تاهج اول PortChannel1. طاقتل الا تافلم حتفا ئيساساً:

1. طقف ICMP ئدص بلىط مزح طاقتل امتى.

2. ئممالع نودب يلىصاً ئمزحلا سأر VLAN.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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 res)
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x9444 (38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, ttl=64 (no res)
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 res)
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 res)
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 res)
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 res)
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 res)
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x9822 (38922)	64 Echo (ping) request	id=0x0035, seq=11/2816, ttl=64 (no res)
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 res)
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 res)
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 res)
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 res)
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 res)
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 res)
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0xb98e (39822)	64 Echo (ping) request	id=0x0035, seq=18/4608, ttl=64 (no res)

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 16 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...M...b...
   
 0030 00 00 9e 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 55 55 67UUUU

## حرشلا

واً PortChannel1. تاهج اولا لوحملها طاقتللا نيوكت متي Ethernet1/1.

مهملا لودجلها اذه صخلي:

هادىء مەمەلە	نەھەن طاقەتلا	لەماع ئەي فەصەت يەلخاد	هاجتىا	اهىلع ئەلۋەت سەملە رورمەلە ئەكەر
ئەم زەن ئەقەتلا نېو كەن لىع ھەتھىص نەم ققەتلا و اەجەجەن Ethernet1/1	Ethernet1/1	None	لەخ دەم * طاقەف	نەم ICMP ئىدىص تابلەت لىلە 192.0.2.100 فيي ضەملە و اەجەجەن 198.51.100.100 فيي ضەملە
لىع ئەم زەن ئەقەتلا نېو كەن PortChannel1 ئەجەجەن ھەتھىص نەم ققەتلا و وضعلا تاھاج او مادختسەب Ethernet1/3 و Ethernet1/4	1/3 تەنرەتىي Ethernet1/4	None	لەخ دەم * طاقەف	نەم ICMP ئىدىص تابلەت لىلە 192.0.2.100 فيي ضەملە و اەجەجەن 198.51.100.100 فيي ضەملە

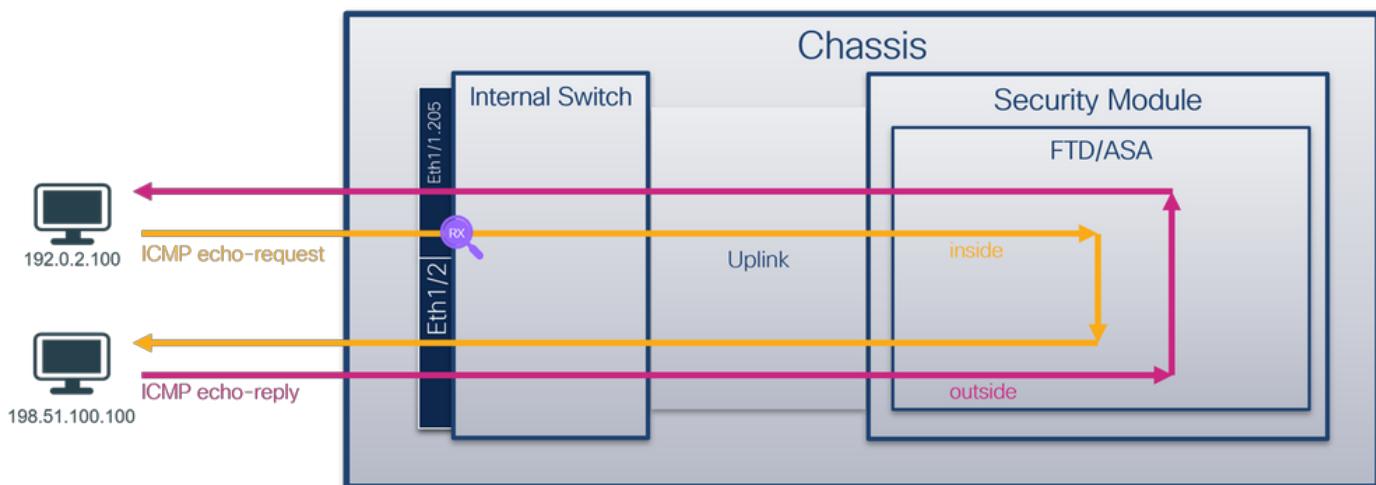
لۇخدىلا) هاجتىلا ئەي ئانث طاقەتلا تايىلمۇ 4200 نەم آلا ئەيامحلا رادىج معدى، 3100 سۈكۈ ئەلۋەت.  
جورخەلە.

### ذىنەم ئانق ئەجەجەن و ئەيدام ئەجەجەن ئەي عەرف ئەجەجەن ئەلۋەت ئەقەتلا

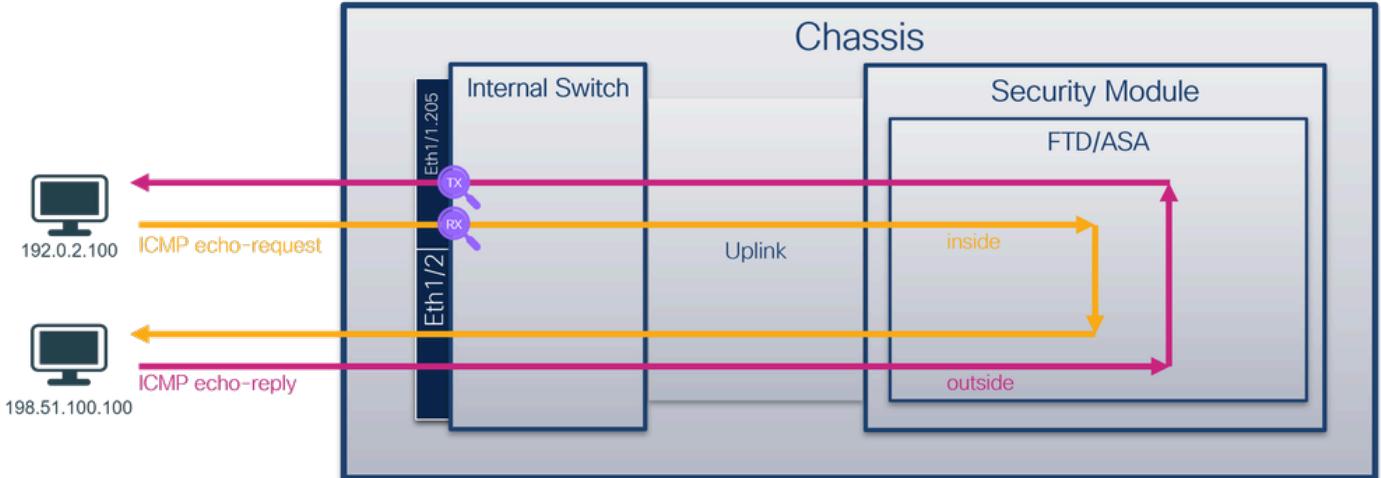
نەم ققەتلا و ئەم زەن ئەقەتلا نېو كەن ASA و FTD عون نەم (CLI) رەماؤلا رەتس ئەجەجەن مەدختىسى  
تاھاجەنلا الڭ يەوتەت. PortChannel1.205 و Ethernet1/1.205 ئەي عەرفلىلا تاھاجەنلا ئەلۋەت ھەتھىص  
لەخادلىپ مەسالا ئەلۋەت ئەي عەرفلىلا.

طاقەتلا طاقىن و ئەم زەن ئەقەتلا قىفتىت، طەطخەملا

3100 نەم آلا ئەيامحلا رادىج:



4200 نەم آلا ئەيامحلا رادىج:



نیوکتل

1/1 تینرث نراق ىلۇ طېرىلىكشى نا ASA CLI وۇ steps ئىلۇ اذە تىزجىنأ:

مسالا نم قىقىخت.

<#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. ئاشنامىنىڭ سىلاچقا:

<#root>

> capture caps/w switch interface inside

Secure Firewall 4200 هي جوٰت اٰ لالٰ مُعدي:

<#root>

> capture caps/w switch interface inside direction ?

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

> capture caps/w switch interface inside direction both

**3: طاقتل الا ةسلج نيكمنتب مق.**

<#root>

> no capture caps w switch stop

ققحتل

نأ نم دكأت . فرعمل او ةهجاولا ٔحتفو ليغشتلاو ةرادإلا ٔلح و طاقتلالا ٔسلج مسا نم ققحت ارفص سيل اهطاقتلا مت يبتلا مزحلا ددع نأو تيابلاب دادزت PCAPSIZE ٔميق

<#root>

>

```
show capture caps w detail
```

## Packet Capture info

Name: caps w

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: caps-w-1-1
```

Packet Capture Filter Info

```
Name: caps-w-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

نراقل اىل ع تقب طو VLAN=205 يج راخ ع م حشرم تقلخ، ئلاحلا هذه يف.

عيمج اىل ع تقب طو VLAN=205 يفصت لماع مادختس اب طاق تل الـ Port-channel1 نيوكت متى عاضع الـ تاهج او:

```
<#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:             caps-w-1-3

Packet Capture Filter Info
Name:               caps-w-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

رمألا لالخ نم رمأ يف fxsos local-mgmt show portchannel summary:

```
<#root>
>
connect fxsos

...
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

```

قايسلا ٽلاح يف connect fxos admin. رمألا ليغشتب مق، ىلع FXOS ىلإ لوصولل ٽرادإلا قايس يف رمألا اذه ليغشتب مق، ددعتملا.

### طاقتلala تافلم عي مجت

يلخادلا ٽيامحلا رادج لوحm طاقتلala تافلم عي مجت مسقلala يف ٽدوجوملا تاوطلخla عارجاب مق نمآل.

### طاقتلala فلم لي لحت

يف 1.205. 1 تنرثي إل طاقتلala تافلم حتفل مزحلala طاقتلala تافلم ئراق قي ب طت مدختسا صحفو ٽلوا ٽمزحلala ددح. 3100 نمآلala ٽيامحلا رادج ىلع مزحلala طاقتلala لي لحت متى، لاثملala اذه: ٽي ساسألا طاقنلا.

1. طقف ICMP ىدص بـ لـ طـ مـ زـ طـ طـ اـ قـ تـ لـ الـ مـ تـ يـ.
2. ٽـ مـ اـ لـ عـ ىـ لـ عـ ٽـ لـ صـ أـ لـ الـ ٽـ مـ زـ حلـ الـ سـ أـ رـ يـ وـ تـ حـ يـ.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	1 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 21:21:08.618823	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)

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 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)

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)

Trailer: 55555555

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 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 35 55 55 55 55 55 55 55 55 55 234567UU UU

طاقنلا صحفو لاؤلا ۆمزمحل ددح وضع تاهج اول طاقتل الاتا فەلم حەتفا ئىس اس الـ:

1. طقق ف ICMP يدىص بلىط مزح طاقتل الاتا مەتى.
2. ۆممالع ىلعيلىص الـ VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info	
1	2022-08-07 21:21:01.607187	192.0.2.100	198.51.100.100	ICMP	106	1 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 21:21:08.618823	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)

Frame 1: 106 bytes on wire (848 bits), 106 bytes captured (848 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)

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)

Trailer: 55555555

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 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 35 55 55 55 55 55 55 55 55 55 234567UU UU

حرشلـا

طاقنلا صحفو لـ VLAN 205 و اـ PortChannel1.205 ۆمزمحل ددـح اـ عـرـفـلـا اـ لـ عـ لـ حـ مـ لـ اـ طـ قـ تـ لـ الـ اـ لـ اـ مـ اـ فـ صـ قـ سـ اـ لـ اـ جـ اـ تـ اـ اـ لـ اـ يـ لـ خـ اـ لـ اـ ۆـ مـ مـ مـ لـ اـ لـ وـ دـ جـ لـ اـ اـ ذـ صـ خـ لـ لـ اـ :

ۆمـمـمـلـا	ۆـ طـ قـ نـ	لـ مـ اـ فـ صـ قـ سـ	اـ جـ اـ تـ اـ	ىـ لـ وـ سـ مـ لـ اـ رـ وـ رـ مـ مـ لـ اـ ۆـ كـ حـ
------------	-------------	----------------------	----------------	--

لوجدل) هاجت إلا ئيئانث طاقتللا تايملع 4200 نمآلا ئيامحلا رادج معدي، 3100 سكع ىلע \* جوخرلار.

ةيـلـخـادـلـا تـاهـجـاـوـلـا يـلـعـةـمـنـحـلـا طـاقـتـلـا

نیتیلخاد نیتھجاو ىلع 3100 نمآلا ۆیامحلا رادج یوتحي

- يلخ ادلـا لوحـملـاب قـيـبـطـتـلـا ليـصـوـتـبـ مـوقـيـ - ةـهـجـاـوـىـلـا SSHـلـثـمـ، ئـرـادـلـا تـالـاـصـتـالـاـصـخـمـ ئـمـزـحـ رـاسـمـ رـفـوـيـ - ئـنـمـغـمـ ئـلـاـعـلـكـلـاـ، ئـرـادـلـا ئـلـاصـتـاـ وـأـ، ئـرـادـلـا FMCـ وـ sftunnelـ، FTDـ نـيـبـ.

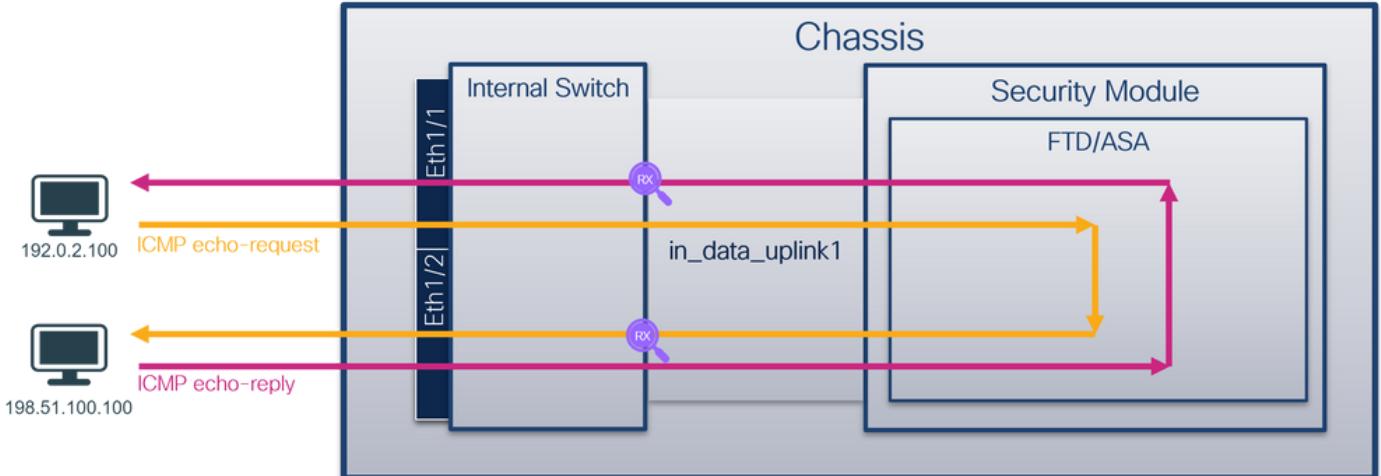
؛ يېلخاد تاهجاو 4 يىلا لصىي ام ئىلع 4200 نمآلا ئىامحلا راجد يوتحىي



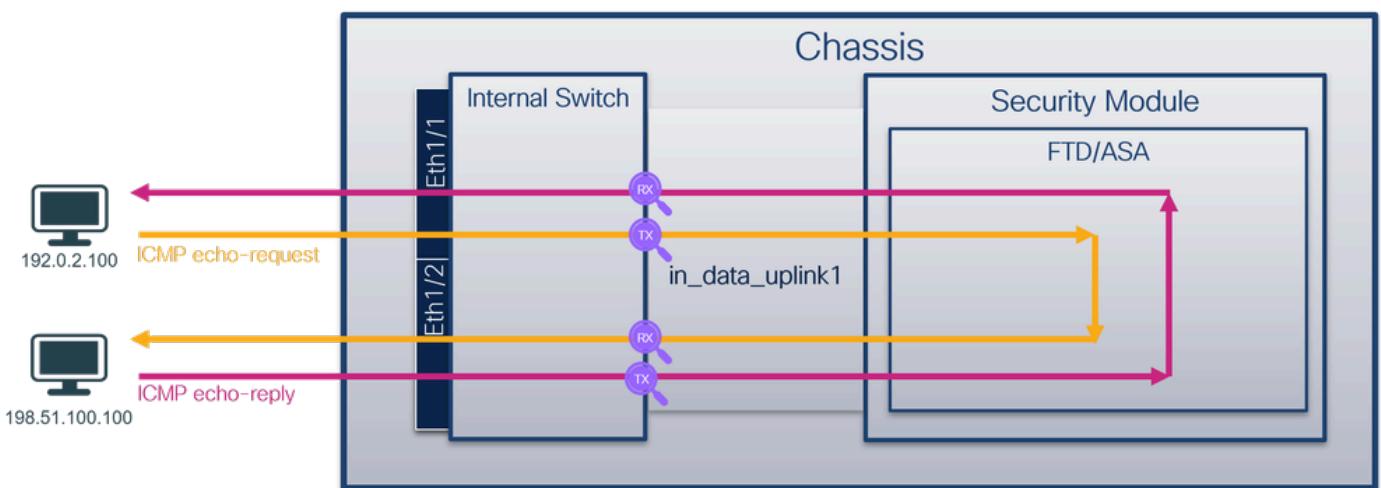
موم ۱

ةلص ول ا ةهج او لع ٥ تحقص نم ققحتل او ٥ مزح طاقتلا نيوكتل ASA CLI او FTD مدخلتسا في\_data\_uplink1.

طاقتل الا طاقنو، ةمزحلا قفدت، ططخملا



راج 4200 نمآل ۆيامحلا زارط:



نیوکتلا

ASA CLI لىع طاقتلارا طبر لکشی نأ steps اذه تزجن data\_uplink1:

1. عاشنإ سلچ ئاسقەتلا:

```
<#root>
>
capture capsw switch interface in_data_uplink1
```

Secure Firewall 4200 ھي جوت مەعدىي:

```
<#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 ingressing traffic
```

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

2. ةسنج طاقتللا تنكـم:

```
<#root>
```

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

3. قـقـحـلـلـا

نـأـ نـمـ دـكـأـتـ . فـرـعـمـلـ اوـ ةـهـجـاـوـلـاـ ةـحـتـفـوـ لـيـغـشـتـلـاـ اوـ ةـرـادـإـلـاـ ةـلـاحـ وـ طـاقـتـلـلـاـ ةـسـلـجـ مـسـاـ نـمـ قـقـحـتـ

ارـفـصـ سـيـلـ اـهـطـاقـتـلـاـ مـثـ يـتـلـاـ مـزـحـلـاـ دـدـعـ نـأـوـتـيـابـلـاـبـ دـادـزـتـ PCAPSIZEـ ةـمـيـقـ

```
<#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:           caps-w-1-18

Packet Capture Filter Info
Name:             caps-w-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

وھج او وھج 18 يلخاد فرعم مادختساب وھج اولا ىلع طاقتلا عاشن امتي، ۋە لاحل اھذھ يف  
in\_data\_uplink1 نمآلا ۋېامحلا راچى ىلع show portManager switch status يف  
fxos local-mgmt shell رمآلما تافرعم اوچى:

```

<#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

قايسلا ۋەلەح يىف connect fxos admin. رمألا لىغشتىپ مۇق، ىلۇ FXOS ASA. ىلۇمىسىنىڭ ۋەلەح ئادىلا قايس يىف رمألا اذە لىغشتىپ مۇق، دەعەتمەلە.

### طاقدىلىكلا تافلم عىمجىت

يىلخادىلا رادىج لوحەم طاقدىلىكلا تافلم عىمجىت مىسىقىلا يىف ۋەدوجۇملا تاوطىخلا ئاراجاب مۇق نەمآلە.

### طاقدىلىكلا فلم لىلەت

ۋەھىجىلىكلا طاقدىلىكلا تافلم حەتىلەنەتلىكلا طاقدىلىكلا ئاراق قىيىبەت مەختىسىنىڭ 3100 نەمآلە ۋەھىجىلىكلا رادىج ىلۇ مزحلا طاقدىلىكلا لىلەت مەتىي، لەئەتمەلە اذە يىف \_data\_uplink1.

ىلۇ درىلا مزح و ICMP ئىدىص بىلەت طاقدىلىكلا مەتىي، ۋەلەحلا ھەذە يىف - حاتىمىلا ۋەطقىن نەم قىققەتلىكلا لىلەت مەتىي، دادتىرىلا نەم ئەلسەرمەلە مزحلا يە ھەذە.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info	
1	2022-08-07 22:40:06.685606	192.0.2.100	198.51.100.100	ICMP	102	0x4d93 (19859)	64	Echo (ping) request	id=0x003a, seq=33/8448, ttl=64 (req)
2	2022-08-07 22:40:06.685615	198.51.100.100	192.0.2.100	ICMP	102	0x6cdc (27868)	64	Echo (ping) reply	id=0x003a, seq=33/8448, ttl=64 (rep)
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4a08 (19944)	64	Echo (ping) request	id=0x003a, seq=34/8704, ttl=64 (req)
4	2022-08-07 22:40:07.683903	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply	id=0x003a, seq=34/8704, ttl=64 (rep)
5	2022-08-07 22:40:08.685736	192.0.2.100	198.51.100.100	ICMP	102	0x4edc (20188)	64	Echo (ping) request	id=0x003a, seq=35/8960, ttl=64 (req)
6	2022-08-07 22:40:08.690886	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply	id=0x003a, seq=35/8960, ttl=64 (rep)
7	2022-08-07 22:40:09.690737	192.0.2.100	198.51.100.100	ICMP	102	0x4f2d (20269)	64	Echo (ping) request	id=0x003a, seq=36/9216, ttl=64 (req)
8	2022-08-07 22:40:09.690744	198.51.100.100	192.0.2.100	ICMP	102	0x6e80 (28288)	64	Echo (ping) reply	id=0x003a, seq=36/9216, ttl=64 (rep)
9	2022-08-07 22:40:10.692266	192.0.2.100	198.51.100.100	ICMP	102	0x4fb1 (20401)	64	Echo (ping) request	id=0x003a, seq=37/9472, ttl=64 (req)
10	2022-08-07 22:40:10.692272	198.51.100.100	192.0.2.100	ICMP	102	0x6eds (28373)	64	Echo (ping) reply	id=0x003a, seq=37/9472, ttl=64 (rep)
11	2022-08-07 22:40:11.691159	192.0.2.100	198.51.100.100	ICMP	102	0x5008 (20488)	64	Echo (ping) request	id=0x003a, seq=38/9728, ttl=64 (req)
12	2022-08-07 22:40:11.691166	198.51.100.100	192.0.2.100	ICMP	102	0x6f3b (28475)	64	Echo (ping) reply	id=0x003a, seq=38/9728, ttl=64 (rep)
13	2022-08-07 22:40:12.692135	192.0.2.100	198.51.100.100	ICMP	102	0x50b8 (20664)	64	Echo (ping) request	id=0x003a, seq=39/9984, ttl=64 (req)
14	2022-08-07 22:40:12.697209	198.51.100.100	192.0.2.100	ICMP	102	0x6fd7 (28631)	64	Echo (ping) reply	id=0x003a, seq=39/9984, ttl=64 (rep)
15	2022-08-07 22:40:13.697320	192.0.2.100	198.51.100.100	ICMP	102	0x5184 (20868)	64	Echo (ping) request	id=0x003a, seq=40/10240, ttl=64 (req)
16	2022-08-07 22:40:13.697327	198.51.100.100	192.0.2.100	ICMP	102	0x703e (28734)	64	Echo (ping) reply	id=0x003a, seq=40/10240, ttl=64 (rep)
17	2022-08-07 22:40:14.698512	192.0.2.100	198.51.100.100	ICMP	102	0x51d8 (20952)	64	Echo (ping) request	id=0x003a, seq=41/10496, ttl=64 (req)
18	2022-08-07 22:40:14.698518	198.51.100.100	192.0.2.100	ICMP	102	0x70dd (28893)	64	Echo (ping) reply	id=0x003a, seq=41/10496, ttl=64 (rep)

# حـشـلـا

ىلإ قيبر طتللا نم ٩لسرملا مزحللا طاقتلا متي، ٩لص وللا ٩هجاو ٩لعل لوحمل طاقتلا متي وكت دنع  
قيبر طتللا ىلإ ٩لسرملا مزحللا طاقتلا متي الـ . طقف يلخادلا لوحمل

## لوجلا اذه سخلي مهملة:

ةمملا	ةطقن طاقتللا	لماع ئيفصت يلخاد	اچت اهيلع	ىلولتس ملا رورملا ةكرح
ققحتل او ۋەمىزح طاقتلا نېوكت ۋەلىدۇلار ئەھجاولىع ھەتھىص نم يىف_data_uplinkink1	in_data_uplink1	None	لخدم طقف*	نم ICMP ئابلىك لى 192.0.2.100 فيضملا نم ICMP دودر نى 198.51.100.100 فيضملا نم ICMP ECHO دودر نى 198.51.100.100 فيضملا نى 192.0.2.100 فيضملا

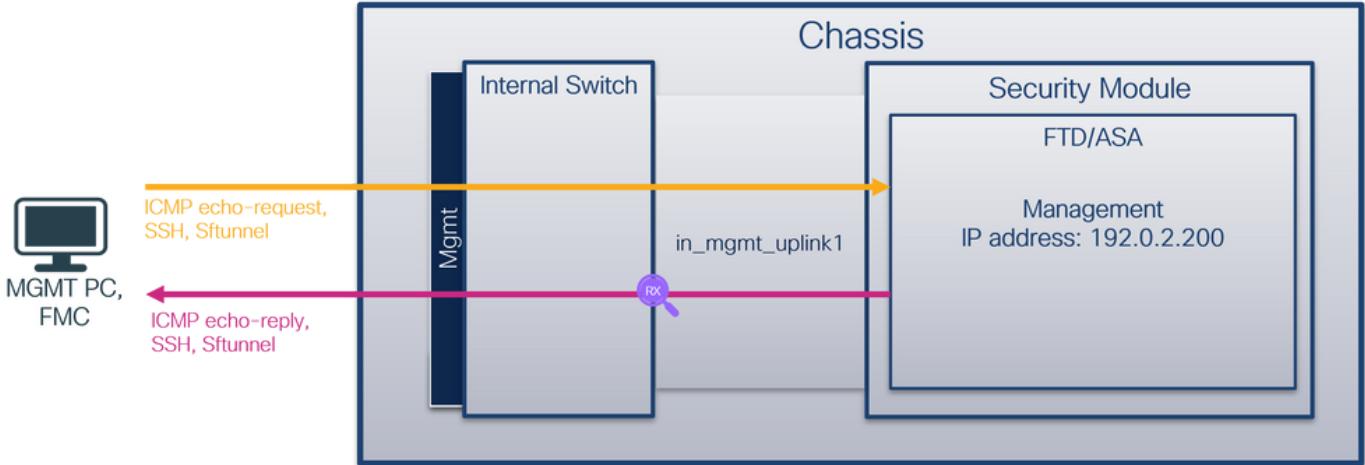
لوفدلا) هاجت إلا ئيئانث طاقدلل إلا تايبل مع 4200 نمآل ئيامحلا رادج معدي، 3100 سكع ىلע \* جوخر لالاو.

مومه ۲

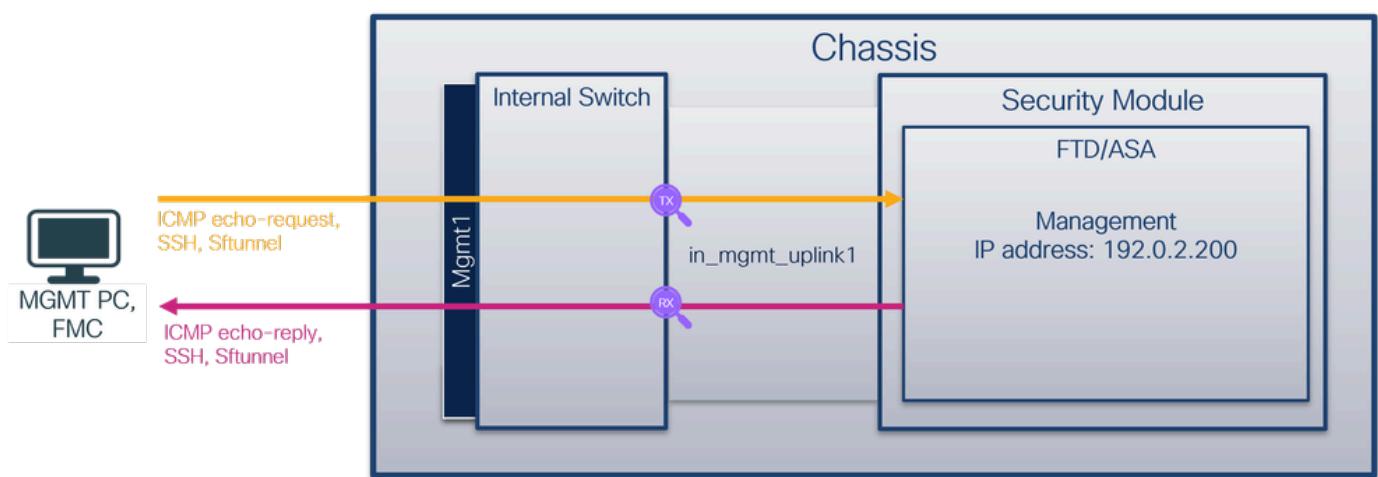
لصوص ولاؤ جاوى لع متحص نم ققحتل او ممزح طاقتلا نيوكتل ASA CLI وأ FTD مدختسأ  
طقف ةرادلإا ئوتسم تالاصت امزح طاقتلا متى in\_mgmt\_uplink1.

طاقت لا طاقن و، مزح لا قفت، طط خمل ا

رادج 3100: نمآل امیا ڦیام



4200 زارط نمآل اوامحلا رادج:



نیوکتل

ASA ىل ع طاقـتـلـا طـبـرـلـكـشـي نـأ FTD CLI وـأ steps تـزـجـنـاـ:

1. طـاقـتـلـا ئـسـلـجـ ئـاشـنـاـ:

```
<#root>
>
capture capsw switch interface in_mgmt_uplink1
```

Secure Firewall 4200 ھـيـجـوـتـ مـعـدـيـ:

```
<#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
```

```
> capture caps/w switch interface in_mgmt_uplink1 direction both
```

## 2: طاقتل الا ةسلج نيڪمتپ مق.

<#root>

> no capture caps w switch stop

## ققتلا

نأ نم دكأت . فرعمل او ةهجاولا ٔحتفول يغشتلاو ٔرادإلا ٔلاب و طاقتلالا ٔسلج مسا نم ققحت  
: ارفص سيل اهطاقتلا مث ٚ يتلا مزحلا ددع نأو تيابلاب دادزت PCAPSIZE ٔميق

<#root>

```
> show capture caps w detail
```

## Packet Capture info

Name : caps w

Session: 1

Admin State: enabled

Oper State: up

Oper State Reason: Active

Config Success: yes

Config Success:

Append Flag: overwrite

Session Mem Usage: 356

Session Mem Usage: 256

## Session PCap Snap Len

Error Code: 0  
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

## Physical parts

Slat Ed.

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

Pcapsize: 137248

Filter: caps-w-1-19

## Packet Capture Filter Info

Name:	capsw-1-19
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

281 packets captured on disk using switch capture

Reading of capture file from disk is not supported

يـف 3130 نـمـآلـا ةـيـامـحـلـا رـادـجـ لـعـ in\_mgmt\_uplink1 show portManager switch status مـتـي ، ةـلـاحـلـا 5ـهـذـهـ يـف 19 يـلـخـادـ فـرـعـمـ مـادـخـتـسـابـ ةـهـجـاـوـلـاـ ئـلـعـ طـاقـتـلـاـ ءـاشـنـاـ مـتـي ، ةـلـاحـلـاـ 5ـهـذـهـ يـف shell fxos local-mgmt رـمـآلـا تـافـرـعـمـ:

```
<#root>
>
connect fxos
...
firewall#
connect local-mgmt
firewall(local-mgmt)#
show portmanager switch
```

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

قاييسلا ٩لاح يف connect fxos admin. رمألا ليغشتب مق، ASA ىلع FXOS ىلإ لوصولل ٩رادإلا قاييس يف رمألا اذه ليغشتب مق، ددعتملا

## طة قتل الـا تافـل م عـي مجـت

يـلـخـادـلـا ئـيـامـحـلـا رـادـجـ لـوـحـمـ طـاقـتـلـا تـافـلـمـ عـيـمـجـتـ مـسـقـلـا يـفـ ئـدـوـجـوـمـلـا تـاوـطـخـلـا ذـيـفـنـتـ نـمـآلـا.

طاقتلا فلم ليحلت

in\_mgmt\_uplink1. ةهجاول طاقتل الا تافلم حتفل مزحلا طاقتل اتافلم ئراق قي بط مدخلتسا 3100 نمآلأ ئيامحل رادج ىلع مزحلا طاقتل ا ليلحت متى ، لاثمل ا اذه يف.

ةرادرالاب صاخلا IP ناونع نم مزحلا ضرع متى طقف ةلاحلا هذه يف - حاتفملا ةطقن نم ققحت  
مزحلا يه هذه ICMP echo وأ Sftunnel وـ SSH لوكوتورب ىلع درلا مزح يه ةلثملأا.  
يـلخـادـلـا لـوـحـمـلـا لـالـخـ نـم ةـكـبـشـلـا ىـلـا قـيـبـطـتـلـا ةـرـادـا ةـهـجـاـوـ نـم ةـلـسـرـمـلـا

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.1.101	TCP	1518	0xb7d0 (47056)	64	39181 → 8305 [ACK] Seq=61372 Ack=875 Win=1384 Len=1448 TS
197	2022-08-07 23:21:45.133385	192.0.2.200	192.0.2.1.101	TCP	1518	0xb7d1 (47057)	64	39181 → 8305 [ACK] Seq=62820 Ack=875 Win=1384 Len=1448 TS
198	2022-08-07 23:21:45.133388	192.0.2.200	192.0.2.1.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.1.100	ICMP	78	0xbdb48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949924	192.0.2.200	192.0.2.1.101	TLSv1.2	128	0xa497 (19095)	64	Application Data
201	2022-08-07 23:21:45.949927	192.0.2.200	192.0.2.1.101	TCP	70	0xa498 (19096)	64	8305 → 58885 [ACK] Seq=21997 Ack=26244 Win=4116 Len=0 TSv
202	2022-08-07 23:21:46.019895	192.0.2.200	192.0.2.1.101	TLSv1.2	100	0xa499 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.1.101	TLSv1.2	96	0xa49a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.1.101	TCP	70	0xa49b (19099)	64	8305 → 58885 [ACK] Seq=22053 Ack=26274 Win=4116 Len=0 TSv
205	2022-08-07 23:21:46.019906	192.0.2.200	192.0.2.1.101	TCP	70	0xa49c (19100)	64	8305 → 58885 [ACK] Seq=22053 Ack=26300 Win=4116 Len=0 TSv
206	2022-08-07 23:21:46.136415	192.0.2.200	192.0.2.1.101	TCP	70	0xb7d3 (47059)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
207	2022-08-07 23:21:46.958148	192.0.2.200	192.0.2.1.100	ICMP	78	0xbdb9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.1.100	ICMP	78	0xbdf2 (48626)	64	Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.1.101	TCP	70	0xa49d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.983236	192.0.2.200	192.0.2.1.101	TLSv1.2	747	0xa49e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.1.100	ICMP	78	0xbbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.1.100	ICMP	78	0xbbea6 (48806)	64	Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.1.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=1448 TS
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.1.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=1448 TS
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.1.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.1.100	ICMP	78	0xbbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.1.101	TCP	70	0xb7d7 (47063)	64	39181 → 8305 [ACK] Seq=69004 Ack=967 Win=1384 Len=0 TSval
218	2022-08-07 23:21:52.030118	192.0.2.200	192.0.2.1.100	ICMP	78	0xbff02 (48988)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.1.100	ICMP	78	0xbff59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.1.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.1.100	TCP	64	0xad35 (44341)	64	22 → 53249 [ACK] Seq=1025 Ack=881 Win=946 Len=0
222	2022-08-07 23:21:53.905480	192.0.2.200	192.0.2.1.101	TLSv1.2	747	0xa49f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.1.100	ICMP	78	0xbff63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.1.101	TCP	70	0xa4a0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.126700	192.0.2.200	192.0.2.1.100	TCPMD	70	authent (40000)	64	Echo (ping) reply id=0x0001, seq=4540/50102, ttl=64

## حشرلما

طقف لخدملا مزح طاقتلا متي، ةرادللا ليصوت ٰههجاو لوحم طاقتلا نيوكت متي امدنع ةرادا ٰههجاول ٰههجومنا طحللا طاقتلا متي ال. قيبطتللا ةرادا ٰههجاونم اهلاسرا متي يتلا قيبطتللا.

ةممملما لودجلما اذه صخلي:

ةممملما	طةقنة طاقتللا	لماع ئيفصت يلخاد	هاجتا	اهيلع ىلوتسملما رورملما ٰكح
طاقتلا نيوكت قيقحتلما او ٰههجاونم يلع ٰهتهص نم ليصوت ٰههجاونم ةرادللا	in_mgmt_uplink1	None	* طقف لخدم ةرادللا ٰههجاونم) نم ٰكبسنلا ىلإ لوجهملالا لالخ يلخادلا	IP ناونع نم ICMP ECHO دودر FTD 192.0.2.200 فيضمملما ىلإ 192.0.2.100  صاخللا IP ناونع نم Sftunnel ىلإ FTD 192.0.2.200 ةرادلاب IP ناونع FMC 192.0.2.101  ةرادلاب صاخللا IP ناونع نم FTD 192.0.2.200 فيضمملما ىلإ 192.0.2.100

\* هاجتللا ئيئانث طاقتللا تايملمع 4200 نمآللا ئيامحللا رادج معدي، 3100 سكع ىلع

جورخل او.

## مزحلا طاقتلا ةيفرضت لماع

اهب متى يتلا ةقيرطلا سفنب يلخادلا لوحمل ا ةمزح طاقتلا ةمزح لماع نيوكت متى لماع نيوكتل ةقباطمل او تنرثي الا عون تارايخ مدخلت سأ . تانايبل ا ىوتسم نيوكت ةيفرضتلا.

نيوكتلا

ةمزح طاقتلا نيوكتل FTD و ا ل ASA (CLI) رم اول ا رطس ةهج او لع تاوطلخلا هذه عارج اب مق ةهج او لع 198.51.100.100 فيضملا نم ICMP تاراطا قباطي حشرم مدخلتساب 1/1 تنرثي ا:

1. مسالا نم ققحت:

```
<#root>
>
show nameif

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

2. ل طاقتلا ةسلج عاشن ا ARP و ICMP:

```
<#root>
>
capture capsw switch interface inside ethernet-type arp

<#root>
> capture capsw switch interface inside match icmp 198.51.100.100
```

CCCحتلا

وي Rush 2054 EtherType ه ةميق . ةيفرضتلا لماع و طاقتلا ا ةسلج مسا نم ققحت Rush يسادس يف:

```
<#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

هذا هو ICMP: قchetla IP 1 و لوكوتورب. يفصنم ققحتلا واه اذه

<#root>

>

show capture caps w detail

Packet Capture info

Name: caps w

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-caps w-ethernet-1-1-0.pcap  
Pcapsize: 0

Filter: caps w-1-1

Packet Capture Filter Info

Name: caps w-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

## نـمـآلـا ةـيـامـحـلـا رـادـجـلـ يـلـخـادـلـا لـوـحـمـلـا طـاقـتـلـا تـافـلـمـ عـيـمـجـتـ

اضـيـأـ نـكـمـيـ، يـلـخـادـلـا لـوـحـمـلـا طـاقـتـلـا تـافـلـمـ عـيـمـجـتـلـ اـسـاـ FTDـ، اـسـاـ FTDـ مـدـخـتـسـأـ  
لـالـخـ نـمـ اـهـيـلـا لـوـصـوـلـا نـكـمـيـ يـتـلـا تـاهـجـوـلـا يـلـاـ CLIـ لـ copyـ رـمـأـلـاـ copyـ لـ CLIـ تـاهـجـوـلـاـ فـلـمـ رـيـدـصـتـ.  
تـاصـيـخـشـتـلـاـ وـأـ تـانـاـيـبـلـاـ وـأـ تـاهـجـاوـ.

FMCـ نـمـ هـلـيـزـنـتـ وـرـيـبـخـلـاـ عـضـوـيـفـ /ngfw/var/commonـ فـلـمـلـاـ خـسـنـ نـكـمـيـ، كـلـذـ نـمـ الـدـبـ.  
فـلـمـلـاـ لـيـزـنـتـ رـايـخـ لـالـخـ نـمـ.

عـاصـعـأـلـاـ تـاهـجـاوـ عـيـمـجـ نـمـ مـزـحـلـاـ طـاقـتـلـاـ تـافـلـمـ عـيـمـجـتـ نـمـضـتـ ذـفـنـمـلـاـ ةـانـقـ تـاهـجـاوـ ةـلـاحـ يـفـ.

ASA

ASAـ CLIـ دـرـبـمـ طـاقـتـلـاـ حـاتـفـمـ يـلـخـادـعـمـجـيـ نـأـ قـوـفـ stepsـ اـذـهـ تـزـجـنـأـ:

1. فـاقـيـاـ طـاقـتـلـاـ:

```
<#root>
asa#
capture capsw switch stop
```

2. فـلـمـ مـسـاـ ظـحـالـوـ طـاقـتـلـاـ ةـسـلـجـ فـاقـيـاـ نـمـ قـقـحـتـ.

```
<#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. دیعب تاچویل ای فلملا ریدصتل CLI copy مدخلس ا:

```

<#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

```

## ماظن Firepower Threat Defense (FTD)

(CLI) رمأوألا رطس ڦه جاو یل ع ڦيلخ ادل لوحمل طاقتلا تا فلم عي مجتل تاو طخل هذه عارجاب مق ناصي خشتلا وأ تان اي بـلا تاهـج او ربـع اـهـيلـلـا نـكـمـيـ يـتـلـا مـداـخـلـا ـيلـا اـهـخـسـنـ وـيـفـ FTDـ:

يـصـيـخـشـتـلـا ـيلـا CLـIـ لـاـقـتـنـاـلـاـ 1ـ.

```

<#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. طاقدل الا فاقيا:

```
<#root>  
firepower#  
capture capi switch stop
```

3. طاقدل الا فلم مسا ظحالو طاقدل الا ةسلج فاقيا نم ققحت:

```
<#root>  
firepower#  
show capture caps w detail  
  
Packet Capture info  
  
Name: caps w  
  
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-caps w-ethernet-1-1-0.pcap  
  
Pcapsize: 139826  
Filter: caps w-1-1
```

```

Packet Capture Filter Info
Name:           caps-w-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 تاهجوىل| فلملا ريدصل رمألا مدخلتسا.

```

<#root>

firepower#
copy flash:/packet-capture/sess-1-caps-w-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-caps-w-ethernet-1-1-0.pcap tftp://198.51.100.10/

Source filename [/packet-capture/sess-1-caps-w-ethernet-1-1-0.pcap]?
Destination filename [sess-1-caps-w-ethernet-1-1-0.pcap]?
Copy in progress...C

139826 bytes copied in 0.532 secs

```

فلملا لىزنـت رايـخ لـالـخ نـم طـاقـتـلـالـا تـافـلـم عـيـمـجـتـلـا هـذـه عـارـجـابـمـقـ:

1. طـاقـتـلـالـا فـاقـيـا:

```
<#root>
>
capture caps w switch stop
```

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

```
<#root>
>
show capture caps w detail
```

Packet Capture info

Name: caps w

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-caps w-ethernet-1-1-0.pcap

Pcapsize: 139826

Filter: caps w-1-1

Packet Capture Filter Info

Name: caps w-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
```

رذجلا عضویل ا لقتنا او ریبخلا عضویل ا لقتنا .3.

```
<#root>
>
expert

admin@firepower:~$ 
sudo su

root@firepower:/home/admin
```

4. یل ا طاقتل ال ا فلم خسنا:

```
<#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. FMC، يف فلملا لیزنـت > ۋـزـجـأـلـا رـتـخـأـ:

## 6. لىزنٰت رقن او، طاقتل الا فلم مسا ريفوتب مق و، FTD رت خا.

يـلـخـادـلـا لـوـحـمـلا ةـمـزـحـ طـاقـتـلـا لـضـفـأـو دـيـدـحـتـو تـادـاشـرا

دوـيـقـلـاو ئـيـجـوـتـلـا ئـادـابـمـلا

- لمع ئـسـلـجـ نـوـكـتـ نـأـ نـكـمـيـ نـكـلـوـ، دـدـعـتـمـ لـوـحـمـ طـاقـتـلـا نـيـوـكـتـ لـمـعـ تـاسـلـجـ مـعـ دـمـتـيـ
- نم رـثـكـأـ وـأـ 2ـ نـيـكـمـتـ ئـلـواـحـمـ نـعـ جـتـنـيـ. ئـرـمـ لـكـ يـفـ ئـطـشـنـ طـقـفـ ئـدـحـاـوـ لـوـحـمـ طـاقـتـلـا
- دـحـلـاـ ئـلـاـ لـوـصـوـلـاـ مـتـ ثـيـحـ، ئـسـلـجـلـاـ نـيـكـمـتـ لـشـفـ: ERROR: "أـطـخـ طـاقـتـلـالـا لـمـعـ تـاسـلـجـ
- ةـطـشـنـلـاـ مـزـحـلـاـ طـاقـتـلـاـ تـاسـلـجـ نـمـ 1ـ يـصـقـأـلـاـ".
- طـشـنـ لـوـحـمـ طـاقـتـلـاـ فـذـخـ نـكـمـيـ الـ.
- تـافـلـمـلـاـ رـيـدـصـتـ مـدـخـتـسـمـلـاـ ئـلـعـ بـجـيـ. قـيـبـطـتـلـاـ ئـلـعـ لـوـحـمـلـاـ تـاطـقـلـ ئـعـارـقـ نـكـمـيـ الـ.
- اهـزـيـمـرـتـ كـفـوـتـالـوـحـمـلـاـ غـيـرـفـتـ لـثـمـ ئـنـيـعـمـ تـانـاـيـبـ ئـوـتـسـمـ طـاقـتـلـاـ تـارـايـخـ مـعـ دـمـتـيـ الـ.
- تـالـوـحـمـلـاـ طـاقـتـلـالـاـ تـالـوـحـمـلـاـ نـمـ اـهـرـيـغـ وـعـبـتـلـاـوـ ئـمـزـحـلـاـ مـقـرـوـ.
- يـفـ تـانـاـيـبـلـاـ تـاهـجـاـوـ ئـلـعـ لـوـحـمـلـاـ طـاقـتـلـاـ نـيـوـكـتـ مـتـيـ، تـاقـاـيـسـلـاـ دـدـعـتـمـ ASAـ ئـلـاحـ يـفـ
- وـ، يـفـ تـاهـجـاـوـلـاـ ئـلـعـ لـوـحـمـلـاـ طـاقـتـلـاـ مـعـ دـمـتـيـ. مـدـخـتـسـمـلـاـ تـاقـاـيـسـ

in\_mgmt\_uplink1 يف طقف قايسلا رادإ.

TAC: مزحلا طاقتلا مادختسا يلإ دنتسملا تاسرامملا لصفاً ۆمىاق يه ھذه

- دويقلاو ۆيەيجوتلا ئابملاب ۆياردىلע نك.
- طاقتلاا ۆيفصت لماع مادختسا.
- حشرم طاقتلا تلکش ام دنع ناونع طبرلا يلع NAT رىثأت رابتغاا يف تعضو.
- ۆميقلانع هفالتخا ۆلاح يف ، راطإلا مجح ددحت يتلا ۆمزحلا لوط ليلىقت وأ ۆدایزب مق.
- ۆطقتلملما مزحلا نم ديازتم ددع رصقألا مجحلا نع جتنى . تياب 1518 ۆيضاارتفالا سكعالاب سكعالاو.
- ۆجاجلاب سح تقوىملا نزخملما مجح طبضب مق.
- درجمب show cap <cap\_name> detail. طاقسإلا دادع دادزي ، تقوىملا نزخملما مجح دح يلإ لوصولما.

## ۆلص تاذ تامولعم

- يـف رـمـاـوـأـلـاـ رـطـسـ ۆـهـجـاـوـنـيـوـكـتـ قـلـدـأـ [Firepower 4100/9300](#)
- نـمـ 3100 نـمـأـلـاـ ۆـيـاـمـحـلـاـ رـادـجـ لـيـغـشـتـ عـدـبـ لـيـلـدـ [Cisco](#)
- رمـاـوـأـعـجـرـمـ [Cisco Firepower 4100/9300 FXOS](#)

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).