

# Configurazione e verifica delle acquisizioni dello switch interno Secure Firewall e Firepower

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica generale dell'architettura del sistema](#)

[Panoramica generale delle operazioni dello switch interno](#)

[Flusso di pacchetti e punti di acquisizione](#)

[Configurazione e verifica su Firepower 4100/9300](#)

[Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta](#)

[Acquisizioni di pacchetti su interfacce backplane](#)

[Acquisizione di pacchetti su porte applicazioni e porte applicazioni](#)

[Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta](#)

[Filtri di acquisizione pacchetti](#)

[Raccolta Dei File Di Acquisizione Dello Switch Interno Firepower 4100/9300](#)

[Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni](#)

[Configurazione e verifica su Secure Firewall 3100](#)

[Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta](#)

[Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta](#)

[Acquisizione pacchetti su interfacce interne](#)

[Filtri di acquisizione pacchetti](#)

[Raccogli file di acquisizione switch interno Secure Firewall 3100](#)

[Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritta la configurazione e la verifica di Firepower e delle acquisizioni dello switch interno Secure Firewall.

## Prerequisiti

### Requisiti

Conoscenze base dei prodotti, analisi delle acquisizioni.

### Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

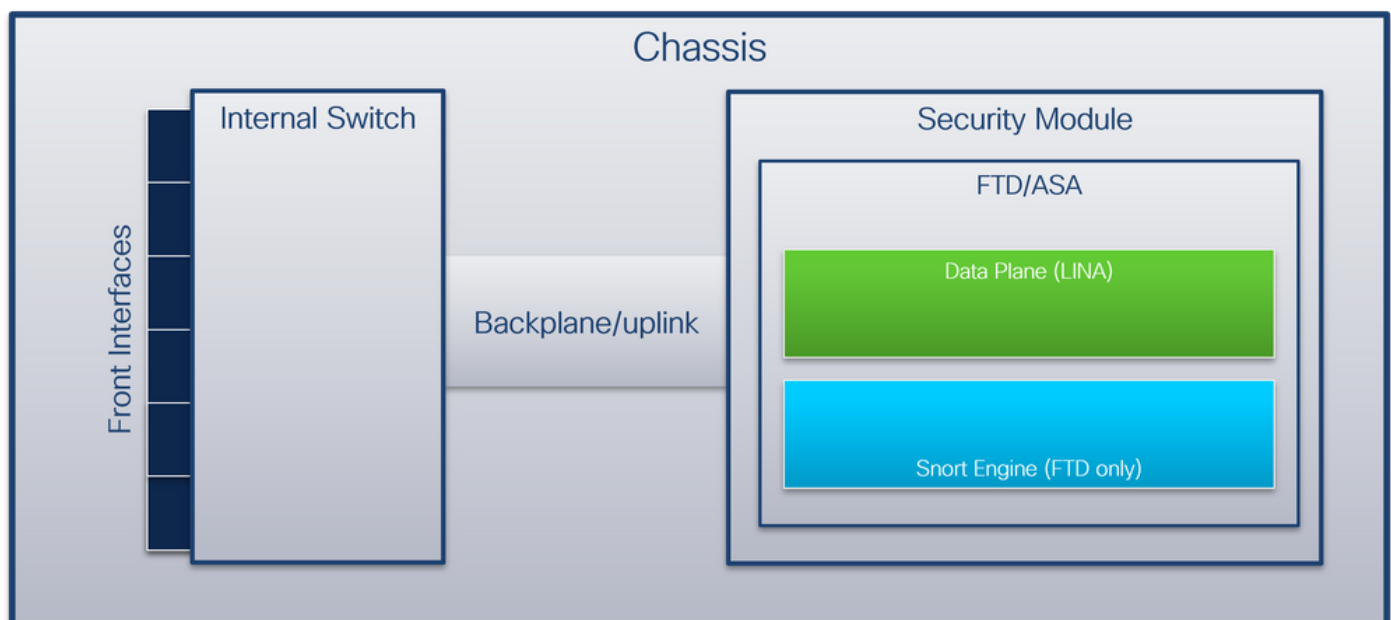
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure eXtensible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defense (FTD) 7.2.0.x
- Cisco Secure Firewall Management Center (FMC) 7.2.0.x
- Cisco Secure Firewall Device Manager (FDM) 7.2.0.x
- Adaptive Security Appliance (ASA) 9.18(1)x
- Adaptive Security Appliance Device Manager (ASDM) 7.18.1.x
- Wireshark 3.6.7 (<https://www.wireshark.org/download.html>)

## Premesse

### Panoramica generale dell'architettura del sistema

Dal punto di vista del flusso dei pacchetti, l'architettura di Firepower 4100/9300 e Secure Firewall 3100 può essere visualizzata come mostrato nella seguente figura:



Lo chassis comprende i seguenti componenti:

- **Switch interno:** inoltra il pacchetto dalla rete all'applicazione e viceversa. Lo switch interno è collegato alle **interfacce anteriori** che risiedono sul modulo di interfaccia incorporato o sui moduli di rete esterni e si connette a dispositivi esterni, ad esempio switch. Esempi di interfacce anteriori sono Ethernet 1/1, Ethernet 2/4 e così via. Il "fronte" non è una definizione tecnica forte. In questo documento viene usato per distinguere le interfacce collegate a

dispositivi esterni dal backplane o dalle interfacce uplink.

- **Backplane o uplink:** interfaccia interna che connette il modulo di sicurezza (SM) allo switch interno. Nella tabella seguente vengono mostrate le interfacce backplane su Firepower 4100/9300 e l'interfaccia uplink su Secure Firewall 3100:

Piattaforma	Numero di moduli di sicurezza supportati	Interfacce backplane/uplink	Interfacce applicaz mappate
Firepower 4100 (eccetto Firepower 4110/4112)	1	SM1: Ethernet 1/9 Ethernet 1/10	Dati interni0/0 Dati interni0/1
Firepower 4110/4112	1	Ethernet 1/9	Dati interni0/0
Firepower 9300	3	SM1: Ethernet 1/9 Ethernet 1/10	Dati interni0/0 Dati interni0/1
		SM2: Ethernet 1/11 Ethernet 1/12	Dati interni0/0 Dati interni0/1
		SM3 Ethernet 1/13 Ethernet 1/14	Dati interni0/0 Dati interni0/1
Secure Firewall 3100	1	SM1: in_data_uplink1	Dati interni0/1

Nel caso di 2 interfacce backplane per modulo, lo switch interno e le applicazioni sui moduli eseguono il bilanciamento del carico del traffico sulle 2 interfacce.

- **Modulo di sicurezza, motore di sicurezza o blade :** il modulo in cui sono installate applicazioni quali FTD o ASA. Firepower 9300 supporta fino a 3 moduli di sicurezza.
- **Interfaccia applicazione mappata:** le applicazioni, ad esempio FTD o ASA, mappano le interfacce backplane o uplink alle interfacce interne. In altre parole, le interfacce backplane o uplink sono visibili come interfacce interne nelle applicazioni.

Utilizzare il comando **show interface detail** per verificare le interfacce interne:

```
> 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 Internal-Data0/3 "ccl_ha_nlp_int_tap", is up, line protocol is up
Control Point Interface States:
Interface number is 5
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

```

## Panoramica generale delle operazioni dello switch interno

### Firepower 4100/9300

Per prendere una decisione di inoltrare, lo switch interno usa un **tag interface VLAN**, o **tag port VLAN**, e un **tag virtual network (VN)**.

Il tag port VLAN viene usato dallo switch interno per identificare un'interfaccia. Lo switch inserisce il tag VLAN della porta in ciascun pacchetto in entrata inviato sulle interfacce anteriori. Il tag VLAN viene configurato automaticamente dal sistema e non può essere modificato manualmente. Il valore del tag può essere controllato nella shell dei comandi **fxos**:

```

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
udld disable
no shutdown

```

Il tag VN viene inoltre inserito dallo switch interno e utilizzato per inoltrare i pacchetti all'applicazione. Viene configurato automaticamente dal sistema e non può essere modificato manualmente.

Il tag VLAN della porta e il tag VN vengono condivisi con l'applicazione. L'applicazione inserisce i rispettivi tag VLAN dell'interfaccia in uscita e i tag VN in ciascun pacchetto. Quando uno switch interno riceve un pacchetto dall'applicazione sulle interfacce del backplane, lo switch legge il tag VLAN dell'interfaccia in uscita e il tag VN, identifica l'applicazione e l'interfaccia in uscita, rimuove



il tag VLAN della porta e il tag VN, quindi inoltra il pacchetto alla rete.

## Secure Firewall 3100

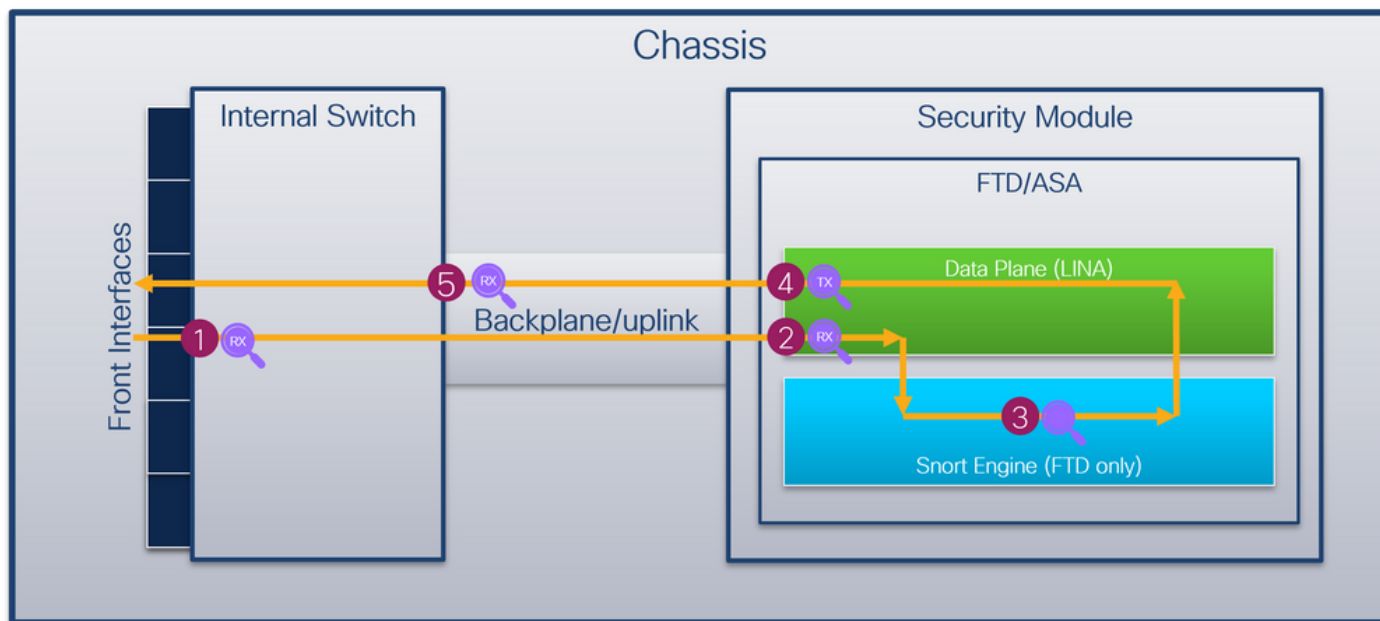
Come in Firepower 4100/9300, il tag della porta VLAN viene usato dallo switch interno per identificare un'interfaccia.

Il tag della porta VLAN è condiviso con l'applicazione. L'applicazione inserisce i rispettivi tag VLAN dell'interfaccia in uscita in ciascun pacchetto. Quando uno switch interno riceve un pacchetto dall'applicazione sull'interfaccia uplink, lo switch legge il tag dell'interfaccia VLAN in uscita, identifica l'interfaccia in uscita, rimuove il tag della porta VLAN e inoltra il pacchetto alla rete.

## Flusso di pacchetti e punti di acquisizione

I firewall Firepower 4100/9300 e Secure Firewall 3100 supportano le acquisizioni di pacchetti sulle interfacce dello switch interno.

La figura mostra i punti di acquisizione del pacchetto lungo il percorso del pacchetto all'interno dello chassis e dell'applicazione:



I punti di acquisizione sono:

1. Punto di acquisizione in entrata interfaccia anteriore switch interno. Un'interfaccia anteriore è un'interfaccia connessa ai dispositivi peer, ad esempio gli switch.
2. Punto di acquisizione in entrata interfaccia piano dati
3. Punto di acquisizione snort
4. Punto di acquisizione uscita interfaccia piano dati
5. Punto di acquisizione in entrata uplink o backplane interno dello switch. Un'interfaccia di backplane o uplink collega lo switch interno all'applicazione.

Lo switch interno supporta solo le acquisizioni dell'interfaccia in entrata. In questo modo, è possibile acquisire solo i pacchetti ricevuti dalla rete o dall'applicazione ASA/FTD. **Le acquisizioni di pacchetti in uscita non sono supportate.**

## Configurazione e verifica Firepower 4100/9300

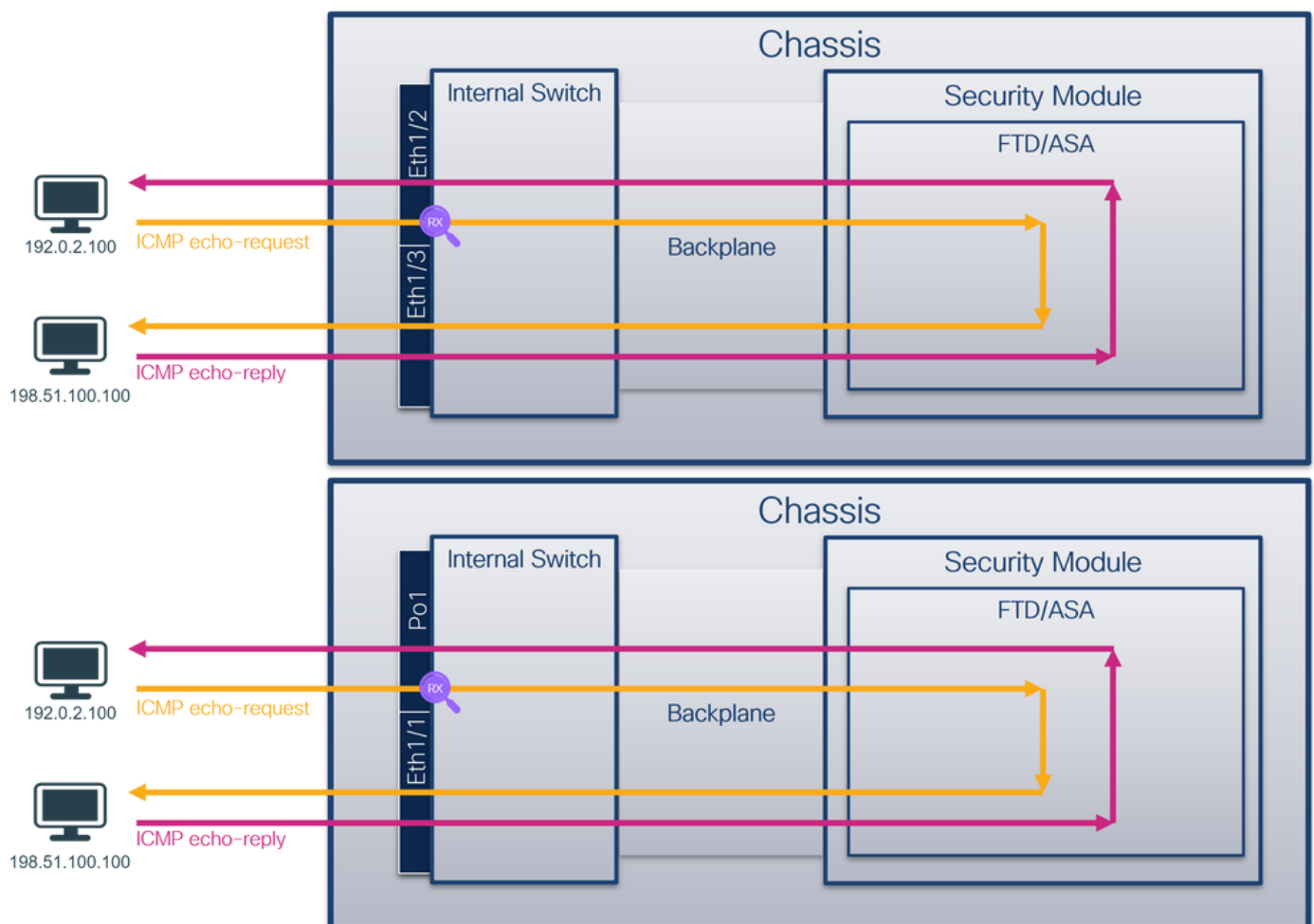
Le acquisizioni dello switch interno Firepower 4100/9300 possono essere configurate in **Strumenti > Packet Capture** su FCM o in **Scope Packet Capture** nella CLI di FXOS. **Per la descrizione delle opzioni di acquisizione dei pacchetti, consultare la guida alla configurazione di Cisco Firepower 4100/9300 FXOS Chassis Manager o la guida alla configurazione della CLI di Cisco Firepower 4100/9300 FXOS, capitolo Risoluzione dei problemi, sezione Acquisizione pacchetti.**

In questi scenari vengono illustrati i casi di utilizzo comuni delle acquisizioni dello switch interno Firepower 4100/9300.

## Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia Ethernet1/2 o Portchannel1. Nel caso di un'interfaccia di canale della porta, assicurarsi di selezionare tutte le interfacce membro fisiche.

### Topologia, flusso dei pacchetti e punti di acquisizione

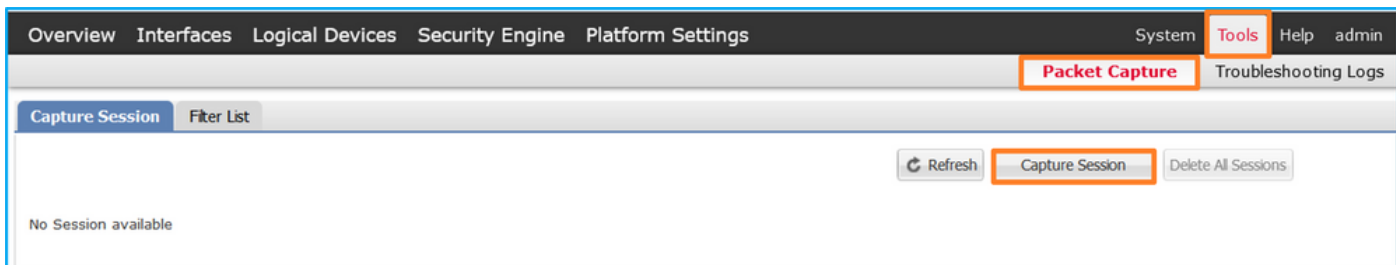


## Configurazione

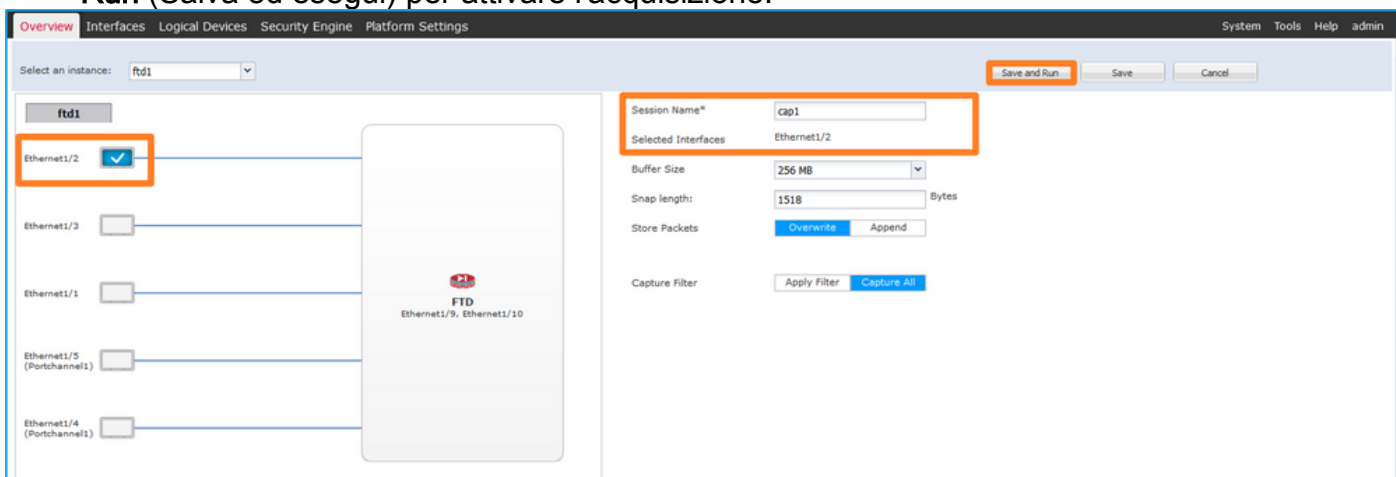
### FCM

Per configurare l'acquisizione di un pacchetto sulle interfacce Ethernet1/2 o Portchannel1, attenersi alla seguente procedura in FCM:

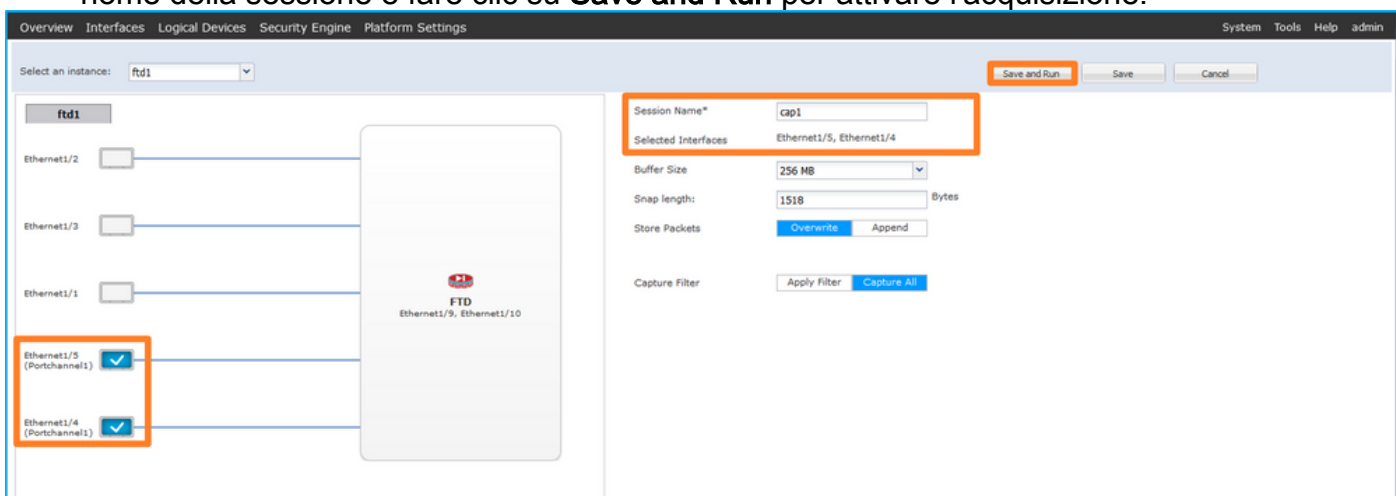
1. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova sessione di acquisizione:



2. Selezionare l'interfaccia **Ethernet1/2**, fornire il nome della sessione e fare clic su **Save and Run** (Salva ed esegui) per attivare l'acquisizione:



3. Nel caso di un'interfaccia di canale della porta, selezionare tutte le interfacce fisiche, fornire il nome della sessione e fare clic su **Save and Run** per attivare l'acquisizione:



## CLI FXOS

Per configurare un'acquisizione pacchetto sulle interfacce Ethernet1/2 o Portchannel1, attenersi alla seguente procedura dalla CLI di FXOS:

1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name  Identifier Slot ID  Admin State Oper State  Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd       ftd1       1           Enabled   Online    7.2.0.82    7.2.0.82
```

Native No Not Applicable None

## 2. Nel caso di un'interfaccia porta-canale, identificare le relative interfacce membro:

```
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. Creare una sessione di acquisizione:

```
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 #
```

Per le interfacce port-channel, viene configurata un'acquisizione separata per ciascuna interfaccia membro:

```
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 #
```

## Verifica

### FCM

Verificare il **nome** dell'interfaccia, verificare che lo **stato operativo** sia attivo e che le **dimensioni del file (in byte)** aumentino:

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

Portchannel1 con interfacce membro Ethernet1/4 ed Ethernet1/5:

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

## CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

```
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
```

Port-channel 1 con interfacce membro Ethernet1/4 ed Ethernet1/5:

```
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**

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione per Ethernet1/2. Selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN **102** aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
4. Lo switch interno inserisce un tag VN aggiuntivo.



No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (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	0x9f2d (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	0x9f88 (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	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	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	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086627	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 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)

```

  1. .... = Direction: From Bridge
  .0. .... = Pointer: vif_id
  ..00 0000 0000 1010 ..... = Destination: 10
  ..... = Looped: No
  .....0. .... = Reserved: 0
  .....00 ..... = 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
  
```

Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
2	2022-07-13 06:23:58.285082858	192.0.2.100	198.51.100.100	ICMP	102	0x90dc (40428)	64	Echo (ping) request id=0x001a, seq=7/1792, ttl=64 (no response found)
3	2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
4	2022-07-13 06:23:59.309193731	192.0.2.100	198.51.100.100	ICMP	102	0x9e0d (40656)	64	Echo (ping) request id=0x001a, seq=8/2048, ttl=64 (no response found)
5	2022-07-13 06:24:00.333054190	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (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	0x9f2d (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	0x9f88 (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	0x9f88 (40840)	64	Echo (ping) request id=0x001a, seq=11/2816, ttl=64 (no response found)
11	2022-07-13 06:24:03.405199041	192.0.2.100	198.51.100.100	ICMP	108	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
12	2022-07-13 06:24:03.405200261	192.0.2.100	198.51.100.100	ICMP	102	0xa077 (41079)	64	Echo (ping) request id=0x001a, seq=12/3072, ttl=64 (no response found)
13	2022-07-13 06:24:04.429155683	192.0.2.100	198.51.100.100	ICMP	108	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
14	2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64	Echo (ping) request id=0x001a, seq=13/3328, ttl=64 (no response found)
15	2022-07-13 06:24:05.453156612	192.0.2.100	198.51.100.100	ICMP	108	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
16	2022-07-13 06:24:05.453158052	192.0.2.100	198.51.100.100	ICMP	102	0xa16a (41322)	64	Echo (ping) request id=0x001a, seq=14/3584, ttl=64 (no response found)
17	2022-07-13 06:24:06.477127687	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	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
20	2022-07-13 06:24:07.501293041	192.0.2.100	198.51.100.100	ICMP	102	0xa1f6 (41462)	64	Echo (ping) request id=0x001a, seq=16/4096, ttl=64 (no response found)
21	2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
22	2022-07-13 06:24:08.525092088	192.0.2.100	198.51.100.100	ICMP	102	0xa257 (41559)	64	Echo (ping) request id=0x001a, seq=17/4352, ttl=64 (no response found)
23	2022-07-13 06:24:09.549236500	192.0.2.100	198.51.100.100	ICMP	108	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
24	2022-07-13 06:24:09.549238564	192.0.2.100	198.51.100.100	ICMP	102	0xa2a9 (41641)	64	Echo (ping) request id=0x001a, seq=18/4608, ttl=64 (no response found)
25	2022-07-13 06:24:10.573110146	192.0.2.100	198.51.100.100	ICMP	108	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
26	2022-07-13 06:24:10.573112504	192.0.2.100	198.51.100.100	ICMP	102	0xa345 (41797)	64	Echo (ping) request id=0x001a, seq=19/4864, ttl=64 (no response found)
27	2022-07-13 06:24:11.597086627	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\_u0\_1, id 0  
 > Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

```

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

Aprire i file di acquisizione per le interfacce membro Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.



2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.
4. Lo switch interno inserisce un tag VN aggiuntivo.

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture\_u0\_3, in Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:25 (a2:76:f2:00:00:25)

**VN-Tag**

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

**802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001**

- 000... .. = 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**

Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richiesta echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture\_u0\_3, in 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)

**802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001**

- 000... .. = Priority: Best Effort (default) (0)
- ...0 ... = DEI: Ineligible
- ... 0011 1110 1001 = ID: 1001
- Type: IPv4 (0x0800)

**Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100**

**Internet Control Message Protocol**

## Spiegazione

Quando si configura un pacchetto da acquisire su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:



- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN.

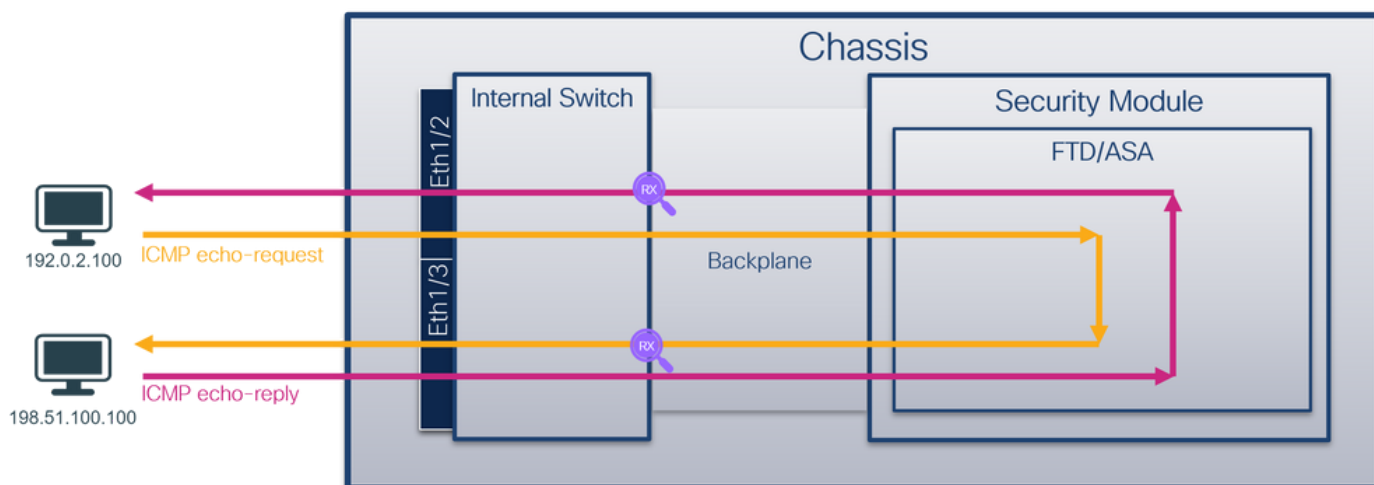
Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/2	Ethernet 1/2	102	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.1
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Portchannel1 con le interfacce membro Ethernet1/4 ed Ethernet1/5	Ethernet1/4 Ethernet1/5	1001	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.1

## Acquisizioni di pacchetti su interfacce backplane

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sulle interfacce backplane.

### Topologia, flusso dei pacchetti e punti di acquisizione

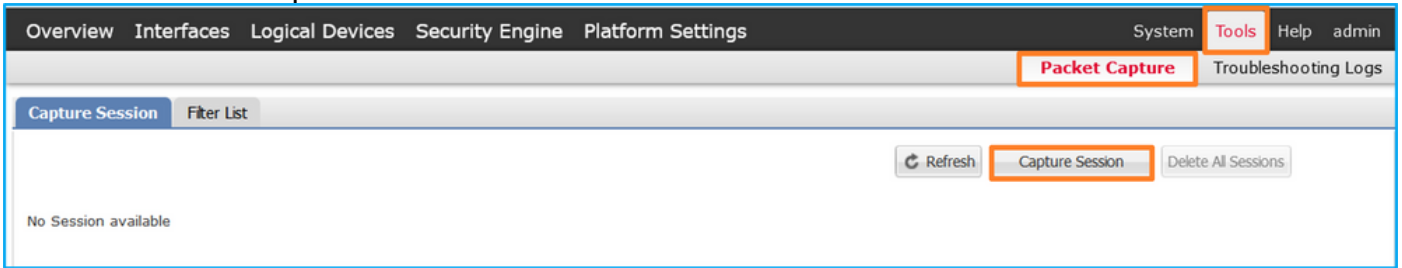


## Configurazione

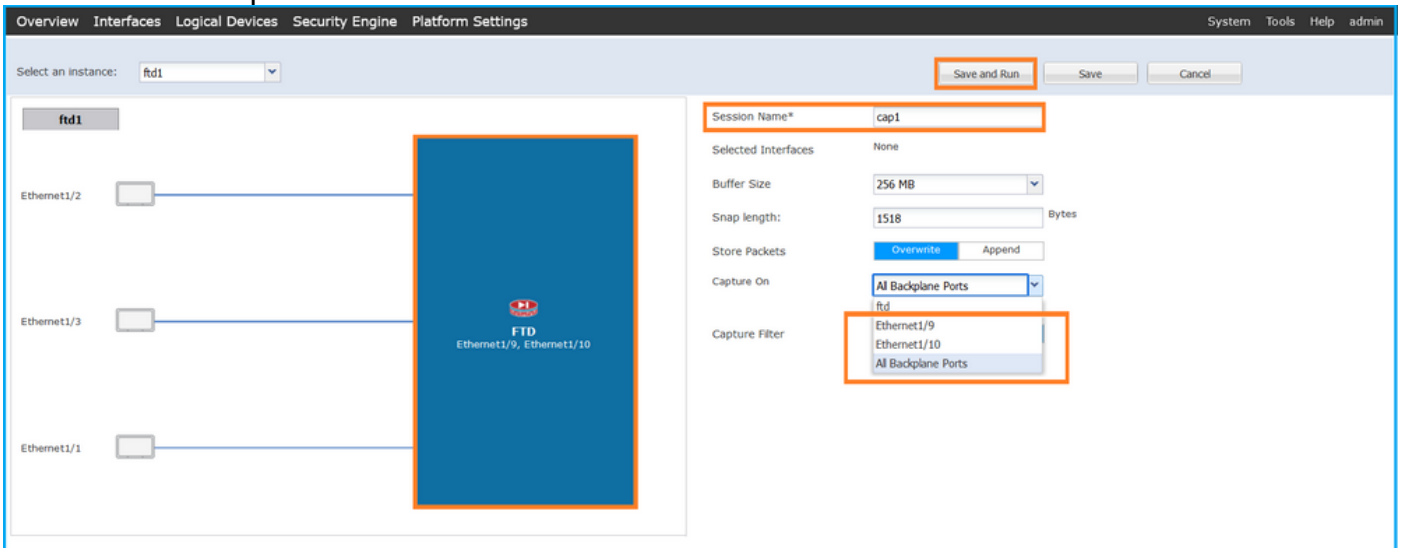
### FCM

Per configurare le acquisizioni dei pacchetti sulle interfacce backplane, eseguire la procedura seguente in FCM:

1. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova sessione di acquisizione:



2. Per acquisire i pacchetti su tutte le interfacce backplane, selezionare l'applicazione, quindi **Tutte le porte backplane** dall'elenco a discesa **Acquisisci su**. In alternativa, selezionate l'interfaccia del backplane specifica. In questo caso, sono disponibili interfacce backplane Ethernet1/9 ed Ethernet1/10. Specificare il **Nome sessione** e fare clic su **Salva ed esegui** per attivare l'acquisizione:



## CLI FXOS

Seguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name  Identifier Slot ID  Admin State Oper State  Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd       ftd1         1           Enabled   Online    7.2.0.82      7.2.0.82
Native   No           Not Applicable  None
```

2. Creare una sessione di acquisizione:

```
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 #

```

## Verifica

## FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:

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

## CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

```

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

### Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300.

### Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. In caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Selezionare il primo e il secondo pacchetto e verificare i punti principali:

1. Ogni pacchetto di richiesta echo ICMP viene acquisito e visualizzato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 103 aggiuntivo che identifica l'interfaccia Ethernet1/3 in uscita.
4. Lo switch interno inserisce un tag VN aggiuntivo.

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	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64 (request in 2)
4	2022-07-14 20:20:36.514119312	198.51.100.100	192.0.2.100	ICMP	108	0xc2c2 (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
5	2022-07-14 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a80 (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	0x5a80 (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	0xc9b (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	0xc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
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 20:20:38.561778310	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 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xc44 (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	0xc44 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677843	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 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (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	0xcd8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (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	0x5b7b (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	0xcd8f (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	0xcd8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
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	0xc36 (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	0xc36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657799898	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 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xc49 (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	0xc49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
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!)

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
  > VN-tag
    0... .. = Direction: To Bridge
    .0... .. = Pointer: vif_id
    ..00 0000 0000 0000 .. = Destination: 0
    .. .. = Looped: No
    .. .. = Reserved: 0
    .. .. = Version: 0
    .. .. 0000 0000 1010 = Source: 10
    Type: 802.1Q Virtual LAN (0x8100)
  > 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
    000... .. = Priority: Best Effort (default) (0)
    ..0... .. = DEI: Ineligible
    .... 0000 0110 0111 = ID: 103
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  > Internet Control Message Protocol
  
```



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	0xccc2c (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	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
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	0xccc9b (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	0xccc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0xccc9b (52379)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0xccc9b (52379)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (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	0xccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	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 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xccc8d (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	0xccc8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (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	0x5b7b (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	0xccc8f (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	0xccc8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
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	0xccc36 (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	0xccc36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709998	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 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xccc49 (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	0xccc49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
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!)

```
Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:2d (58:97:bd:b9:77:2d), Dst: VMware 9d:e7:50 (00:50:56:9d:e7:50)
VN-Tag
0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000... .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 103
000... .. = Priority: Best Effort (default) (0)
... .. = DEI: Ineligible
... 0000 0110 0111 = ID: 103
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
```

Selezionare il terzo e il quarto pacchetto e verificare i punti chiave:

- 1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
- 2. L'intestazione del pacchetto originale è senza il tag VLAN.
- 3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
- 4. Lo switch interno inserisce un tag VN aggiuntivo.

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	0xccc2c (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	0xccc2c (52268)	64	Echo (ping) reply id=0x0001, seq=15/3840, ttl=64
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	0xccc9b (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	0xccc9b (52379)	64	Echo (ping) reply id=0x0001, seq=16/4096, ttl=64
9	2022-07-14 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (no response found!)
10	2022-07-14 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23419)	64	Echo (ping) request id=0x0001, seq=17/4352, ttl=64 (reply in 11)
11	2022-07-14 20:20:38.562048288	198.51.100.100	192.0.2.100	ICMP	108	0xccc4 (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	0xccc4 (52420)	64	Echo (ping) reply id=0x0001, seq=17/4352, ttl=64
13	2022-07-14 20:20:39.585677043	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 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xccc8d (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	0xccc8d (52621)	64	Echo (ping) reply id=0x0001, seq=18/4608, ttl=64
17	2022-07-14 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (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	0x5b7b (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	0xccc8f (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	0xccc8f (52623)	64	Echo (ping) reply id=0x0001, seq=19/4864, ttl=64
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	0xccc36 (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	0xccc36 (52790)	64	Echo (ping) reply id=0x0001, seq=20/5120, ttl=64
25	2022-07-14 20:20:42.657709998	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 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xccc49 (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	0xccc49 (52809)	64	Echo (ping) reply id=0x0001, seq=21/5376, ttl=64
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!)

```
Frame 3: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:b6 (00:50:56:9d:e8:b6)
VN-Tag
0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000... .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. 0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
... .. = 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
```

## Spiegazione

Quando si configura un pacchetto da acquisire su un'interfaccia backplane, lo switch acquisisce simultaneamente ciascun pacchetto due volte. In questo caso, lo switch interno riceve i pacchetti che sono già stati contrassegnati dall'applicazione sul modulo di sicurezza con il tag port VLAN e il tag VN. Il tag VLAN identifica l'interfaccia in uscita usata dallo chassis interno per inoltrare i pacchetti alla rete. Il tag VLAN 103 nei pacchetti di richiesta echo ICMP identifica Ethernet 1/3 come interfaccia di uscita, mentre il tag VLAN 102 nei pacchetti di risposta echo ICMP identifica Ethernet 1/2 come interfaccia di uscita. Lo switch interno rimuove il tag VN e il tag VLAN dell'interfaccia interna prima che i pacchetti vengano inoltrati alla rete.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di VLAN della porta acquisizi one interna nei pacchetti acquisiti	Direzio ne	Traffico acquisito
Configurazione e verifica delle acquisizioni dei pacchetti sulle interfacce backplane	Interfacc e backpla ne 102 103	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100 ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100

## Acquisizione di pacchetti su porte applicazioni e porte applicazioni

Le acquisizioni di pacchetti di porte applicative o applicazioni vengono sempre configurate sulle interfacce backplane e sulle interfacce anteriori se l'utente specifica la direzione di acquisizione dell'applicazione.

Esistono principalmente 2 casi di utilizzo:

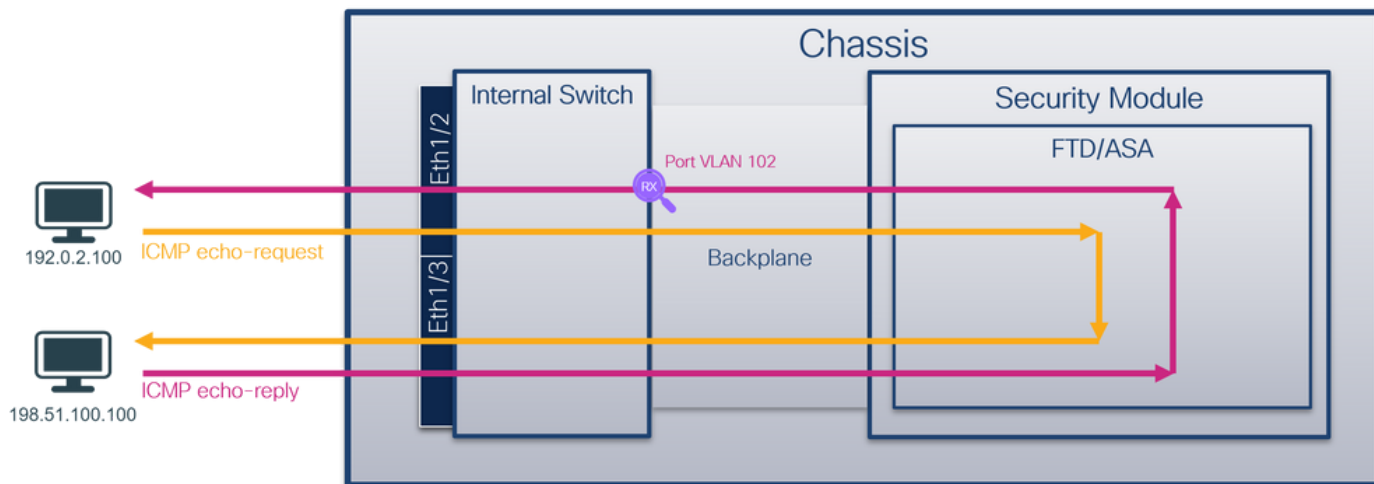
- Configurare le acquisizioni dei pacchetti sulle interfacce backplane per i pacchetti che lasciano un'interfaccia anteriore specifica. Ad esempio, configurare le acquisizioni dei pacchetti sull'interfaccia Ethernet1/9 del backplane per i pacchetti che lasciano l'interfaccia Ethernet1/2.
- Configurare le acquisizioni simultanee dei pacchetti su un'interfaccia anteriore specifica e sulle interfacce del backplane. Ad esempio, configurare l'acquisizione simultanea dei pacchetti sull'interfaccia Ethernet1/2 e sull'interfaccia backplane Ethernet1/9 per i pacchetti che lasciano l'interfaccia Ethernet1/2.

In questa sezione vengono illustrati entrambi i casi di utilizzo.

### Attività 1

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia del backplane. Vengono acquisiti i pacchetti per i quali la porta dell'applicazione Ethernet1/2 è identificata come interfaccia in uscita. In questo caso, vengono acquisite le risposte ICMP.

### Topologia, flusso dei pacchetti e punti di acquisizione

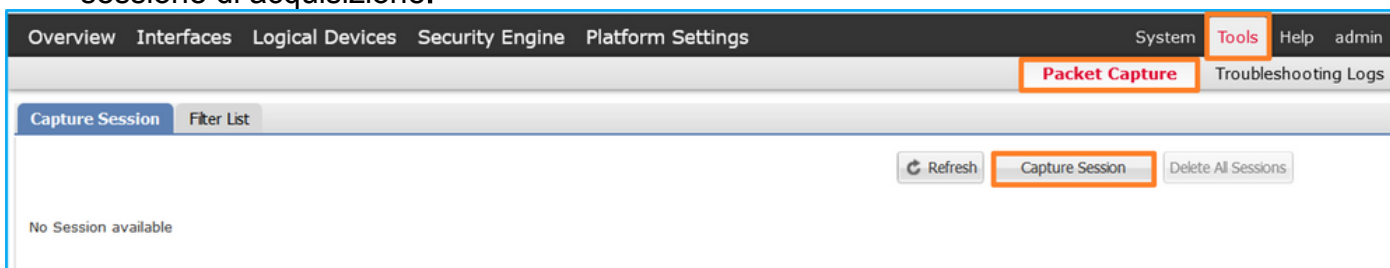


## Configurazione

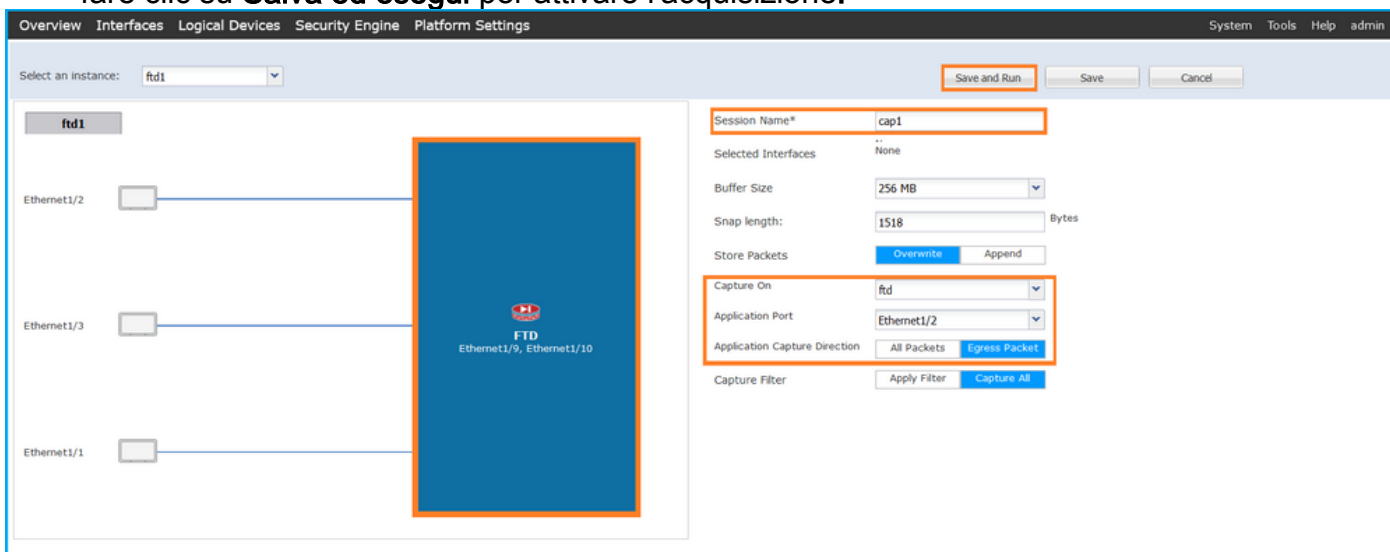
### FCM

Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2 dell'applicazione, attenersi alla procedura descritta di seguito in FCM:

1. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova sessione di acquisizione:



2. Selezionare l'applicazione **Ethernet1/2** nell'elenco a discesa **Porta applicazione** e selezionare **Pacchetto in uscita** in **Direzione di acquisizione applicazione**. Specificare il **Nome sessione** e fare clic su **Salva ed esegui** per attivare l'acquisizione:



### CLI FXOS

Seguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle

interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup Version
Deploy Type  Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd          ftd1      1              Enabled      Online          7.2.0.82       7.2.0.82
Native       No                Not Applicable None
```

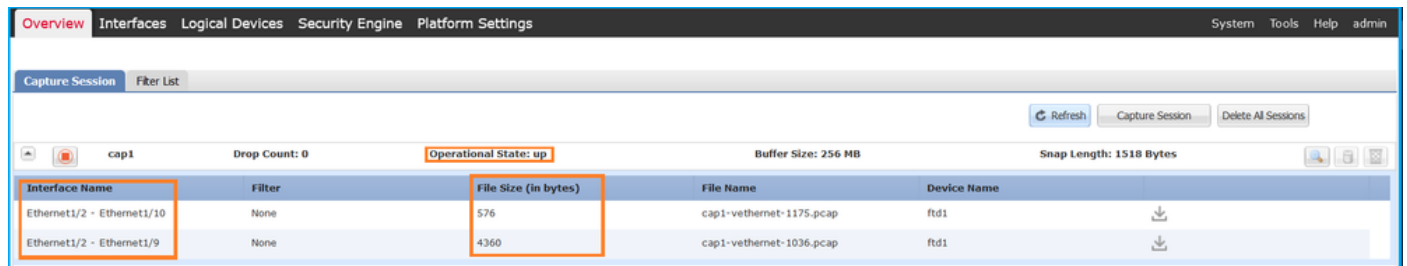
2. Creare una sessione di acquisizione:

```
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 #
```

Verifica

FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:



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

CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

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

Traffic Monitoring Session:

```
Packet Capture Session Name: cap1
Session: 1
Admin State: Enabled
Oper State: Up
Oper State Reason: Active
Config Success: Yes
Config Fail Reason:
Append Flag: Overwrite
Session Mem Usage: 256 MB
```



Session Pcap Snap Len: 1518 Bytes  
Error Code: 0  
Drop Count: 0

Application ports involved in Packet Capture:

**Slot Id: 1**  
**Link Name: 112**  
**Port Name: Ethernet1/2**  
App Name: ftd  
Sub Interface: 0  
**Application Instance Identifier: ftd1**

Application ports resolved to:

**Name: vnic1**  
**Eq Slot Id: 1**  
**Eq Port Id: 9**  
**Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1036.pcap**  
**Pcapsize: 53640 bytes**  
**Vlan: 102**  
Filter:

**Name: vnic2**  
**Eq Slot Id: 1**  
**Eq Port Id: 10**  
**Pcapfile: /workspace/packet-capture/session-1/cap1-vethernet-1175.pcap**  
**Pcapsize: 1824 bytes**  
**Vlan: 102**  
Filter:

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. Nel caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Selezionare il primo e il secondo pacchetto e verificare i punti principali:

1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN **102** aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
4. Lo switch interno inserisce un tag VN aggiuntivo.

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	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

> Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)

VLAN-Tag
0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. = Source: 10
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
...0... .. = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)

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

0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...M...&..
0010	00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00	...b...d...
0040	00 00 00 00 11 12 13 14 15 16 17 18 19 1a 1b	...b...d...
0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b	...l...\$%&'()*+...
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	.../0123 4567

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	0x42f8 (17144)	64	Echo (ping) reply
2	2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64	Echo (ping) reply
3	2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0x4303 (17331)	64	Echo (ping) reply
4	2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64	Echo (ping) reply
5	2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
6	2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64	Echo (ping) reply
7	2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
8	2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64	Echo (ping) reply
9	2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
10	2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64	Echo (ping) reply
11	2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
12	2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64	Echo (ping) reply
13	2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
14	2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64	Echo (ping) reply
15	2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
16	2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64	Echo (ping) reply
17	2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
18	2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64	Echo (ping) reply
19	2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
20	2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64	Echo (ping) reply
21	2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply
22	2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64	Echo (ping) reply

```

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
> Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)

VLAN-Tag
0... .. = Direction: To Bridge
.0... .. = Pointer: vif_id
..00 0000 0000 0000 .. = Destination: 0
... .. = Looped: No
... .. = Reserved: 0
... .. = Version: 0
... .. = Source: 10
Type: 802.1Q Virtual LAN (0x8100)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
000... .. = Priority: Best Effort (default) (0)
...0... .. = DEI: Ineligible
... 0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)

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

0000	00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00	PV...X...M...&..
0010	00 0a 81 00 00 66 08 00 45 00 00 54 42 f8 00 00	...f...E...TB...
0020	40 01 4a b5 c6 33 64 64 c0 00 02 64 00 00 00 04	@J...3dd...d...
0030	00 12 00 01 dd a4 e7 62 00 00 00 e3 0d 09 00	...b...d...
0040	00 00 00 00 11 12 13 14 15 16 17 18 19 1a 1b	...b...d...
0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b	...l...\$%&'()*+...
0060	2c 2d 2e 2f 30 31 32 33 34 35 36 37	.../0123 4567

### Spiegazione

In questo caso, Ethernet 1/2 con tag VLAN 102 è l'interfaccia di uscita per i pacchetti di risposta echo ICMP.

Quando la direzione di acquisizione dell'applicazione è impostata su **Egress** nelle opzioni di acquisizione, i pacchetti con il tag VLAN della porta 102 nell'intestazione Ethernet vengono catturati sulle interfacce del backplane nella direzione in entrata.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica delle acquisizioni sulla porta dell'applicazione e sulla porta Ethernet1/2	Interfacce backplane	102	Solo entrata	ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100

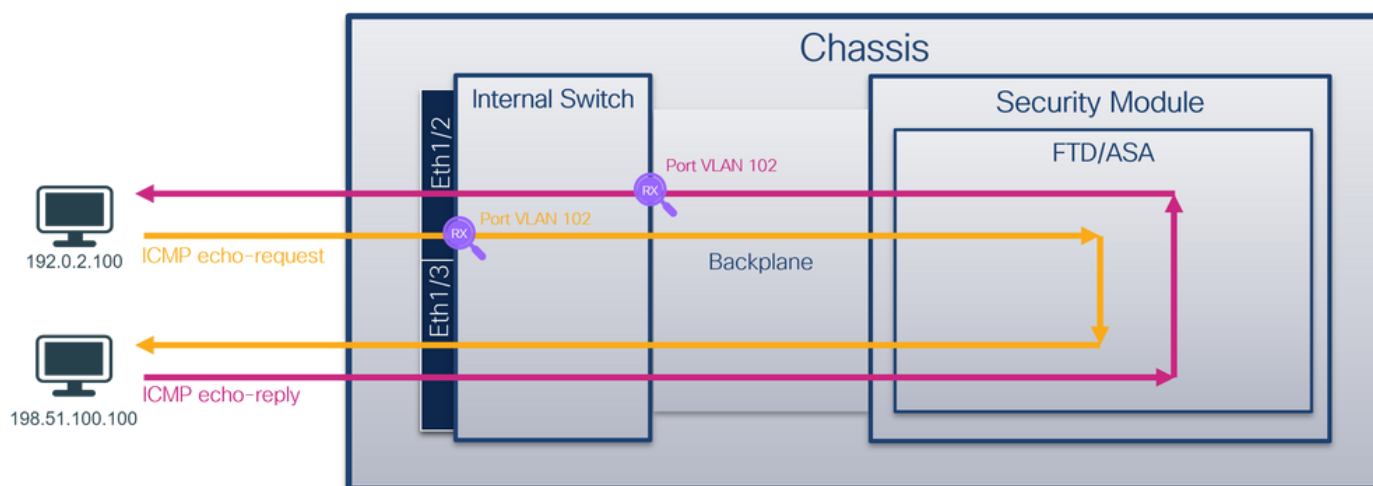
## Attività 2

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia backplane e sull'interfaccia anteriore Ethernet1/2.

Le acquisizioni simultanee dei pacchetti sono configurate su:

- Front interface (interfaccia anteriore) - cattura i pacchetti con la porta VLAN 102 sull'interfaccia Ethernet 1/2. I pacchetti acquisiti sono richieste echo ICMP.
- Interfacce backplane: pacchetti per cui Ethernet1/2 è identificata come interfaccia in uscita o pacchetti con la porta VLAN 102 vengono acquisiti. I pacchetti acquisiti sono risposte echo ICMP.

### Topologia, flusso dei pacchetti e punti di acquisizione

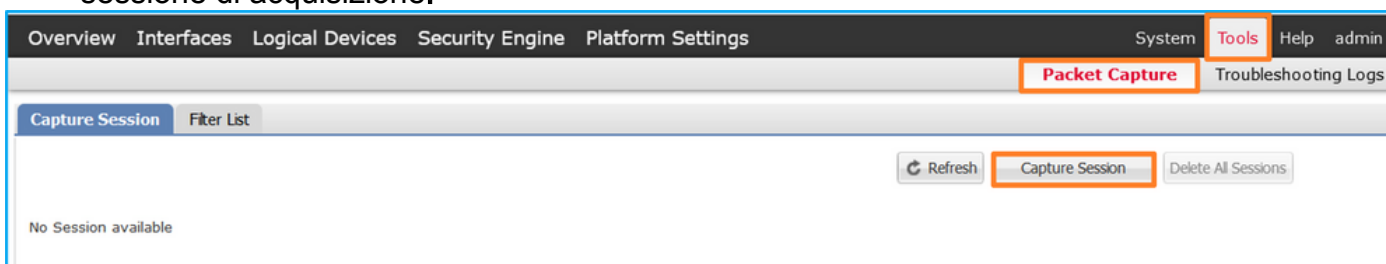


## Configurazione

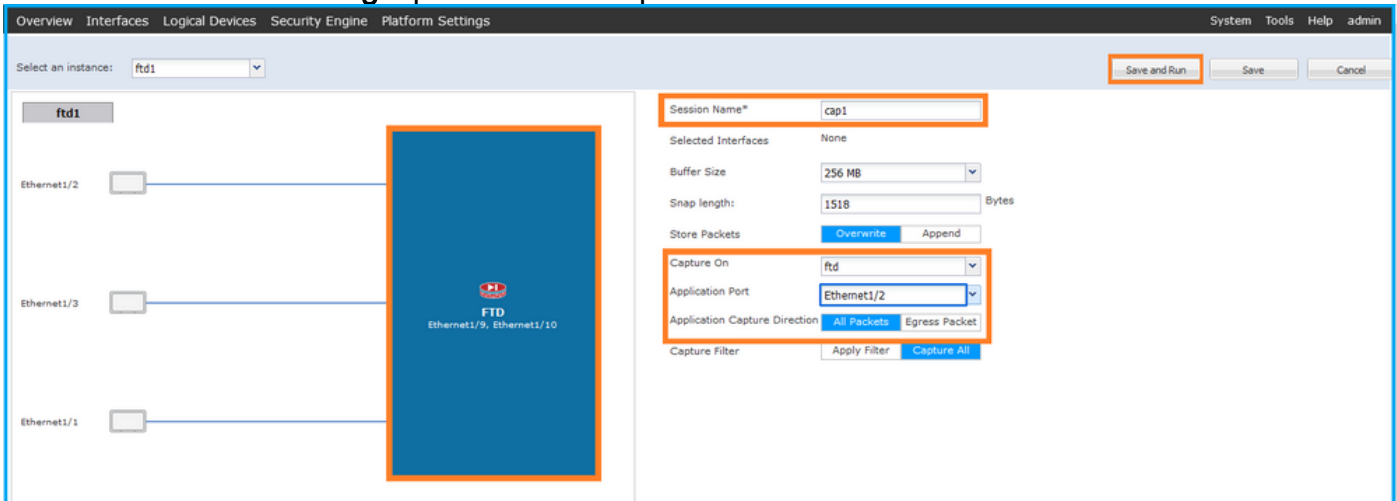
### FCM

Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2 dell'applicazione, attenersi alla procedura descritta di seguito in FCM:

1. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova sessione di acquisizione:



2. Selezionare l'applicazione FTD **Ethernet1/2** nell'elenco a discesa **Porta applicazione** e selezionare **All Packets** in **Application Capture Direction**. Specificare il **Nome sessione** e fare clic su **Salva ed esegui** per attivare l'acquisizione:



## CLI FXOS

Seguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name  Identifier Slot ID  Admin State Oper State  Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State  Cluster Role
-----
ftd      ftd1      1          Enabled   Online    7.2.0.82      7.2.0.82
Native   No                Not Applicable  None
```

2. Creare una sessione di acquisizione:

```
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
```

## Verifica

### FCM

Verificare il **nome dell'interfaccia**, verificare che lo **stato operativo** sia attivo e che le **dimensioni del file (in byte)** aumentino:

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

## CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

```
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:

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione. Nel caso di più interfacce backplane, assicurarsi di aprire tutti i file di acquisizione per ciascuna interfaccia backplane. In questo caso, i pacchetti vengono acquisiti sull'interfaccia Ethernet1/9 del backplane.

Aprire il file di acquisizione per l'interfaccia Ethernet1/2, selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
4. Lo switch interno inserisce un tag VN aggiuntivo.

The screenshot displays a network capture analysis tool interface. The top section shows a list of captured packets, with the first packet selected. The packet details are shown in a tree view on the left, and the raw packet data is shown in hexadecimal and ASCII on the right.

No.	Time	Source	Destination	Protocol	Length	IP ID	P TTL Info	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64 Echo (ping) request	id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request	id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request	id=0x0013, seq=1/256, ttl=64 (no response found)
4	2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) request	id=0x0013, seq=1/256, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64 Echo (ping) request	id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038999	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 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) request	id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) request	id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) request	id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) request	id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) request	id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) request	id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) request	id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) request	id=0x0013, seq=6/1536, ttl=64 (no response found)
15	2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) request	id=0x0013, seq=7/1792, ttl=64 (no response found)
16	2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) request	id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) request	id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) request	id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) request	id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) request	id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.17847175	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 11:33:28.17849075	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
- ..00 0000 0000 1010 .... = Destination: 10
- .....0. .... = Looped: No
- .....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**

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

Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
2	2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found)
3	2022-08-01 11:33:19.071217121	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64	Echo (ping) request id=0x0013, seq=2/512, 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=2/512, ttl=64 (no response found)
5	2022-08-01 11:33:20.072036625	192.0.2.100	198.51.100.100	ICMP	108	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
6	2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found)
7	2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
8	2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64	Echo (ping) request id=0x0013, seq=3/768, ttl=64 (no response found)
9	2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
10	2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64	Echo (ping) request id=0x0013, seq=4/1024, ttl=64 (no response found)
11	2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
12	2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64	Echo (ping) request id=0x0013, seq=5/1280, ttl=64 (no response found)
13	2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64	Echo (ping) request id=0x0013, seq=6/1536, ttl=64 (no response found)
14	2022-08-01 11:33:24.081841396	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	0xc262 (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	0xc262 (49890)	64	Echo (ping) request id=0x0013, seq=7/1792, ttl=64 (no response found)
17	2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
18	2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64	Echo (ping) request id=0x0013, seq=8/2048, ttl=64 (no response found)
19	2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
20	2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64	Echo (ping) request id=0x0013, seq=9/2304, ttl=64 (no response found)
21	2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
22	2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64	Echo (ping) request id=0x0013, seq=10/2560, ttl=64 (no response found)
23	2022-08-01 11:33:29.201804760	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 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
0000 .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
....0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
Internet Control Message Protocol
  
```

Aprire il file di acquisizione per l'interfaccia Ethernet1/9, selezionare il primo e il secondo pacchetto e controllare i punti chiave:

1. Ogni risposta echo ICMP viene acquisita e visualizzata 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia di uscita Ethernet1/2.
4. Lo switch interno inserisce un tag VN aggiuntivo.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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	0x4ffb (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	0x50ba (20652)	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	0x50ba (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	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	0x51c9 (20937)	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	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	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	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x5446 (21574)	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	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=9/2304, ttl=64
19	2022-08-01 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250838708	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 11:33:31.250838971	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

```

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0
Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)
VN-Tag
0000 .... = Direction: To Bridge
...0 .... = Pointer: vif id
....0000 0000 0000 .... = Destination: 0
...0 .... = Logged: No
...0 .... = Reserved: 0
...0 .... = Version: 0
....0000 0000 1010 = Source: 10
Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
0000 .... = Priority: Best Effort (default) (0)
...0 .... = DEI: Ineligible
....0000 0110 0110 = ID: 102
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100
Internet Control Message Protocol
  
```



No.	Time	Source	Destination	Protocol	Length	IP ID	IP 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	0x4f70 (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	0x4ffb (20475)	64	Echo (ping) reply id=0x0013, seq=2/512, ttl=64
5	2022-08-01 11:33:21.073913640	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
6	2022-08-01 11:33:21.073915690	198.51.100.100	192.0.2.100	ICMP	108	0x50ac (20652)	64	Echo (ping) reply id=0x0013, seq=3/768, ttl=64
7	2022-08-01 11:33:22.075239381	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
8	2022-08-01 11:33:22.075241491	198.51.100.100	192.0.2.100	ICMP	108	0x513e (20798)	64	Echo (ping) reply id=0x0013, seq=4/1024, ttl=64
9	2022-08-01 11:33:23.076447152	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
10	2022-08-01 11:33:23.076449303	198.51.100.100	192.0.2.100	ICMP	108	0x51c9 (20937)	64	Echo (ping) reply id=0x0013, seq=5/1280, ttl=64
11	2022-08-01 11:33:24.082407896	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
12	2022-08-01 11:33:24.082410099	198.51.100.100	192.0.2.100	ICMP	108	0x528e (21134)	64	Echo (ping) reply id=0x0013, seq=6/1536, ttl=64
13	2022-08-01 11:33:25.106382424	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
14	2022-08-01 11:33:25.106384549	198.51.100.100	192.0.2.100	ICMP	108	0x52af (21167)	64	Echo (ping) reply id=0x0013, seq=7/1792, ttl=64
15	2022-08-01 11:33:26.130437851	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
16	2022-08-01 11:33:26.130440320	198.51.100.100	192.0.2.100	ICMP	108	0x53a6 (21414)	64	Echo (ping) reply id=0x0013, seq=8/2048, ttl=64
17	2022-08-01 11:33:27.154398212	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 11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
20	2022-08-01 11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64	Echo (ping) reply id=0x0013, seq=10/2560, ttl=64
21	2022-08-01 11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
22	2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21740)	64	Echo (ping) reply id=0x0013, seq=11/2816, ttl=64
23	2022-08-01 11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
24	2022-08-01 11:33:30.226401817	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64	Echo (ping) reply id=0x0013, seq=12/3072, ttl=64
25	2022-08-01 11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
26	2022-08-01 11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64	Echo (ping) reply id=0x0013, seq=13/3328, ttl=64
27	2022-08-01 11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
28	2022-08-01 11:33:32.274418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64	Echo (ping) reply id=0x0013, seq=14/3584, ttl=64
29	2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64	Echo (ping) reply id=0x0013, seq=15/3840, ttl=64

> Frame 2: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture_u0_8, id 0 > Ethernet II, Src: Cisco b9:77:0e (58:97:bd:b9:77:0e), Dst: VMware 9d:e8:be (00:50:56:9d:e8:be)		<pre> 0000  00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00  -PV...X...m...&amp;- 0010  00 0a 81 00 00 66 08 00 45 00 00 54 4f 27 00 00  -.....F...E..TO.. 0020  40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c  -@-&gt;...3dd...d...  0030  00 13 00 01 f2 b9 e7 62 c0 00 00 00 cb 7f 06 00  -.....b..... 0040  00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b  -..... 0050  1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b  -.....l'm \$58'()*+ 0060  2c 2d 2e 2f 30 31 32 33 34 35 36 37             -,-./0123 4567       </pre>
> VN-Tag 0..... = Direction: To Bridge .0..... = Pointer: vif_id ..00 0000 0000 0000..... = Destination: 0 .....0..... = Looped: No .....0..... = Reserved: 0 .....00..... = Version: 0 .....0000 0000 1010..... = Source: 10 Type: 802.1Q Virtual LAN (0x8100)		
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102 000..... = Priority: Best Effort (default) (0) ...0..... = DEI: Ineligible ....0000 0110 0110 = ID: 102 Type: IPv4 (0x0000)		
> Internet Protocol Version 4, Src: 198.51.100.100, Dst: 192.0.2.100 > Internet Control Message Protocol		

## Spiegazione

Se l'opzione **Tutti i pacchetti** nella **direzione di acquisizione** dell'applicazione è selezionata, vengono configurate 2 acquisizioni simultanee di pacchetti relative alla porta dell'applicazione selezionata Ethernet1/2: un'acquisizione sull'interfaccia anteriore Ethernet1/2 e un'acquisizione su interfacce selezionate del backplane.

Quando si configura un pacchetto da acquisire su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN. Nell'esempio, il tag VLAN 102 nei pacchetti di richiesta echo ICMP identifica Ethernet 1/2 come interfaccia in entrata.

Quando si configura un pacchetto da acquisire su un'interfaccia backplane, lo switch acquisisce simultaneamente ciascun pacchetto due volte. Lo switch interno riceve i pacchetti che sono già stati contrassegnati dall'applicazione sul modulo di sicurezza con il tag della porta VLAN e il tag VN. Il tag port VLAN identifica l'interfaccia in uscita usata dallo chassis interno per inoltrare i pacchetti alla rete. Nell'esempio, il tag VLAN 102 nei pacchetti di risposta echo ICMP identifica Ethernet1/2 come interfaccia di uscita.

Lo switch interno rimuove il tag VN e il tag VLAN dell'interfaccia interna prima che i pacchetti vengano inoltrati alla rete.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizion	VLAN della porta interna nei pacchetti	Direzione Traffico acquisito
----------	----------------------	--	------------------------------

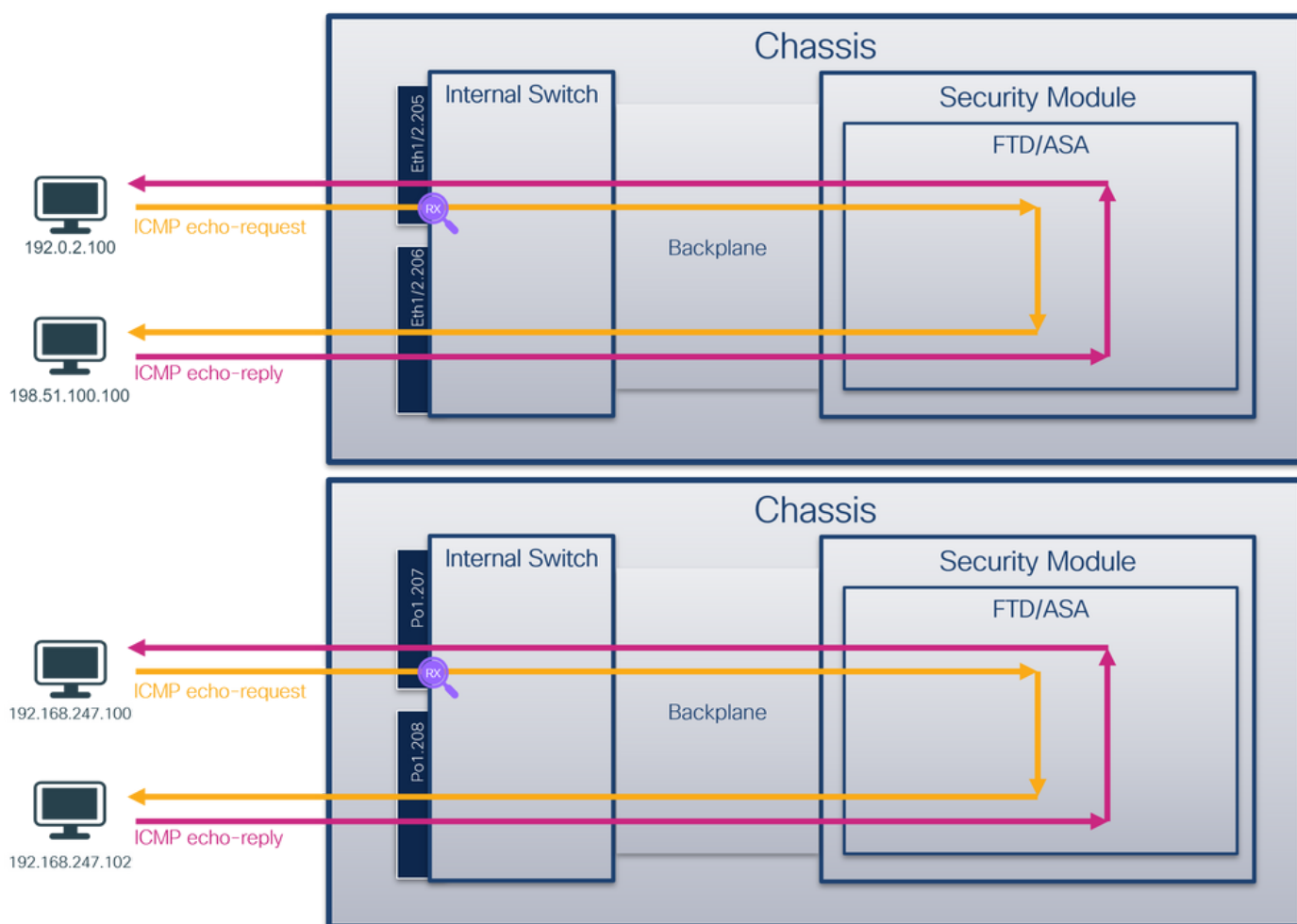


	e	acquisiti		
Configurazione e verifica delle acquisizioni sulla porta dell'applicazione e sulla porta Ethernet1/2	Interfacce backplane	102	Solo entrata	ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.100
	Interfaccia Ethernet1/2	102	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

## Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un canale della porta

Usare FCM e CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia secondaria Ethernet1/2.205 o Portchannel1.207. Le sottointerfacce e le acquisizioni sulle sottointerfacce sono supportate solo per l'applicazione FTD in modalità contenitore. In questo caso, viene configurata l'acquisizione di un pacchetto su Ethernet1/2.205 e Portchannel1.207.

### Topologia, flusso dei pacchetti e punti di acquisizione



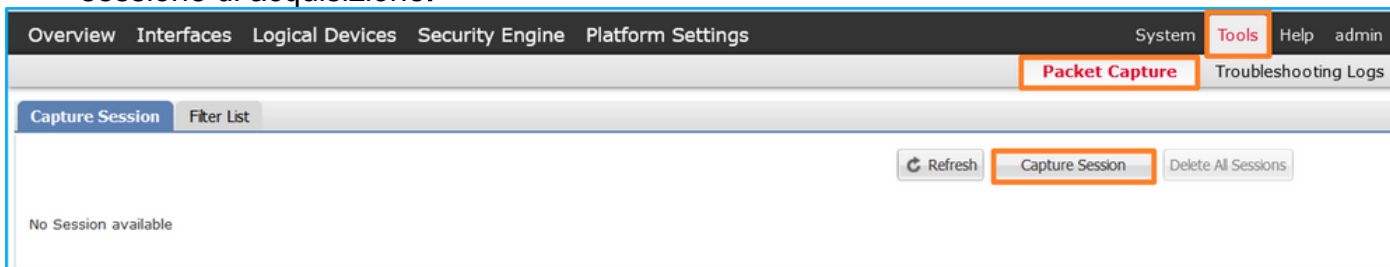
## Configurazione

### FCM

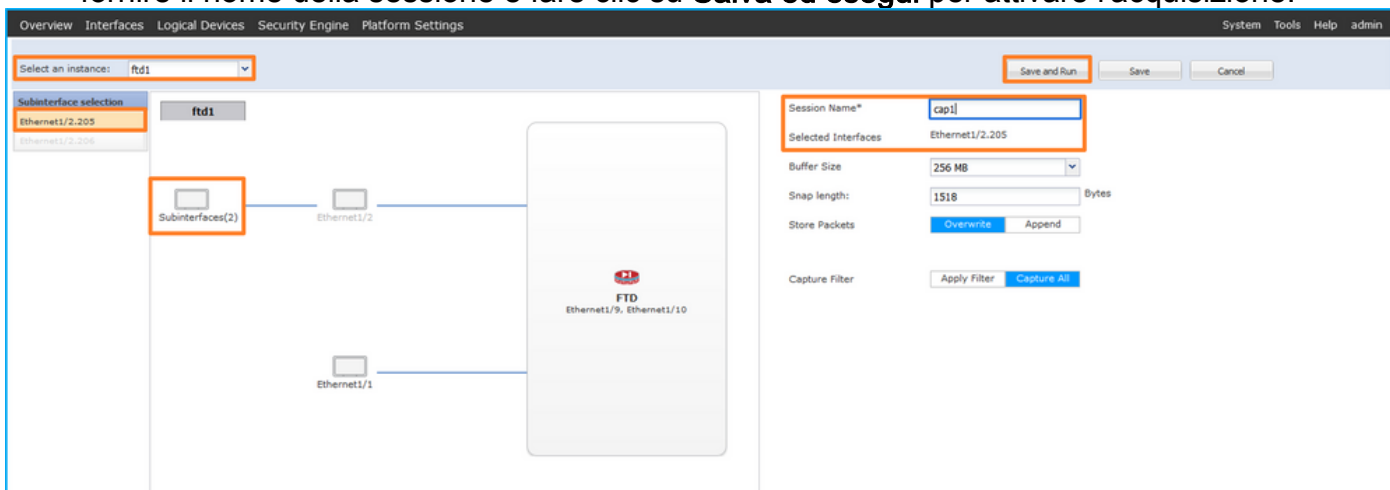
Per configurare l'acquisizione di un pacchetto sull'applicazione FTD e sulla porta Ethernet1/2 dell'applicazione, attenersi alla procedura descritta di seguito in FCM:

1. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova

## sessione di acquisizione:



2. Selezionare l'istanza specifica dell'applicazione ftd1, la sottointerfaccia Ethernet1/2.205, fornire il nome della sessione e fare clic su **Salva ed esegui** per attivare l'acquisizione:



3. Nel caso di una sottointerfaccia port-channel, a causa dell'ID bug Cisco [CSCvq3119](#) le sottointerfacce non sono visibili in FCM. Usare la CLI di FXOS per configurare le acquisizioni sulle sottointerfacce del canale della porta.

## CLI FXOS

Seguire questi passaggi nella CLI di FXOS per configurare un'acquisizione pacchetto sulle sottointerfacce Ethernet1/2.205 e Portchannel1.207:

1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name  Identifier Slot ID   Admin State Oper State   Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
-----
ftd       ftd1       1           Enabled   Online       7.2.0.82     7.2.0.82
Container No      RP20          Not Applicable None
ftd       ftd2       1           Enabled   Online       7.2.0.82     7.2.0.82
Container No      RP20          Not Applicable None
```

2. Nel caso di un'interfaccia porta-canale, identificare le relative interfacce membro:

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

---

### 3. Creare una sessione di acquisizione:

```
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 #
```

Per le sottointerfacce del canale della porta, creare un'acquisizione di pacchetto per ogni interfaccia membro del canale della porta:

```
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 #
```

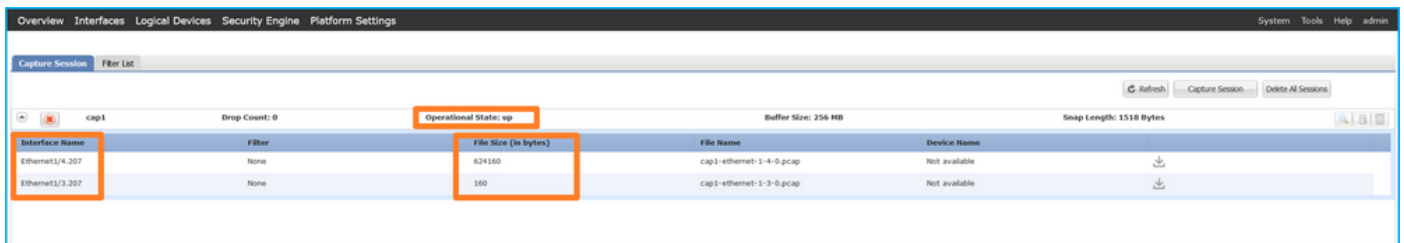
## Verifica

## FCM

Verificare il **nome dell'interfaccia**, verificare che lo **stato operativo** sia attivo e che le **dimensioni del file (in byte)** aumentino:

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/2_205	None	233992	cap1-ethernet-1-2-0-pcap	Rui1

Le acquisizioni della sottointerfaccia del canale della porta configurate sulla CLI di FXOS sono visibili anche su FCM; tuttavia, non possono essere modificati:



## CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

```
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
```

Port-channel 1 con interfacce membro Ethernet1/3 e Ethernet1/4:

```
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

```

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione. Selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale ha il tag VLAN 205.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.
4. Lo switch interno inserisce un tag VN aggiuntivo.

No.	Time	Source	Destination	Protocol	Length	P ID	P TTL	Info
1	2022-08-04 07:21:56.993302182	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f68 (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	0x9f68 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa1de (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found)

```

> Frame 1: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface capture_u0_1, id 0
Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
  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: 102
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  ... 0000 0110 0110 = ID: 102
  Type: 802.1Q Virtual LAN (0x8100)
  802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = DEI: Ineligible
  ... 0000 1100 1101 = ID: 205
  Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
  Internet Control Message Protocol
  0000 a2 76 f2 00 00 1b 00 50 5d 9d e8 be 89 26 80 54 ..v...IPV...&T
  0010 00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54 .....f...E..T
  0020 95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64 ..t@.-8...d3dd
  0030 00 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00 .....s.b...
  0040 d9 9d 00 00 00 00 00 10 11 12 13 14 15 16 17 .....!*$%&'
  0050 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 .....()*+,-./01234567
  0060 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 .....

```



Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale ha il tag VLAN 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL	Info
1	2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
2	2022-08-04 07:21:56.993303597	192.0.2.100	198.51.100.100	ICMP	102	0x9574 (38260)	64	Echo (ping) request id=0x0022, seq=1/256, ttl=64 (no response found!)
3	2022-08-04 07:22:06.214264777	192.0.2.100	198.51.100.100	ICMP	112	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
4	2022-08-04 07:22:06.214267373	192.0.2.100	198.51.100.100	ICMP	102	0x9a81 (39553)	64	Echo (ping) request id=0x0022, seq=10/2560, ttl=64 (no response found!)
5	2022-08-04 07:22:07.215113393	192.0.2.100	198.51.100.100	ICMP	112	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
6	2022-08-04 07:22:07.215115445	192.0.2.100	198.51.100.100	ICMP	102	0x9ac3 (39619)	64	Echo (ping) request id=0x0022, seq=11/2816, ttl=64 (no response found!)
7	2022-08-04 07:22:08.229938577	192.0.2.100	198.51.100.100	ICMP	112	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
8	2022-08-04 07:22:08.229940829	192.0.2.100	198.51.100.100	ICMP	102	0x9b33 (39731)	64	Echo (ping) request id=0x0022, seq=12/3072, ttl=64 (no response found!)
9	2022-08-04 07:22:09.253944601	192.0.2.100	198.51.100.100	ICMP	112	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
10	2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64	Echo (ping) request id=0x0022, seq=13/3328, ttl=64 (no response found!)
11	2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
12	2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64	Echo (ping) request id=0x0022, seq=14/3584, ttl=64 (no response found!)
13	2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
14	2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64	Echo (ping) request id=0x0022, seq=15/3840, ttl=64 (no response found!)
15	2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
16	2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64	Echo (ping) request id=0x0022, seq=16/4096, ttl=64 (no response found!)
17	2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
18	2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64	Echo (ping) request id=0x0022, seq=17/4352, ttl=64 (no response found!)
19	2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
20	2022-08-04 07:22:14.341946249	192.0.2.100	198.51.100.100	ICMP	102	0x9e6a (40554)	64	Echo (ping) request id=0x0022, seq=18/4608, ttl=64 (no response found!)
21	2022-08-04 07:22:15.365941588	192.0.2.100	198.51.100.100	ICMP	112	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
22	2022-08-04 07:22:15.365942566	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0022, seq=19/4864, ttl=64 (no response found!)
23	2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9f68 (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	0x9f68 (40936)	64	Echo (ping) request id=0x0022, seq=20/5120, ttl=64 (no response found!)
25	2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
26	2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64	Echo (ping) request id=0x0022, seq=21/5376, ttl=64 (no response found!)
27	2022-08-04 07:22:18.437954335	192.0.2.100	198.51.100.100	ICMP	112	0xa11e (41246)	64	Echo (ping) request id=0x0022, seq=22/5632, ttl=64 (no response found!)

```
> Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture_u0_1, id 0
  Ethernet II, Src: VMware 9d:1e:8b (00:50:56:9d:e8:8b), Dst: a2:76:f2:00:00:1b (a2:76:f2:00:00:1b)
    802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 205
      0000. .... = Priority: Best Effort (default) (0)
      ...0 .... = DEI: Ineligible
      .... 0000 1100 1101 = ID: 205
      Type: IPv4 (0x0800)
    Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
    Internet Control Message Protocol
```

Aprire i file di acquisizione per Portchannel1.207. Selezionare il primo pacchetto e controllare i punti chiave

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale ha il tag VLAN 207.
3. Lo switch interno inserisce un tag VLAN 1001 aggiuntivo che identifica l'interfaccia in entrata Portchannel1.
4. Lo switch interno inserisce un tag VN aggiuntivo.

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
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
12	2022-08-04 08:18:24.575443611	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
18	2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request
19	2022-08-04 08:18:24.577394238	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
24	2022-08-04 08:18:24.578449999	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
26	2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request

> Frame 1: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface capture\_u0\_3, id 0  
 > Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

```

  0000  a2 76 f2 00 00 1c 00 17 df d6 ec 00 00 89 26 80 3d  -V.....-.-.-.-.-&-
  0010  00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64  -.....-.-.-.-.-E-d
  0020  60 9e 00 00 ff 01 ea dd c0 ab f7 64 c0 ab f7 66  -.....-.-.-.-.-d.-f
  0030  00 00 e5 c8 00 7b 00 00 00 00 02 4d 8c 4a 78  -.....-.-.-.-.-M.-X
  0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.....-.-.-.-.-
  0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.....-.-.-.-.-
  0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.....-.-.-.-.-
  0070  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.....-.-.-.-.-
  
```

1. .... = Direction: From Bridge  
 .0. .... = Pointer: vif\_id  
 ..00 0000 0011 1101 .... = Destination: 61  
 .... = Looped: No  
 .... = Reserved: 0  
 .... = Version: 0  
 .... = Source: 0  
 Type: 802.1Q Virtual LAN (0x8100)  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1001  
 000. .... = Priority: Best Effort (default) (0)  
 ...0 .... = DEI: Ineligible  
 ... 0011 1110 1001 = ID: 1001  
 Type: 802.1Q Virtual LAN (0x8100)  
 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207  
 000. .... = Priority: Best Effort (default) (0)  
 ...0 .... = DEI: Ineligible  
 ... 0000 1100 1111 = ID: 207  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102  
 Internet Control Message Protocol

Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale ha il tag VLAN 207.

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
2	2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255	Echo (ping) request
3	2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255	Echo (ping) request
4	2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255	Echo (ping) request
5	2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255	Echo (ping) request
6	2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255	Echo (ping) request
7	2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255	Echo (ping) request
8	2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255	Echo (ping) request
9	2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255	Echo (ping) request
10	2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255	Echo (ping) request
11	2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255	Echo (ping) request
12	2022-08-04 08:18:24.575443611	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255	Echo (ping) request
13	2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255	Echo (ping) request
14	2022-08-04 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255	Echo (ping) request
15	2022-08-04 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255	Echo (ping) request
16	2022-08-04 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255	Echo (ping) request
17	2022-08-04 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255	Echo (ping) request
18	2022-08-04 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255	Echo (ping) request
19	2022-08-04 08:18:24.577394238	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255	Echo (ping) request
20	2022-08-04 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255	Echo (ping) request
21	2022-08-04 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255	Echo (ping) request
22	2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255	Echo (ping) request
23	2022-08-04 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255	Echo (ping) request
24	2022-08-04 08:18:24.578449999	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255	Echo (ping) request
25	2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255	Echo (ping) request
26	2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255	Echo (ping) request
27	2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255	Echo (ping) request

> Frame 2: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface capture\_u0\_3, id 0  
 > Ethernet II, Src: Cisco d6:ec:00 (00:17:df:d6:ec:00), Dst: a2:76:f2:00:00:1c (a2:76:f2:00:00:1c)

```

  0000  a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf  -V.....-.-.-.-.-
  0010  f7 64 c0 ab f7 66 08 00 e5 c8 00 7b 00 00 00 00  -.-.-.-.-E-d
  0020  00 02 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-d.-f
  0030  00 02 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-M.-X
  0040  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-
  0050  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-
  0060  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-
  0070  ab cd ab cd ab cd ab cd ab cd ab cd ab cd ab cd  -.-.-.-.-
  
```

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 207  
 000. .... = Priority: Best Effort (default) (0)  
 ...0 .... = DEI: Ineligible  
 ... 0000 1100 1111 = ID: 207  
 Type: IPv4 (0x0800)  
 Internet Protocol Version 4, Src: 192.168.247.100, Dst: 192.168.247.102  
 Internet Control Message Protocol

## Spiegazione

Quando si configura un pacchetto da acquisire su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascuno pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN. Inoltre, nel caso delle sottointerfacce, nei file di acquisizione il pacchetto ogni secondo non contiene il tag port VLAN.

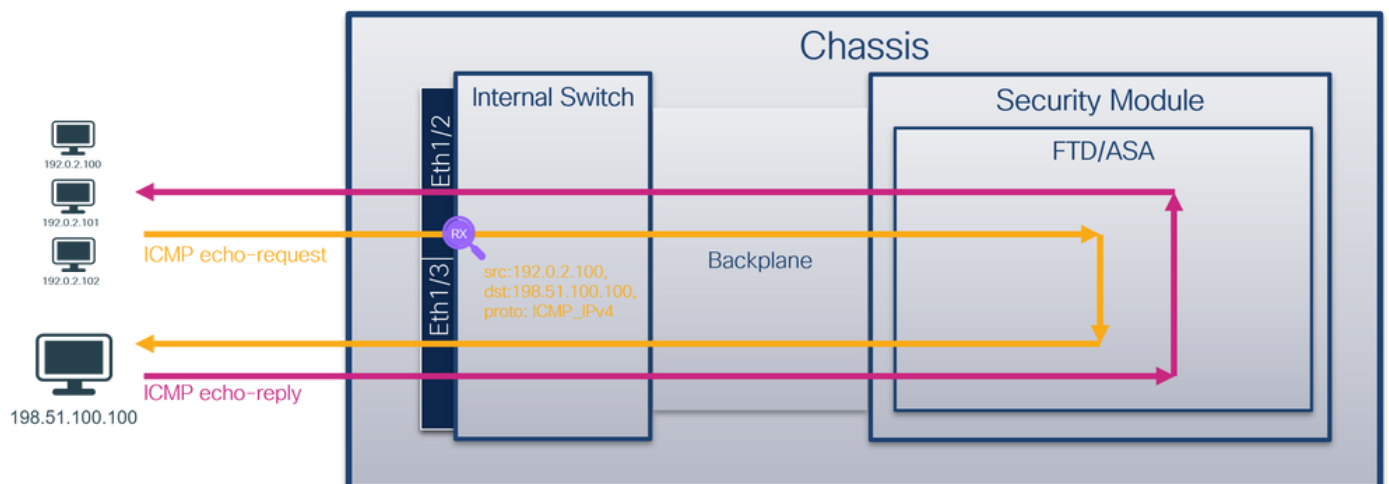
Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	VLAN della porta interna nei pacchetti acquisiti	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/2.205	Ethernet 1/2.205	102	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia secondaria di Portchannel1 con le interfacce membro Ethernet1/3 ed Ethernet1/4	Ethernet 1/3 Ethernet 1/4	1001	Solo entrata	Richieste echo ICMP da 192.168.207.100 all'host 192.168.207.102

## Filtri di acquisizione pacchetti

Usare FCM e CLI per configurare e verificare un'acquisizione pacchetto sull'interfaccia Ethernet1/2 con un filtro.

### Topologia, flusso dei pacchetti e punti di acquisizione



## Configurazione

### FCM

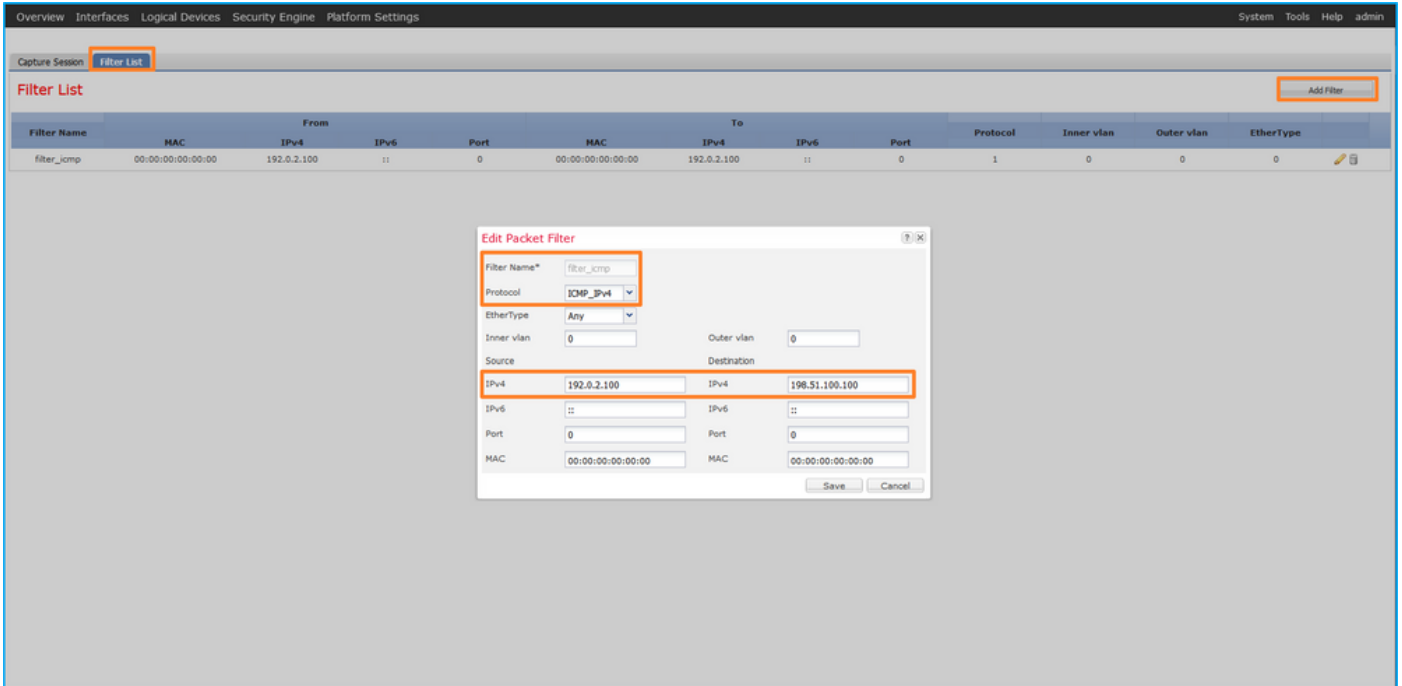
Seguire questa procedura su FCM per configurare un filtro di acquisizione per i pacchetti di richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100 e applicarlo all'acquisizione dei pacchetti sull'interfaccia Ethernet1/2:

1. Utilizzare **Strumenti > Acquisizione pacchetti > Elenco filtri > Aggiungi filtro** per creare un

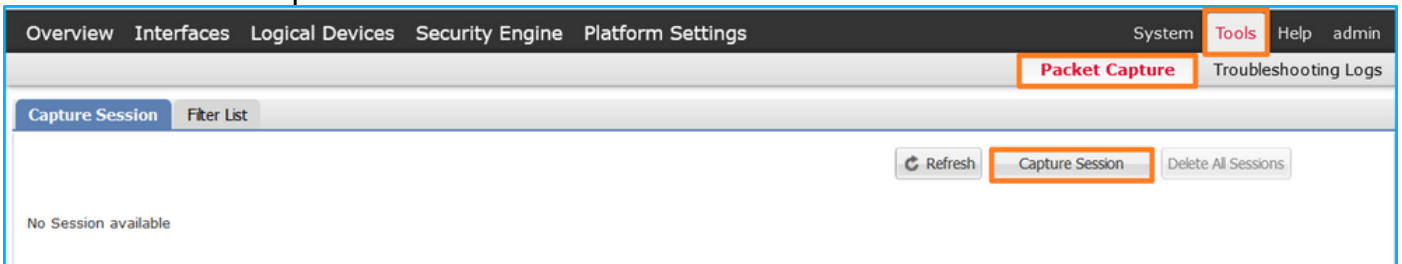


filtro di acquisizione.

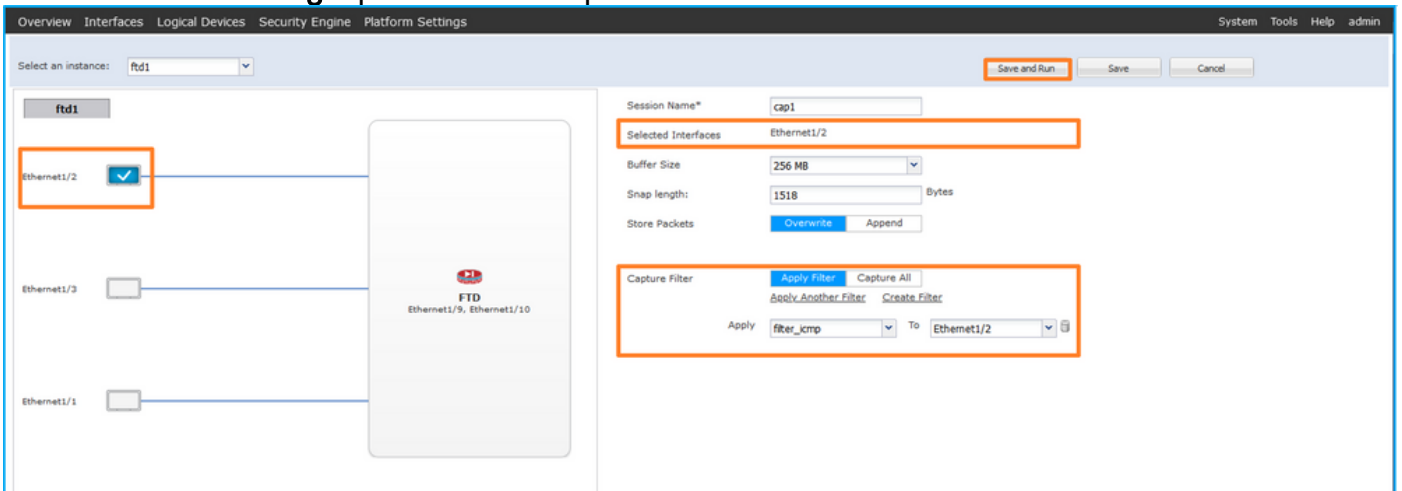
2. Specificare il nome del filtro, il protocollo, l'IPv4 di origine e quello di destinazione, quindi fare clic su **Salva**:



3. Utilizzare **Strumenti > Acquisizione pacchetti > Acquisisci sessione** per creare una nuova sessione di acquisizione:



4. Selezionare Ethernet1/2, fornire il **Nome sessione**, applicare il filtro di acquisizione e fare clic su **Salva ed esegui** per attivare l'acquisizione:



## CLI FXOS

Seguire questi passaggi sulla CLI di FXOS per configurare le acquisizioni dei pacchetti sulle interfacce backplane:

### 1. Identificare il tipo di applicazione e l'identificatore:

```
firepower# scope ssa
firepower /ssa# show app-instance
App Name      Identifier Slot ID      Admin State Oper State      Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
-----
ftd           ftd1         1             Enabled      Online          7.2.0.82       7.2.0.82
Native       No           Not Applicable None
```

2. Identificare il numero del protocollo IP in <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>. In questo caso, il numero di protocollo ICMP è 1.

### 3. Creare una sessione di acquisizione:

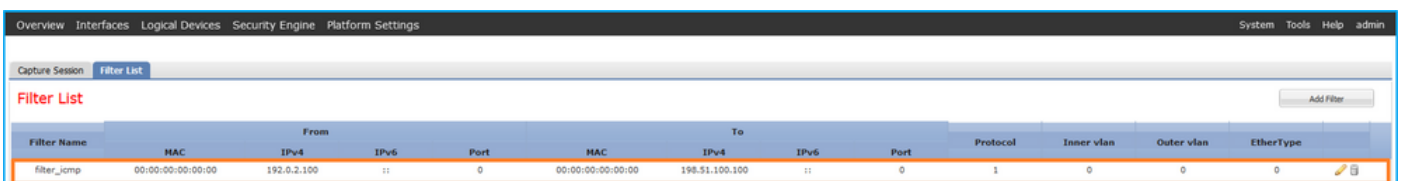
2.

```
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 #
```

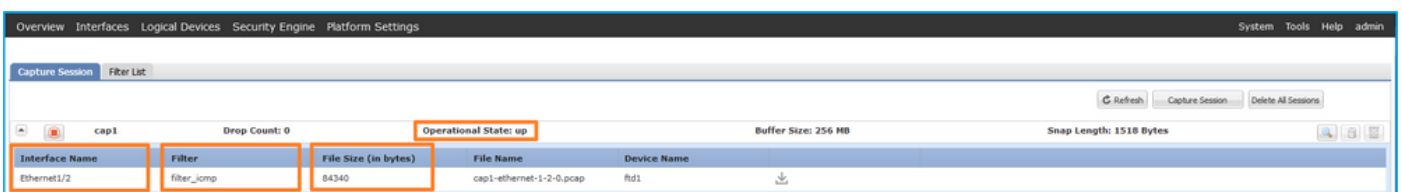
### Verifica

#### FCM

Verificare il nome dell'interfaccia, verificare che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino:



Verificare il nome dell'interfaccia, il filtro, accertarsi che lo stato operativo sia attivo e che le dimensioni del file (in byte) aumentino in Strumenti > Acquisizione pacchetti > Sessione di acquisizione:



### CLI FXOS

Verificare i dettagli di acquisizione nell'ambito packet-capture:

```
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
```

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Firepower 4100/9300**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire il file di acquisizione. Selezionare il primo pacchetto e controllare i punti chiave

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN **102** aggiuntivo che identifica l'interfaccia in entrata

## Ethernet 1/2.

### 4. Lo switch interno inserisce un tag VN aggiuntivo.

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 15:47:01.747163783	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

Frame 1: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface capture\_u0\_1, i  
> 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 1010 .. = Destination: 10
- .....0..... = Looped: No
- .....0..... = Reserved: 0
- .....000..... = 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

Selezionare il secondo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP. Ogni pacchetto viene acquisito e mostrato 2 volte.
2. L'intestazione del pacchetto originale è senza il tag VLAN.
3. Lo switch interno inserisce un tag VLAN 102 aggiuntivo che identifica l'interfaccia in entrata Ethernet 1/2.

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 15:47:01.747163783	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

Frame 2: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface capture\_u0\_1, i  
> Ethernet II, Src: VMware 9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco b9:77:0e (58:97:bd:b9:77:0e)

▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102

- 000. .... = Priority: Best Effort (default) (0)
- ...0 .. = DEI: Ineligible
- ... 0000 0110 0110 = ID: 102
- Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100

> Internet Control Message Protocol

## Spiegazione

Quando si configura un pacchetto da acquisire su un'interfaccia anteriore, lo switch acquisisce simultaneamente ciascun pacchetto due volte:

- Dopo l'inserimento del tag VLAN della porta.
- Dopo l'inserimento del tag VN.

Nell'ordine delle operazioni, il tag VN viene inserito in una fase successiva all'inserimento del tag VLAN della porta. Tuttavia, nel file di acquisizione, il pacchetto con il tag VN viene visualizzato prima del pacchetto con il tag port VLAN.

Quando si applica un filtro di acquisizione, vengono acquisiti solo i pacchetti che corrispondono al filtro nella direzione in entrata.

Nella tabella seguente viene riepilogata l'attività:

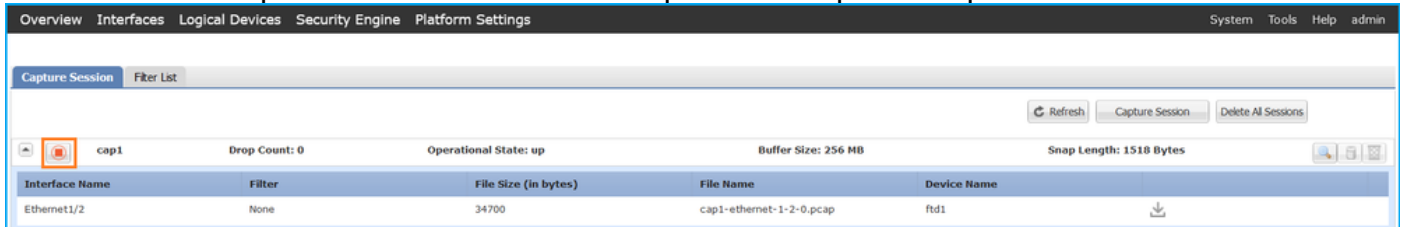
Attività	Punto di VLAN della porta acquisizione interna nei pacchetti acquisiti	Direzione	Filtro utente	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto con un filtro sull'interfaccia anteriore Ethernet1/2	Ethernet 1/2	102	Solo entrata	Protocollo: ICMP Fonte:192.0.2.100 Destinazione: 198.51.100.100 Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

## Raccolta Dei File Di Acquisizione Dello Switch Interno Firepower 4100/9300

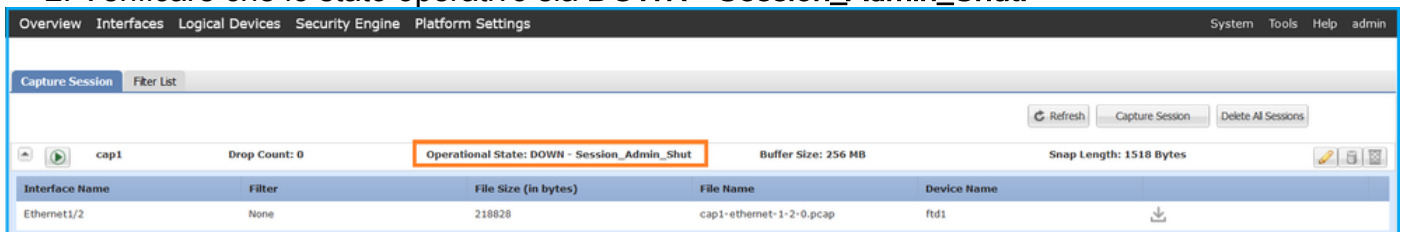
### FCM

Per raccogliere i file di acquisizione dello switch interno, eseguire la procedura seguente in FCM:

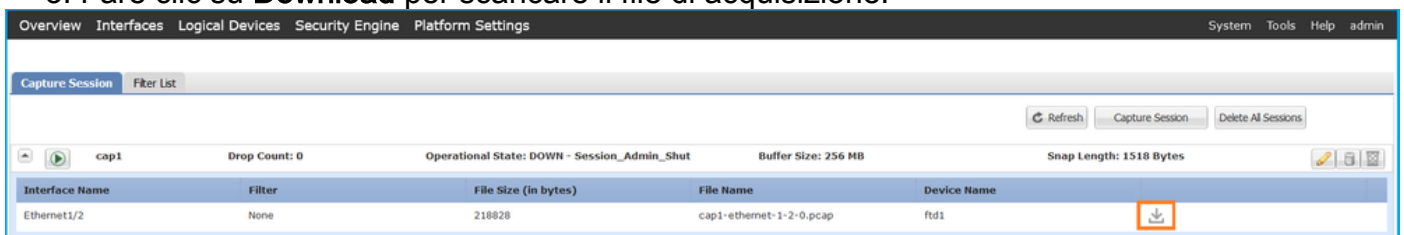
1. Fare clic sul pulsante **Disabilita sessione** per interrompere l'acquisizione attiva:



2. Verificare che lo stato operativo sia **DOWN - Session\_Admin\_Shut**:



3. Fare clic su **Download** per scaricare il file di acquisizione:





Nel caso di interfacce porta-canale, ripetere questo passaggio per ciascuna interfaccia membro.

## CLI FXOS

Per raccogliere i file di acquisizione, attenersi alla seguente procedura nella CLI di FXOS:

### 1. Arrestare l'acquisizione attiva:

```
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: ftdl
Application Name: ftd
```

### 2. Caricare il file di acquisizione dall'ambito del comando local-mgmt:

```
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:
```

Nel caso delle interfacce port-channel, copiare il file di acquisizione per ciascuna interfaccia membro.

## Linee guida, limitazioni e best practice per Switch interno Acquisizione pacchetti

Per le linee guida e i limiti relativi all'acquisizione degli switch interni Firepower 4100/9300, fare riferimento alla *guida alla configurazione di Cisco Firepower 4100/9300 FXOS Chassis Manager* o alla *guida alla configurazione della CLI di Cisco Firepower 4100/9300 FXOS*, capitolo **Risoluzione dei problemi**, sezione **Packet Capture**.

Questo è l'elenco delle best practice basate sull'uso della cattura di pacchetti nei casi TAC:

- Stai attento alle linee guida e ai limiti.
- Acquisire pacchetti su tutte le interfacce membro del canale della porta e analizzare tutti i file di acquisizione.
- Utilizzare i filtri di acquisizione.
- Considerare l'impatto di NAT sugli indirizzi IP dei pacchetti quando viene configurato un filtro di acquisizione.
- Aumentate o diminuite la **Lunghezza snap** che specifica le dimensioni del fotogramma nel caso in cui differisca dal valore predefinito di 1518 byte. Dimensioni inferiori determinano un numero maggiore di pacchetti acquisiti e viceversa.
- Regolare le **dimensioni del buffer** in base alle esigenze.
- Tenere presente il **conteggio di perdita** sulla CLI di FCM o FXOS. Una volta raggiunto il limite delle dimensioni del buffer, il contatore di rilascio aumenta.
- Usare il filtro **!vntag** su Wireshark per visualizzare solo i pacchetti senza tag VN. Questa opzione permette di nascondere i pacchetti con tag VN nei file di acquisizione dei pacchetti dell'interfaccia anteriore.
- Utilizzare il filtro **frame.number&1** su Wireshark per visualizzare solo i frame dispari. Ciò è utile per nascondere i pacchetti duplicati nei file di acquisizione dei pacchetti dell'interfaccia del backplane.
- Nel caso di protocolli come TCP, Wireshark applica per impostazione predefinita regole di colorizzazione che visualizzano pacchetti con condizioni specifiche in colori diversi. Nel caso di acquisizioni interne dello switch causate da pacchetti duplicati nei file di acquisizione, il pacchetto può essere colorato e contrassegnato in modo falso positivo. Se si analizzano i file di acquisizione dei pacchetti e si applica un filtro, esportare i pacchetti visualizzati in un nuovo file e aprire il nuovo file.

## Configurazione e verifica Secure Firewall 3100

A differenza di Firepower 4100/9300, le acquisizioni dello switch interno su Secure Firewall 3100 vengono configurate sull'interfaccia della riga di comando dell'applicazione tramite il comando **capture <name> switch**, dove l'opzione **switch** specifica che le acquisizioni sono configurate sullo switch interno.

Questo è il comando **capture** con l'opzione **switch**:

```
> 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>

```

Di seguito sono riportati i passi generali per la configurazione dell'acquisizione dei pacchetti:

### 1. Specificare un'interfaccia in entrata:

La configurazione di acquisizione dello switch accetta il **nome dell'interfaccia** in entrata, **se presente**. L'utente può specificare i nomi delle interfacce dati, l'uplink interno o le interfacce di gestione:

```
> capture capsw switch interface ?
```

```
Available interfaces to listen:
```

```

in_data_uplink1  Capture packets on internal data uplink1 interface
in_mgmt_uplink1  Capture packets on internal mgmt uplink1 interface
inside          Name of interface Ethernet1/1.205

```

```
management      Name of interface Management1/1
```

### 2. Specificare EtherType del frame Ethernet. Il valore predefinito di EtherType è IP. I valori dell'opzione **ethernet-type** specificano EtherType:

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

```

802.1Q
<0-65535>  Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
sgt
vlan

```

### 3. Specificare le condizioni di corrispondenza. L'opzione di acquisizione **corrispondenza** specifica i criteri di corrispondenza:

```
> 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
pstp
sctp
snp
spi      SPI value
tcp
udp
<cr>
```

4. Specificare altri parametri facoltativi, ad esempio le dimensioni del buffer, la lunghezza del pacchetto e così via.
5. Abilitare l'acquisizione. Il comando **no capture <name> switch stop** attiva l'acquisizione:

```
> capture capsw switch interface inside match ip
>no capture capsw switch stop
```

6. Verificare i dettagli di acquisizione:

- Lo stato amministrativo è **abilitato** e lo stato operativo è **attivo** e attivo.
- Le dimensioni del file di acquisizione del pacchetto **aumentano**.
- Il numero di pacchetti acquisiti nell'output del comando **show capture <cap\_name>** è diverso da zero.
- Percorso di acquisizione **Pcapfile**. I pacchetti catturati vengono salvati automaticamente nella cartella **/mnt/disk0/packet-capture/**.
- Condizioni di acquisizione. Il software crea automaticamente i filtri di acquisizione in base alle condizioni di acquisizione.

```
> 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. Arrestare le clip quando necessario:

```
> 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:          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

## 8. Raccogliere i file di acquisizione. Attenersi alla procedura descritta nella sezione Raccolta dei



## file di acquisizione degli switch interni Secure Firewall 3100.

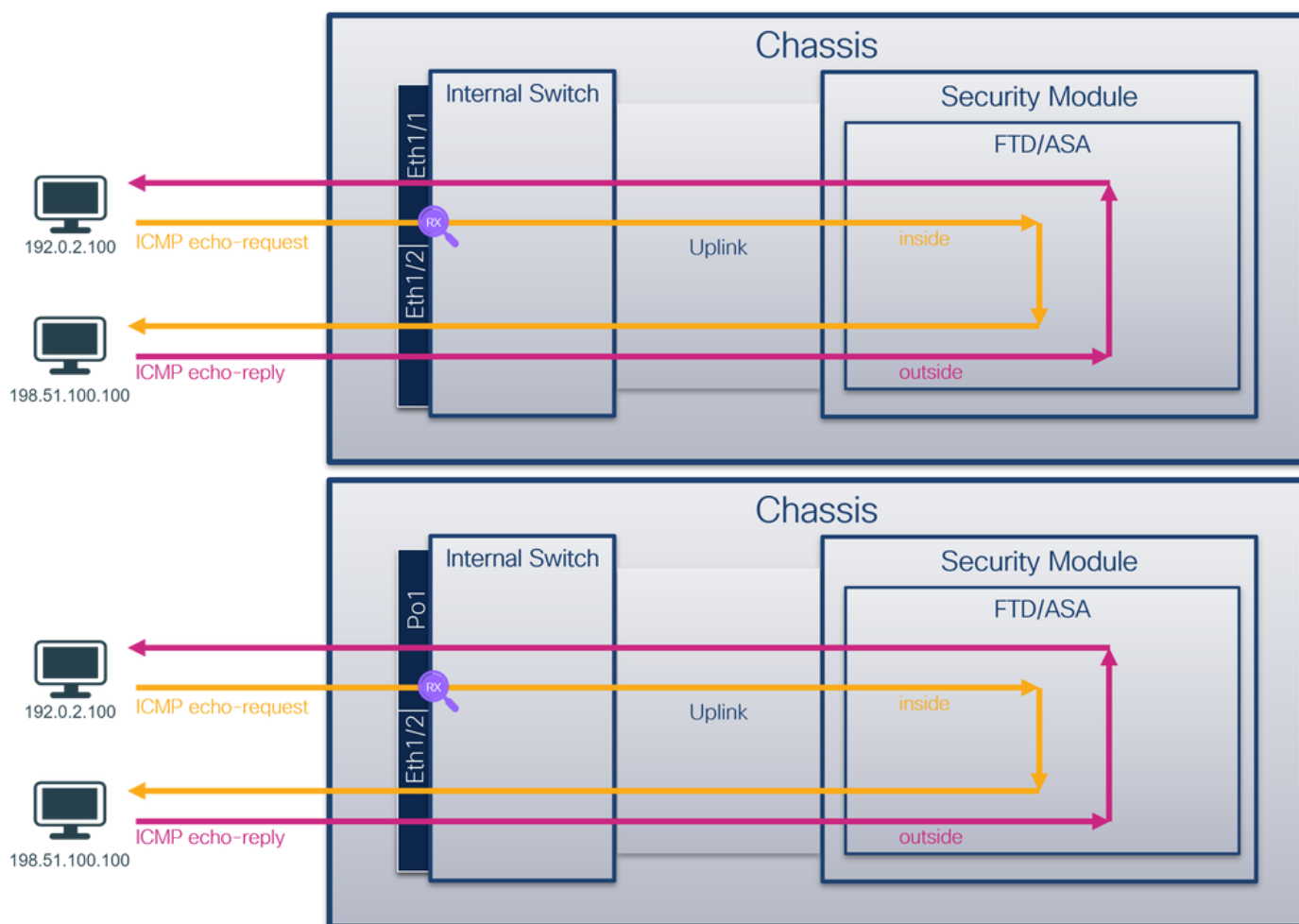
Nella versione 7.2, la configurazione di acquisizione dello switch interno non è supportata in FMC o FDM. Nel caso del software ASA versione 9.18(1) e successive, le acquisizioni dello switch interno possono essere configurate in ASDM versione 7.18.1.x e successive.

In questi scenari vengono illustrati i casi di utilizzo comuni di acquisizioni di switch interni Secure Firewall 3100.

## Acquisizione dei pacchetti su un'interfaccia fisica o su un canale della porta

Usare FTD o ASA CLI per configurare e verificare un'acquisizione pacchetto sull'interfaccia Ethernet1/1 o Portchannel1. Entrambe le interfacce hanno il nome if **inside**.

### Topologia, flusso dei pacchetti e punti di acquisizione



## Configurazione

Per configurare un'acquisizione pacchetto sull'interfaccia Ethernet1/1 o Port-channel1, attenersi alla seguente procedura su ASA o su CLI FTD:

1. Verificare il nome se:

```
> show nameif
Interface          Name          Security
Ethernet1/1       inside       0
```

```
Ethernet1/2          outside          0
Management1/1       diagnostic       0
```

> **show nameif**

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

## 2. Creare una sessione di acquisizione:

> **capture capsw switch interface inside**

## 3. Abilitare la sessione di acquisizione:

> **no capture capsw switch stop**

## Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore **Pcapsize** in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

> **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

Nel caso di Port-channel1, l'acquisizione viene configurata su tutte le interfacce membro:

> **show capture capsw detail**

Packet Capture info

**Name:** capsw  
Session: 1  
**Admin State:** enabled  
**Oper State:** up  
**Oper State Reason:** Active  
Config Success: yes  
Config Fail Reason:  
Append Flag: overwrite  
Session Mem Usage: 256  
Session Pcap Snap Len: 1518  
Error Code: 0  
Drop Count: 0

Total Physical ports involved in Packet Capture: 2

Physical port:

**Slot Id:** 1  
**Port Id:** 4  
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-4-0.pcap  
**Pcapsize:** 28824  
**Filter:** capsw-1-4

Packet Capture Filter Info

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

Physical port:

**Slot Id:** 1  
**Port Id:** 3  
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap  
**Pcapsize:** 18399  
Filter: capsw-1-3

Packet Capture Filter Info

Name: capsw-1-3  
Protocol: 0  
Ivlan: 0  
Ovlan: 0  
Src Ip: 0.0.0.0  
Dest Ip: 0.0.0.0

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

Total Physical breakout ports involved in Packet Capture: 0

#### 56 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Le interfacce membro port-channel possono essere verificate nella shell dei comandi FXOS **local-mgmt** tramite il comando **show portchannel summary**:

```
> connect fxos
```

```
...
```

```
KSEC-FPR3100-1 connect local-mgmt
```

```
KSEC-FPR3100-1(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
```

Per accedere a FXOS su ASA, eseguire il comando **connect fxos admin**. In caso di contesto multiplo, eseguire il comando nel contesto admin.

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Secure Firewall 3100**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per Ethernet1/1. Selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
2. L'intestazione del pacchetto originale è senza il tag VLAN.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39440)	64	Echo (ping) request id=0x0034, seq=1/256, ttl=64 (no res
2	2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	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 re
5	2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39696)	64	Echo (ping) request id=0x0034, seq=5/1280, ttl=64 (no re
6	2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39732)	64	Echo (ping) request id=0x0034, seq=6/1536, ttl=64 (no re
7	2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39811)	64	Echo (ping) request id=0x0034, seq=7/1792, ttl=64 (no re
8	2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39819)	64	Echo (ping) request id=0x0034, seq=8/2048, ttl=64 (no re
9	2022-08-07 19:50:14.932804	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39943)	64	Echo (ping) request id=0x0034, seq=9/2304, ttl=64 (no re
10	2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40134)	64	Echo (ping) request id=0x0034, seq=10/2560, ttl=64 (no r
11	2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40296)	64	Echo (ping) request id=0x0034, seq=11/2816, ttl=64 (no r
12	2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40429)	64	Echo (ping) request id=0x0034, seq=12/3072, ttl=64 (no r
13	2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40538)	64	Echo (ping) request id=0x0034, seq=13/3328, ttl=64 (no r
14	2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40699)	64	Echo (ping) request id=0x0034, seq=14/3584, ttl=64 (no r
15	2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40784)	64	Echo (ping) request id=0x0034, seq=15/3840, ttl=64 (no r
16	2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40923)	64	Echo (ping) request id=0x0034, seq=16/4096, ttl=64 (no r
17	2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41009)	64	Echo (ping) request id=0x0034, seq=17/4352, ttl=64 (no r
18	2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41063)	64	Echo (ping) request id=0x0034, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:14 (bc:e7:12:34:9a:14) Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 Internet Control Message Protocol		<pre> 0000 bc e7 12 34 9a 14 00 50 56 9d e8 be 08 00 45 00  ....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...X.5  ..MH 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  &amp;'()*+,-./012345 0060 36 37 55 55 55 55 67 UUUU </pre>
---	--	--

Aprire i file di acquisizione per le interfacce membro Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

1. Vengono acquisiti solo pacchetti di richieste echo ICMP.
2. L'intestazione del pacchetto originale è senza il tag VLAN.

No.	Time	Source	Destination	Protocol	Length	IP ID	TTL	Info
1	2022-08-07 20:40:58.657533	192.0.2.100	198.51.100.100	ICMP	102	0x9296 (37526)	64	Echo (ping) request id=0x0035, seq=1/256, ttl=64 (no res
2	2022-08-07 20:40:59.658611	192.0.2.100	198.51.100.100	ICMP	102	0x9370 (37744)	64	Echo (ping) request id=0x0035, seq=2/512, ttl=64 (no res
3	2022-08-07 20:41:00.655662	192.0.2.100	198.51.100.100	ICMP	102	0x93f0 (37872)	64	Echo (ping) request id=0x0035, seq=3/768, ttl=64 (no res
4	2022-08-07 20:41:01.659749	192.0.2.100	198.51.100.100	ICMP	102	0x946f (37999)	64	Echo (ping) request id=0x0035, seq=4/1024, ttl=64 (no re
5	2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94aa (38052)	64	Echo (ping) request id=0x0035, seq=5/1280, ttl=64 (no re
6	2022-08-07 20:41:03.663226	192.0.2.100	198.51.100.100	ICMP	102	0x952d (38189)	64	Echo (ping) request id=0x0035, seq=6/1536, ttl=64 (no re
7	2022-08-07 20:41:04.661262	192.0.2.100	198.51.100.100	ICMP	102	0x958d (38285)	64	Echo (ping) request id=0x0035, seq=7/1792, ttl=64 (no re
8	2022-08-07 20:41:05.665955	192.0.2.100	198.51.100.100	ICMP	102	0x95d8 (38360)	64	Echo (ping) request id=0x0035, seq=8/2048, ttl=64 (no re
9	2022-08-07 20:41:06.666538	192.0.2.100	198.51.100.100	ICMP	102	0x964b (38475)	64	Echo (ping) request id=0x0035, seq=9/2304, ttl=64 (no re
10	2022-08-07 20:41:07.667298	192.0.2.100	198.51.100.100	ICMP	102	0x972b (38699)	64	Echo (ping) request id=0x0035, seq=10/2560, ttl=64 (no r
11	2022-08-07 20:41:08.670540	192.0.2.100	198.51.100.100	ICMP	102	0x980a (38922)	64	Echo (ping) request id=0x0035, seq=11/2816, ttl=64 (no r
12	2022-08-07 20:41:09.668278	192.0.2.100	198.51.100.100	ICMP	102	0x9831 (38961)	64	Echo (ping) request id=0x0035, seq=12/3072, ttl=64 (no r
13	2022-08-07 20:41:10.672417	192.0.2.100	198.51.100.100	ICMP	102	0x98a2 (39074)	64	Echo (ping) request id=0x0035, seq=13/3328, ttl=64 (no r
14	2022-08-07 20:41:11.671369	192.0.2.100	198.51.100.100	ICMP	102	0x98f7 (39159)	64	Echo (ping) request id=0x0035, seq=14/3584, ttl=64 (no r
15	2022-08-07 20:41:12.675462	192.0.2.100	198.51.100.100	ICMP	102	0x99e4 (39396)	64	Echo (ping) request id=0x0035, seq=15/3840, ttl=64 (no r
16	2022-08-07 20:41:13.674993	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64	Echo (ping) request id=0x0035, seq=16/4096, ttl=64 (no r
17	2022-08-07 20:41:14.674093	192.0.2.100	198.51.100.100	ICMP	102	0x9af3 (39667)	64	Echo (ping) request id=0x0035, seq=17/4352, ttl=64 (no r
18	2022-08-07 20:41:15.676904	192.0.2.100	198.51.100.100	ICMP	102	0x9b8e (39822)	64	Echo (ping) request id=0x0035, seq=18/4608, ttl=64 (no r

Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) Ethernet II, Src: VMware_9d:e8:be (00:50:56:9d:e8:be), Dst: Cisco_34:9a:2c (bc:e7:12:34:9a:2c) Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100 Internet Control Message Protocol		<pre> 0000 bc e7 12 34 9a 2c 00 50 56 9d e8 be 08 00 45 00  ....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  ..MH b... 0030 00 00 0e c8 04 00 00 00 00 00 10 11 12 13 14 15  .... 0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ....! " # \$ % 0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &amp;'()*+,-./012345 0060 36 37 55 55 55 55 67 UUUU </pre>
---	--	--

### Spiegazione

Le clip dello switch sono configurate sulle interfacce Ethernet1/1 o Portchannel1.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/1	Ethernet 1/1	Nessuna	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Portchannel1 con le interfacce membro Ethernet1/3 ed Ethernet1/4	Ethernet 1/3 Ethernet 1/4	Nessuna	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100

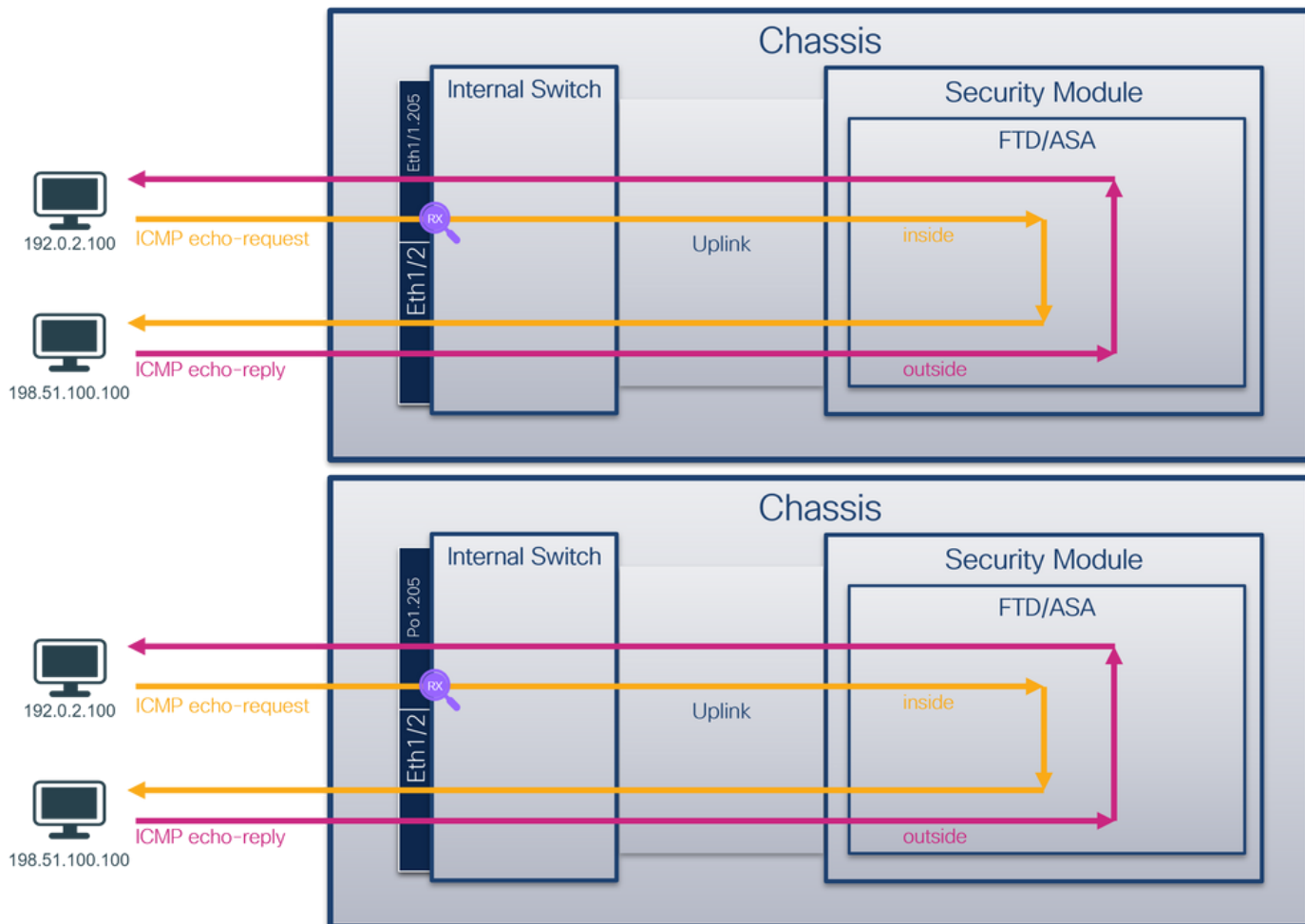
Acquisizione di pacchetti su una sottointerfaccia di un'interfaccia fisica o di un



## canale della porta

Usare FTD o ASA CLI per configurare e verificare l'acquisizione di un pacchetto sulle sottointerfacce Ethernet1/1.205 o Portchannel1.205. Entrambe le sottointerfacce hanno il nome se contenute.

## Topologia, flusso dei pacchetti e punti di acquisizione



## Configurazione

Per configurare un'acquisizione pacchetto sull'interfaccia Ethernet1/1 o Port-channel1, attenersi alla seguente procedura su ASA o su CLI FTD:

1. Verificare il nome se:

```
> show nameif
Interface          Name          Security
Ethernet1/1.205   inside        0
Ethernet1/2        outside       0
Management1/1     diagnostic    0
```

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

2. Creare una sessione di acquisizione:

```
> capture capsw switch interface inside
```

### 3. Abilitare la sessione di acquisizione:

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

## Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore **Pcapsize** in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

```
> show capture capsw detail
```

Packet Capture info

```
Name:                capsw
Session:                1
Admin State:        enabled
Oper State:         up
Oper State Reason:  Active
Config Success:        yes
Config Fail Reason:
Append Flag:           overwrite
Session Mem Usage:     256
Session Pcap Snap Len: 1518
Error Code:            0
Drop Count:           0
```

Total Physical ports involved in Packet Capture: 1

Physical port:

```
Slot Id:            1
Port Id:            1
Pcapfile:              /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:          6360
Filter:                caps-1-1
```

Packet Capture Filter Info

```
Name:                caps-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

In questo caso, viene creato un filtro con VLAN **Ovlan=205** esterna che viene applicato all'interfaccia.

Nel caso di Port-channel1, l'acquisizione con un filtro **Ovlan=205** è configurata su tutte le interfacce membro:

```
> show capture capsw detail
```

Packet Capture info

```
Name:                capsw  
Session:                1  
Admin State:        enabled  
Oper State:         up  
Oper State Reason: Active  
Config Success:        yes  
Config Fail Reason:  
Append Flag:           overwrite  
Session Mem Usage:     256  
Session Pcap Snap Len: 1518  
Error Code:            0  
Drop Count:            0
```

Total Physical ports involved in Packet Capture: 2

Physical port:

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

Packet Capture Filter Info

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

Physical port:

```
Slot Id:            1  
Port Id:            3  
Pcapfile:              /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-3-0.pcap  
Pcapsize:          5600  
Filter:                capsw-1-3
```

Packet Capture Filter Info

```
Name:                  capsw-1-3  
Protocol:              0  
  Ivlan:               0  
Ovlan:              205  
Src Ip:                0.0.0.0  
Dest Ip:               0.0.0.0  
Src Ipv6:              ::  
  Dest Ipv6:           ::  
Src MAC:               00:00:00:00:00:00  
Dest MAC:              00:00:00:00:00:00  
Src Port:              0  
Dest Port:             0
```

Ethertype: 0

Total Physical breakout ports involved in Packet Capture: 0

#### 49 packet captured on disk using switch capture

Reading of capture file from disk is not supported

Le interfacce membro port-channel possono essere verificate nella shell dei comandi FXOS **local-mgmt** tramite il comando **show portchannel summary**:

```
> connect fxos
```

```
...
```

```
KSEC-FPR3100-1 connect local-mgmt
```

```
KSEC-FPR3100-1(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
```

Per accedere a FXOS su ASA, eseguire il comando **connect fxos admin**. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Secure Firewall 3100**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per Ethernet1/1.205. Selezionare il primo pacchetto e controllare i punti chiave:

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

```

> 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
  
```

Aprire i file di acquisizione per le interfacce membro Portchannel1. Selezionare il primo pacchetto e controllare i punti chiave:

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

```

> 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
  
```

## Spiegazione

Le acquisizioni dello switch vengono configurate sulle sottointerfacce Ethernet1/1.205 o Portchannel1.205 con un filtro che corrisponde alla VLAN 205 esterna.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia Ethernet1/1.205	Ethernet 1/1	VLAN esterna 2005	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100
Configurare e verificare l'acquisizione di un pacchetto sull'interfaccia secondaria Portchannel1.205 con le interfacce	Ethernet 1/3 Ethernet	VLAN esterna 2005	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.100



## Acquisizione pacchetti su interfacce interne

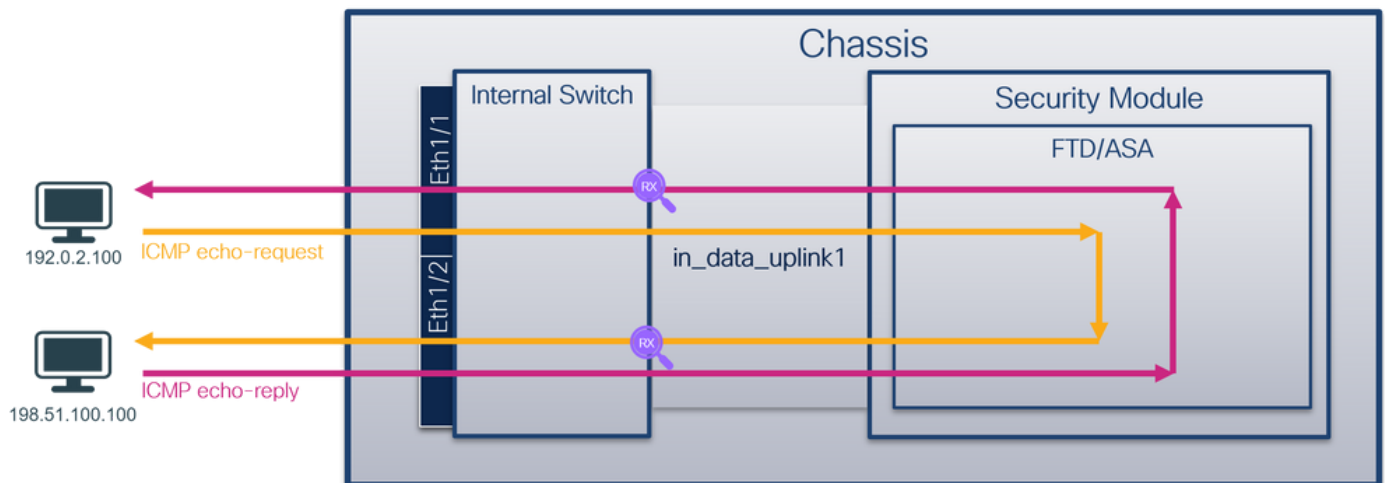
Secure Firewall ha due interfacce interne:

- **in\_data\_uplink1**: connette l'applicazione allo switch interno.
- **in\_mgmt\_uplink1**: fornisce un percorso di pacchetto dedicato per le connessioni di gestione, ad esempio SSH all'interfaccia di gestione o la connessione di gestione, nota anche come sftunnel, tra FMC e FTD.

### Attività 1

Usare la CLI FTD o ASA per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink in\_data\_uplink1.

### Topologia, flusso dei pacchetti e punti di acquisizione



### Configurazione

Per configurare un'acquisizione pacchetto sull'interfaccia **in\_data\_uplink1**, attenersi alla procedura seguente su ASA o CLI FTD:

1. Creare una sessione di acquisizione:

```
> capture capsw switch interface in_data_uplink1
```

2. Abilitare la sessione di acquisizione:

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

### Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore **Pcapsize** in byte aumenti e che il numero di pacchetti acquisiti sia diverso da zero:

> **show capture capsw detail**

Packet Capture info

**Name:** capsw  
Session: 1  
**Admin State:** enabled  
**Oper State:** up  
**Oper State Reason:** Active  
Config Success: yes  
Config Fail Reason:  
Append Flag: overwrite  
Session Mem Usage: 256  
Session Pcap Snap Len: 1518  
Error Code: 0  
Drop Count: 0

Total Physical ports involved in Packet Capture: 1

Physical port:

**Slot Id:** 1  
**Port Id:** 18  
Pcapfile: /mnt/disk0/packet-capture/sess-1-capsw-data-uplink1.pcap  
**Pcapsize:** 7704  
Filter: capsw-1-18

Packet Capture Filter Info

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

Total Physical breakout ports involved in Packet Capture: 0

**66 packets captured on disk using switch capture**

Reading of capture file from disk is not supported

In questo caso, viene creata un'acquisizione sull'interfaccia con ID interno **18** che è l'interfaccia **in\_data\_uplink1** sul Secure Firewall 3130. Il comando **show portmanager switch status** nella shell dei comandi FXOS **local-mgmt** mostra gli ID dell'interfaccia:

> **connect fxos**

...

KSEC-FPR3100-1 **connect local-mgmt**

KSEC-FPR3100-1(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
<b>0/18</b>	<b>KR2</b>	<b>Up</b>	<b>50G</b>	<b>Full</b>	<b>None</b>	<b>Link-Up</b>
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

Per accedere a FXOS su ASA, eseguire il comando **connect fxos admin**. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Secure Firewall 3100**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per l'interfaccia in\_data\_uplink1. Controllare il punto chiave. In questo caso, vengono acquisiti i pacchetti di richiesta echo ICMP e di risposta echo. Questi sono i pacchetti inviati dall'applicazione allo switch interno.

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 (repl
3	2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4d08 (19944)	64	Echo (ping) request id=0x003a, seq=34/8704, ttl=64 (req
4	2022-08-07 22:40:07.689300	198.51.100.100	192.0.2.100	ICMP	102	0x6db2 (28082)	64	Echo (ping) reply id=0x003a, seq=34/8704, ttl=64 (repl
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 22:40:08.690806	198.51.100.100	192.0.2.100	ICMP	102	0x6dbf (28095)	64	Echo (ping) reply id=0x003a, seq=35/8960, ttl=64 (repl
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 (repl
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	0x6ed5 (28373)	64	Echo (ping) reply id=0x003a, seq=37/9472, ttl=64 (repl
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 (repl
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 (repl
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 (repl
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 (repl

```

> Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
> Ethernet II, Src: Cisco_34:9a:15 (bc:e7:12:34:9a:15), Dst: VMware_9d:e7:50 (00:50:56:9d:e7:50)
> Internet Protocol Version 4, Src: 192.0.2.100, Dst: 198.51.100.100
> Internet Control Message Protocol
0000 00 50 56 9d e7 50 bc e7 12 34 9a 15 08 00 45 00  .PV.P...d...E.
0010 00 54 4d 93 40 00 40 01 00 1a c0 00 02 64 c6 33  .TM.@.@...d3
0020 64 64 08 00 7f 15 00 20 01 21 39 3f f0 62 00 00  dd...197.b...
0030 00 00 8b 1a 05 00 00 00 00 00 10 11 12 13 14 15  .
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060 36 37 55 55 55 55  .67UUUU

```

## Spiegazione

Quando si configura l'acquisizione di uno switch sull'interfaccia uplink, vengono acquisiti solo i pacchetti inviati dall'applicazione allo switch interno. I pacchetti inviati all'applicazione non vengono acquisiti.

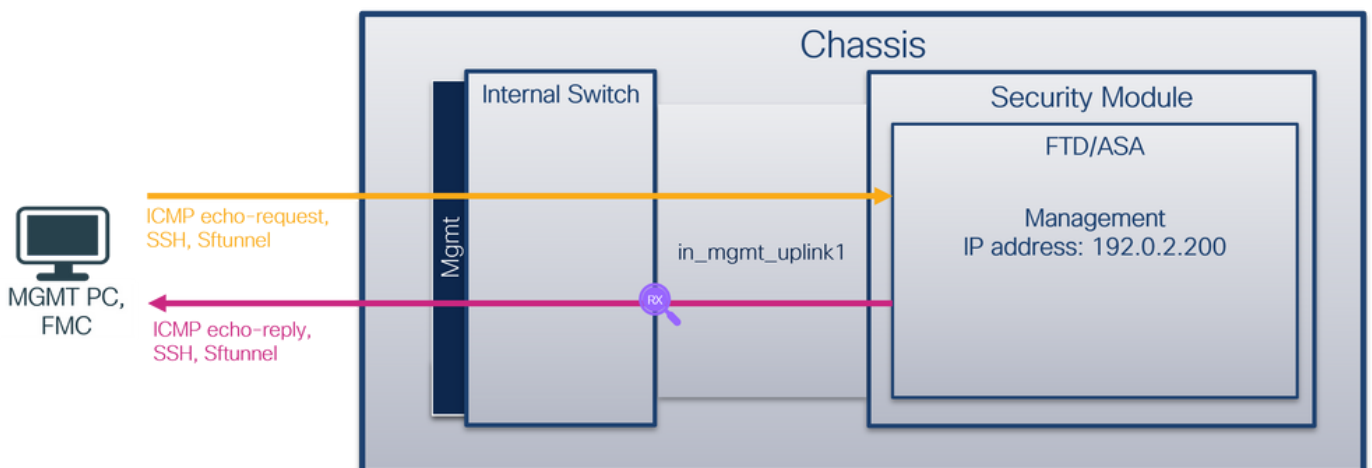
Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink <code>in_data_uplink1</code>	<code>in_data_uplink1</code>	Nessuna	Solo entrata	Richieste echo ICMP dall'host 192.0.2.100 all'host 198.51.100.1 ICMP echo risponde dall'host 198.51.100.100 all'host 192.0.2.1

## Attività 2

Usare FTD o ASA CLI per configurare e verificare l'acquisizione di un pacchetto sull'interfaccia uplink `in_mgmt_uplink1`. Vengono acquisiti solo i pacchetti delle connessioni del piano di gestione.

## Topologia, flusso dei pacchetti e punti di acquisizione



## Configurazione

Per configurare un'acquisizione pacchetto sull'interfaccia `in_mgmt_uplink1`, attenersi alla procedura seguente su ASA o CLI FTD:

1. Creare una sessione di acquisizione:

```
> capture capsw switch interface in_mgmt_uplink1
```

2. Abilitare la sessione di acquisizione:

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

## Verifica

Verificare il nome della sessione di acquisizione, lo stato amministrativo e operativo, lo slot di interfaccia e l'identificatore. Verificare che il valore **Pcapsize** in byte aumenti e che il numero di

pacchetti acquisiti sia diverso da zero:

```
> 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:       19
Pcapfile:      /mnt/disk0/packet-capture/sess-1-capsw-mgmt-uplink1.pcap
Pcapsize:     137248
Filter:        capsw-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

In questo caso, viene creata un'acquisizione sull'interfaccia con ID interno 19, che è l'interfaccia **in\_mgmt\_uplink1** sul Secure Firewall 3130. Il comando **show portmanager switch status** nella shell dei comandi FXOS **local-mgmt** visualizza gli ID dell'interfaccia:

```
> connect fxos
```

...

```
KSEC-FPR3100-1 connect local-mgmt
```

```
KSEC-FPR3100-1(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
<b>0/19</b>	<b>KR</b>	<b>Up</b>	<b>25G</b>	<b>Full</b>	<b>None</b>	<b>Link-Up</b>
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

Per accedere a FXOS su ASA, eseguire il comando **connect fxos admin**. In caso di contesto multiplo, eseguire questo comando nel contesto admin.

## Raccogli file di acquisizione

Attenersi alla procedura descritta nella sezione **Raccolta dei file di acquisizione degli switch interni Secure Firewall 3100**.

## Analisi dei file di acquisizione

Utilizzare un'applicazione per la lettura dei file di acquisizione dei pacchetti per aprire i file di acquisizione per l'interfaccia **in\_mgmt\_uplink1**. Controllare il punto chiave: in questo caso vengono visualizzati solo i pacchetti dell'indirizzo IP di gestione 192.0.2.200. Ad esempio, i pacchetti di risposta echo SSH, Sftunnel o ICMP. Si tratta dei pacchetti inviati dall'interfaccia di gestione delle applicazioni alla rete tramite lo switch interno.

No.	Time	Source	Destination	Protocol	Length	IP ID	PTTL	Info
196	2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	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	192.0.2.101	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	192.0.2.101	TLSv1.2	990	0xb7d2 (47058)	64	Application Data
199	2022-08-07 23:21:45.928772	192.0.2.200	192.0.2.100	ICMP	78	0xbd48 (48456)	64	Echo (ping) reply id=0x0001, seq=4539/47889, ttl=64
200	2022-08-07 23:21:45.949024	192.0.2.200	192.0.2.101	TLSv1.2	128	0x4a97 (19095)	64	Application Data
201	2022-08-07 23:21:45.949027	192.0.2.200	192.0.2.101	TCP	70	0x4a98 (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	192.0.2.101	TLSv1.2	100	0x4a99 (19097)	64	Application Data
203	2022-08-07 23:21:46.019899	192.0.2.200	192.0.2.101	TLSv1.2	96	0x4a9a (19098)	64	Application Data
204	2022-08-07 23:21:46.019903	192.0.2.200	192.0.2.101	TCP	70	0x4a9b (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	192.0.2.101	TCP	70	0x4a9c (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	192.0.2.101	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	192.0.2.100	ICMP	78	0xbd9e (48542)	64	Echo (ping) reply id=0x0001, seq=4540/48145, ttl=64
208	2022-08-07 23:21:47.980409	192.0.2.200	192.0.2.100	ICMP	78	0xbd9f (48543)	64	Echo (ping) reply id=0x0001, seq=4541/48146, ttl=64
209	2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	TCP	70	0x4a9d (19101)	64	8305 → 58885 [ACK] Seq=22053 Ack=26366 Win=4116 Len=0 TSv
210	2022-08-07 23:21:48.903236	192.0.2.200	192.0.2.101	TLSv1.2	747	0x4a9e (19102)	64	Application Data
211	2022-08-07 23:21:48.994386	192.0.2.200	192.0.2.100	ICMP	78	0xbe48 (48712)	64	Echo (ping) reply id=0x0001, seq=4542/48657, ttl=64
212	2022-08-07 23:21:50.008576	192.0.2.200	192.0.2.100	ICMP	78	0xbe4e (48806)	64	Echo (ping) reply id=0x0001, seq=4543/48913, ttl=64
213	2022-08-07 23:21:50.140167	192.0.2.200	192.0.2.101	TCP	1518	0xb7d4 (47060)	64	39181 → 8305 [ACK] Seq=65188 Ack=921 Win=1384 Len=0 TSval
214	2022-08-07 23:21:50.140171	192.0.2.200	192.0.2.101	TCP	1518	0xb7d5 (47061)	64	39181 → 8305 [ACK] Seq=66636 Ack=921 Win=1384 Len=0 TSv
215	2022-08-07 23:21:50.140175	192.0.2.200	192.0.2.101	TLSv1.2	990	0xb7d6 (47062)	64	Application Data
216	2022-08-07 23:21:51.015884	192.0.2.200	192.0.2.100	ICMP	78	0xbec1 (48833)	64	Echo (ping) reply id=0x0001, seq=4544/49169, ttl=64
217	2022-08-07 23:21:51.142842	192.0.2.200	192.0.2.101	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	192.0.2.100	ICMP	78	0xbf02 (48898)	64	Echo (ping) reply id=0x0001, seq=4545/49425, ttl=64
219	2022-08-07 23:21:53.042744	192.0.2.200	192.0.2.100	ICMP	78	0xbf59 (48985)	64	Echo (ping) reply id=0x0001, seq=4546/49681, ttl=64
220	2022-08-07 23:21:53.073144	192.0.2.200	192.0.2.100	SSH	170	0xad34 (44340)	64	Server: Encrypted packet (len=112)
221	2022-08-07 23:21:53.194906	192.0.2.200	192.0.2.100	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	192.0.2.101	TLSv1.2	747	0x4a9f (19103)	64	Application Data
223	2022-08-07 23:21:54.102899	192.0.2.200	192.0.2.100	ICMP	78	0xbf63 (48995)	64	Echo (ping) reply id=0x0001, seq=4547/49937, ttl=64
224	2022-08-07 23:21:54.903675	192.0.2.200	192.0.2.101	TCP	70	0x4aa0 (19104)	64	8305 → 58885 [ACK] Seq=23407 Ack=26424 Win=4116 Len=0 TSv
225	2022-08-07 23:21:55.136700	192.0.2.200	192.0.2.100	TCP	70	0xbf64 (48996)	64	Echo (ping) reply id=0x0001, seq=4548/50103, ttl=64

## Spiegazione

Quando si configura l'acquisizione di uno switch sull'interfaccia uplink di gestione, vengono acquisiti solo i pacchetti in entrata inviati dall'interfaccia di gestione dell'applicazione. I pacchetti destinati all'interfaccia di gestione delle applicazioni non vengono acquisiti.

Nella tabella seguente viene riepilogata l'attività:

Attività	Punto di acquisizione	Filtro interno	Direzione	Traffico acquisito
Configurazione e verifica dell'acquisizione di un pacchetto sull'interfaccia uplink di gestione	in_mgmt_uplink1	Nessuna	Solo entrata (dall'interfaccia di gestione alla rete tramite lo switch interno)	Risposte echo ICMP da gestione FTD in IP 192.0.2.200 all'host 192.0.2.100 Sftunnel dall'indirizzo IP di gestione FTD 192.0.2.200 all'indirizzo IP FMC 192.0.2.100 SSH da FTD management IP address 192.0.2.200 all'host 192.0.2.100

## Filtri di acquisizione pacchetti

I filtri di acquisizione dei pacchetti dello switch interno sono configurati allo stesso modo delle acquisizioni del piano dati. Utilizzare le opzioni **ethernet-type** e **match** per configurare i filtri.

## Configurazione

Attendersi alla seguente procedura sull'interfaccia ASA o sulla CLI FTD per configurare un'acquisizione dei pacchetti con un filtro che corrisponda ai frame ARP o ai pacchetti ICMP dell'host 198.51.100.100 sull'interfaccia Ethernet1/1:

1. Verificare il nome se:

> **show nameif**

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

## 2. Creare una sessione di acquisizione per ARP o ICMP:

> **capture capsw switch interface inside ethernet-type arp**

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

### Verifica

Verificare il nome della sessione di acquisizione e il filtro. Il valore di Ethertype è **2054** in decimale e **0x0806** in esadecimale:

> **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

Questa è la verifica del filtro per ICMP. Il protocollo IP 1 è l'ICMP:

```
> show capture capsw detail
```

Packet Capture info

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

Total Physical ports involved in Packet Capture: 1

Physical port:

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

Packet Capture Filter Info

```
Name:                capsw-1-1
Protocol:           1
Ivlan:                  0
Ovlan:                  0
Src Ip:             198.51.100.100
Dest Ip:                 0.0.0.0
Src Ipv6:                ::
Dest Ipv6:               ::
Src MAC:                 00:00:00:00:00:00
Dest MAC:                00:00:00:00:00:00
Src Port:                0
Dest Port:               0
Ethertype:               0
```

Total Physical breakout ports involved in Packet Capture: 0

0 packets captured on disk using switch capture

Reading of capture file from disk is not supported

## Raccogli file di acquisizione switch interno Secure Firewall 3100

Usare ASA o FTD CLI per raccogliere i file di acquisizione dello switch interno. Su FTD, il file di acquisizione può anche essere esportato tramite il comando **copy** della CLI verso destinazioni raggiungibili tramite le interfacce di dati o di diagnostica.

In alternativa, il file può essere copiato in **/ngfw/var/common** in modalità Expert e scaricato da FMC tramite l'opzione **File Download**.

Nel caso delle interfacce port-channel, assicurarsi di raccogliere i file di acquisizione dei pacchetti da tutte le interfacce membro.

## ASA

Per raccogliere i file di acquisizione dello switch interno sulla CLI di ASA, attenersi alla procedura seguente:

### 1. Interrompere l'acquisizione:

```
asa# capture capsw switch stop
```

### 2. Verificare che la sessione di acquisizione sia stata arrestata e annotare il nome del file di acquisizione.

```
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. Utilizzare il comando **copy** della CLI per esportare il file in destinazioni remote:

```
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
```

## FTD

Seguire questi passaggi per raccogliere i file di acquisizione switch interni sulla CLI FTD e copiarli sui server raggiungibili tramite interfacce di dati o di diagnostica:

### 1. Andare alla CLI di diagnostica:

```
> 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. Interrompere l'acquisizione:

```
firepower# capture capi switch stop
```

### 3. Verificare che la sessione di acquisizione sia stata arrestata e annotare il nome del file di acquisizione:

```
firepower# show capture capsw detail
Packet Capture info
Name:          capsw
Session:         1
Admin State:  disabled
Oper State:   down
Oper State Reason: Session_Admin_Shut
Config Success:  yes
Config Fail Reason:
Append Flag:     overwrite
Session Mem Usage: 256
Session Pcap Snap Len: 1518
Error Code:      0
Drop Count:      0

Total Physical ports involved in Packet Capture: 1
Physical port:
Slot Id:         1
Port Id:         1
Pcapfile:     /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
Pcapsize:        139826
```



Filter: capsu-1-1

#### Packet Capture Filter Info

Name: capsu-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. Usare il comando **copy** della CLI per esportare il file in destinazioni remote.

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

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

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

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

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

Per raccogliere i file di acquisizione da FMC tramite l'opzione **Download file**, procedere come segue:

#### 1. Interrompere l'acquisizione:

```
> capture capsu switch stop
```

#### 2. Verificare che la sessione di acquisizione sia interrotta e prendere nota del nome del file e del percorso completo del file di acquisizione:

```
> show capture capsu detail
```

```
Packet Capture info
```

```
Name: capsu  
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. Andare alla modalità Expert e passare alla modalità root:

```
> expert
```

```
admin@firepower:~$ sudo su
```

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

### 4. Copiare il file di acquisizione in /ngfw/var/common/:

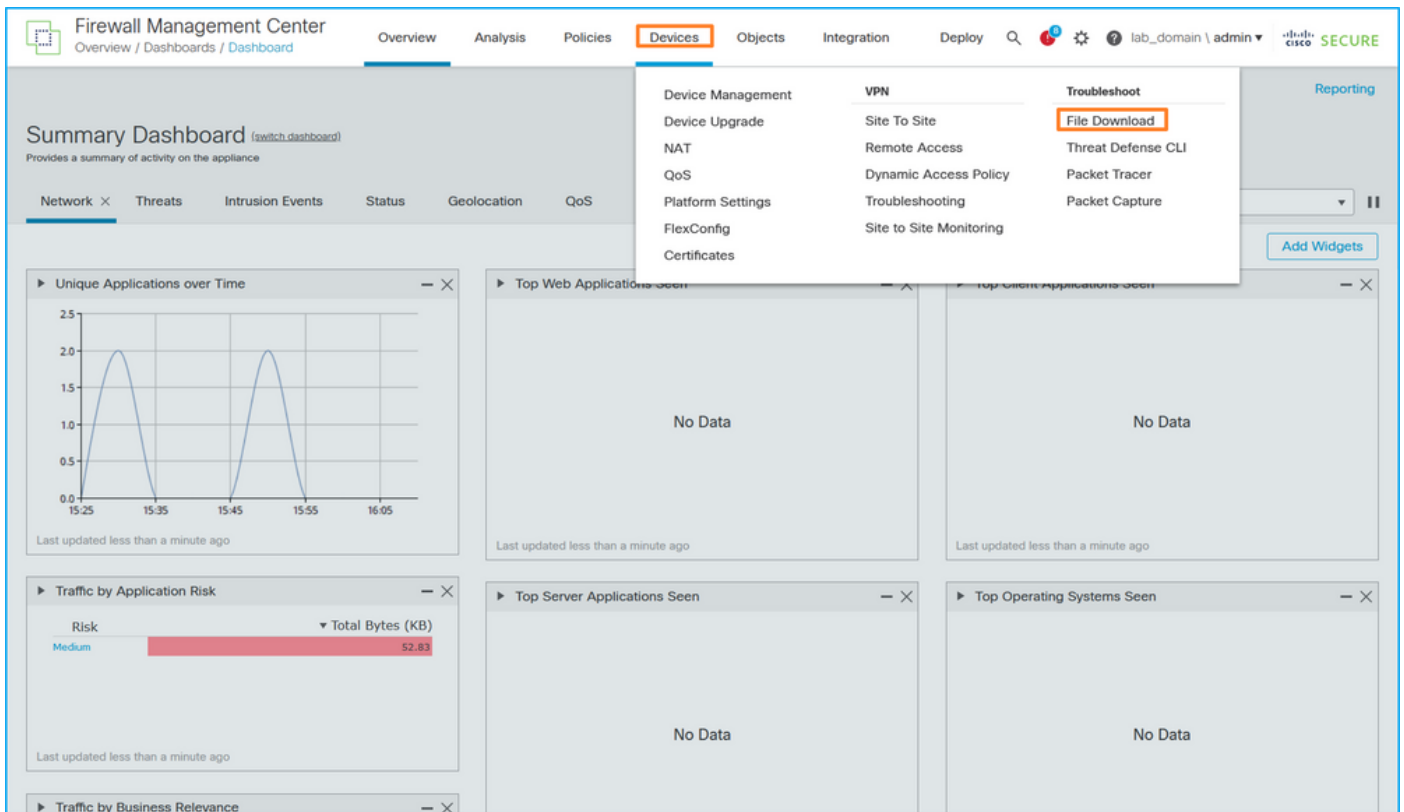
```
root@KSEC-FPR3100-1:/home/admin cp /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap
/ngfw/var/common/
```

```
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. In FMC scegliere Dispositivi > Download file:



## 6. Scegliere l'FTD, fornire il nome del file di acquisizione e fare clic su **Download**:



## Linee guida, limitazioni e best practice per l'acquisizione di pacchetti di switch interni

Linee guida e limitazioni:

- Sono supportate più sessioni di configurazione dell'acquisizione degli switch, ma può essere attiva solo una sessione di acquisizione alla volta. Un tentativo di abilitare 2 o più sessioni di acquisizione genera un errore **"ERRORE: Impossibile abilitare la sessione. È stato raggiunto il limite massimo di 1 sessione di acquisizione pacchetti attiva"**.
- Impossibile eliminare un'acquisizione switch attiva.
- Impossibile leggere le acquisizioni di switch nell'applicazione. L'utente deve esportare i file.
- Alcune opzioni di acquisizione del piano dati, quali **dump**, **decode**, **packet-number**, **trace** e altre, non sono supportate per le acquisizioni dello switch.
- Nel caso di un'ASA multi-contesto, le acquisizioni dello switch sulle interfacce dati vengono configurate nei contesti utente. Le acquisizioni dello switch sulle interfacce `in_data_uplink1` e `in_mgmt_uplink1` sono supportate solo nel contesto admin.

Questo è l'elenco delle best practice basate sull'uso della cattura di pacchetti nei casi TAC:

- Stai attento alle linee guida e ai limiti.

- Utilizzare i filtri di acquisizione.
- Considerare l'impatto di NAT sugli indirizzi IP dei pacchetti quando viene configurato un filtro di acquisizione.
- Aumenta o diminuisce la **lunghezza del pacchetto** che specifica le dimensioni del frame, nel caso differisca dal valore predefinito di 1518 byte. Dimensioni inferiori determinano un numero maggiore di pacchetti acquisiti e viceversa.
- Regolare le dimensioni del **buffer** in base alle esigenze.
- Prendere nota del **valore Drop Count** nell'output del comando **show cap<cap\_name>detail**. Una volta raggiunto il limite delle dimensioni del buffer, il contatore di rilascio aumenta.

## Informazioni correlate

- [Guide alla configurazione di Firepower 4100/9300 Chassis Manager e FXOS CLI](#)
- [Guida introduttiva a Cisco Secure Firewall 3100](#)
- [Guida di riferimento ai comandi di Cisco Firepower 4100/9300 FXOS](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).