# Interne Switch-opnamen van beveiligde firewall en firewall configureren en controleren

# Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Overzicht op hoog niveau van de systeemarchitectuur Overzicht op hoog niveau van de interne Switch Packet Flow en Capture points Configuratie en verificatie op FirePOWER-applicatie 4100/9300 PacketCapture op een fysieke of poortkanaal-interface PacketCaptures op backplane interfaces Packet Capture op toepassingen en toepassingspoorten Packet Capture op een subinterface van een fysieke of poortkanaal-interface PacketCapture filters Opnamebestanden van FirePOWER 4100/9300 interne Switch verzamelen Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch Configuratie en verificatie van beveiligde firewall 3100 PacketCapture op een fysieke of poortkanaal-interface Packet Capture op een subinterface van een fysieke of poortkanaal-interface Packet Capture op interne interfaces PacketCapture filters Opnamebestanden van beveiligde firewall 3100 interne Switch Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch Gerelateerde informatie

# Inleiding

In dit document worden de configuratie en verificatie van de Firepower beschreven en wordt de Secure Firewall interne switch weergegeven.

# Voorwaarden

## Vereisten

Basisproductkennis, opnameanalyse.

## Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall 31xx
- Firepower 41xx
- Firepower 93xx
- Cisco Secure Xersible Operating System (FXOS) 2.12.0.x
- Cisco Secure Firewall Threat Defence (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
- Adaptieve security applicatie (ASA) 9.18(1)x
- Adaptieve security applicatie Apparaatbeheer (ASDM) 7.18.1.x
- Wireshark 3.6.7 (<u>https://www.wireshark.org/download.html</u>)

# Achtergrondinformatie

## Overzicht op hoog niveau van de systeemarchitectuur

Vanuit het pakketstroomperspectief kan de architectuur van de Firepower 4100/9300 en Secure Firewall 3100 worden gevisualiseerd zoals in deze afbeelding:



Het chassis bevat deze onderdelen:

Interne switch - doorstuurt pakket van het netwerk naar de applicatie en vice versa. De switch wordt aangesloten op de voorinterfaces die zich op de ingebouwde interfacemodule of de externe netwerkmodules bevinden en kan bijvoorbeeld worden aangesloten op switches. Voorbeelden van frontinterfaces zijn Ethernet 1/1, Ethernet 2/4, enzovoort. De "voorkant" is geen sterke technische definitie. In dit document wordt het gebruikt om interfaces die zijn aangesloten op externe apparaten te onderscheiden van de backplane of uplink-interfaces.

 Backplane of uplink - een interfaceinterface die de beveiligingsmodule (SM) verbindt met de switch. Deze tabel toont backplane interfaces op Firepower 4100/9300 en uplink-interface op Secure Firewall 3100:

Platform	Aantal ondersteunde beveiligingsmodules	Backplane/uplink- interfaces	In kaart gebrachte toepassingsinterfa
FirePOWER 4100 (behalve FirePOWER 4110/4112)	1	SM1: Ethernet1/9 Ethernet1/10	Interne gegevens0/0 Interne gegevens0/1
FirePOWER-applicatie 4110/4112	1	Ethernet1/9	Interne gegevens0/0
FirePOWER-applicatie 9300	3	SM1: Ethernet1/9 Ethernet1/10 SM2: Ethernet T1/E1 Ethernet T1/E1 SM3: Ethernet T1/E1 Ethernet T1/E1	Interne gegevens Interne gegevens Interne gegevens Interne gegevens Interne gegevens Interne gegevens
Secure-firewall 3100	1	SM1: in_data_uplink1	Interne gegevens0/1

In het geval van 2 backplane interfaces per module, de interne switch en de toepassingen op de modules voeren verkeer load-balancing over de 2 interfaces uit.

- Security module, security engine of blade de module waarin applicaties zoals FTD of ASA zijn geïnstalleerd. Firepower 9300 ondersteunt maximaal 3 beveiligingsmodules.
- **Toegewezen applicatie interface** applicaties, zoals FTD of ASA, brengen de backplane of uplink interfaces in kaart naar interne interfaces. Met andere woorden, de backplane of uplink interfaces zijn zichtbaar als interne interfaces in toepassingen.

Gebruik de opdracht show interface detail om interne interfaces te verifiëren:

```
> 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
```

### Overzicht op hoog niveau van de interne Switch

#### FirePOWER-applicatie 4100/9300

Om een doorsturen besluit te nemen gebruikt de switch een interface-VLAN-tag, of poort-VLAN-tag, en een Virtual Network-tag (VN-tag).

De port VLAN-tag wordt gebruikt door de interne switch om een interface te identificeren. De switch voegt de poort VLAN-tag in op elk toegangspakket dat op de voorinterfaces kwam. De VLAN-tag wordt automatisch geconfigureerd door het systeem en kan niet handmatig worden gewijzigd. De waarde van de tag kan worden gecontroleerd in de **fxos** opdrachtshell:

```
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
```

De VN-tag wordt ook door de inwendige switch ingevoegd en gebruikt om de pakketten door te sturen naar de applicatie. Het wordt automatisch ingesteld door het systeem en kan niet handmatig worden gewijzigd.

De port VLAN-tag en de VN-tag worden gedeeld met de applicatie. De applicatie voegt de respectievelijke uitgaande interface VLAN-tags en de VN-tags in elk pakket in. Wanneer een pakketje van de applicatie wordt ontvangen door de switch op de backplane interfaces, leest de switch de VLAN-tag voor de uitgaande interface en de VN-tag, identificeert de toepassing en de uitgangsinterface, stript de VLAN-tag voor poorten en de VN-tag en stuurt het pakketbestand door

naar het netwerk.

### Secure-firewall 3100

Net zoals in Firepower 4100/9300, wordt de poort VLAN tag gebruikt door de switch om een interface te identificeren.

De poort VLAN-tag wordt gedeeld met de toepassing. De toepassing voegt de respectievelijke uitgaande interface VLAN-tags in elk pakket in. Wanneer een pakketje uit de applicatie wordt ontvangen door de switch op de uplink-interface, leest de switch de VLAN-tag van de uitgaande interface, identificeert hij de uitgangsinterface, stript hij de VLAN-tag van de poort en stuurt hij het pakketje door naar het netwerk.

## Packet Flow en Capture points

Firepower 4100/9300 en Secure Firewall 3100 ondersteunen pakketvastlegging op de interfaces van de switch.

Dit getal toont de pakketopnamepunten langs het pakketpad in het chassis en de toepassing:



De opnamepunten zijn:

- 1. Inwendig switch-frontinterface-ingangspunt. Een voorinterface is elke interface die is aangesloten op de peer devices zoals switches.
- 2. Opnamepunt voor interface-ingang van gegevensvlak
- 3. Snelopnamepunt
- 4. Uitgangspunt van de gegevensvlak-interface
- 5. Interne switch-backplane of uplink-ingangspunt. Een backplane of uplink-interface verbindt de interne switch met de toepassing.

De interne switch ondersteunt alleen invoerinterfaceopnamen. Dat zijn alleen de pakketten die van het netwerk of van de ASA/FTD-toepassing worden ontvangen. **Uitgangspakket-opnamen worden niet ondersteund.** 

# Configuratie en verificatie op FirePOWER-applicatie 4100/9300

De interne switch Firepower 4100/9300 kan worden geconfigureerd in **Tools > Packet Capture** op FCM of in **scope packet-capture** in FXOS CLI. Raadpleeg voor de beschrijving van de pakketopnameopties de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS Chassis Manager* of de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS CLI*, hoofdstuk **Problemen oplossen**, sectie **Packet Capture**.

Deze scenario's behandelen de gemeenschappelijke gevallen van het gebruik van Firepower 4100/9300 interne switch vangt.

## PacketCapture op een fysieke of poortkanaal-interface

Gebruik de FCM en CLI om een pakketopname op interface Ethernet1/2 of Portchannel1 interface te configureren en te verifiëren. Zorg er in het geval van een poort-kanaal interface voor dat u alle fysieke lidinterfaces selecteert.

#### Topologie, pakketstroom en de opnamepunten



### Configuratie

### FCM

Volg deze stappen op FCM om een pakketopname op interfaces Ethernet1/2 of Portchannel1 te configureren:

1. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

2. Selecteer de interface **Ethernet1/2**, geef de sessienaam op en klik op **Save and Run** om de opname te activeren:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admi
Select an instance: ftd1 v	Save and Run Save Cancel
ftd1	Session Name*         Cap1           Selected Interfaces         Ethermet1/2
Dhamet1/2	Buffer Size 256 MB 💙
Ethernet1/3	Store Packets Overventer Append
Ethernet1/1 FTD Ethernet1/9, Ethernet1/10	Capture Filter Apply Filter Costure All
Ethernet1/5 (Portchannet2)	
Ebhanel1/4 (Portchanel1)	

3. In het geval van een poort-kanaal interface, selecteer alle fysieke lidinterfaces, geef de sessienaam en klik op **Save and Run** om de opname te activeren:

Overview interfaces cogical bevices security engine mattorni securitys		System tools Help admini
Select an instance: ftd1		Save and Run Save Cancel
ftd1	Session Name* Cap1 Selected Interfaces Ethernet1/5, Ethernet1/4	
Ethemet1/2	Buffer Size 256 MB 💙	•
Ethemati/3	Shap length: 1518 Bytes Store Packets Overwrite Append	
Ethernet1/1 FTD Ethernet1/10	Capture Filter Apply Filter Capture All	
Ethernet1/3 (Portchannel1)		
Ethernet1/4 (Potthannel1)		

### **FXOS CLI**

Volg deze stappen op FXOS CLI om een pakketopname op interfaces Ethernet1/2 of Portchannel1 te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

firepower#	scope ssa					
firepower /	ssa # <b>show</b>	app-instanc	e			
App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Turbo Mode	e Profile Na	ame Cluster S	State Cluster Ro	ole	
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82

Native No

#### Not Applicable None

#### 2. In het geval van een poort-kanaal-interface, identificeer zijn lidinterfaces:

```
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
_____
            Туре
Group Port-
                  Protocol Member Ports
   Channel
.....
                                        _____
                 LACP
                        Eth1/4(P) Eth1/5(P)
```

- Pol(SU) Eth 1
  - 3. Een opnamesessie maken:

```
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 #
```

Voor poort-kanaal interfaces wordt een afzonderlijke opname voor elke lidinterface geconfigureerd:

```
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 #
Verificatie
```

**FCM** 

Controleer de interfacenaam, zorg ervoor dat de operationele status omhoog is en dat de bestandsgrootte (in bytes) toeneemt:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings				Syste	m Tools	Help	admin
Capture Sess	sion Filter Lis	t									
							C Refresh Capture	Session Delete	AI Sessions		
	cap1	Drop Coun	t: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518	Bytes			
Interface Nar	me	Filter		File Size (in bytes)	File Name	Device Name					
Ethernet1/2		None		28632	cap1-ethernet-1-2-0.pcap	ftd1		$\pm$			

Portchannel1 met lid interfaces Ethernet1/4 en Ethernet1/5:

Overview Interfaces Li	ogical Devices Security Engine Platform S	ettings						System Tools Help admin
Capture Session Filter List								
							C Refresh Capture Session	Delete All Sessions
a 🔳 cap1	Drop Count: 0	Operat	ional State: up		Buffer Size: 256 MB		Snap Length: 1518 Bytes	
Interface Name	Filter		File Size (in bytes)	Fil	ile Name	Device Name		
Ethernet1/5	None		160	caj	sp1-ethernet-1-5-0.pcap	ftd1	*]	
Ethernet1/4	None		85000	Caj	p1-ethernet-1-4-0.pcap	ftd1	2	

## **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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
Poortkanaal 1 met lidinterfaces Ethernet1/4 en 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
```

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketopname om het opnamebestand voor Ethernet1/2 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

No. Time	Source	Destination	Protocol	Length	PD	IP TTL Info	
1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (40428)	64 Echo (ping) reque	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	0x9dec (40428)	64 Echo (ping) reque	<pre>id=0x001a, seq=7/1792, ttl=64 (no response found!)</pre>
3 2022-07-13 06:23:59.309048886	192.0.2.100	198.51.100.100	ICMP	108	0x9ed0 (40656)	64 Echo (ping) reque	it 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	0x9ed0 (40656)	64 Echo (ping) reque	it 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	0x9f20 (40736)	64 Echo (ping) reque	it id=0x001a, seq=9/2304, ttl=64 (no response found!)
6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736)	64 Echo (ping) reque	it 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	it 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) reque	<pre>it id=0x001a, seq=13/3328, ttl=64 (no response found!)</pre>
14 2022-07-13 06:24:04.429156831	192.0.2.100	198.51.100.100	ICMP	102	0xa10f (41231)	64 Echo (ping) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	st 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) reque	<pre>it id=0x001a, seq=16/4096, ttl=64 (no response found!)</pre>
21 2022-07-13 06:24:08.525089956	192.0.2.100	198.51.100.100	ICMP	108	0xa257 (41559)	64 Echo (ping) reque	st 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) reque	st 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) reque	st 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) reque	t 1d=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) reque	st 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) reque	it id=0x001a, seq=19/4864, ttl=64 (no response found!)
27 2022-07-13 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801)	64 Echo (ping) reque	it id=0x001a, seq=20/5120, tt1=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) reque	it id=0x001a, seq=20/5120, tt1=64 (no response found!)
29 2022-07-13 06:24:12.621061022	192.0.2.100	198.51.100.100	ICMP	168	0xa30c (41948)	64 Echo (ping) reque	tt 1d=0x001a, seq=21/53/6, tt1=64 (no response found))
< C							
> Frame 1: 108 bytes on wire (864 bit	(s), 108 bytes (	captured (864 bits)	on interface	capture_u	0_1, id 0		0000 58 97 bd b9 77 0e 00 50 56 9d e8 be 89 26 80 0a X ··· w · P V ··· & ·
> Ethernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8	:be), Dst: Cisco b9	:77:0e (58:97:	bd:b9:77:	0e)		0010 00 00 81 00 00 66 08 00 45 00 00 54 9d ec 40 00 ·····f·· E··T··@·
✓ VN-Tag							0020 40 01 af c0 c0 00 02 64 c6 33 64 64 08 00 4e a2 @·····d ·3dd··N·
1	= Direc	tion: From Bridge					0030 00 1a 00 07 14 64 ce 62 00 00 00 00 20 a2 07 00d.b
.0	= Point	er: vif_id					0040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 10
00 0000 0000 1010	= Desti	nation: 10					0050 IC 10 10 17 20 21 22 23 24 25 20 27 28 29 24 20 ····· 1 # \$M&()-+
···· ··· ··· ··· ··· ··· ··· ··· ··· ·	= Loope	d: No	41				, ., 0123 4307
0	= Reser	ved: 0	- I -				
	= Versi	on: 0					
0000 00	00 0000 = Sourc	e: 0					
Type: 802.10 Virtual LAN (0x8100	)						
802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102						
000 = Priority:	Best Effort (de	fault) (0)	~				
0 = DEI: Ineli	gible		31				
0000 0110 0110 = ID: 102			-				
Type: IPv4 (0x0800)							
> Internet Protocol Version 4, Src: 1	192.0.2.100, Dst	t: 198.51.100.100	2				
> Internet Control Message Protocol			2				

Selecteer het tweede pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.

No	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info			
Г	1 2022-07-13 06:23:58.285080930	192.0.2.100	198.51.100.100	ICMP	108	0x9dec (48428	) 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	0x9dec (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	0x9ed0 (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	0x9ed0 (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	0x9f20 (40736)	) 64 Echo	(ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	6 2022-07-13 06:24:00.333056014	192.0.2.100	198.51.100.100	ICMP	102	0x9f20 (40736	) 64 Echo	(ping)	request	id=0x001a, seq=9/2304, ttl=64 (no response found!)
	7 2022-07-13 06:24:01.357173530	192.0.2.100	198.51.100.100	ICMP	108	0x9f2d (40749	) 64 Echo	(ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	8 2022-07-13 06:24:01.357174708	192.0.2.100	198.51.100.100	ICMP	102	0x9f2d (40749	) 64 Echo	(ping)	request	id=0x001a, seq=10/2560, ttl=64 (no response found!)
	9 2022-07-13 06:24:02.381073741	192.0.2.100	198.51.100.100	ICMP	108	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 06:24:11.597086027	192.0.2.100	198.51.100.100	ICMP	108	0xa349 (41801	) 64 Echo	(ping)	request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	28 2022-07-13 06:24:11.597088170	192.0.2.100	198.51.100.100	ICMP	102	0xa349 (41801	) 64 Echo	(ping)	request	id=0x001a, seq=20/5120, ttl=64 (no response found!)
	29 2022-07-13 06:24:12.621061022	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!)
<										
5	Frame 2: 102 bytes on wire (816 bit	s), 102 bytes (	aptured (816 bits)	on interface	capture u	9 1. id 0			0	000 58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 Xw.P Vf
5	Ethernet II, Src: VMware 9d:e8:be	00:50:56:9d:e8	be), Dst: Cisco b9:	77:0e (58:97:	bd:b9:77:	3e)			0	010 08 00 45 00 00 54 9d ec 40 00 40 01 af c0 c0 00 ··E··T··@·@····
4	802.10 Virtual LAN, PRI: 0, DEI: 0.	ID: 102				,			0	020 02 64 c6 33 64 64 08 00 4e a2 00 1a 00 07 f4 64 ·d·3dd·· N·····d
	000 = Priority:	Best Effort (de	fault) (0)	-					0	030 ce 62 00 00 00 00 20 a2 07 00 00 00 00 00 10 11 ·b·····
	0 = DEI: Ineli	gible		21					0	040 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 I
	0000 0110 0110 = ID: 102			- I						050 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$X&"() "+,/01
	Type: IPv4 (0x0800)									32 55 54 55 50 37 Z34567
>	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst	: 198.51.100.100							
>	Internet Control Message Protocol			2						
1										

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.

- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt een extra poort VLAN-tag **1001 in** die de toegangsinterface Portchannel1 identificeert.
- 4. Op de switch staat een extra VN-tag.

				0									
No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info					^
<b>C</b>	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e	(12846)	64 Echo (ping) r	equest	id=0x002d,	seq=245/62720,	ttl=64 (r	nc
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e	(12846)	64 Echo (ping) r	equest	id=0x002d,	seq=245/62720,	ttl=64 (r	nc
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	Øx32b9	(12985)	64 Echo (ping) r	equest	id=0x002d,	seq=246/62976,	ttl=64 (r	nc
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	0x32b9	(12985)	64 Echo (ping) r	equest	id=0x002d,	seq=246/62976,	ttl=64 (r	nc
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	Øx32d8	(13016)	64 Echo (ping) r	equest	id=0x002d,	seq=247/63232,	ttl=64 (r	nc
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8	(13016)	64 Echo (ping) r	equest	id=0x002d,	seq=247/63232,	ttl=64 (r	nc
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373	(13171)	64 Echo (ping) r	equest	id=0x002d,	seq=248/63488,	ttl=64 (r	nc
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	Øx3373	(13171)	64 Echo (ping) r	equest	id=0x002d,	seq=248/63488,	ttl=64 (r	nc
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427	(13351)	64 Echo (ping) r	equest	id=0x002d,	seq=249/63744,	ttl=64 (r	nc
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427	(13351)	64 Echo (ping) r	equest	id=0x002d,	seq=249/63744,	ttl=64 (r	nc
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	Øx34de	(13534)	64 Echo (ping) r	equest	id=0x002d,	seq=250/64000,	ttl=64 (r	nc
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	Øx34de	(13534)	64 Echo (ping) r	equest	id=0x002d,	seq=250/64000,	ttl=64 (r	nc
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c	(13644)	64 Echo (ping) r	equest	id=0x002d,	seq=251/64256,	ttl=64 (r	nc
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c	(13644)	64 Echo (ping) r	equest	id=0x002d,	seq=251/64256,	ttl=64 (r	nc
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602	(13826)	64 Echo (ping) r	equest	id=0x002d,	seq=252/64512,	ttl=64 (r	nc
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602	(13826)	64 Echo (ping) r	equest	id=0x002d,	seq=252/64512,	ttl=64 (r	nc
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	Øx36ed	(14061)	64 Echo (ping) r	equest	id=0x002d,	seq=253/64768,	ttl=64 (r	nc
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	Øx36ed	(14061)	64 Echo (ping) r	equest	id=0x002d,	seq=253/64768,	ttl=64 (r	nc
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5	(14293)	64 Echo (ping) r	equest	id=0x002d,	seq=254/65024,	ttl=64 (r	nc ~
<													>
> Fr	ame 1: 108 bytes on wire (864 bits)	, 108 bytes capt	tured (864 bits) on	interface	capture_u0_3,	i 0000	a2 76	f2 00 00 25 00 50 5	5 9d e8 b	e 89 26 80	54 · v · · · % · P	V · · · · & · T	
> Et	hernet II, Src: VMware_9d:e8:be (00	:50:56:9d:e8:be)	), Dst: a2:76:f2:00	:00:25 (a2	:76:f2:00:00:2	5) 0010	00 00	81 00 03 e9 08 00 4	00 00 5	54 32 2e 40	00	E	
VN VN	-Tag					0020	40 01	1b 7f c0 00 02 64 c	33 64 6	54 08 00 1e	d6 @d	· 3dd · · · ·	
	1	= Directio	n: From Bridge			0030	00 2d	00 f5 a6 a2 ed 62 0	00 00 0	90 7a 2f 0b	00 ·-···b	····z/··	
	.0	= Pointer:	vif_id			0040	00 00	00 00 10 11 12 13 1	15 16 1	17 18 19 1a	10	49/01/38.	
	00 0000 0101 0100	= Destinat	ion: 84			0050	1C 10	10 1f 20 21 22 23 2	25 26 2	27 28 29 2a	20	\$%& ()"+ 4567	
	····· ···· ···· ···· 0 ····	<pre> = Looped:</pre>	No 4			0000	20 20	26 51 20 21 22 22 24	55 50 5		,/0125	4307	
	0	= Reserved	: 0										
	00	<pre> = Version:</pre>	0										
	0000 0000	0000 = Source:	0										
	Type: 802.10 Virtual LAN (0x8100)												
× 80	2.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 1001											
	000 Beriority: Be	st Effort (defau	lt) (0)										
	0 = DEI: Ineligi	ble	2										
	0011 1110 1001 = ID: 1001		5										
	Type: IPv4 (0x0800)												
: In	ternet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	198.51.100.100 🚬										
: In	ternet Control Message Protocol		2										
_													

Selecteer het tweede pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-pakketten voor echoverzoek worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt een extra poort VLAN-tag **1001 in** die de toegangsinterface Portchannel1 identificeert.

No.	Time	Source	Destination	Protocol	Length	IP ID		IP T	TL Info			1				^
<b>_</b>	1 2022-08-05 23:07:31.865872877	192.0.2.100	198.51.100.100	ICMP	108	Øx322e	(12846)		64 Echo	(ping)	request	id=0x002d,	seq=245/62726	), ttl=64	(nc	
	2 2022-08-05 23:07:31.865875131	192.0.2.100	198.51.100.100	ICMP	102	Øx322e	(12846)		64 Echo	(ping)	request	id=0x002d,	seq=245/62726	), ttl=64	(nc	
	3 2022-08-05 23:07:32.867144598	192.0.2.100	198.51.100.100	ICMP	108	Øx32b9	(12985)		64 Echo	(ping)	request	id=0x002d,	seq=246/62976	, ttl=64	(nc	
	4 2022-08-05 23:07:32.867145852	192.0.2.100	198.51.100.100	ICMP	102	Øx32b9	(12985)		64 Echo	(ping)	request	id=0x002d,	seq=246/62976	, ttl=64	(nc	
	5 2022-08-05 23:07:33.881902485	192.0.2.100	198.51.100.100	ICMP	108	0x32d8	(13016)		64 Echo	(ping)	request	id=0x002d,	seq=247/63232	2, ttl=64	(nc	
	6 2022-08-05 23:07:33.881904191	192.0.2.100	198.51.100.100	ICMP	102	0x32d8	(13016)		64 Echo	(ping)	request	id=0x002d,	seq=247/63232	2, ttl=64	(nc	
	7 2022-08-05 23:07:34.883049425	192.0.2.100	198.51.100.100	ICMP	108	Øx3373	(13171)		64 Echo	(ping)	request	id=0x002d,	seq=248/63488	3, ttl=64	(nc	
	8 2022-08-05 23:07:34.883051649	192.0.2.100	198.51.100.100	ICMP	102	Øx3373	(13171)		64 Echo	(ping)	request	id=0x002d,	seq=248/63488	3, ttl=64	(nc	
	9 2022-08-05 23:07:35.883478016	192.0.2.100	198.51.100.100	ICMP	108	0x3427	(13351)		64 Echo	(ping)	request	id=0x002d,	seq=249/63744	, ttl=64	(nc	
	10 2022-08-05 23:07:35.883479190	192.0.2.100	198.51.100.100	ICMP	102	0x3427	(13351)		64 Echo	(ping)	request	id=0x002d,	seq=249/63744	, ttl=64	(nc	
	11 2022-08-05 23:07:36.889741625	192.0.2.100	198.51.100.100	ICMP	108	0x34de	(13534)		64 Echo	(ping)	request	id=0x002d,	seq=250/64000	), ttl=64	(nc	
	12 2022-08-05 23:07:36.889742853	192.0.2.100	198.51.100.100	ICMP	102	0x34de	(13534)		64 Echo	(ping)	request	id=0x002d,	seq=250/64000	), ttl=64	(nc	
	13 2022-08-05 23:07:37.913770117	192.0.2.100	198.51.100.100	ICMP	108	0x354c	(13644)		64 Echo	(ping)	request	id=0x002d,	seq=251/64256	5, ttl=64	(nc	
	14 2022-08-05 23:07:37.913772219	192.0.2.100	198.51.100.100	ICMP	102	0x354c	(13644)		64 Echo	(ping)	request	id=0x002d,	seq=251/64256	, ttl=64	(nc	
	15 2022-08-05 23:07:38.937829879	192.0.2.100	198.51.100.100	ICMP	108	0x3602	(13826)		64 Echo	(ping)	request	id=0x002d,	seq=252/64517	2, ttl=64	(nc	
	16 2022-08-05 23:07:38.937831215	192.0.2.100	198.51.100.100	ICMP	102	0x3602	(13826)		64 Echo	(ping)	request	id=0x002d,	seq=252/64517	2, ttl=64	(nc	
	17 2022-08-05 23:07:39.961786128	192.0.2.100	198.51.100.100	ICMP	108	0x36ed	(14061)		64 Echo	(ping)	request	id=0x002d,	seq=253/64768	3, ttl=64	(nc	
	18 2022-08-05 23:07:39.961787284	192.0.2.100	198.51.100.100	ICMP	102	0x36ed	(14061)		64 Echo	(ping)	request	id=0x002d,	seq=253/64768	3, ttl=64	(nc	
	19 2022-08-05 23:07:40.985773090	192.0.2.100	198.51.100.100	ICMP	108	0x37d5	(14293)		64 Echo	(ping)	request	id=0x002d,	seq=254/65024	4, ttl=64	(nc	~
<															>	
>	Frame 2: 102 bytes on wire (816 bits)	), 102 bytes capt	ured (816 bits) on	interface cap	ture u0 3,	i 0000	a2 76	f2 00	00 25 (	<b>80 50</b>	56 9d e8	be 81 00 03	e9 ·v···%·	P V		
>	Ethernet II, Src: VMware_9d:e8:be (00	3:50:56:9d:e8:be)	, Dst: a2:76:f2:00	:00:25 (a2:76:	f2:00:00:2	25) 0010	08 00	45 00	00 54 3	32 2e	40 00 40	01 1b 7f ce	00 ··E··T2	. @.@	-	
	802.1Q Virtual LAN, PRI: 0, DEI: 0, 1	ID: 1001				0020	02 64	c6 33	64 64 6	98 99	1e d6 00	2d 00 f5 a6	a2 ·d·3dd·		-	
	000 Be	st Effort (defau	lt) (0)			0030	ed 62	00 00	00 00 7	7a 2f	0b 00 00	00 00 00 10	) 11 ·b····z/	/		
	0 = DEI: Ineligi	ble	3			0040	12 13	14 15	16 17 1	18 19	1a 1b 1c	1d 1e 1f 20	21			
ш	0011 1110 1001 = ID: 1001		-			0050	22 23	24 25	26 27 2	28 29	2a 20 2C	2d 2e 2f 30	31 #\$%& (	) "+,/0	1	
н.	Type: IPv4 (0x0800)					0000	32 33	34 35	30 37				234507			
I h	Internet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	98.51.100.100													
H	Internet Control Message Protocol		2													

### Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. In het opnamebestand wordt het pakket met de VN-tag echter eerder weergegeven dan het pakket met de poort VLAN-tag.

In deze tabel wordt de taak samengevat:

Taak	Opnamep unt	Interne poort VLAN in opgenomen pakketten	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op interface Ethernet1/2	Ethernet1/ 2	102	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100
Configureer en controleer een pakketopname op interface Portchannel1 met lidinterfaces Ethernet1/4 en Ethernet1/5	Ethernet1/ 4 Ethernet1/ Ethernet5	1001	Alleen inspringen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.

## PacketCaptures op backplane interfaces

Gebruik FCM en CLI om een pakketopname op backplane interfaces te configureren en te verifiëren.

#### Topologie, pakketstroom en de opnamepunten



### Configuratie

#### FCM

Volg deze stappen op FCM om pakketopnamen op backplane interfaces te configureren:

1. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Inte	erfaces	Logical Devices	Security Engine	Platform Settings		Syster	n Tools	Help	admin
						Packet Capture	Troubl	eshooti	ng Logs
Capture Session	Filter Lis	t							
					C Refresh	Capture Session De	ete All Sessi	ons	
No Session available	9								

2. Als u pakketten op alle backplane interfaces wilt opnemen, selecteert u de toepassing en vervolgens Alle backplane poorten uit de vervolgkeuzelijst Capture On. U kunt ook de specifieke backplane interface kiezen. In dit geval zijn backplane interfaces Ethernet1/9 en Ethernet1/10 beschikbaar. Geef de sessienaam op en klik op Opslaan en Uitvoeren om de opname te activeren:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings		System Tools Help admi	n
Select an ins	tance: ftd1	~				Save and Run Save Cancel	
ftd1					Session Name*	cap1	
					Selected Interfaces	None	
Ethernet1/2					Buffer Size	256 MB 👻	
	0				Snap length:	1518 Bytes	
					Store Packets	Overwrite Append	
					Capture On	Al Backplane Ports	
Ethernet1/3				<b>.</b>		ftd Ethernet1/9	
	G			FTD Ethernet1/9, Ethernet1/10	Capture Filter	Ethernet1/10	
						Al Backplane Ports	
Ethomost /1							
Ethemet1/1							

## **FXOS CLI**

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

firepower# firepower App Name Deploy Typ	firepower# <b>scope ssa</b> firepower /ssa# <b>show app-instance</b> App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role										
ftd Native	ftd1 No	1 	Enabled Not Appl	Online Licable 1	None	7.2.0.82	7.2.0.82				
2. Een	opnameses	ssie maken:									
firepower#	scope pack	et-capture									
firepower	/packet-cap	oture # <b>crea</b>	te session o	ap1							
firepower	/packet-cap	oture/sessio	n* <b># create</b>	phy-port	Eth1/9						
firepower	/packet-cap	oture/sessio	n/phy-port*	<pre># set app</pre>	o ftd						
firepower	/packet-cap	oture/sessio	n/phy-port*	# set app	p-identifie	er ftd1					
firepower	/packet-cap	oture/sessio	n/phy-port*	# up							
firepower	/packet-cap	oture/sessio	n* # <b>create</b>	phy-port	t Eth1/10						
firepower	/packet-cap	ture/sessio	n/phy-port*	# set app	o ftd						
firepower	/packet-cap	oture/sessio	n/phy-port*	# set app	p-identifie	er ftd1					

```
firepower /packet-capture/session/phy-port* # up
firepower /packet-capture/session* # enable
firepower /packet-capture/session* # commit
firepower /packet-capture/session #
Verificatie
```

#### FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

Overview	Interfaces	Logical Devices Se	ecurity Engine	Platform Settings				System To	ols Help	admin
Capture Ses	sion Filter L	ist								
							Capture Session	Delete Al Sess	ions	
•	cap1	Drop Count: 0	)	Operational State: up	Buffer Size: 256 M	18	Snap Length: 1518 Bytes			8
Interface Na	ame	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	*			
L										

### **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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
```

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. Zorg er bij meer dan 1 backplane interface voor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Selecteer het eerste en het tweede pakket en controleer de belangrijkste punten:

- 1. Elk pakket met ICMP-echoverzoek wordt opgenomen en 2 keer weergegeven.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **103 in** die de uitgaande interface Ethernet1/3 identificeert.
- 4. Op de switch staat een extra VN-tag.

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	Øxcc2c (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	Øxcc2c (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	0xcc9b (52379)	64 Echo (ping)	reply	id=0x0001, seq=16/4096, ttl=64 (request in 6)
8 2022-07-14 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52379)	64 Echo (ping)	reply	id=0x0001, seq=16/4096, ttl=64
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	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	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	0xce36 (52790)	64 Echo (ping)	reply	id=0x0001, seq=20/5120, ttl=64 (request in 22)
24 2022-07-14 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52790)	64 Echo (ping)	reply	id=0x0001, seq=20/5120, ttl=64
25 2022-07-14 20:20:42.657709898	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	0xce49 (52809)	64 Echo (ping)	reply	id=0x0001, seq=21/5376, ttl=64 (request in 26)
28 2022-07-14 20:20:42.657981971	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52809)	64 Echo (ping)	reply	id=0x0001, seq=21/5376, ttl=64
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!)
ć		_						
> Frame 1: 108 bytes on wire (864 bits	s), 108 bytes ca	aptured (864 bits)	on interface o	apture u	0 8. id 0			000 00 50 56 9d e7 50 58 97 bd b9 77 2d 89 26 00 00 -PV-PX
> Ethernet II, Src: Cisco b9:77:2d (5)	8:97:bd:b9:77:2d	d). Dst: VMware 9d:	e7:50 (00:50:5	6:9d:e7:	50)		0	010 00 0a 81 00 00 67 08 00 45 00 00 54 59 90 40 00g. E. TY @-
VN-Tag		·// ····			/		0	020 40 01 f4 1c c0 00 02 64 c6 33 64 64 08 00 22 68 @·····d ·3dd··"h
0	= Direct	ion: To Bridge					0	030 00 01 00 0f 89 7a d0 62 00 00 00 00 b3 d7 09 00 ·····z·b ······
.0	= Pointe	r: vif id					0	040 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b ······
	= Destin	ation: 0					0	050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
	= Looped	: No	A				0	060 2C 2d 2e 2t 30 31 32 33 34 35 36 37 ,/0123 4567
	= Reserv	ed: 0	4 I					
	= Versio	n: 0						
0000 000	0 1010 = Source	: 10						
Type: 802.10 Virtual LAN (0x8100)								
✓ 802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 103							
000 Briority: B	Best Effort (def	ault) (0)						
0 = DEI: Inelig	ible		2					
0000 0110 0111 = ID: 103			- I					
Type: IPv4 (0x0800)								
> Internet Protocol Version 4, Src: 19	92.0.2.100, Dst:	: 198.51.100.100						
> Internet Control Message Protocol			2					

No.	Time	Source	Destination	Protocol	Length	PD		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)	
4-	3 2022-07-14 20:20:36.514117394	198.51.100.10	9 192.0.2.100	ICMP	108	0xcc2c	(52268)	64 Echo	(ping)	reply	id=0x0001	, seq=15/3840,	ttl=64	(request in 2)	
	4 2022-07-14 20:20:36.514119312	198.51.100.10	0 192.0.2.100	ICMP	108	Øxcc2c	(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	9 192.0.2.100	ICMP	108	0xcc9b	(52379)	64 Echo	(ping)	reply	id=0x0001	, seq=16/4096,	ttl=64	(request in 6)	
	8 2022-07-14 20:20:37.538048311	198.51.100.10	9 192.0.2.100	ICMP	108	0xcc9b	(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,	tt1=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	198.51.100.10	3 192.0.2.100	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	198.51.100.10	0 192.0.2.100	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	9 192.0.2.100	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	9 192.0.2.100	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,	tt1=64	(reply in 19)	
	19 2022-07-14 20:20:40.610179685	198.51.100.10	3 192.0.2.100	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	198.51.100.10	0 192.0.2.100	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	0 192.0.2.100	ICMP	108	0xce36	(52790)	64 Echo	(ping)	reply	id=0x0001	, seq=20/5120,	tt1=64	(request in 22)	
	24 2022-07-14 20:20:41.634085368	198.51.100.100	9 192.0.2.100	ICMP	108	0xce36	(52790)	64 Echo	(ping)	reply	id=0x0001	, seq=20/5120,	tt1=64		
	25 2022-07-14 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0	(23536)	64 Echo	(ping)	request	id=0x0001	, seq=21/5376,	tt1=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	1d=0x0001	, seq=21/5376,	tt1=64	(reply in 27)	
	27 2022-07-14 20:20:42.657980675	198.51.100.10	3 192.0.2.100	ICMP	108	0xce49	(52809)	64 Echo	(ping)	reply	id=0x0001	, seq=21/5376,	tt1=64	(request in 26)	
	28 2022-07-14 20:20:42.657981971	198.51.100.10	9 192.0.2.100	ICMP	108	0xce49	(52809)	64 Echo	(ping)	reply	1d=0x0001	, seq=21/5376,	tt1=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	1d=0x0001	, seq=22/5632,	tt1=64	(no response found!)	
<															
>	Frame 2: 108 bytes on wire (864 bit	s), 108 bytes (	captured (864 bits)	) on int	erface capture_u	u0_8, id	0			6	000 <b>00 50</b>	56 9d e7 50 5	8 97 bo	1 b9 77 2d 89 26 00 00	·PV ··PX · ··w ··& ··
>	Ethernet II, Src: Cisco b9:77:2d (5	8:97:bd:b9:77:	2d), Dst: VMware 9	d:e7:50	(00:50:56:9d:e7:	:50)				6	0010 00 0a	81 00 00 67 0	8 00 45	5 00 00 54 59 90 40 00	·····g·· E··TY·@·
4	VN-Tag									6	0020 40 01	f4 1c c0 00 0	2 64 ct	5 33 64 64 08 00 22 68	@·····d ·3dd··"h
	0	= Direc	tion: To Bridge							0	0030 <b>00 01</b>	00 0f 89 7a d	0 62 0	0 00 00 00 b3 d7 09 00	·····z·b ·····
	.0	= Point	er: vif_id								0040 00 00	00 00 10 11 1	2 13 14	15 16 17 18 19 1a 10	1"# #901/18.
		= Desti	nation: 0								0050 1C 10	10 1f 20 21 2	2 23 24	25 26 27 28 29 28 20	
	···· ··· ··· ··· ··· 0 ····	= Loope	d: No	4							20 20	20 21 50 51 5			y-1/0125 4507
	0	= Reser	ved: 0	- 1											
		= Versi	on: 0												
	0000 000	90 1010 = Sourc	e: 10												
	Type: 802.1Q Virtual LAN (0x8100)	)													
М	802.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 103		_											
11	000 = Priority: E	Best Effort (de	fault) (0)												
11	0 = DEI: Inelig	gible		31											
11	0000 0110 0111 = ID: 103			-											
L	Type: IPv4 (0x0800)		. 100 51 100 100												
P	Internet Protocol Version 4, Src: 1	92.0.2.100, DS	t: 198.51.100.100	2											
2	Internet control Message Protocol			4											
Ц															

Selecteer het derde en vierde pakket en controleer de belangrijkste punten:

- 1. Elk ICMP-echoantwoord wordt opgenomen en 2 keer weergegeven.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de uitgangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

					_	-									
No.	Time		Source	Destination	Protocol	Length	PD	IP TTL Info							
-	1 2022-07-14	4 20:20:36.513854256	192.0.2.100	198.51.100.100	ICMP	108	0x5990 (22	2928) 64 Echo	(ping)	request	id=0x000:	, seq=15/384	0, ttl=64	(no response found!)	
-	2 2022-07-14	4 20:20:36.513857289	192.0.2.100	198.51.100.100	ICMP	108	8x5998 (22	2928) 64 Echo	(ning)	request	id=0x000	, seg=15/384	0, ttl=64	(reply in 3)	
-	3 2022-07-14	4 20:20:36.514117394	198,51,100,100	192.0.2.100	ICMP	108 1	0xcc2c (52	2268) 64 Echo	(ping)	reply	id=0x000	, seg=15/384	a, ttl=64	(request in 2)	
	4 3033-07-14	1 20-20-26 514110212	100 51 100 100	102 0 2 100	TCMD	109	0xcc2c (52	(2269) 64 Echo	(ning)	reply	id-exees	£00=15/20A	a ++1-64	(. equeve an ey	
	4 2022-07-14	20.20.30.314119312	198.51.100.100	192.0.2.100	TCHP	100	0xcc2c (52	2200) 04 ECHO	(prug)	repry	id-outpool	, seq=15/304	o, tt1-04	(as assessed found))	
	5 2022-07-14	4 20:20:37.537723822	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23	3040) 64 Echo	(ping)	request	10=0x000	, seq=16/409	5, tt1=64	(no response round1)	
	6 2022-07-14	4 20:20:37.537726588	192.0.2.100	198.51.100.100	ICMP	108	0x5a00 (23	3040) 64 Echo	(ping)	request	1d=0x000	, seq=16/409	6, ttl=64	(reply in 7)	
	7 2022-07-14	4 20:20:37.538046165	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52	2379) 64 Echo	(ping)	reply	id=0x000	l, seq=16/409	6, ttl=64	(request in 6)	
	8 2022-07-14	4 20:20:37.538048311	198.51.100.100	192.0.2.100	ICMP	108	0xcc9b (52	2379) 64 Echo	(ping)	reply	id=0x000	l, seq=16/409	6, ttl=64		
	9 2022-07-14	4 20:20:38.561776064	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23	3223) 64 Echo	(ping)	request	id=0x000	, seq=17/435	2, ttl=64	(no response found!)	
	10 2022-07-14	4 20:20:38.561778310	192.0.2.100	198.51.100.100	ICMP	108	0x5ab7 (23	3223) 64 Echo	(ping)	request	id=0x000	, seg=17/435	2. ttl=64	(reply in 11)	
	11 2022-07-14	4 20:20:38,562048288	198,51,100,100	192.0.2.100	ICMP	108	Oxccc4 (52	2420) 64 Echo	(ping)	reply	id=0x000	, seg=17/435	2. ttl=64	(request in 10)	
	12 2022-07-14	4 20:20:38.562050333	198,51,100,100	192.0.2.100	TCMP	108	Oxccc4 (52	2420) 64 Echo	(ping)	reply	id=0x000	seg=17/435	2. ttl=64		
	13 2022-07-14	1 20-20-30 595677043	102 0 2 100	108 51 100 100	TCMD	109	avsha6 (22	3366) 64 Echo	(ning)	request	id-avaaa	500-19/460	e ++1-64	(no response found))	
	13 2022-07-14	4 20:20:39:383077043	192.0.2.100	198.51.100.100	TCHP	108	0,3040 (23	3300) 04 ECHU	(ping)	request	10=0x000	, seq=18/400	o, ttl=04	(no response round)	
	14 2022-07-14	4 20:20:39.585678455	192.0.2.100	198.51.100.100	ICMP	108	0X5046 (23	3306) 64 ECNO	(ping)	request	1d=0x000	, seq=18/460	8, ttl=64	(reply in 15)	
	15 2022-07-14	4 20:20:39.585936554	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52	2621) 64 Echo	(ping)	reply	1d=0x000	, seq=18/460	8, ttl=64	(request in 14)	
	16 2022-07-14	4 20:20:39.585937900	198.51.100.100	192.0.2.100	ICMP	108	0xcd8d (52	2621) 64 Echo	(ping)	reply	id=0x000	, seq=18/460	8, ttl=64		
	17 2022-07-14	4 20:20:40.609804804	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23	3419) 64 Echo	(ping)	request	id=0x000	, seq=19/486	4, ttl=64	(no response found!)	
	18 2022-07-14	4 20:20:40.609807618	192.0.2.100	198.51.100.100	ICMP	108	0x5b7b (23	3419) 64 Echo	(ping)	request	id=0x000	, seq=19/486	4, ttl=64	(reply in 19)	
	19 2022-07-14	4 20:20:40.610179685	198.51.100.100	192.0.2.100	ICMP	108	0xcd8f (52	2623) 64 Echo	(ping)	reply	id=0x000	, seg=19/486	4, ttl=64	(request in 18)	
	20 2022-07-14	4 20:20:40.610181944	198,51,100,100	192.0.2.100	TCMP	198	excdaf (52	2623) 64 Echo	(ping)	reply	id=exeee	seg=19/486	4. ttl=64		
	21 2022-07-14	1 20-20-41 622005152	102 0 2 100	109 51 100 100	TCMD	109	Ovsh7e (22	(422) 64 Echo	(ning)	request	id-avaaa	500=20/512	a ++1-64	(no response found))	
	22 2022-07-14	20.20.41 63300607	102 0 2 100	100 51 100 100	TCHO	100	0x507e (25	3422) 04 Echo	(ping)	request	id-0x000	, seq-20/512	0, ++1-64	(no response roundry	
	22 2022-07-14	4 20:20:41.055800997	192.0.2.100	198.51.100.100	ICHP	108	0,5070 (25	Sazz) Galecho	(brug)	request	10-00000	, seq=20/512	0, LLI-04	(reply in 25)	
	23 2022-07-14	4 20:20:41.634084102	198.51.100.100	192.0.2.100	TCMP	108	0xce36 (52	2790) 64 Echo	(ping)	repty	10=0x000	, seq=20/512	0, tt1=64	(request in 22)	
	24 2022-07-14	4 20:20:41.634085368	198.51.100.100	192.0.2.100	ICMP	108	0xce36 (52	2790) 64 Echo	(ping)	reply	1d=0x000	, seq=20/512	0, ttl=64		
	25 2022-07-14	4 20:20:42.657709898	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23	3536) 64 Echo	(ping)	request	id=0x000:	l, seq=21/537	6, ttl=64	(no response found!)	
	26 2022-07-14	4 20:20:42.657711660	192.0.2.100	198.51.100.100	ICMP	108	0x5bf0 (23	3536) 64 Echo	(ping)	request	id=0x000	, seq=21/537	6, ttl=64	(reply in 27)	
	27 2022-07-14	4 20:20:42.657980675	198.51.100.100	192.0.2.100	ICMP	108	0xce49 (52	2809) 64 Echo	(ping)	reply	id=0x000	, seq=21/537	6, ttl=64	(request in 26)	
	28 2022-07-14	4 20:20:42.657981971	198,51,100,100	192.0.2.100	ICMP	108	0xce49 (52	2809) 64 Echo	(ping)	reply	id=0x000	, seg=21/537	6. ttl=64		
	29 2022-07-14	1 20:20:43.681736697	192.0.2.100	198.51.100.100	TCMP	108	8x5c52 (23	3634) 64 Echo	(ning)	request	id=exeee	seq=22/563	2. ttl=64	(no response found!)	
	LO LOLL OF L		1011011100			100	CHIPCOL (LD		(1940-0)	. equese		i) bed reises		(no response roundry	
<															
> F	rame 3: 108 b	vtes on wire (864 bit	s), 108 bytes ca	ptured (864 bits)	on interf	face capture u0	8, id 0				000 00 54	56 9d e8 be	58 97 b	d b9 77 0e 89 26 00 00	·PV···X· ··w··&··
> E	thernet II. S	rc: Cisco b9:77:0e (5	8:97:bd:b9:77:0e	), Dst: VMware 9d:	e8:be (00	a:50:56:9d:e8:b	e)				0010 00 0	81 00 00 66	08 00 4	5 00 00 54 cc 2c 00 00	·····f·· E··T·,··
J v	M-Tag			,,			-,				0020 40 0	c1 80 c6 33	64 64 c	0 00 02 64 00 00 2a 68	@3dd*h
	a		- Direct	ion: To Bridge							00 00 0000	00 0f 89 7a	d0 62 0	0 00 00 00 b3 d7 09 00	·····z·b ······
	0		· ···· = Direct	ion: to Bridge							0040 00 0	00 00 10 11	12 13 1	4 15 16 17 18 19 1a 1b	
	.0		= Pointe	r: v1f_10							0050 1c 1	1e 1f 20 21	22 23 2	4 25 26 27 28 29 2a 2b	···· !"# \$%8'()"+
	00 0000 00		= Destin	ation: 0							0060 2c 2	2e 2f 30 31	32 33 3	4 35 36 37	/0123 4567
		0	= Looped	: No	<b>4</b> I										,
		0	= Reserv	ed: 0	<b>-</b>										
			= Versio	n: 0											
			0 1010 = Source	: 10											
	Type: 802.10	Victual LAN (0x8100)													
	102 10 Vietual	IAN DET & DET &	10: 102												
10	002.10 1110001	Char, Phil. 0, Dell. 0,	10. 10z	···14) (0)	_										
	000	= Priority: E	est Effort (def	auit) (0)	<u> </u>										
	0	= DEI: Inelig	ible		31										
	0000 01	110 0110 = ID: 102			-										
L	Type: IPv4 (	(0x0800)													
> 1	internet Proto	col Version 4, Src: 1	98.51.100.100, [	st: 192.0.2.100											
> 1	Internet Contr	ol Message Protocol			2										
					_										
-															

## Uitleg

Wanneer een pakketopname op een backplane interface is geconfigureerd, neemt de switch elk pakket twee keer op. In dit geval ontvangt de switch binnen de poort pakketten die al door de toepassing op de beveiligingsmodule zijn gelabeld met de port VLAN-tag en de VN-tag. De VLAN-tag identificeert de uitgangsinterface die het interne chassis gebruikt om de pakketten naar het netwerk te doorsturen. De VLAN-tag 103 in ICMP-echoverdrachtpakketten identificeert Ethernet1/3 als de uitgangsinterface, terwijl VLAN-tag 102 in ICMP-echoantwoordpakketten Ethernet1/2 als de uitgangsinterface identificeert. De switch verwijdert de VN-tag en de interne VLAN-tag voordat de pakketten naar het netwerk worden doorgestuurd.

In deze tabel wordt de taak samengevat:

Taak	Opname punt	Interne poort VLAN in opgenomen pakketten	Richtin g	Opgenomen verkeer
Configureer en controleer pakketopnamen op backplane interfaces	Backpla ne interface s	102 103	Alleen insprin gen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.10 ICMP-echoantwoorden van hos 198.51.100.100 op host 192.0.2

## Packet Capture op toepassingen en toepassingspoorten

Het pakket van de toepassing of van de toepassingspoort wordt altijd gevormd op backplane interfaces en bovendien op de voorinterfaces als de gebruiker de richting van de toepassingsopname specificeert.

Er zijn voornamelijk 2 gevallen van gebruik:

- Configureer pakketopnamen op backplane interfaces voor pakketten die een specifieke frontinterface verlaten. Configureer bijvoorbeeld pakketopnamen op de backplane interface Ethernet1/9 voor pakketten die interface Ethernet1/2 verlaten.
- Configureer de gelijktijdige pakketopname op een specifieke voorinterface en de backplane interfaces. Configureer bijvoorbeeld gelijktijdige pakketopname op interface Ethernet1/2 en op de backplane interface Ethernet1/9 voor pakketten die interface Ethernet1/2 verlaten.

Deze paragraaf behandelt beide gebruiksgevallen.

## Taak 1

Gebruik de FCM en CLI om een pakketopname op de backplane interface te configureren en te verifiëren. Pakketten waarvoor de toepassingspoort Ethernet1/2 is geïdentificeerd als de uitgangsinterface worden opgenomen. In dit geval worden ICMP-antwoorden opgenomen.

### Topologie, pakketstroom en de opnamepunten



### Configuratie

#### FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

2. Selecteer de toepassing, **Ethernet1/2** in de vervolgkeuzelijst **Toepassingspoort** en selecteer **Uitgangspakket** in de **richting Toepassingsopname**. Geef de **sessienaam op** en klik op **Opslaan en Uitvoeren** om de opname te activeren:

Overview Interraces Logical Devices Security Engine Platform Settings	System loois Help admin
Select an instance: ftd1 ×	Save and Run Save Cancel
ftd1	Session Name* cap1
	Selected Interfaces None Buffer Size 256 MB
Ethemeti/2	Snap length: 1518 Bytes Store Packets Overwrite Append
Ethernet1/3 FTD Ethernet1/9, Ethernet1/10	Capture On ftd v Application Port Ethernet1/2 v Application Capture Direction All Packets Egress Packet
Ethematl/1	Capture Filter Apply Filter Capture All

## **FXOS CLI**

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

firepower#	scope sa	a					
firepower	/ssa# <b>s</b> ł	low app-ins	tance				
App Name	Identifi	er Slot ID	Admin Stat	e Oper S	State	Running Versi	on Startup Version
Deploy Typ	e Turbo M	Node Profil	e Name Cluster	State	Cluster R	ole	
ftđ	ftd1	1	Enabled	Online	e	7.2.0.82	7.2.0.82
Native	No		Not App	licable	None		
2. Een	opnames	essie mak	en:				
	•						
firepower#	scope pa	icket-captu	re				
firepower	/packet-c	apture # <b>c</b>	reate session	cap1			
firepower	/packet-c	apture/ses	sion* # create	арр-ро	rt 1 112 Et	hernet1/2 ftd	
firepower	/packet-c	apture/ses	sion/app-port*	# set a	app-identif	ier ftd1	
firepower	/packet-c	apture/ses	sion/app-port*	# set f	filter ""		
firepower	/packet-c	apture/ses	sion/app-port*	# set s	subinterfac	e 0	
firepower	/packet-c	apture/ses	sion/app-port*	# up			
firepower	/packet-c	apture/ses	sion* # commit				
firepower	/packet-c	apture/ses	sion #				
Verificatie	)						

#### FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

ſ	Overview	Interfaces	Logical Devices	Security Engine	Platform Setti	ngs					System Too	ls Help	admin
1	Capture Ses	sion Fiter Lis	t										
									C Refresh Capt	ure Session	Delete All Sessi	ons	
[	•	cap1	Drop Count	t: 0	Operational St	ate: up	Buffer Size: 256 MB			Bytes			8
	Interface N	ame	Filter		File Si	ize (in bytes)	File Name	Device Name					
	Ethernet1/2	- Ethernet1/10	None		576		cap1-vethernet-1175.pcap	ftd1		$\pm$			
	Ethernet1/2	- Ethernet1/9	None		4360		cap1-vethernet-1036.pcap	ftd1		⊻			

#### **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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:
```

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. In het geval van meerdere backplane interfaces, zorg ervoor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Selecteer het eerste en het tweede pakket en controleer de belangrijkste punten:

- 1. Elk ICMP-echoantwoord wordt opgenomen en 2 keer weergegeven.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de uitgangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

No. Time	Source	Destination	Protocol	Length	PD	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	y id=0x0012, seq=1/256, ttl=64
2 2022-08-01 10:03:22.231239747	198.51.100.100	192.0.2.100	ICMP	108	0x42f8 (17144)	64 Echo (ping) reply	y id=0x0012, seq=1/256, ttl=64
3 2022-08-01 10:03:23.232244769	198.51.100.100	192.0.2.100	ICMP	108	0X4303 (17331)	64 ECHO (DINR) LEDI	y id=0x0012, seq=2/512, ttl=64
4 2022-08-01 10:03:23.232247753	198.51.100.100	192.0.2.100	ICMP	108	0x43b3 (17331)	64 Echo (ping) reply	y id=0x0012, seq=2/512, ttl=64
5 2022-08-01 10:03:24.234703981	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	y id=0x0012, seq=3/768, ttl=64
6 2022-08-01 10:03:24.234706751	198.51.100.100	192.0.2.100	ICMP	108	0x445e (17502)	64 Echo (ping) reply	y id=0x0012, seq=3/768, ttl=64
7 2022-08-01 10:03:25.258672449	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	y id=0x0012, seq=4/1024, ttl=64
8 2022-08-01 10:03:25.258674861	198.51.100.100	192.0.2.100	ICMP	108	0x4464 (17508)	64 Echo (ping) reply	y id=0x0012, seq=4/1024, ttl=64
9 2022-08-01 10:03:26.282663169	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	y id=0x0012, seq=5/1280, ttl=64
10 2022-08-01 10:03:26.282666183	198.51.100.100	192.0.2.100	ICMP	108	0x44c3 (17603)	64 Echo (ping) reply	y id=0x0012, seq=5/1280, ttl=64
11 2022-08-01 10:03:27.306671694	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	y id=0x0012, seq=6/1536, ttl=64
12 2022-08-01 10:03:27.306674378	198.51.100.100	192.0.2.100	ICMP	108	0x44e7 (17639)	64 Echo (ping) reply	y id=0x0012, seq=6/1536, ttl=64
13 2022-08-01 10:03:28.330664677	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	y id=0x0012, seq=7/1792, ttl=64
14 2022-08-01 10:03:28.330667153	198.51.100.100	192.0.2.100	ICMP	108	0x4550 (17744)	64 Echo (ping) reply	y id=0x0012, seq=7/1792, ttl=64
15 2022-08-01 10:03:29.354795931	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	y id=0x0012, seq=8/2048, ttl=64
16 2022-08-01 10:03:29.354936706	198.51.100.100	192.0.2.100	ICMP	108	0x4553 (17747)	64 Echo (ping) reply	y id=0x0012, seq=8/2048, ttl=64
17 2022-08-01 10:03:30.378795204	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	y id=0x0012, seq=9/2304, ttl=64
18 2022-08-01 10:03:30.378798172	198.51.100.100	192.0.2.100	ICMP	108	0x4597 (17815)	64 Echo (ping) reply	y id=0x0012, seq=9/2304, ttl=64
19 2022-08-01 10:03:31.402772217	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18842)	64 Echo (ping) reply	y id=0x0012, seq=10/2560, ttl=64
20 2022-08-01 10:03:31.402774775	198.51.100.100	192.0.2.100	ICMP	108	0x467a (18042)	64 Echo (ping) reply	y id=0x0012, seq=10/2560, ttl=64
21 2022-08-01 10:03:32.426693254	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	y id=0x0012, seq=11/2816, ttl=64
22 2022-08-01 10:03:32.426695691	198.51.100.100	192.0.2.100	ICMP	108	0x468a (18058)	64 Echo (ping) reply	y id=0x0012, seq=11/2816, ttl=64
<pre>c Frame 1: 108 bytes on wire (864 bi Ethernet II, Src: Cisco b9:77:0e (' Wn-Tag 0</pre>	ts), 108 bytes ca 58:97:bd:b9:77:0e = Direct = Pointer	aptured (864 bits) e), Dst: VMware 9d ion: To Bridge r: vif id	) on interface 1:e8:be (00:50:	capture_u :56:9d:e8:	0_8, id 0 be)		0000         00         50         56         od         e8         58         97         bd         b9         77         0e         89         26         00         00         -         PVX-        w&-           0010         00         0a         81         00         06         66         00         05         54         24         78         00
	= Destin = Looped = Reserv = Versio 00 1010 = Source )) , ID: 102	ation: 0 : No ed: 0 n: 0 : 10	4				0050 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ····· 1"# \$%\$()*+ 0060 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,-·/0123 4567
000 = Priority: 0 = DEI: Ineli	Best Effort (defa gible	ault) (0)	3				
0000 0110 0110 = ID: 102			<b>2</b>				
Internet Protocol Version 4, Src: :	198.51.100.100, D	ost: 192.0.2.100	2				
Internet Control Message Protocol			2				
No. Time	Source	Destination	Protocol	Length	PD	19° TTL, Info	
No. Time 1 2022-08-01 10:03:22.231237959	Source 198.51.100.100	Destination 192.0.2.100	Protocol ICMP	Length 108 1	PD 0x42f8 (17144)	₽TTL №6 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747	Source 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100	Protocol ICMP ICMP	Length 108 1 108	PD 0x42f8 (17144) 0x42f8 (17144)	PTTL №0 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.232244769	Source 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP	Length 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331)	PTTL 100 64 Echo (ping) reply 64 Echo (ping) reply 04 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.331239747 3 2022-08-01 10:03:23.232244769 4 2022-08-01 10:03:23.232244753	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP	Length 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17331)	PTTL 160 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231239747 3 2022-08-01 10:03:23.23224769 4 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.2324703951	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17331) 0x445e (17502)	PTTL M0 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64
Ime         1           1         2022-08-01         10:03:22.231237959           2         2022-08-01         10:03:22.231239747           3         2022-08-01         10:03:22.231239747           4         2022-08-01         10:03:23.232247753           5         2022-08-01         10:03:24.2327533           6         2022-08-01         10:03:24.232753	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x43b3 (17331) 0x445e (17502)	PTR. №6           64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64
No.         Time           1 2022-08-01         10:03:22.23123759           2 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:23.232247753           4 2022-08-01         10:03:23.232247753           5 2022-08-01         10:03:24.234709981           6 2022-08-01         10:03:25.258672440	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 108 1 08 1 08 1 08 1	PD           0x42f8 (17144)           0x42f8 (17144)           0x43f8 (17144)           0x43b3 (17311)           0x43b3 (17331)           0x445e (17502)           0x445e (17508)           0x4464 (17508)	PTTL 160 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64
Ime           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.231239747           3 2022-08-01 10:03:23.23224706           5 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:24.2347086751           7 2022-08-01 10:03:24.2347086751           7 2022-08-01 10:03:25.2586742649           8 2022-08-01 10:03:25.2586742649	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 108 1 108 1 108 1 08 1 08 1	PD 0x42f8 (17144) 0x422f8 (17144) 0x4303 (17331) 0x445e (17502) 0x445e (17502) 0x4454 (17508) 0x4464 (17508)	PTR 26 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64
Ho.         Time           1 2022-08-01 10:03:22.231237959         2 2032-08-01 10:03:22.23123747           3 2022-08-01 10:03:22.231239747         3 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:23.232247753         5 2022-08-01 10:03:23.232247753           6 2022-08-01 10:03:23.232247753         5 2022-08-01 10:03:23.232247753           7 2022-08-01 10:03:25.258672449         8 2022-08-01 10:03:25.258672449           8 2022-08-01 10:03:25.258672461         9 2022-08-01 10:03:26.226265160	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 1 108 1 109 100 100 100 100 100 1000 1000 100000000	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4450 (17502) 0x4454 (17502) 0x4454 (17508) 0x4454 (17508) 0x4454 (17603)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1026, ttl=64
Ime           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.231237959           3 2022-08-01 10:03:23.23224709           5 2022-08-01 10:03:23.232247703           5 2022-08-01 10:03:24.23470391           6 2022-08-01 10:03:25.25867240           7 2022-08-01 10:03:25.2586724061           9 2022-08-01 10:03:25.2586724061           9 2022-08-01 10:03:26.226601309           10 2022-08-01 10:03:26.226601309	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	▶ D           0x42f8 (17144)           0x42f8 (17144)           0x43f8 (1731)           0x43b3 (1731)           0x43b3 (1731)           0x445e (17502)           0x445e (17502)           0x445e (17502)           0x445e (17508)           0x445 (17508)           0x445 (17508)           0x445 (17603)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1264, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64
In.         Time           1 2022-08-01         10:03:22.231237959           2 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:22.231239747           4 2022-08-01         10:03:23.232247753           5 2022-08-01         10:03:24.234703981           6 2022-08-01         10:03:24.234706731           7 2022-08-01         10:03:25.258672449           8 2022-08-01         10:03:25.2586746611           9 2022-08-01         10:03:26.232666169           11 2022-08-01         10:03:27.30667166413           11 2022-08-01         10:03:27.30667166413	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192. 0. 2. 100 192. 0. 2. 100	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4644 (17508) 0x4643 (17603) 0x4642 (17639)	PTI, 146           64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=6/1356, ttl=64
No.         Time           1 2022-08-01         10:03:22.231237959           2 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:22.231239747           4 2022-08-01         10:03:23.232247753           5 2022-08-01         10:03:23.232247753           6 2022-08-01         10:03:24.23470571           7 2022-08-01         10:03:25.258672449           8 2022-08-01         10:03:25.258672449           9 2022-08-01         10:03:26.282666183           11 2022-08-01         10:03:27.3066764613           12 2022-08-01         10:03:27.306674378	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol I CMP I CMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x445e (17502) 0x445e (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17633) 0x4467 (17633)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=6/1536, ttl=64
Ime           1 2022-08-01         10:03:22.231237959           2 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:23.23224706           5 2022-08-01         10:03:23.232247763           5 2022-08-01         10:03:24.23470591           6 2022-08-01         10:03:24.23470631           7 2022-08-01         10:03:24.23470631           9 2022-08-01         10:03:26.282663169           10 2022-08-01         10:03:27.306674594           12 2022-08-01         10:03:27.306674574           13 2022-08-01         10:03:28.3306646777           13 2022-08-01         10:03:28.3306646777	Source 1988, 51, 100, 100 198, 51, 100, 100	Destination 192. 0. 2. 100 192. 0. 2. 100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x43b3 (17331) 0x4456 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17639) 0x467 (17639) 0x4556 (17744)	PTI, 166           64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64 id=0x0012, seq=6/1536, ttl=64
In.         Time           1 2022-08-01         10:03:22.231237959           2 2022-08-01         10:03:22.231239747           3 0022-08-01         10:03:22.231239747           3 0022-08-01         10:03:23.232247753           5 2022-08-01         10:03:23.232247753           5 2022-08-01         10:03:24.232405713           6 2022-08-01         10:03:25.258672449           8 2022-08-01         10:03:26.232666183           10 2022-08-01         10:03:26.232666183           11 2022-08-01         10:03:27.306671604           12 2022-08-01         10:03:27.306674378           13 2022-08-01         10:03:28.3306667753           14 2022-08-01         10:03:28.330667753	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100 192.0.2.100	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x42b3 (17331) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17744) 0x4550 (17744)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=7/1792, ttl=64
Ime           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.23123747           3 2022-08-01 10:03:23.23224709           4 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:24.234709751           7 2022-08-01 10:03:25.2566724601           9 2022-08-01 10:03:25.2566724601           9 2022-08-01 10:03:25.2566724601           9 2022-08-01 10:03:25.256672461           10 2022-08-01 10:03:27.366674737           12 2022-08-01 10:03:27.366674737           13 2022-08-01 10:03:27.36654737           14 2022-08-01 10:03:28.330664575           15 2022-08-01 10:03:28.330671594           12 2022-08-01 10:03:28.330664575           14 2022-08-01 10:03:29.347999211           14 2022-08-01 10:03:29.347999211	Source 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100	Destrution 192,0,2,100 192,0,	Protocol I CNPP I CNPP	Length 108 1 108 1 109 100 100 100 100 100 100 10000000000	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (1752) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (1763) 0x4467 (1763) 0x4467 (1763) 0x467 (17743) 0x4556 (17744) 0x4555 (17744)	PTL 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64
Ime           1 2022-08-01         10:03:22.231237959           2 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:22.231239747           3 2022-08-01         10:03:22.3212247753           5 2022-08-01         10:03:22.232247753           5 2022-08-01         10:03:24.234703981           6 2022-08-01         10:03:24.23470573           8 2022-08-01         10:03:25.258672449           9 2022-08-01         10:03:26.232663169           10 2022-08-01         10:03:27.306671694           12 2022-08-01         10:03:27.306671694           13 2022-08-01         10:03:27.30667153           13 2022-08-01         10:03:27.30667153           15 2022-08-01         10:03:27.30667153           16 2022-08-01         10:03:27.30667153           16 2022-08-01         10:03:27.30667153           16 2022-08-01         10:03:27.30667153           16 2022-08-01         10:03:28.3306467153           16 2022-08-01         10:03:29.354393931           16 2022-08-01         10:03:29.354393931	Source 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100 198.51,100,100	Destination 192,0,2,100 192,0	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x4455 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4455 (17744) 0x4555 (17747) 0x4553 (17747)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=5/1356, ttl=64 id=0x0012, seq=7/1792, ttl=64
Ime           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237959           3 2022-08-01 10:03;22,231239747           3 2022-08-01 10:03;23,232247705           5 2022-08-01 10:03;23,232247763           5 2022-08-01 10:03;24,2347096751           7 2022-08-01 10:03;25,2586774061           9 2022-08-01 10:03;25,2586774061           9 2022-08-01 10:03;25,2586774061           10 2022-08-01 10:03;27,3066747681           12 2022-08-01 10:03;27,30667476           13 2022-08-01 10:03;27,30667476           13 2022-08-01 10:03;28,33066757           14 2022-08-01 10:03;29,3439667151           15 2022-08-01 10:03;29,354397606           16 2022-08-01 10:03;29,354397606           17 2022-08-01 10:03;29,354397606           17 2022-08-01 10:03;29,354397606           16 2022-08-01 10:03;29,354397606           17 2022-08-01 10:03;29,354397606           16 2022-08-01 10:03;20,354397606           17 2022-08-01 10:03;20,354397606           17 2022-08-01 10:03;20,354397606           19 2022-08-01 10:03;20,354397606           19 2022-08-01 10:03;20,354397606           19 2022-08-01 10:03;20,354397606           10 2022-08-01 10:03;20,354397606           10 2022-08-01 10:03;20,354397606           10 2022-08-01 10:03;20,354397606	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destruction 192, 0, 2, 100 192, 0, 100 192,	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 108 108 108 108 108 108 108	P.D 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x445c (17502) 0x445c (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (17639) 0x4467 (17639) 0x4675 (17744) 0x4553 (17744) 0x4555 (17744) 0x4557 (17747) 0x4597 (17815)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012,
Ime           1         2022-08-01         10:03:22.231237959           2         2022-08-01         10:03:22.231239747           3         2022-08-01         10:03:22.231239747           3         2022-08-01         10:03:23.2322477053           5         2022-08-01         10:03:24.2477053           5         2022-08-01         10:03:24.24776378           6         2022-08-01         10:03:25.258672449           8         2022-08-01         10:03:25.258674661           9         2022-08-01         10:03:27.306674534           10         2022-08-01         10:03:27.306674534           12         2022-08-01         10:03:27.306674534           12         2022-08-01         10:03:28.33066457153           13         2022-08-01         10:03:28.33066457153           14         2022-08-01         10:03:28.330667153           15         2022-08-01         10:03:28.330667153           16         2022-08-01         10:03:28.330667153           16         2022-08-01         10:03:28.33067153           16         2022-08-01         10:03:28.33067153           16         2022-08-01         10:03:28.33067153           17         2022-08-01	Source 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100 198,51,100,100	Destination 192, 0, 2, 100 192, 0,	Protocol ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4353 (17331) 0x4454 (17502) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17749) 0x4556 (17744) 0x4555 (17747) 0x4555 (17747) 0x4557 (17747) 0x4597 (17815) 0x4697 (17815)	PTI, 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=6/156, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=8/2048, ttl=64 id=0x0012, seq=9/2048, ttl=64 id=0x0012, seq=9/2048, ttl=64 id=0x0012, seq=9/2048, ttl=64
<ul> <li>Time         <ol> <li>Time             <ol></ol></li></ol></li></ul>	Source 198.51.100.100 199.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destruction 192, 0, 2, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100 192, 0, 100	Protocol ICHP ICH	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x4454 (17502) 0x4454 (17502) 0x4454 (17503) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4455 (17744) 0x4555 (17747) 0x4557 (17815) 0x4677 (18162)	PTL Me 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping)	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1206, ttl=64 id=0x0012, seq=5/1206, ttl=64 id=0x0012, seq=5/1206, ttl=64 id=0x0012, seq=5/1206, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012,
Ime           1         2022-08-01         10:03:22.231237959           2         2022-08-01         10:03:22.23123747           3         2022-08-01         10:03:22.23123747           3         2022-08-01         10:03:23.232247753           5         2022-08-01         10:03:23.232247753           5         2022-08-01         10:03:24.234706751           7         2022-08-01         10:03:25.258674861           8         2020-08-01         10:03:25.258674861           9         2022-08-01         10:03:27.306672439           10         2022-08-01         10:03:27.306671644           12         2022-08-01         10:03:27.306671644           12         2022-08-01         10:03:27.30667153           13         2022-08-01         10:03:29.354759331           16         2022-08-01         10:03:29.354759331           16         2022-08-01         10:03:29.354759331           16         2022-08-01         10:03:29.354759331           16         2022-08-01         10:03:29.354759347           17         2022-08-01         10:03:29.354759347           18         2022-08-01         10:03:29.354759347           19         2022-08-01	Source 199, 51, 100, 100 199, 51, 100, 100 199, 51, 100, 100 198, 51, 100, 100	Destrution 192.0.2.100 192.0.	Protocol ICANP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x4455 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x467 (1763) 0x4550 (17744) 0x4555 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4557 (17815) 0x4677 (18042) 0x4676 (18042) 0x4676 (18042)	PTI, 160 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=3/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=3/2048, ttl=64
Ime           1         2022-08-01         10:03:22.231237959           2         2022-08-01         10:03:22.231239747           3         2022-08-01         10:03:22.231239747           3         2022-08-01         10:03:23.232247763           5         2022-08-01         10:03:23.232247753           5         2022-08-01         10:03:24.2477673           6         2022-08-01         10:03:25.258672449           8         202-08-01         10:03:25.258672461           9         2022-08-01         10:03:27.306674634           10         2022-08-01         10:03:27.306674634           12         2022-08-01         10:03:27.306674634           13         2022-08-01         10:03:28.330664757           14         2022-08-01         10:03:28.33066457153           15         202-08-01         10:03:28.33066457153           16         2022-08-01         10:03:28.33066457153           16         2022-08-01         10:03:28.33067153           16         2022-08-01         10:03:28.33067153           16         2022-08-01         10:03:28.33067153           16         2022-08-01         10:03:28.33067153           16         2022-08-01	Source 198, 51, 100, 100 198, 51, 100, 100	Destination 192, 0, 2, 100 192, 0, 2, 100 1	Protocol ICHP ICHP ICHP ICHP ICHP ICHP ICHP ICHP	Length 108 1 108 1 1	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x43b3 (17331) 0x4452 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4457 (17744) 0x4555 (17744) 0x4555 (17747) 0x4553 (17815) 0x4677 (18042) 0x4684 (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 66 Echo (ping) reply 67 Echo (pin	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=9/2304, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64
Ime           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,23123747           3 2022-08-01 10:03;23,232247053           5 2022-08-01 10:03;23,232247753           5 2022-08-01 10:03;24,23470391           6 2022-08-01 10:03;25,25867240           8 2022-08-01 10:03;25,25867240           9 2022-08-01 10:03;25,25867240           9 2022-08-01 10:03;25,25867240           1 2022-08-01 10:03;27,36667378           1 2022-08-01 10:03;27,36667478           1 2022-08-01 10:03;27,36667478           1 2022-08-01 10:03;20,350671694           1 2022-08-01 10:03;27,36667478           1 2022-08-01 10:03;20,350671694           1 2022-08-01 10:03;21,350671694           1 2022-08-01 10:03;21,350671694           1 2022-08-01 10:03;21,35057153           1 5 2022-08-01 10:03;31,30277959311           1 6 2022-08-01 10:03;31,402772177           2 2022-08-01 10:03;31,4027724777           2 2022-08-01 10:03;31,402724775           2 2022-08-01 10:03;32,426695691	Source 198, 51, 100, 100 198, 51, 100, 100	Destruction 192, 0, 2, 100 192, 0, 2, 100	Protocol ICANP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17141) 0x4356 (17502) 0x4456 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4467 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4597 (17815) 0x4674 (18042) 0x4668 (18058)	PTL 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/2048, ttl=64
<ul> <li>Tme         <ol> <li>1 2022-08-01 10:03:22.231237959</li> <li>2 2022-08-01 10:03:22.23123747</li> <li>3 2022-08-01 10:03:22.331239747</li> <li>3 2022-08-01 10:03:23.232247763</li> <li>5 2022-08-01 10:03:23.232247753</li> <li>5 2022-08-01 10:03:24.2347096751</li> <li>7 2022-08-01 10:03:24.2347096751</li> <li>7 2022-08-01 10:03:25.258674261</li> <li>9 2022-08-01 10:03:25.258674261</li> <li>9 2022-08-01 10:03:27.306674378</li> <li>1 2022-08-01 10:03:27.306674564</li> <li>1 2022-08-01 10:03:27.306674564</li> <li>1 2022-08-01 10:03:28.330664677</li> <li>1 4022-08-01 10:03:28.330664677</li> <li>1 2022-08-01 10:03:28.330664677</li> <li>1 2022-08-01 10:03:28.330664675</li> <li>1 2022-08-01 10:03:17.306574378</li> <li>2 2022-08-01 10:03:1.40277217</li> <li>2 0022-08-01 10:03:1.402774775</li> <li>2 1 2022-08-01 10:03:12.42660354</li> <li>2 2 2022-08-01 10:03:12.42660354</li> <li>2 2 2022-08-01 10:03:12.426605501</li> </ol></li></ul>	Source 198.51,100,100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4358 (17331) 0x4458 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4455 (17744) 0x4556 (17744) 0x4556 (17744) 0x4556 (17747) 0x4557 (17815) 0x4677 (18042) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	id-exc012, seq=1/256, ttl=64 id-exc0012, seq=1/256, ttl=64 id-exc0012, seq=2/512, ttl=64 id-exc0012, seq=2/512, ttl=64 id-exc012, seq=2/512, ttl=64 id-exc012, seq=3/768, ttl=64 id-exc012, seq=4/1024, ttl=64 id-exc012, seq=6/1536, ttl=64 id-exc0012, seq=6/1536, ttl=64 id-exc0012, seq=6/1536, ttl=64 id-exc0012, seq=6/1536, ttl=64 id-exc0012, seq=6/1536, ttl=64 id-exc0012, seq=6/1536, ttl=64 id-exc0012, seq=7/1792, ttl=64 id-exc0012, seq=7/1792, ttl=64 id-exc0012, seq=10/2560, ttl=64 id-exc0012, seq=10/2560, ttl=64 id-exc0012, seq=10/2560, ttl=64 id-exc0012, seq=11/2816, ttl=64
Ime           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237959           3 2022-08-01 10:03;23,232247053           5 2022-08-01 10:03;23,232247753           5 2022-08-01 10:03;23,232247753           5 2022-08-01 10:03;24,23470391           7 2022-08-01 10:03;25,258674061           9 2022-08-01 10:03;25,258674061           9 2022-08-01 10:03;26,22660133           10 2022-08-01 10:03;27,36674737           12 2022-08-01 10:03;27,36674737           13 2022-08-01 10:03;27,36674737           14 2022-08-01 10:03;27,36674737           14 2022-08-01 10:03;27,36674737           16 2022-08-01 10:03;21,323,3066757           17 2022-08-01 10:03;21,32,35495706           18 2022-08-01 10:03;31,402772177           21 2022-08-01 10:03;31,4027724775           22 2022-08-01 10:03;31,402774775           22 2022-08-01 10:03;32,426695501	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICAPP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x4395 (17502) 0x4356 (17502) 0x4456 (17502) 0x4456 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4675 (17764) 0x4555 (17744) 0x4555 (17744) 0x4555 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4573 (18042) 0x4668 (18058) 0x4688 (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/568, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/248, ttl=64 id=0x0012, seq=3/236, ttl=64 id=0x0012, seq=3/236, ttl=64 id=0x0012, seq=1/2816, ttl=64 id=0x0012, seq=0x02, seq=10x02, seq=10x02, seq=10x02, seq=10x02, seq=10x02, se
In. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:27.306674787 1 2022-08-01 10:03:27.306674787 1 2022-08-01 10:03:27.306674787 1 2022-08-01 10:03:29.354795331 16 2022-08-01 10:03:29.354795331 17 20 2022-08-01 10:03:29.354795331 27 2022-08-01 10:03:29.3426695691 27 2022-08-01 10:03:29.3426695691 27 2022-08-01 10:03:29.3426695691 28 2022-08-01 10:03:29.3426695691 29 72:00 29 202-08-01 10:03:29.3426695691 20 2022-08-01 10:03:29.3426695691 20 20 20 20 20 20 20 20 20 20 20 20 20 2	Source 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100 198.51.100.100	Destrution 192.0.2.100 192.0.	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (17331) 0x4352 (17502) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4455 (17744) 0x4555 (17744) 0x4555 (17744) 0x4555 (17747) 0x4553 (17747) 0x4597 (17815) 0x4697 (18042) 0x468a (18042) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=7/1792, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=6/1586, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=10/2560, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=0, s
Ime           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237959           3 2022-08-01 10:03;23,232247053           5 2022-08-01 10:03;23,232247053           5 2022-08-01 10:03;23,232247053           6 2022-08-01 10:03;24,2347096751           7 2022-08-01 10:03;25,2586724061           9 2022-08-01 10:03;25,2586724061           9 2022-08-01 10:03;25,2586724061           1 2 0022-08-01 10:03;27,306674761           1 2 0022-08-01 10:03;27,306674761           1 2 0022-08-01 10:03;27,306674761           1 2 0022-08-01 10:03;27,306674761           1 2 0022-08-01 10:03;27,306674761           1 2 0022-08-01 10:03;27,306574761           1 2 0022-08-01 10:03;27,306574761           1 2 0022-08-01 10:03;27,306574776           1 2 0022-08-01 10:03;20,327959121           1 6 0022-08-01 10:03;20,32795912           1 6 0022-08-01 10:03;20,32795912           1 6 0022-08-01 10:03;21,402774777           2 1 2022-08-01 10:03;21,402774775           2 1 2022-08-01 10:03;22,426695591           2 7eme 2: 108 bytes on wire (864 bit           3 fthermet II, src: Cisco b9:77;08 (5           9 H-rag           0,	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICAPP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x4455 (17502) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4550 (17744) 0x4557 (17741) 0x4557 (17745) 0x4557 (17745) 0x4568 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=3/768, ttl=64         1d=0x0012, seq=3/768, ttl=64         1d=0x0012, seq=3/768, ttl=64         1d=0x0012, seq=3/768, ttl=64         1d=0x0012, seq=3/1280, ttl=64         1d=0x0012, seq=5/1280, ttl=64         1d=0x0012, seq=7/1792, ttl=64         1d=0x0012, seq=9/2304, ttl=64         1d=0x0012, seq=9/2304, ttl=64         1d=0x0012, seq=10/2560, ttl=64         1d=0x0012, seq=11/2816, ttl=64         1d=0x0012, seq=11/2816, ttl=64         1d=0x0012, seq=11/2816, ttl=64         000 00 08 81 00 00 66 08 00 45 00 00 54 42 f8 00 00 0
No.         Time           1 2022-08-01 10:03:22, 231237959           2 2022-08-01 10:03:22, 231237479           3 2022-08-01 10:03:23, 232247793           5 2022-08-01 10:03:23, 232247793           5 2022-08-01 10:03:23, 232247793           5 2022-08-01 10:03:24, 22470931           6 2022-08-01 10:03:25, 2586724601           9 2022-08-01 10:03:25, 2586724601           10 2022-08-01 10:03:25, 2586724611           10 2022-08-01 10:03:27, 306674737           13 2022-08-01 10:03:27, 306674737           13 2022-08-01 10:03:27, 306674737           14 2022-08-01 10:03:24, 334067154           17 2022-08-01 10:03:21, 330667154           18 2022-08-01 10:03:21, 3354795931           16 2022-08-01 10:03:124, 334067154           17 2022-08-01 10:03:131, 402727177           20 2022-08-01 10:03:131, 402724777           21 2022-08-01 10:03:131, 402724777           21 2022-08-01 10:03:131, 402724775           22 2022-08-01 10:03:131, 402724775           22 2022-08-01 10:03:132, 426695691           2           22 2022-08-01 10:03:132, 426695691	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	P D 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (1731) 0x43b5 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (1774) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x457 (18042) 0x4668 (18058) 0x4668 (18058)	PTT, 166 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64         1d=0x0012, seq=1/256, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=3/108, ttl=64         1d=0x0012, seq=11/2816, ttl=64
Ime           1         2022-08-01         10:03:22.231237959           2         2022-08-01         10:03:22.23123747           3         2022-08-01         10:03:22.23123747           3         2022-08-01         10:03:23.232247053           5         5022-08-01         10:03:24.234706751           7         7022-08-01         10:03:25.258672449           8         202-08-01         10:03:25.258674661           9         2022-08-01         10:03:27.306674738           10         202-08-01         10:03:27.306674764           12         2022-08-01         10:03:27.306674764           12         2022-08-01         10:03:27.306674751           13         2022-08-01         10:03:28.3306646775           14         2022-08-01         10:03:30.378975244           16         2022-08-01         10:03:31.40277217           16         2022-08-01         10:03:31.40277217           19         202-08-01         10:03:31.4027724775           21         2022-08-01         10:03:31.402774775           21         2022-08-01         10:03:32.426605501           2         2022-08-01         10:03:32.426605501           2         2022-08-01	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4353 (17331) 0x4454 (17502) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4553 (17742) 0x4553 (17742) 0x4553 (17742) 0x4553 (17742) 0x4568 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	1d=0x0012, seq=1/256, ttl=64         1d=0x0012, seq=1/256, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=2/512, ttl=64         1d=0x0012, seq=3/08, ttl=64         1d=0x0012, seq=3/08, ttl=64         1d=0x0012, seq=3/08, ttl=64         1d=0x0012, seq=3/168, ttl=64         1d=0x0012, seq=3/168, ttl=64         1d=0x0012, seq=6/156, ttl=64         1d=0x0012, seq=6/156, ttl=64         1d=0x0012, seq=6/156, ttl=64         1d=0x0012, seq=7/1792, ttl=64         1d=0x0012, seq=7/1792, ttl=64         1d=0x0012, seq=7/1792, ttl=64         1d=0x0012, seq=7/1792, ttl=64         1d=0x0012, seq=10/2560, ttl=64         1d=0x0012, seq=10/2560, ttl=64         1d=0x0012, seq=11/2816, ttl=64
Ime           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237479           3 2022-08-01 10:03;23,23224709           4 2022-08-01 10:03;23,23224779           5 2022-08-01 10:03;23,23224779           5 2022-08-01 10:03;24,2347096751           7 2022-08-01 10:03;25,258674461           9 2022-08-01 10:03;25,258674461           9 2022-08-01 10:03;25,258674461           9 2022-08-01 10:03;27,36667478           13 2022-08-01 10:03;27,36667478           13 2022-08-01 10:03;27,36667478           14 2022-08-01 10:03;27,36667478           14 2022-08-01 10:03;21,30667453           15 2022-08-01 10:03;21,30567453           16 2022-08-01 10:03;21,30567453           17 2022-08-01 10:03;12,30567453           18 2022-08-01 10:03;13,40272477           19 2022-08-01 10:03;13,402724777           21 2022-08-01 10:03;13,402724777           22 2022-08-01 10:03;13,402724775           22 2022-08-01 10:03;12,426695691           C           C           C           C           0	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICAPP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17141) 0x43b3 (1731) 0x43b3 (1731) 0x43b2 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (1763) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4673 (17741) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4554 (17748) 0x4674 (18042) 0x4668 (18058) 0x4668 (18058)	PTL 146 64 Echo (ping) reply 64 Echo (ping	id=0x0012, seq=1/256, ttl=64         id=0x0012, seq=1/256, ttl=64         id=0x0012, seq=2/512, ttl=64         id=0x0012, seq=3/56, ttl=64         id=0x0012, seq=3/56, ttl=64         id=0x0012, seq=3/102, ttl=64         id=0x0012, seq=3/2048, ttl=64         id=0x0012, seq=3/2048, ttl=64         id=0x0012, seq=3/2048, ttl=64         id=0x0012, seq=3/2048, ttl=64         id=0x0012, seq=10/2560, ttl=64         id=0x0012, seq=11/2816, ttl=64         id=0x0012, seq=10, seq=0, seq=0, seq
In. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.24703961 6 2022-08-01 10:03:24.247036751 7 2022-08-01 10:03:24.234706751 9 2022-08-01 10:03:25.258674661 1 2022-08-01 10:03:25.258674661 1 2022-08-01 10:03:27.306674378 13 2022-08-01 10:03:27.306674578 13 2022-08-01 10:03:27.306674578 13 2022-08-01 10:03:29.354759531 16 2022-08-01 10:03:29.354759531 20 2022-08-01 10:03:29.426695591 20 20 20 20 20 20 20 20 20 20 20 20 20 2	Source 198.51.100.100 198.51.000 198.50.000 198.50.000 198.50.000 198.50	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4358 (17331) 0x4458 (17502) 0x4454 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1774) 0x4555 (17744) 0x4555 (17744) 0x4555 (17747) 0x4597 (17815) 0x4674 (18042) 0x468a (18042) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1026, ttl=64 id=0x0012, seq=4/1026, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=0x0, seq=0x0, seq=0x0, seq=0x0, seq</pre>
C         Time           1 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237479           3 2022-08-01 10:03;23,232247053           5 2022-08-01 10:03;23,23224779           5 2022-08-01 10:03;23,23224779           7 2022-08-01 10:03;24,23479391           6 2022-08-01 10:03;25,258672461           9 2022-08-01 10:03;25,258672461           9 2022-08-01 10:03;27,30667378           13 2022-08-01 10:03;27,306674781           12 2022-08-01 10:03;27,306674781           13 2022-08-01 10:03;27,306674781           13 2022-08-01 10:03;27,306674781           13 2022-08-01 10:03;27,306674781           14 2022-08-01 10:03;27,306674781           15 2022-08-01 10:03;27,3066747841           16 2022-08-01 10:03;28,330667153           15 2022-08-01 10:03;29,35493706           16 2022-08-01 10:03;20,32799912           16 2022-08-01 10:03;21,402772217           20 202-08-01 10:03;31,402774775           21 2022-08-01 10:03;32,4266955691           22 2022-08-01 10:03;32,4266955691           2 5 Ethernet II, src: C isco b9:77:08 (5           9	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICAP ICAP ICAP ICAP ICAP ICAP ICAP ICAP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43b3 (17331) 0x4455 (17502) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4550 (17744) 0x4557 (17741) 0x4557 (17742) 0x4557 (17742) 0x4558 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=5/1280, ttl=64 id=0x0012, seq=3/1280, ttl=64 id=0x0012, seq=3/2380, ttl=64 id=0x0012, seq=3/2380, ttl=64 id=0x0012, seq=3/2380, ttl=64 id=0x0012, seq=3/2380, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=0000, seq=0000, seq=0000, seq=0000, seq=0000, seq=00000, seq=00000, s</pre>
No.         Time           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.23123747           3 2022-08-01 10:03:23.232247053           5 2022-08-01 10:03:23.232247053           5 2022-08-01 10:03:23.232247053           5 2022-08-01 10:03:24.247070571           7 2022-08-01 10:03:25.2586724801           9 2022-08-01 10:03:25.2586724801           10 2022-08-01 10:03:25.2586724801           10 2022-08-01 10:03:25.2586724801           10 2022-08-01 10:03:27.306671694           12 2022-08-01 10:03:27.306671694           12 2022-08-01 10:03:29.354795931           16 2022-08-01 10:03:29.354795931           16 2022-08-01 10:03:21.4330607151           17 2022-08-01 10:03:13.40272217           20 202-08-01 10:03:13.402724777           20 202-08-01 10:03:13.402724777           21 2022-08-01 10:03:13.402724775           22 2022-08-01 10:03:13.402724775           22 2022-08-01 10:03:13.402724775           22 2022-08-01 10:03:13.402724775           22 2022-08-01 10:03:13.402724775           20 202-08-01 10:03:13.402724775           20 202-08-01 10:03:13.402724775           21 2022-08-01 10:03:13.402724775           22 2022-08-01 10:03:13.402724775           21 2022-08-01 10:03:13.402724775           21 2022-08-01 10:03:13.402724775	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17145) 0x43b3 (17331) 0x43b5 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17633) 0x467 (17633) 0x467 (17633) 0x467 (17744) 0x4555 (17744) 0x4555 (17744) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (18042) 0x4668 (18058) 0x4668 (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=exc0012, seq=1/256, ttl=64 id=exc0012, seq=2/512, ttl=64 id=exc0012, seq=2/512, ttl=64 id=exc0012, seq=2/512, ttl=64 id=exc0012, seq=2/1024, ttl=64 id=exc0012, seq=2/2048, ttl=64 id=exc0012, seq=2/2048, ttl=64 id=exc0012, seq=11/2816, ttl=64 id=exc0012, se</pre>
Ime           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.231237959           3 2022-08-01 10:03:22.322247053           5 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:23.232247763           5 2022-08-01 10:03:23.232247763           7 2022-08-01 10:03:24.2347090751           7 2022-08-01 10:03:25.2586724061           9 3022-08-01 10:03:25.2586724061           9 3022-08-01 10:03:25.2586724061           1 2 022-08-01 10:03:27.306671694           12 2022-08-01 10:03:27.306671694           12 2022-08-01 10:03:27.306671694           12 2022-08-01 10:03:27.306571694           12 2022-08-01 10:03:27.306571694           12 2022-08-01 10:03:27.306571694           12 2022-08-01 10:03:27.306571694           12 2022-08-01 10:03:27.306571694           12 2022-08-01 10:03:27.305571694           13 2022-08-01 10:03:27.30574775           14 2022-08-01 10:03:27.30574777           20 2022-08-01 10:03:27.426693591           14 2022-08-01 10:03:27.426695691           20 2022-08-01 10:03:22.426695691           20 2022-08-01 10:03:22.426695691           9 7.788           9 0.700 0000 00000 00000 00000 00000 00000 0000	Server 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	P D 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4353 (17331) 0x4454 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4457 (17741) 0x4553 (17742) 0x4553 (17742) 0x4553 (17742) 0x4568 (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=11/</pre>
Solution         Time           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.231237479           3 2022-08-01 10:03:23.23224709           4 2022-08-01 10:03:23.232247053           5 2022-08-01 10:03:23.232247053           5 2022-08-01 10:03:24.247070571           7 2022-08-01 10:03:24.24270531           9 2022-08-01 10:03:25.2586724801           9 2022-08-01 10:03:25.2586724801           10 2022-08-01 10:03:25.2586724801           10 2022-08-01 10:03:27.306671694           12 2022-08-01 10:03:27.306674737           13 2022-08-01 10:03:27.306674737           14 2022-08-01 10:03:29.354936706           17 2022-08-01 10:03:20.3787959311           16 2022-08-01 10:03:20.3787959311           16 2022-08-01 10:03:20.3787959312           17 2022-08-01 10:03:20.3787959312           17 20 202-08-01 10:03:20.3787959312           18 2022-08-01 10:03:20.3787959312           19 2022-08-01 10:03:20.3787959312           10 202-08-01 10:03:20.378795042           17 20 202-08-01 10:03:20.3787959312           18 2022-08-01 10:03:20.378795041           18 2022-08-01 10:03:20.426695691           10 80:20.20.40.01 10:03:20.20.20.000           10 80:20.20.01.01.01.01.01.01.01.01.01.01.0000           00.000000000000000000000           00.00000000	Source 198.51.100.100 198.51	Destrution 192.0.2.100 192.0.	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	P D 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43b3 (1731) 0x43b5 (17502) 0x4456 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (1763) 0x4467 (1763) 0x4467 (1763) 0x467 (1763) 0x467 (1763) 0x467 (1774) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x457 (18042) 0x4668 (18058) 0x4668 (18058) 0x4668 (18058)	PTL 166 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/2048, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0018</pre>
No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:24.24703931 6 2022-08-01 10:03:24.24703931 9 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:24.234706751 9 2022-08-01 10:03:25.258674691 1 2022-08-01 10:03:27.306674578 11 2022-08-01 10:03:27.306674578 12 2022-08-01 10:03:27.306674578 13 2022-08-01 10:03:27.306674578 13 2022-08-01 10:03:29.354795931 16 2022-08-01 10:03:29.3426693264 12 2022-08-01 10:03:29.426693254 22 2022-08-01 10:03:29.426695691 VH-Tag 0	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol ICMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4358 (17331) 0x4458 (17502) 0x4454 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4455 (17744) 0x4556 (17744) 0x4556 (17744) 0x4556 (17747) 0x4557 (171815) 0x4597 (171815) 0x4678 (18042) 0x4688 (18058) 0x4688 (18058) 0x4688 (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=10/256, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=10, seq=11/2816, tt</pre>
Ko.         Time           1 2022-08-01 10:03:22.231237959           2 2022-08-01 10:03:22.231237479           3 2022-08-01 10:03:23.23224709           4 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:23.232247753           5 2022-08-01 10:03:24.23470391           7 2022-08-01 10:03:25.258674861           9 2022-08-01 10:03:25.258674861           9 2022-08-01 10:03:25.258674861           9 2022-08-01 10:03:25.258674861           9 2022-08-01 10:03:27.30667478           13 2022-08-01 10:03:27.30667478           13 2022-08-01 10:03:27.30667478           13 2022-08-01 10:03:27.30667478           14 2022-08-01 10:03:27.30657478941           16 2022-08-01 10:03:12.4254939591           16 2022-08-01 10:03:13.0.378795204           17 2022-08-01 10:03:13.1.402772177           21 2022-08-01 10:03:13.1.4027724775           22 2022-08-01 10:03:13.1.4027724775           21 2022-08-01 10:03:12.426695691           VM-Tag           0	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	Protocol           ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17141) 0x43b3 (1731) 0x43b3 (1731) 0x43b2 (17502) 0x445c (17502) 0x44c4 (17508) 0x44c4 (17508) 0x44c4 (1763) 0x44c7 (1763) 0x44c7 (1763) 0x44c7 (1763) 0x44c7 (1763) 0x455 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4554 (180c2) 0x46c6 (18058) 0x4668 (18058) 0x4668 (18058)	PTL 146 64 Echo (ping) reply 64 Echo (ping	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/768, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/102, ttl=64 id=0x0012, seq=3/128, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=3/12816, ttl=64 id=0x0012,</pre>
<pre>No. Time 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:23.232247753 5 2022-08-01 10:03:24.234706751 7 2022-08-01 10:03:24.234706751 9 2022-08-01 10:03:25.258674861 9 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:25.258674861 1 2022-08-01 10:03:27.306674788 1 2022-08-01 10:03:27.306674788 1 2022-08-01 10:03:27.30667478 1 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 1 6 2022-08-01 10:03:29.354795331 2 9 2022-08-01 10:03:29.354795331 2 9 2022-08-01 10:03:29.354795331 2 2 2022-08-01 10:03:29.354795331 2 2 2022-08-01 10:03:29.354795331 2 2 2022-08-01 10:03:29.354795331 2 2 2022-08-01 10:03:29.354795331 2 6 20.20 40.00 10:03:29.354795331 2 6 20.20 40.00 10:03:29.354795331 2 6 20.20 40.00 10:03:29.354795331 2 6 20.20 40.00 10:03:29.354795331 2 6 20.20 40.00 10:03:29.354795331 2 6 20.20 40.00 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.35479533 2 7 20 202-08-01 10:03:29.3547953 2 7 20 202-08-01 10:03:29.426695691 2 2 2022-08-01 10:03:29.426695691 2 0 000 0000 0000 0000 0 0000 0 0000 0000 0000 0000 0 0000 0 0000 0000 0000 0 0000 0 0000 0000 0000 0 0000 0 0000 0000 0000 0 0000 0 0000 0000 0000 0 0000 0 0000 0000 0 0000 0 0000 0000 0 0000 0 0000 0 0000 0 0000 0000 0 0000 0 0000 0 0000 0 0000 0 0000 0000 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</pre>	Source 198.51.100.100 198.51	Destination 192.0.2.100 192.0	notecal ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4303 (17331) 0x4352 (17502) 0x4454 (17502) 0x4454 (17502) 0x4454 (17508) 0x4464 (17508) 0x4464 (17603) 0x4467 (1763) 0x4467 (1763) 0x46755 (17744) 0x4555 (17744) 0x4555 (17747) 0x4555 (17747) 0x4553 (17747) 0x4597 (17815) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=10</pre>
<pre>     Tme     1 2022-08-01 10:03:22.231237959     2 2022-08-01 10:03:22.231237959     2 2022-08-01 10:03:22.23123747     3 2022-08-01 10:03:23.232247753     5 2022-08-01 10:03:23.232247753     5 2022-08-01 10:03:24.234709511     7 2022-08-01 10:03:25.258674061     9 2022-08-01 10:03:25.258674061     9 2022-08-01 10:03:25.258674061     9 2022-08-01 10:03:25.258674061     1 2022-08-01 10:03:27.306674737     13 2022-08-01 10:03:27.306674737     13 2022-08-01 10:03:27.306674737     13 2022-08-01 10:03:21.30274295931     16 2022-08-01 10:03:21.3027495931     16 2022-08-01 10:03:21.30274775     21 2022-08-01 10:03:21.4027724775     21 2022-08-01 10:03:21.4027724775     21 2022-08-01 10:03:22.426695691     Content I, Src: Cisco D9:7740 (Signature)</pre>	Source 198.51.100.100 198.51	Destruction 192.0.2.100 192.0	Protocol           ICMP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x43f8 (17144) 0x43f8 (17141) 0x43b3 (1731) 0x445e (17502) 0x445e (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4467 (1763) 0x4467 (1763) 0x4467 (1763) 0x4673 (17741) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4553 (17747) 0x4574 (18042) 0x468a (18058) 0x468a (18058)	PTL 146 64 Echo (ping) reply 64 Echo (ping) reply 65 Echo (ping) reply 66 Echo (ping) reply 67 Echo (ping) reply 68 Echo (ping) reply 69 Echo (ping) reply 60 Echo (ping	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=3/266, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=10, seq=0, s</pre>
<pre> 8. Tme 1 2022-08-01 10:03:22.231237959 2 2022-08-01 10:03:22.231237959 3 2022-08-01 10:03:22.23123747 3 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:23.232247053 5 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:25.258672461 9 2022-08-01 10:03:25.258672461 1 2022-08-01 10:03:25.258672461 1 2022-08-01 10:03:25.258672461 1 2022-08-01 10:03:27.306671694 1 2022-08-01 10:03:27.306671694 1 2022-08-01 10:03:29.354795931 1 5 2022-08-01 10:03:29.354795931 1 5 2022-08-01 10:03:29.354795931 1 6 202-08-01 10:03:29.354795931 1 6 202-08-01 10:03:29.354795931 1 6 202-08-01 10:03:29.354795931 1 6 202-08-01 10:03:13.40272477 2 2 2022-08-01 10:03:13.402724775 2 2 2022-08-01 10:03:13.402724775 2 2 2022-08-01 10:03:12.426695691 </pre>	Source 198.51.100.100 100 100 100 100 10	Destrution 192.0.2.100 192.0.	notecal ICNP ICNP ICNP ICNP ICNP ICNP ICNP ICNP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x432f8 (17144) 0x43b3 (17331) 0x445e (17502) 0x4464 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17683) 0x4464 (17683) 0x4647 (17633) 0x467 (17633) 0x4674 (17744) 0x4555 (17744) 0x4555 (17744) 0x4556 (17744) 0x4556 (17744) 0x4558 (18042) 0x4674 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/166, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=3/186, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=10, ttl=64 i</pre>
C         Time           1 2022-08-01 10:03;22,231237959         2 2022-08-01 10:03;22,231237959           2 2022-08-01 10:03;22,231237479         3 2022-08-01 10:03;23,2322477053           5 2022-08-01 10:03;23,2322477053         5 2022-08-01 10:03;24,2347090751           7 2022-08-01 10:03;25,2586724061         9 2022-08-01 10:03;25,2586724061           9 2022-08-01 10:03;25,2586724061         9 2022-08-01 10:03;27,3066747861           1 2022-08-01 10:03;27,3066747861         2 2022-08-01 10:03;27,3066747861           1 2 2022-08-01 10:03;27,3066747861         2 2022-08-01 10:03;27,3066747861           1 2 2022-08-01 10:03;27,3066747861         2 2022-08-01 10:03;27,3066747861           1 2 2022-08-01 10:03;27,3066747861         2 2022-08-01 10:03;27,3066747861           1 2 2022-08-01 10:03;20,32793912         16 2022-08-01 10:03;20,32793912           1 6 2022-08-01 10:03;21,402774775         21 2022-08-01 10:03;21,402774775           2 1 2022-08-01 10:03;21,402774775         21 2022-08-01 10:03;22,426695591           2 7 Frame 2: 108 bytes on wire (864 bit 51 51,402774775         21 2022-08-01 10:03;22,426695591           3 Frame 2: 108 bytes on wire (864 bit 51 51,402774775         21 2022-08-01 10:03;22,426695591           4 H-ag	Sovee 198.51.100.100 101.102 1	Destination 192.0.2.100 192.0	Protocol           ICNP	Length 108 108 108 108 108 108 108 108	PD 0x42f8 (17144) 0x42f8 (17144) 0x4305 (17331) 0x4458 (17331) 0x4458 (17331) 0x4458 (17502) 0x4464 (17508) 0x4464 (17508) 0x4464 (17508) 0x4464 (17639) 0x4467 (17639) 0x4467 (17639) 0x4467 (17639) 0x4553 (17741) 0x4553 (17742) 0x4553 (17742) 0x4587 (18042) 0x468a (18058) 0x468a (18058) 0x468a (18058)	PTT, 146 64 Echo (ping) reply 64 Echo (ping) reply	<pre>id=0x0012, seq=1/256, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=2/512, ttl=64 id=0x0012, seq=3/766, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/1024, ttl=64 id=0x0012, seq=4/136, ttl=64 id=0x0012, seq=4/136, ttl=64 id=0x0012, seq=4/136, ttl=64 id=0x0012, seq=4/136, ttl=64 id=0x0012, seq=11/2816, ttl=64 id=0x0012, seq=1</pre>

## Uitleg

In dit geval is Ethernet1/2 met poort VLAN-tag 102 de uitgangsinterface voor de ICMPechoantwoordpakketten.

Wanneer de richting van de toepassingsopname is ingesteld op **Uitgang** in de opnameopties, worden pakketten met de poort VLAN-tag 102 in de Ethernet-header opgenomen op de backplane interfaces in de toegangsrichting.

In deze tabel wordt de taak samengevat:

Taak	Opnamepun t	Interne poort VLAN in opgenomen pakketten	Richting	Opgenomen verkeer
Configureren en verifiëren van opnamen op applicatie- en toepassingspoort Ethernet1/2	Backplane interfaces	102	Alleen inspring en	ICMP-echoantwoorden van ho 198.51.100.100 op host 192.0.2.100

### Taak 2

Gebruik de FCM en CLI om een pakketopname op de backplane interface en de voorinterface Ethernet1/2 te configureren en te verifiëren.

Gelijktijdige pakketopnamen worden geconfigureerd op:

- Voorinterface de pakketten met de poort VLAN 102 op de interface Ethernet1/2 worden opgenomen. Opgenomen pakketten zijn ICMP-echoverzoeken.
- Backplane interfaces pakketten waarvoor Ethernet1/2 is geïdentificeerd als de uitgaande interface, of de pakketten met de poort VLAN 102, worden opgenomen. Opgenomen pakketten zijn ICMP-echoantwoorden.

### Topologie, pakketstroom en de opnamepunten



#### Configuratie

#### FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Dele	e All Sessions
No Session available		

2. Selecteer de FTD-toepassing, **Ethernet1/2** in de vervolgkeuzelijst **Toepassingspoorten** en selecteer **Alle pakketten** in de **toepassingsopnamerichtlijn**. Geef de **sessienaam op** en klik op **Opslaan en Uitvoeren** om de opname te activeren:

Overview Interfaces Logical Devices Security Engine	Natform Settings	System Tools Help	admin
Select an instance: ftd1 🗸		Save and Run Save Ca	ncel
ftd1		Session Name* Cap1	
		Selected Interfaces None	
Ethernet1/2		Buffer Size 256 MB V	
		Snap length: 1518 Bytes	
		Store Packets Overwrite Append	
		Capture On ftd 🗸	
Ethernet1/3		Application Port Ethernet1/2	
	FTD Ethernet1/9, Ethernet1/10	Application Capture Direction All Packets Egress Packet	
		Capture Filter Apply Filter Capture All	
Ethernet1/1			

### **FXOS CLI**

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

firepower# scope ssa firepower /ssa# show app-instance Admin State Oper State Running Version Startup Version Identifier Slot ID App Name Deploy Type Turbo Mode Profile Name Cluster State Cluster Role \_\_\_\_\_\_ \_\_\_\_\_ \_\_\_\_\_ \_\_\_\_ 1 Enabled Online 7.2.0.82 7.2.0.82 ftd ftd1 Not Applicable None Native No 2. Een opnamesessie maken: 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

#### Verificatie

FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

Overview Interfaces Log	gical Devices Security Engine Plat	form Settings				System To	ols Help	admin
Capture Session Filter List								
					į.	C Refresh	Capture Sess	ion De
Cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes			8
Interface Name	Filter	File Size (in bytes)	File Name	Device Name				
Ethernet1/2	None	95040	cap1+ethernet+1+2+0.pcap	ftd1	*			
Ethernet1/2 - Ethernet1/10	None	368	cap1-vethernet-1175.pcap	ftd1	*			
Ethernet1/2 - Ethernet1/9	None	13040	cap1-vethernet-1036.pcap	ftd1	*			

### **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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
```

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

### Capture file analyse

Gebruik een applicatie voor pakketvastlegging om de opnamebestanden te openen. In het geval van meerdere backplane interfaces, zorg ervoor dat alle opnamebestanden voor elke backplane interface worden geopend. In dit geval worden de pakketten opgenomen op de backplane interface Ethernet1/9.

Open het opnamebestand voor de interface Ethernet1/2, selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

140.	1 mg	Source	Descriación	Protocol	Lengon		FILL BRO		
-	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping) requ	d=0x0013, seq=1/256, ttl=64 (no response for	und!)
	2 2022-08-01 11:33:19.070695347	192.0.2.100	198.51.100.100	ICMP	102	0xc009 (49161)	64 Echo (ping) requ	d=0x0013, seg=1/256, ttl=64 (no response for	und!)
	3 2022-08-01 11:33:19.071217121	192.0.2.100	198,51,100,100	ICMP	102	8XC889 (49161)	64 ECRO (DING) FEQU	d=0x0013, seg=1/256, ttl=64 (no response for	und!)
	4 2022-08-01 11:33:19.071218458	192.0.2.100	198.51.100.100	TCMP	102	8x(889 (49161)	64 Echo (ning) requi	d=0x0013, seg=1/256, ttl=64 (no response for	(Ibnu
	5 2022-00-01 11:22:20 07202625	102 0 2 100	100 51 100 100	TCMD	102	0xc0ae (40226)	64 Echo (ping) requ	d=0x0013, seq=2/513, ttl=64 (no response for	undl)
	5 2022-08-01 11:55:20.072030025	192.0.2.100	198.51.100.100	TCHP	100	0xc0ae (49320)	Galecho (ping) requ	d=0x0013, seq=2/512, tt1=04 (no response for	and 1
	6 2022-08-01 11:33:20.072038399	192.0.2.100	198.51.100.100	ICMP	102	0xc0ae (49326)	64 Ecno (ping) requ	d=0x0013, seq=2/512, tt1=04 (no response for	und ( )
	7 2022-08-01 11:33:21.073266030	192.0.2.100	198.51.100.100	ICMP	108	0xc167 (49511)	64 Echo (ping) requ	d=0x0013, seq=3/768, tt1=64 (no response for	ind!)
	8 2022-08-01 11:33:21.073268327	192.0.2.100	198.51.100.100	ICMP	102	0xc167 (49511)	64 Echo (ping) requ	d=0x0013, seq=3/768, ttl=64 (no response for	und!)
	9 2022-08-01 11:33:22.074576640	192.0.2.100	198.51.100.100	ICMP	108	0xc175 (49525)	64 Echo (ping) requ	d=0x0013, seq=4/1024, ttl=64 (no response fo	ound!)
	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) requ	d=0x0013, seq=4/1024, ttl=64 (no response fo	ound!)
	11 2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) requ	d=0x0013, seg=5/1280, ttl=64 (no response for	ound1)
	12 2022-08-01 11:33:23.075781513	192.0.2.100	198,51,100,100	ICMP	102	0xc208 (49672)	64 Echo (ping) requ	d=0x0013, seg=5/1280, ttl=64 (no response fo	ound()
	12 2022-02-01 11:33:34 091930400	102 0 2 100	109 51 100 100	TCMD	109	0x(211 (40691)	64 Echo (ping) requ	d-0x0013, seq-6/1536 ttl-64 (no response fr	ound()
	13 2022-08-01 11.33.24.081833490	102.0.2.100	100 51 100 100	TCHP	100	0xc211 (49081)	64 Echo (ping) requ	d=0x0013, seq=0/1530, tt1=04 (no response fo	aund 1)
	14 2022-08-01 11:33:24.081841380	192.0.2.100	198.51.100.100	ICMP	102	6xc211 (49681)	64 ECHO (ping) requ	d=0x0013, seq=0/1530, ttl=04 (no response fo	Juna I )
	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) requ	d=0x0013, seq=7/1792, tt1=64 (no response fo	Sund!)
	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) requ	d=0x0013, seq=7/1792, ttl=64 (no response fo	bund!)
	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) requ	d=0x0013, seq=8/2048, ttl=64 (no response fo	ound!)
	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) requ	d=0x0013, seq=8/2048, ttl=64 (no response fo	aund!)
	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) requ	d=0x0013, seq=9/2304, ttl=64 (no response for	ound!)
	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) requ	d=0x0013, seg=9/2304, ttl=64 (no response for	ound!)
	21 2022-08-01 11:33:28.177847175	192.0.2.100	198,51,100,100	ICMP	108	0xc516 (50454)	64 Echo (ping) requ	d=0x0013, seg=10/2560, ttl=64 (no response t	found!)
	22 2022-08-01 11:33:28 177849075	192.0.2.100	198.51.100.100	TCMP	102	8x(516 (58454)	64 Echo (ning) requi	d=0x0013, seg=10/2560, ttl=64 (no response t	found1)
	22 2022-08-01 11:33:28:17/849075	192.0.2.100	190.51.100.100	TCHP	102	0xc510 (50454)	Ga Echo (ping) requ	d-0x0013, seq-10/2500, cc1-04 (no response i	foundly
	23 2022-08-01 11:33:29.201804/60	192.0.2.100	198.51.100.100	TCMP	108	0xc578 (50552)	64 ECHO (ping) requi	d=0x0013, seq=11/2816, ttl=64 (no response	round ( )
	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) requ	d=0x0013, seq=11/2816, tt1=64 (no response 1	round1)
	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) requ	d=0x0013, seq=12/3072, ttl=64 (no response 1	found!)
	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) requ	d=0x0013, seq=12/3072, ttl=64 (no response 1	found!)
	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) requ	d=0x0013, seq=13/3328, ttl=64 (no response 1	found1)
	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) requ	d=0x0013, seq=13/3328, ttl=64 (no response 1	found1)
	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) requ	d=0x0013, seg=14/3584, ttl=64 (no response t	found1)
κī						,			
	4. 400 b. b	->	-					re of he he fit as an re, of an he as as	00.00 X 0.W 0
1	Frame 1: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 Dits) (	on incertace ca	prure_uo_	1, 10 0			40 00 x
2	Ethernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:b	e), Dst: Cisco b9:	7:0e (58:97:b)	:b9:77:0e	)		40 01 24 22 20 00 02 64 26 22 64 64 02 00	40 00 Tr E Tr W
M	vn-Tag							40 01 80 83 C0 00 02 04 C0 33 64 64 68 60	80 70 00 00
	1	= Directi	ion: From Bridge					00 13 00 01 T2 D9 E7 62 00 00 00 00 CD 7T	00 00 ····· 0 ·····
	.0	= Pointer	<pre>r: vif_id</pre>						13 10
		= Destina	ation: 10					10 10 10 17 20 21 22 23 24 25 26 27 28 29	20 20 1 = \$48 ()-+
	···· ··· ··· ··· ··· 0 ····	= Looped:	No	4 1				2C 20 2e 2t 30 31 32 33 34 35 36 37	,/0123 456/
		= Reserve	d: 0	*					
	89	= Version							
	0000 000	00 0000 - Sources							
	Turner 002 40 History 144 (0-0102)	bo bobb = source.							
	Type: 802.10 Virtual LAN (0x8100	)		_					
M	802.10 Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
	000 = Priority: 6	Best Effort (defa	ault) (0)						
	0 = DEI: Inelig	gible		5 1					
	0000 0110 0110 = ID: 102			-					
L	Type: IPv4 (0x0800)								
>	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198,51,100,100						
5	Internet Control Message Protocol			2					
	control internege in otocor								

Selecteer het tweede pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		
E	1 2022-08-01 11:33:19.070693081	192.0.2.100	198.51.100.100	ICMP	108 1	0xc009 (49161)	64 Echo (ping) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=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) req	quest i	d=0x0013, seq=4/1024, ttl=64 (no response found!)
1	10 2022-08-01 11:33:22.074578010	192.0.2.100	198.51.100.100	ICMP	102	0xc175 (49525)	64 Echo (ping) req	quest i	d=0x0013, seq=4/1024, ttl=64 (no response found!)
1	11 2022-08-01 11:33:23.075779089	192.0.2.100	198.51.100.100	ICMP	108	0xc208 (49672)	64 Echo (ping) req	quest i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
1	12 2022-08-01 11:33:23.075781513	192.0.2.100	198.51.100.100	ICMP	102	0xc208 (49672)	64 Echo (ping) req	quest i	d=0x0013, seq=5/1280, ttl=64 (no response found!)
1	13 2022-08-01 11:33:24.081839490	192.0.2.100	198.51.100.100	ICMP	108	0xc211 (49681)	64 Echo (ping) req	quest i	d=0x0013, seq=6/1536, ttl=64 (no response found!)
1	14 2022-08-01 11:33:24.081841386	192.0.2.100	198.51.100.100	ICMP	102	0xc211 (49681)	64 Echo (ping) req	quest i	d=0x0013, seq=6/1536, ttl=64 (no response found!)
1	15 2022-08-01 11:33:25.105806249	192.0.2.100	198.51.100.100	ICMP	108	0xc2e2 (49890)	64 Echo (ping) req	quest i	d=0x0013, seq=7/1792, ttl=64 (no response found!)
1	16 2022-08-01 11:33:25.105807895	192.0.2.100	198.51.100.100	ICMP	102	0xc2e2 (49890)	64 Echo (ping) req	quest i	d=0x0013, seq=7/1792, ttl=64 (no response found!)
1	17 2022-08-01 11:33:26.129836278	192.0.2.100	198.51.100.100	ICMP	108	0xc3b4 (50100)	64 Echo (ping) req	quest i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
1	18 2022-08-01 11:33:26.129838114	192.0.2.100	198.51.100.100	ICMP	102	0xc3b4 (50100)	64 Echo (ping) req	quest i	d=0x0013, seq=8/2048, ttl=64 (no response found!)
1	19 2022-08-01 11:33:27.153828653	192.0.2.100	198.51.100.100	ICMP	108	0xc476 (50294)	64 Echo (ping) req	quest i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
2	20 2022-08-01 11:33:27.153830201	192.0.2.100	198.51.100.100	ICMP	102	0xc476 (50294)	64 Echo (ping) req	quest i	d=0x0013, seq=9/2304, ttl=64 (no response found!)
2	21 2022-08-01 11:33:28.177847175	192.0.2.100	198.51.100.100	ICMP	108	0xc516 (50454)	64 Echo (ping) req	quest i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
2	22 2022-08-01 11:33:28.177849075	192.0.2.100	198.51.100.100	ICMP	102	0xc516 (50454)	64 Echo (ping) req	quest i	d=0x0013, seq=10/2560, ttl=64 (no response found!)
2	23 2022-08-01 11:33:29.201804760	192.0.2.100	198.51.100.100	ICMP	108	0xc578 (50552)	64 Echo (ping) req	quest i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
2	24 2022-08-01 11:33:29.201806488	192.0.2.100	198.51.100.100	ICMP	102	0xc578 (50552)	64 Echo (ping) req	quest i	d=0x0013, seq=11/2816, ttl=64 (no response found!)
2	25 2022-08-01 11:33:30.225834765	192.0.2.100	198.51.100.100	ICMP	108	0xc585 (50565)	64 Echo (ping) req	quest i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
2	26 2022-08-01 11:33:30.225836835	192.0.2.100	198.51.100.100	ICMP	102	0xc585 (50565)	64 Echo (ping) req	quest i	d=0x0013, seq=12/3072, ttl=64 (no response found!)
2	27 2022-08-01 11:33:31.249828955	192.0.2.100	198.51.100.100	ICMP	108	0xc618 (50712)	64 Echo (ping) req	quest i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
2	28 2022-08-01 11:33:31.249831121	192.0.2.100	198.51.100.100	ICMP	102	0xc618 (50712)	64 Echo (ping) req	quest i	d=0x0013, seq=13/3328, ttl=64 (no response found!)
2	29 2022-08-01 11:33:32.273867960	192.0.2.100	198.51.100.100	ICMP	108	0xc64f (50767)	64 Echo (ping) req	quest i	d=0x0013, seq=14/3584, ttl=64 (no response found!)
<									
> Eni	ame 2: 102 bytes on wire (816 bit	s), 102 bytes cap	otured (816 bits) or	interface ca	pture_u0	_1, id 0		0000	58 97 bd b9 77 0e 00 50 56 9d e8 be 81 00 00 66 X ··· w · P V ··· · · f
> Etł	hernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:be	e), Dst: Cisco b9:77	:0e (58:97:bd	:b9:77:0	e)		0010	08 00 45 00 00 54 c0 09 40 00 40 01 8d a3 c0 00 ···E··T·· @·@·····
✓ 802	2.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102						0020	02 64 c6 33 64 64 08 00 8d 7c 00 13 00 01 f2 b9 d.3dd
	000 = Priority: B	est Effort (defa	ult) (0)					0030	e7 62 00 00 00 00 cb 7f 06 00 00 00 00 00 10 11 b
	0 = DEI: Inelig	ible						0040	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	0000 0110 0110 = ID: 102							0050	22 23 24 25 26 27 28 29 28 20 20 20 20 20 21 30 31 #\$M& () "+,/01
	Type: IPv4 (0x0800)							0000	32 33 34 33 30 37 Z34307
> Int	ternet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100 _						
> Int	ternet Control Message Protocol		6						
_									

Open het opnamebestand voor de interface Ethernet1/9, selecteer de eerste en de tweede pakketten en controleer de belangrijkste punten:

- 1. Elk ICMP-echoantwoord wordt opgenomen en 2 keer weergegeven.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de uitgangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

No.	Time		Source	Destination	Protocol	Length	PD	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) r	eply	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) r	eply	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	084110 (20475)	04 ECHO (bruß) 1	epry	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	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) r	eply	1d=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) r	eply	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) r	eply	1d=0x0013, seq=9/2304, tt1=64
	19 2022-08-01	11:33:28.178469866	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) r	eply	1d=0x0013, seq=10/2560, tt1=64
	20 2022-08-01	11:33:28.178471810	198.51.100.100	192.0.2.100	ICMP	108	0x5493 (21651)	64 Echo (ping) r	epty	1d=0x0013, seq=10/2560, tt1=64
	21 2022-08-01	11:33:29.202395869	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) r	epty	1d=0x0013, seq=11/2816, tt1=64
	22 2022-08-01	11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54t4 (21748)	64 Echo (ping) r	epty	1d=0x0013, seq=11/2816, tt1=64
	23 2022-08-01	11:33:30.226398735	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) r	eply	1d=0x0013, seq=12/3072, tt1=64
	24 2022-08-01	11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) r	eply	1d=0x0013, seq=12/3072, tt1=64
	25 2022-08-01	11:33:31.250387808	198.51.100.100	192.0.2.100	ICMP	108	0x5512 (22002)	64 Echo (ping) r	epty	10=0X0013, seq=13/3328, tt1=64
	26 2022-08-01	11:33:31.250389971	198.51.100.100	192.0.2.100	ICMP	108	0x55f2 (22002)	64 Echo (ping) r	eply	1d=0x0013, seq=13/3328, tt1=64
	27 2022-08-01	11:33:32.274416011	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) r	epty	10-0x0013, seq=14/3584, tt1=64
	28 2022-08-01	11:33:32.2/4418229	198.51.100.100	192.0.2.100	ICMP	108	0x5660 (22112)	64 Echo (ping) r	epty	10-0x0013, seq=14/3584, tt1=64
сI	29 2022-08-01	11:33:33.298397657	198.51.100.100	192.0.2.100	TCHP	108	0x5007 (22247)	ea cono (bruĝ) u	epry	10=0X0013, Seq=15/3840, CC1=64
	Correct 100 hr	tes en vine (064 bit	<li>A 100 butos so</li>	aturad (Off hits) a	a intenface c	nture ut				0 00 50 55 0d a0 ha 50 07 hd h0 77 0a 90 35 00 00
2	Frame 1: 108 Dy	tes on wire (864 bit	s), 108 bytes ca	ptured (864 Dits) o	n interface ca	ipture_u0_	8, 10 0		0000	0 00 50 50 90 08 00 58 97 00 09 77 00 89 20 00 00 PV X W A
í.	Ethernet II, Sr	C: CISCO D3://:00 (5	819710010917710e	), Dst: vmware 9d:e	8:De (00:50:50	51901e810e	)		0020	40 01 3e 86 c6 33 64 64 c0 00 02 64 00 00 95 7c 0.5.3ddd
ň	vn-rag		- Directi	ons To Deidao					0030	0 00 13 00 01 f2 b9 e7 62 00 00 00 00 cb 7f 06 00bb
			- Pointer	wif id					0040	0 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
	00 0000 00	00 0000	= Doction	tion: A					0050	0 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ···· !"# \$%&'()"+
		a	= Looped:	No	4				0066	0 2c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
		A	= Posocial	di a	+					
			= Version							
			90 1010 = Source:	10						
	Type: 802.10	Virtual LAN (0x8100)	)	10						
J	802.10 Virtual	LAN, PRI' 0, DEL' 0.	ID: 102							
	000	= Priority:	Best Effort (defa	ult) (0)						
		= DEI: Ineli	rible		2					
	0000 01	10 0110 = ID: 102			2					
	Type: IPv4 (	0x0800)								
5	Internet Protoc	ol Version 4, Src: 1	98.51.100.100, D	st: 192.0.2.100						
>	Internet Contro	1 Message Protocol	, .		2					
	29 202-06-01           Frame 11: 108 bby           B02-06-01           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0           .0.0	<pre>rtes on wire (864 bit rc: cico b9:77:00 (5 00 0000</pre>	<pre>&gt;&gt;</pre>	192.0.2.100 ptured (864 bits) or ), Dst: VMware 90 on: To Bridge : vif_id tion: 0 NO d: 0 : 0 : 10 pult) (0) st: 192.0.2.100	a ninterface ca 8:be (00:50:50 4 3	100 ppture_u0_ :9d:e8:be	0x3067 (22247)	General (pring) r	0000 0011 0020 0033 0044 0055 0066	0       00       50       56       90       85       97       b0       97       0e       89       26       00       01       20       00       00       00       07       0e       00       05       7       6       89       26       00       00       00       00       00       00       00       00       00       00       01       12       14       15       16       17       18       10       10       10       10       10       10       10       10       10       10       10       11       11       11       11       15       16       17       18       10       10       10       10       11

No. Time	Source	Destination	Protocol	Length	1P 1D	IP TTL 11/0		
1 2022-08-01 11:33:19.071512698	198.51.100.100	192.0.2.100	ICMP	108 -	0x4f27 (20263)	64 Echo (ping) rep	ly	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) rep.	ly	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	0X4TTU (204/5)	os Ecno (ping) rep.	i y	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) repl	ly	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) repl	ly	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) repl	ly	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) repl	ly :	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) repl	ly :	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) repl	ly :	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) repl	ly :	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) rep	ly :	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) repl	ly :	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) rep	ly :	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) rep	ly :	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) rep.	ly :	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) rep	ly :	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) rep	ly :	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) rep.	ly	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) rep	ly	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) repl	ly	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) rep.	ly	id=0x0013, seq=11/2816, ttl=64
22 2022-08-01 11:33:29.202398067	198.51.100.100	192.0.2.100	ICMP	108	0x54f4 (21748)	64 Echo (ping) rep	ly	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) rep.	ly	id=0x0013, seq=12/3072, ttl=64
24 2022-08-01 11:33:30.226401017	198.51.100.100	192.0.2.100	ICMP	108	0x5526 (21798)	64 Echo (ping) rep.	ly	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) rep.	ly	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) rep.	ly	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) rep.	ly	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) rep.	ly	1d=0x0013, seq=14/3584, tt1=64
29 2022-08-01 11:33:33.298397657	198.51.100.100	192.0.2.100	ICMP	108	0x56e7 (22247)	64 Echo (ping) rep.	ly	id=0x0013, seq=15/3840, ttl=64
N								
> Frame 2: 108 bytes on wire (864 bit	s), 108 bytes ca	ptured (864 bits) o	n interface ca	pture_u0_	8, 1d 0			00 50 56 9d e8 be 58 97 bd b9 77 0e 89 26 00 00 PV ··· X ··· W ·· &··
> Ethernet II, Src: Cisco b9:77:0e (5	8:97:bd:b9:77:0e	), Dst: VMware 9d:e	8:be (00:50:50	:9d:e8:be	2)		0010	40 01 30 06 c6 33 64 64 c0 00 03 64 00 00 54 47 27 00 00T. E. 10
VN-Tag							0020	40 01 30 80 00 53 04 04 00 00 02 04 00 00 95 7C g
0	= Direct	ion: To Bridge						00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1b
.0	·· ···· = Pointer	*: v1t_1d					0050	1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b ····· !"# \$%&'()*+
	= Destina	ition: 0					0060	2 c 2d 2e 2f 30 31 32 33 34 35 36 37 ,/0123 4567
0	= Looped	NO d	4 1					
	= кезегче	ia: 0						
	= version	1: 0						
Turner 002 10 Vietural 148 (0:0100	00 1010 = Source:	10						
Type: 882.10 Virtual LAN (8X8188	70- 100		_					
and and an and an	Doct Effort (dof	w1+) (0)						
DET. Teoli	aible	urc) (0)						
0000 0110 0110 - 70: 103	Prove							
Tupe: TPv4 (0x0000)								
Internet Protocol Version A. Spc: 1	0.0 51 100 100 0	st: 102 0 2 100						
Internet Control Message Protocol		St. 192.0.2.100						
internet control nessage protocol								

### Uitleg

Als de optie **All Packets** in de **Application Capture Direction** is geselecteerd, worden er 2 simultane pakketopnamen geconfigureerd met betrekking tot de geselecteerde toepassingspoort Ethernet1/2: een opname op de voorinterface Ethernet1/2 en een opname op geselecteerde backplane interfaces.

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag. In dit voorbeeld identificeert de VLAN-tag 102 in ICMP-echoverdrachtpakketten Ethernet1/2 als de toegangsinterface.

Wanneer een pakketopname op een backplane interface is geconfigureerd, neemt de switch elk pakket twee keer op. De internal switch ontvangt pakketten die al zijn getagd door de applicatie op de security module met de port VLAN tag en de VN tag. De port VLAN-tag identificeert de uitgangsinterface die het interne chassis gebruikt om de pakketten door te sturen naar het netwerk. In dit voorbeeld identificeert de VLAN-tag 102 in ICMP-echoantwoordpakketten Ethernet1/2 als de uitgangsinterface.

De switch verwijdert de VN-tag en de interne VLAN-tag voordat de pakketten naar het netwerk worden doorgestuurd.

In deze tabel wordt de taak samengevat:

	Oppamenu	Interne poort VLAN		
Taak	nt	in opgenomen	Richting	Opgenomen verkeer

#### pakketten

Configureren en verifiëren van opnamen op applicatie-	Backplane interfaces	102	Alleen inspringe n	ICMP-echoantwoorden van h 198.51.100.100 op host 192.0.2.100
en toepassingspoort	Intorfago		Alleen	ICMP-echoverzoeken van ho
Ethernet1/2	Ethornot1/2	102	inspringe	192.0.2.10 naar host
	Elliemet 1/2		n	198.51.100.100

## Packet Capture op een subinterface van een fysieke of poortkanaal-interface

Gebruik FCM en CLI om een pakketopname op subinterface Ethernet1/2.205 of poortkanaalsubinterface Portchannel1.207 te configureren en te verifiëren. Subinterfaces en opnamen op subinterfaces worden alleen ondersteund voor de FTD-toepassing in containermodus. In dit geval wordt een pakketopname op Ethernet1/2.205 en Portchannel1.207 geconfigureerd.

#### Topologie, pakketstroom en de opnamepunten



### Configuratie

### FCM

Volg deze stappen op FCM om een pakketopname te configureren op de FTD-toepassing en de toepassingspoort Ethernet1/2:

1. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Delet	te All Sessions
No Session available		

2. Selecteer de specifieke toepassingsinstantie ftd1, de subinterface Ethernet1/2.205, geef de sessienaam op en klik op **Opslaan en Uitvoeren** om de opname te activeren:

Select an instance: ftd1	×				Save and Run Save Cancel
Subinterface selection Ethernet1/2.205 Ethernet1/2.206	ftd1	Ethernet1/2		Session Name* Selected Interfaces Buffer Size Snap length: Store Packets	Cap1        Ethernet1/2.205       256 MB       1518       Bytes       Overwrite       Append
		Ethernet1/1	FD Ethernet1/9. Ethernet1/10	Capture Filter	Apply Filter Capture All

3. In het geval van een poortkanaal-subinterface zijn vanwege de Cisco bug-ID <u>CSC33119</u> subinterfaces niet zichtbaar in de FCM. Gebruik de FXOS CLI om opnamen te configureren op poortkanaal-subinterfaces.

### **FXOS CLI**

Volg deze stappen op FXOS CLI om een pakketopname te configureren op subinterfaces Ethernet1/2.205 en Portchannel1.207:

1. Identificeer het toepassingstype en de identificatiecode:

firepower# firepower	<b>scope</b> /ssa #	ssa show app-inst	ance			
App Name	Identi	ifier Slot ID	Admin Stat	e Oper State	Running Versio	on Startup Version
Deploy Typ	e Turbo	Mode Profile	Name Cluster	State Clust	ter Role	
ftd	ftd1	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not App	licable None		
ftd	ftd2	1	Enabled	Online	7.2.0.82	7.2.0.82
Container	No	RP20	Not App	licable None		
	4		Lenne al links	for a stific	a a u milia li ali at a uf a a a a	

2. In het geval van een poort-kanaal-interface, identificeer zijn lidinterfaces:

firepower# connect fxo	S
<output skipped=""></output>	
<pre>firepower(fxos)# show</pre>	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 Pol(SU) Eth LACP Eth1/3(P) Eth1/3(P)
```

#### 3. Een opnamesessie maken:

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 subinterface 205
firepower /packet-capture/session/phy-port\* # up
firepower /packet-capture/session\* # enable
firepower /packet-capture/session\* # commit
firepower /packet-capture/session #

Voor poort-kanaal subinterfaces, maak een pakketopname voor elke poort-kanaal lidinterface:

```
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 #
Verificatie
```

#### vennca

#### FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

Overview Interfaces Logical Devices Security Engine Platform Settings				Syste	em Tools Help admin
Capture Session Fiter List					
				C Refresh Capture Session Dele	te Al Sessions
🔺 💽 cap1 Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	.8.2
Interface Name Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2.205 None	233992	cap1-ethernet-1-2-0.pcap	ftd1	<u>*</u>	

Poortkanaal subinterface-opnamen die op FXOS CLI zijn geconfigureerd, zijn ook zichtbaar op FCM; ze kunnen echter niet worden bewerkt:

Overview Interfac	ces Logical Devices Security Engine	Platform Settings				System Tools	Help admin
Capture Session R	ter List						
					Capture Session	Delete Al Sessions	9
a ap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes		4.8.0
Interface Name	Filter	File Size (in bytes)	File Name	Device Name			
Ethernet1/4.207	None	624160	cap1-ethernet-1-4-0.pcap	Not available			
Ethernet1/3.207	None	160	cap1-ethernet-1-3-0.pcap	Not available	*		

### **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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
Poortkanaal 1 met lidinterfaces Ethernet1/3 en 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

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
```

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketvastlegging om het opnamebestand te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader heeft de VLAN-tag 2005.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

No.	Time	Source	Destination	Protocol	Length	FD	IP TTL Info		
Г	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) requ	est i	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) requ	est i	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) requ	est i	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) requ	est i	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) requ	est i	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) requ	est i	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) requ	est i	d=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) requ	est i	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) requ	est i	d=0x0022, seq=13/3328, ttl=64 (no response found!)
1	10 2022-08-04 07:22:09.253946899	192.0.2.100	198.51.100.100	ICMP	102	0x9c0e (39950)	64 Echo (ping) requ	est i	id=0x0022, seq=13/3328, ttl=64 (no response found!)
1	11 2022-08-04 07:22:10.277953070	192.0.2.100	198.51.100.100	ICMP	112	0x9ccb (40139)	64 Echo (ping) requ	est i	id=0x0022, seq=14/3584, ttl=64 (no response found!)
1	12 2022-08-04 07:22:10.277954736	192.0.2.100	198.51.100.100	ICMP	102	0x9ccb (40139)	64 Echo (ping) requ	est i	id=0x0022, seq=14/3584, ttl=64 (no response found!)
1	13 2022-08-04 07:22:11.301931282	192.0.2.100	198.51.100.100	ICMP	112	0x9d84 (40324)	64 Echo (ping) requ	est i	d=0x0022, seq=15/3840, ttl=64 (no response found!)
1	14 2022-08-04 07:22:11.301933600	192.0.2.100	198.51.100.100	ICMP	102	0x9d84 (40324)	64 Echo (ping) requ	est i	id=0x0022, seq=15/3840, ttl=64 (no response found!)
1	15 2022-08-04 07:22:12.325936521	192.0.2.100	198.51.100.100	ICMP	112	0x9da2 (40354)	64 Echo (ping) requ	est i	d=0x0022, seq=16/4096, ttl=64 (no response found!)
1	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64 Echo (ping) requ	est i	id=0x0022, seq=16/4096, ttl=64 (no response found!)
1	17 2022-08-04 07:22:13.326988040	192.0.2.100	198.51.100.100	ICMP	112	0x9e07 (40455)	64 Echo (ping) requ	est i	d=0x0022, seq=17/4352, ttl=64 (no response found!)
1	18 2022-08-04 07:22:13.326990258	192.0.2.100	198.51.100.100	ICMP	102	0x9e07 (40455)	64 Echo (ping) requ	est i	id=0x0022, seq=17/4352, ttl=64 (no response found!)
1 3	19 2022-08-04 07:22:14.341944773	192.0.2.100	198.51.100.100	ICMP	112	0x9e6a (40554)	64 Echo (ping) requ	est i	d=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) requ	est i	d=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) requ	est i	d=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) requ	est i	d=0x0022, seq=19/4864, ttl=64 (no response found!)
1	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9fe8 (40936)	64 Echo (ping) requ	est i	d=0x0022, seq=20/5120, ttl=64 (no response found!)
1	24 2022-08-04 07:22:16.389975129	192.0.2.100	198.51.100.100	ICMP	102	0x9fe8 (40936)	64 Echo (ping) requ	est i	d=0x0022, seq=20/5120, ttl=64 (no response found!)
1	25 2022-08-04 07:22:17.413936452	192.0.2.100	198.51.100.100	ICMP	112	0xa079 (41081)	64 Echo (ping) requ	est i	d=0x0022, seq=21/5376, ttl=64 (no response found!)
1	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64 Echo (ping) requ	est i	d=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) requ	est i	d=0x0022, seq=22/5632, ttl=64 (no response found!)
<									
> En	ame 1: 112 bytes on wire (896 bit	s), 112 bytes cap	otured (896 bits) o	n interface ca	pture_u0_	1, id 0		0000	a2 76 f2 00 00 1b 00 50 56 9d e8 be 89 26 80 54 ···································
> Et	hernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:be	e), Dst: a2:76:f2:0	0:00:1b (a2:76	:f2:00:00	:1b)		0010	00 00 81 00 00 66 81 00 00 cd 08 00 45 00 00 54fET
✓ VN-	- Tag							0020	95 74 40 00 40 01 b8 38 c0 00 02 64 c6 33 64 64 ·t@·@·8 ···d·3dd
	1	= Directi	on: From Bridge					0030	08 00 eb 95 00 22 00 01 88 73 eb 62 00 00 00 00
	.0	= Pointer	: vif_id					0040	d9 9d 00 00 00 00 00 00 10 11 12 13 14 15 16 17
	00 0000 0101 0100	= Destina	tion: 84						28 29 2a 2b 2c 2d 2a 2f 38 31 32 33 34 35 36 37 ()*4/ 01234567
	···· ··· ··· ··· ··· 0 ····	= Looped:	No 🖌	11					20 25 20 20 20 20 20 20 20 20 50 50 50 55 54 55 50 57 () 1, 1, 02254507
		= Reserve	d: 0	· I					
		= Version	: 0						
	0000 000	00 0000 = Source:	0						
	Type: 802.1Q Virtual LAN (0x8100)	)							
✓ 80;	2.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102							
	000 = Priority: N	Best Effort (defa	ult) (0) 📕						
	0 = DEI: Inelig	gible		5 1					
	0000 0110 0110 = ID: 102								
	Type: 802.1Q Virtual LAN (0x8100)	)							
× 803	2.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 205							
	000 = Priority: 8	Best Effort (defa	ult) (0)						
	0 = DEI: Inelig	gible							
	0000 1100 1101 = ID: 205								
	Type: IPv4 (0x0800)		4	-					
> In	ternet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100						
> In	ternet Control Message Protocol								

Selecteer het tweede pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader heeft de VLAN-tag 2005.

N	. Time	Source	Destination	Protocol	Length	PD	IP TTL Info		
1	1 2022-08-04 07:21:56.993302102	192.0.2.100	198.51.100.100	ICMP	112	0x9574 (38260)	64 Echo (ping) requ	Jest :	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) requ	jest	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) requ	Jest	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) requ	lest :	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) requ	lest :	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) requ	jest :	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) requ	Jest :	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) requ	jest :	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) requ	Jest :	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) requ	lest :	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) requ	Jest 1	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) requ	Jest 1	id=0x0022, seg=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) requ	Jest :	id=0x0022, seg=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) requ	lest i	id=0x0022, seg=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) requ	Jest :	id=0x0022, seg=16/4096, ttl=64 (no response found!)
li	16 2022-08-04 07:22:12.325937895	192.0.2.100	198.51.100.100	ICMP	102	0x9da2 (40354)	64 Echo (ping) requ	lest :	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) requ	jest :	id=0x0022, seg=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) requ	Jest :	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) requ	Jest :	id=0x0022, seg=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) requ	lest :	id=0x0022, seg=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) requ	Jest :	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) requ	Jest :	id=0x0022, seq=19/4864, ttl=64 (no response found!)
I	23 2022-08-04 07:22:16.389973843	192.0.2.100	198.51.100.100	ICMP	112	0x9fe8 (40936)	64 Echo (ping) requ	Jest :	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	0x9fe8 (40936)	64 Echo (ping) requ	Jest 1	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) requ	Jest 1	id=0x0022, seq=21/5376, ttl=64 (no response found!)
li	26 2022-08-04 07:22:17.413938090	192.0.2.100	198.51.100.100	ICMP	102	0xa079 (41081)	64 Echo (ping) requ	Jest 1	id=0x0022, seg=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) requ	Jest :	id=0x0022, seg=22/5632, ttl=64 (no response found!)
ł						1 1			
Ê	serve as an hotel or since for hit		should find him he	Interfere en					
2	Frame 2: 102 bytes on wire (816 bit	s), 102 Dytes ca	ptured (816 Dits) on	interface ca	pture_ue_	1, 10 0		0000	42 /0 12 00 00 10 00 50 50 90 68 06 81 00 00 Cu
2	Ethernet II, Src: VMware 9d:e8:be (	00:50:56:9d:e8:b	e), Dst: a2:76:12:00:	00:10 (az:76	:12:00:00	9:10)		0010	03 64 66 33 64 64 08 00 eb 05 00 22 00 01 88 73 d 3dd"
ľ	802.10 VIFTUAL LAN, PRI: 0, DEI: 0,	10: 205						0030	eb 62 00 00 00 00 d9 9d 00 00 00 00 00 00 10 11
	000 = Priority: 1	Best Effort (deta	uit) (0)					0040	12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21
	= DEI: Inelig	gible	-					0050	22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 "#\$%&'() "+,/01
	0000 1100 1101 = ID: 205		2					0060	32 33 34 35 36 37 234567
	Type: IPv4 (0x0800)	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~							
12	Internet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100						
Р	Internet control Message Protocol								

Open nu de opnamebestanden voor Portchannel1.207. Selecteer het eerste pakket en controleer de belangrijkste punten

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader heeft de VLAN-tag 207.
- 3. De switch voegt een extra poort VLAN-tag **1001 in** die de toegangsinterface Portchannel1 identificeert.
- 4. Op de switch staat een extra VN-tag.

	Time	Source	Descriacion	PTODOCOI	Length	PD	B-11F NGO		
E.	1 2022-08-04 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) re	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
	2 2022-08-04 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) re	equest	id=0x007b, seq=0/0, ttl=255 (no response found!)
	3 2022-08-04 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) r	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	4 2022-08-04 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) re	equest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	5 2022-08-04 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-04 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) re	equest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	7 2022-08-04 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) re	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-04 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) re	equest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	9 2022-08-04 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	10 2022-08-04 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	Øx60a2 (24738)	255 Echo (ping) re	equest	id=0x007b, seg=4/1024, ttl=255 (no response found!)
	11 2022-08-04 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) re	equest	id=0x007b, seg=5/1280, ttl=255 (no response found))
	12 2022-08-04 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) r	equest	id=0x007b, seg=5/1280, ttl=255 (no response found1)
	13 2022-08-04 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) re	equest	id=0x007b, seg=6/1536, ttl=255 (no response found1)
	14 2022-08-04 08:18:24.575919057	192,168,247,100	192,168,247,102	TCMP	118	9x69a4 (24749)	255 Echo (ping) r	equest	id=0x007b, seg=6/1536, ttl=255 (no response found))
	15 2022-08-04 08:18:24.576407671	192,168,247,100	192.168.247.102	TCMP	128	8x68a5 (24741)	255 Echo (ping) r	equest	id=0x007b, seg=7/1792, ttl=255 (no response found))
	16 2022-08-04 08:18:24 576408585	192.168.247.100	192.168.247.102	TCMP	118	0x60a5 (24741)	255 Echo (ping) r	equest	id=0x007b, seg=7/1792, ttl=255 (no response found))
	17 2022-08-04 08:18:24 576885643	192.168.247.100	192.168.247.102	TCMP	128	8x68a6 (24742)	255 Echo (ping) r	equest	id=0x007b, seq=9/2048, tt]=255 (no response found1)
	19 2022-09-04 09:10:24 576996561	102 169 247 100	102 169 247 102	TCMP	119	0x60a6 (24742)	255 Echo (ping) r	equest	id=0x007b, seq=0/2049, ttl=255 (no response foundl)
	10 2022-00-04 00:10:24:570000501	102 160 247 100	102 169 247 102	TCMD	120	0x60a7 (24742)	255 Echo (ping) r	aquest	id-0x007b, seq-0/2046, cc1-255 (no response found1)
	20 2022-00-04 00:10:24:577304320	102 160 247 100	102 169 247 102	TCMD	110	0x60a7 (24743)	255 Echo (ping) n	equest	id-0x007b, seq-0/2304, ttl-255 (no response found!)
	20 2022-00-04 00:10:24.577555254	192.108.247.100	192.108.247.102	TCMD	110	0x00a7 (24745)	255 Echo (ping) n	equest	id=0x0070, seq=0/2560, ttl=255 (no response found!)
	21 2022-08-04 08:18:24.577967052	192.108.247.100	192.108.247.102	TCHP	120	0x0008 (24744)	255 Echo (ping) In	equest	id-0x007b, seq=10/2500, ttl=255 (no response found!)
	22 2022-08-04 08:18:24.577989290	192.168.247.100	192.168.247.102	TCHP	118	0x60a8 (24744)	255 Echo (ping) P	equest	id-exempts, seq=10/2560, ttl=255 (no response found!)
	23 2022-08-04 08:18:24.5/8448/81	192.168.247.100	192.168.247.102	TCMP	128	0x60a9 (24745)	255 Echo (ping) P	equest	Id=0x007b, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-04 08:18:24.578449909	192.168.247.100	192.168.247.102	TCMP	118	0x60a9 (24745)	255 Echo (ping) P	equest	1d=0x00/D, seq=11/2016, ttl=255 (no response found!)
	25 2022-08-04 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) r	equest	1d=0x007D, seq=12/3072, tt1=255 (no response found!)
	26 2022-08-04 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) r	equest	1d=0x007b, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-04 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) r	equest	1d=0x007b, seq=13/3328, ttl=255 (no response found!)
<									
> 1	Frame 1: 128 bytes on wire (1024 bits	), 128 bytes capt	tured (1024 bits) o	n interface ca	pture u0	3. id 0		0000	a2 76 f2 00 00 1c 00 17 df d6 ec 00 89 26 80 3d
>	Ethernet II, Src; Cisco d6:ec:00 (00:	17:df:d6:ec:00).	Dst: a2:76:f2:00:0	0:1c (a2:76:f)	:00:00:10	)		0010	00 00 81 00 03 e9 81 00 00 cf 08 00 45 00 00 64E.d
1	VN-Tag					·		0020	60 9e 00 00 ff 01 ea dd c0 a8 f7 64 c0 a8 f7 66 `df
L I	1	ad a set of a set							
		$\dots$ = Direction	: From Bridge					0030	08 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78 ·····{·····N·Jx
	.0	= Direction	: From Bridge vif id					0030 0040	08 00 e5 c8 00 7b 00 00 00 00 00 02 4d 8c 4a 78
	.00 0000 0011 1101	= Direction = Pointer: = Destinati	: From Bridge vif_id on: 61					0030 0040 0050	08 09 e5 c8 00 7b 00 00 00 00 00 2 d4 8c 4a 78 ·····{······························
	.00 0000 0011 1101	= Direction = Pointer: = Destinati	: From Bridge vif_id on: 61	4				0030 0040 0050 0060	08         00         e5         c8         00         7b         00         00         00         00         24         8c         4a         78
	.0. 00 0000 0011 1101 0. 	= Direction = Pointer: = Destinati = Looped: N = Reserved:	: From Bridge vif_id on: 61 0	4				0030 0040 0050 0060 0070	08         00         e5         c8         00         00         00         00         2         d4         c4         7.8
	.0. .00 0000 0011 1101 0.  .00	<pre> = Direction  = Pointer:  = Destinati  = Looped: N  = Reserved:  = Version:</pre>	: From Bridge vif_id on: 61 0 0	4				0030 0040 0050 0060 0070	08         00         e5         c8         00         00         00         00         24         d8         c4         a7
	. 0	= Direction = Pointer: = Destinati = Looped: N = Reserved: = Version: = Source: 0	: From Bridge vif_id on: 61 0 0 0	4				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00         00 00 02 dd 8 c4 a 78
	.0	<pre> = Direction  = Pointer:  = Destinati  = Looped: N  = Reserved:  = Version: 0000 = Source: 0</pre>	:: From Bridge vif_id on: 61 0 0 0	4				0030 0040 0050 0050 0070	08         00         e5         c8         00         b0         00         00         24         d8         c4         a78
	.000 0000 0011 1101	<pre> = Direction  = Pointer:  = Destinati  = Looped: N  = Reserved:  = Version: 0000 = Source: 0 D: 1001</pre>	: From Bridge vif_id on: 61 0 θ θ	4				0030 0040 0050 0050 0070	08 00 e5 c8 00 70 00 00       00 00 00 2 dd 8 c4a 78       (H-)x         ab cd ab cd ab cd ab cd       ab cd ab cd ab cd
~ 2	.0. 0000 0011 1101	<pre> = Direction  = Pointer:  = Destinati  = Looped: N  = Reserved:  = Version: 0000 = Source: 0 D: 1001 t Effort (defaul)</pre>	:: From Bridge vif_id on: 61 0 0 0 0	4				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8c 4a 78       ( N-1x)         ab cd ab cd ab cd ab cd       ab cd ab cd ab cd
~ 3	.000 0000 0011 1101	<pre> = Direction = Pointer: = Destinati = Looped: N = Reserved: = Version: 00000 = Source: 0 D: 1001 tt Effort (defaul No</pre>	: From Bridge vif_id on: 61 0 0 0 1 1 1 1 0 1 0	4				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8 c4 a 78
~ 3	.0. 00000 0011 1101	= Direction = Pointer: = Destinati = Looped: N = Reserved: = Version: 0000 = Source: 0 D: 1001 st Effort (defaul ple	: From Bridge vif_id on: 61 0 θ	3				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 dd 8 c4a 78
~ 3	.e	<pre> = Direction = Pointer: = Destinati = Looped: N = Reserved: = Version: 0000 = Source: 0 D: 1001 .t Effort (defaul lle</pre>	: From Bridge vif_id οn: 61 Θ Θ t) (0)	4 3				0030 0040 0050 0060 0070	08 00 e5 c6 00 70 00 00       00 00 02 4d 8c 4a 78
•	.0. 00000 0011 1101	<pre>Direction</pre>	: From Bridge vif_id on: 61 0 0 0 0 1 1 (0)	4				0030 0040 0050 0060 0070	08 00 eS c8 00 70 00 00       00 00 00 2 dd 8 c4 a 78
•	.000 0000 0011 1101	<pre> = Direction = Pointer: = Destinati = Looped: N = Reserved: = Version:</pre>	: From Bridge vif_id on: 61 0 0 0 0 t) (0)	3				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8c 4a 78
• = • =	.00 0000 0011 1101	<pre>Direction</pre>	: From Bridge vif_id on: 61 0 0 0 1 1 1 (0)	3				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8c 4a 78      (HXx)         ab cd
<ul> <li>→ 3</li> <li>→ 3</li> </ul>	.0	<pre> = Pointer:  = Pointer:  = Looped: N  = Reserved:  = Reserved:  = Version: 0000 = Source: 0 D: 1001 le D: 207 tt Effort (defaul le</pre>	<pre>: From Bridge vif_id on: 61 0 0 0 t) (0) t) (0)</pre>	4				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8c 4a 78      (
<ul> <li>■</li> </ul>	.0	<pre> = Pointer:  = Pointer:  = Looped: N  = Looped: N  = Reserved:  = Version: 0000 = Source: 0 D: 1001 D: 1001 D: 207 tt Effort (defaul le</pre>	: From Bridge vif_id on: 61 0 0 1 t) (0)	4				0030 0040 0050 0050 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8 (4a 78)      (H-1x)         ab cd
<ul> <li>■</li> <li>■</li> </ul>	.0	<pre> = Pointer:  = Pointer:  = Looped: N  = Reserved:  = Version: 0000 = Source: 0 D: 1001 D: 1001 D: 207 t: 267 t: 267 t</pre>	: From Bridge vif_id on: 61 0 0 0 t) (0)	4 3 2				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8c 4a 78      (H-1x)         ab cd
• •	.e	= Pointer: = Pointer: = Looped: N = Looped: N = Version: 0000 = Source: 0 D: 1001 D: 1001 D: 207 D: 207 Lt Effort (defaul le 	:: From Bridge vif_id on: 61 0 0 t) (0) t) (0) t: 192.168.247.102	4 3 2				0030 0040 0050 0050 0070	08 00 e5 c8 00 70 00 00       00 00 02 4d 8 (4a 78      (H-1x)         ab cd
	.0. 00000 0011 1101	= Pointer: = Pointer: = Destinati = Looped: N = Reserved: = Version: 00000 = Source: 0 00: 1001 .t Effort (defaul le .168.247.100, Dst	:: From Bridge vif_id on: 61 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 1 1 1 1 0 1	4 3 2				0030 0040 0050 0060 0070	08 00 e5 c8 00 70 00 00       00 00 02 d3 c4 378      (H-1x)         ab cd

Selecteer het tweede pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader heeft de VLAN-tag 207.

N;	a, Time		Source	Destination	Protocol	Length	PD	PTTL Info		
r.	1 2022-08-0	4 08:18:24.572548869	192.168.247.100	192.168.247.102	ICMP	128	0x609e (24734)	255 Echo (ping) red	quest	ld=0x007b, seq=0/0, ttl=255 (no response found!)
	2 2022-08-0	4 08:18:24.572550073	192.168.247.100	192.168.247.102	ICMP	118	0x609e (24734)	255 Echo (ping) rec	quest	id=0x007b, seq=0/0, ttl=255 (no response found!)
	3 2022-08-0	4 08:18:24.573286630	192.168.247.100	192.168.247.102	ICMP	128	0x609f (24735)	255 Echo (ping) rea	quest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	4 2022-08-0	4 08:18:24.573287640	192.168.247.100	192.168.247.102	ICMP	118	0x609f (24735)	255 Echo (ping) red	quest	id=0x007b, seq=1/256, ttl=255 (no response found!)
	5 2022-08-0	4 08:18:24.573794751	192.168.247.100	192.168.247.102	ICMP	128	0x60a0 (24736)	255 Echo (ping) red	quest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	6 2022-08-0	4 08:18:24.573795748	192.168.247.100	192.168.247.102	ICMP	118	0x60a0 (24736)	255 Echo (ping) red	quest	id=0x007b, seq=2/512, ttl=255 (no response found!)
	7 2022-08-0	M 08:18:24.574368638	192.168.247.100	192.168.247.102	ICMP	128	0x60a1 (24737)	255 Echo (ping) red	quest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	8 2022-08-0	M 08:18:24.574369574	192.168.247.100	192.168.247.102	ICMP	118	0x60a1 (24737)	255 Echo (ping) rea	quest	id=0x007b, seq=3/768, ttl=255 (no response found!)
	9 2022-08-0	M 08:18:24.574914512	192.168.247.100	192.168.247.102	ICMP	128	0x60a2 (24738)	255 Echo (ping) red	quest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	10 2022-08-0	4 08:18:24.574915415	192.168.247.100	192.168.247.102	ICMP	118	0x60a2 (24738)	255 Echo (ping) red	quest	id=0x007b, seq=4/1024, ttl=255 (no response found!)
	11 2022-08-0	4 08:18:24.575442569	192.168.247.100	192.168.247.102	ICMP	128	0x60a3 (24739)	255 Echo (ping) rea	quest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	12 2022-08-0	4 08:18:24.575443601	192.168.247.100	192.168.247.102	ICMP	118	0x60a3 (24739)	255 Echo (ping) red	quest	id=0x007b, seq=5/1280, ttl=255 (no response found!)
	13 2022-08-0	4 08:18:24.575918119	192.168.247.100	192.168.247.102	ICMP	128	0x60a4 (24740)	255 Echo (ping) red	quest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	14 2022-08-0	4 08:18:24.575919057	192.168.247.100	192.168.247.102	ICMP	118	0x60a4 (24740)	255 Echo (ping) rea	quest	id=0x007b, seq=6/1536, ttl=255 (no response found!)
	15 2022-08-0	4 08:18:24.576407671	192.168.247.100	192.168.247.102	ICMP	128	0x60a5 (24741)	255 Echo (ping) rea	quest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	16 2022-08-0	4 08:18:24.576408585	192.168.247.100	192.168.247.102	ICMP	118	0x60a5 (24741)	255 Echo (ping) red	quest	id=0x007b, seq=7/1792, ttl=255 (no response found!)
	17 2022-08-0	4 08:18:24.576885643	192.168.247.100	192.168.247.102	ICMP	128	0x60a6 (24742)	255 Echo (ping) rea	quest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	18 2022-08-0	4 08:18:24.576886561	192.168.247.100	192.168.247.102	ICMP	118	0x60a6 (24742)	255 Echo (ping) rea	quest	id=0x007b, seq=8/2048, ttl=255 (no response found!)
	19 2022-08-0	4 08:18:24.577394328	192.168.247.100	192.168.247.102	ICMP	128	0x60a7 (24743)	255 Echo (ping) red	quest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	20 2022-08-0	M 08:18:24.577395234	192.168.247.100	192.168.247.102	ICMP	118	0x60a7 (24743)	255 Echo (ping) red	quest	id=0x007b, seq=9/2304, ttl=255 (no response found!)
	21 2022-08-0	4 08:18:24.577987632	192.168.247.100	192.168.247.102	ICMP	128	0x60a8 (24744)	255 Echo (ping) red	quest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
	22 2022-08-0	4 08:18:24.577989290	192.168.247.100	192.168.247.102	ICMP	118	0x60a8 (24744)	255 Echo (ping) red	quest	id=0x007b, seq=10/2560, ttl=255 (no response found!)
Ш	23 2022-08-0	4 08:18:24.578448781	192.168.247.100	192.168.247.102	ICMP	128	0x60a9 (24745)	255 Echo (ping) red	quest	id=0x007b, seq=11/2816, ttl=255 (no response found!)
	24 2022-08-0	4 08:18:24.578449909	192.168.247.100	192.168.247.102	ICMP	118	0x60a9 (24745)	255 Echo (ping) rec	quest	id=0x007b, seq=11/2816, ttl=255 (no response found!)
Ш	25 2022-08-0	4 08:18:24.578900043	192.168.247.100	192.168.247.102	ICMP	128	0x60aa (24746)	255 Echo (ping) red	quest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
н	26 2022-08-0	4 08:18:24.578900897	192.168.247.100	192.168.247.102	ICMP	118	0x60aa (24746)	255 Echo (ping) red	quest	id=0x007b, seq=12/3072, ttl=255 (no response found!)
	27 2022-08-0	4 08:18:24.579426962	192.168.247.100	192.168.247.102	ICMP	128	0x60ab (24747)	255 Echo (ping) red	quest	id=0x007b, seq=13/3328, ttl=255 (no response found!)
<										
>	Frame 2: 118 by	tes on wire (944 bits)	, 118 bytes captu	red (944 bits) on i	nterface capt	ure_u0_3,	id 0		0000	a2 76 f2 00 00 1c 00 17 df d6 ec 00 81 00 00 cf .v
>	Ethernet II, Sr	c: Cisco d6:ec:00 (00:	17:df:d6:ec:00),	Dst: a2:76:f2:00:00	:1c (a2:76:f2	:00:00:1c	)		0010	08 00 45 00 00 64 60 9e 00 00 ff 01 ea dd c0 a8 ··E··d`· ·····
Ŷ	802.1Q Virtual	LAN, PRI: 0, DEI: 0, I	0: 207						0020	f7 64 c0 a8 f7 66 08 00 e5 c8 00 7b 00 00 00 00 ·d···f·· ···{···
	000	= Priority: Bes	t Effort (default	t) (0)					0030	00 02 4d 8c 4a 78 ab cd ab cd ab cd ab cd ab cd ab cd ··M·Jx······
		= DEI: Ineligib	le						0040	ab cd
	0000 110	0 1111 = ID: 207			21				0050	ab cd
	Type: IPv4 (6	x0800)			~ 1				0000	ab cd ab cd ab cd
>	Internet Protoc	ol Version 4, Src: 192	168.247.100, Dst	: 192.168.247.102					0070	
>	Internet Contro	l Message Protocol								
•										

#### Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag. Bovendien, in het geval van subinterfaces, in de opnamebestanden, bevat elk tweede pakket niet de poort VLAN-tag.

In deze tabel wordt de taak samengevat:

Taak	Opnamep unt	Interne poort VLAN in opgenomen pakketten	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op subinterface Ethernet1/2.205	Ethernet1/ 2.2005	102	Alleen inspring en	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100
Configureer en controleer een pakketopname op Portchannel1 subinterface met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet1/ 3G Ethernet 1/4	1001	Alleen inspring en	ICMP-echoverzoeken van 192.168.207.100 voor host 192.168.207.102

### PacketCapture filters

Gebruik FCM en CLI om een pakketopname op interface Ethernet1/2 met een filter te configureren en te verifiëren.

#### Topologie, pakketstroom en de opnamepunten



#### Configuratie

#### FCM

Volg deze stappen op FCM om een opnamefilter te configureren voor ICMPechoverdrachtpakketten van host 192.0.2.100 naar host 198.51.100.100 en pas deze toe op pakketopname op interface Ethernet1/2:

- 1. Gebruik Gereedschappen > Packet Capture > Filterlijst > Filter toevoegen om een opnamefilter te maken.
- 2. Specificeer de filternaam, het protocol, de bron van IPv4, de bestemming van IPv4 en klik op Opslaan:

Overview Interfa	aces Logical Devices Se	curity Engine Plat	form Settings									System Tools	Help admin	
Capture Session	iter List											_		
Filter List												Ad	i Filter	
Filter Name		From				То			Protocol	Inner vian	Outer vlan	EtherType		
(her inter	MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port				Current Ppe	40	
hiter_icmp	00:00:00:00:00:00	192.0.2.100		0	00:00:00:00:00:00	192.0.2.100		0	1	0	0	0	Ø 0	
				_										
				Edit Packe	t Filter			(? ×						
				Filter Name*	filter_icmp									
				Protocol	ICMP_IPv4									
				EtherType	Any 👻									
				Inner vlan	0	Outer vlan	0							
				Source		Destination		_						
				IPv4	192.0.2.100	IPv4	198.51.100.100							
				IPv6	::	IPv6	:							
				Port	0	Port	0							
				MAC	00:00:00:00:00	MAC	00:00:00:00:00:00	D						
							Save	Cancel						

3. Gebruik Gereedschappen > Packet Capture > Capture Session om een nieuwe opnamesessie te maken:

Overview Interfaces Logical Devices Security Engine Platform Settings	System	Tools Help admin
	Packet Capture	Troubleshooting Logs
Capture Session Filter List		
C Refresh	Capture Session Dele	te All Sessions
No Session available		

4. Selecteer Ethernet1/2, geef de **sessienaam op,** pas het opnamefilter toe en klik op **Opslaan en Uitvoeren** om de opname te activeren:

Overview Interfaces Logical Devices Security Engine Platform Settings	System Tools Help admin
Select an instance: ftd1 v	Seve and Run Seve Cancel
ftd1	Session Name* cap1
Ethemet1/2	Selected Interfaces     Ethernet1/2       Buffer Size     256 MB       Snap length:     1518       Store Packets     Civerwrite
Ethernet1/3 FTD Ethernet1/9, Ethernet1/10	Capture Filter Capture Filter Capture Another
Ethemet1/1	

### **FXOS CLI**

Volg deze stappen op FXOS CLI om pakketopnamen op backplane interfaces te configureren:

1. Identificeer het toepassingstype en de identificatiecode:

```
firepower# scope ssa
firepower /ssa# show app-instance
                         Admin State Oper State Running Version Startup Version
       Identifier Slot ID
App Name
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
 _____ _ ____ ____ ____ ____ ____
      1
                          Enabled Online
        ftd1
ftđ
                                                 7.2.0.82
                                                              7.2.0.82
Native
                             Not Applicable None
         No
2. Identificeer het IP-protocolnummer in https://www.iana.org/assignments/protocol-
```

numbers/protocol-numbers.xhtml. In dit geval is het ICMP-protocolnummer 1.

3. Een opnamesessie maken:

```
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 #
```

### Verificatie

#### FCM

Controleer de **interfacenaam**, zorg ervoor dat de **operationele status** omhoog is en dat de **bestandsgrootte (in bytes)** toeneemt:

Ovi	verview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin													
Cap	ture Session 📑	Filter List												
Fil	Filter List Ad Plan													
_							-							
	ilter Name		From				Тө			Protocol	Inner vlan	Outer vlan	EtherType	
		MAC	IPv4	IPv6	Port	MAC	IPv4	IPv6	Port					
L	filter_icmp	00:00:00:00:00:00	192.0.2.100		0	00:00:00:00:00:00	198.51.100.100		0	1	0	0	0	/8

Controleer de interfacenaam, het **filter**, controleer of de **operationele status** is ingesteld en of de **bestandsgrootte (in bytes)** toeneemt in **Gereedschappen > Packet Capture > Capture Session**:

Overview Interfaces	ogical Devices Security Engine	e Platform Settings					System Tools Help admin
Capture Session Filter List	:						
						C Refresh Capture Session	Delete All Sessions
	Drep Count: 0		nerational States up		Buffas Cize: 256 MB	Coro Lanothy 1518 Ruday	
Сарх	brop count. o	Op	perational state, up		60116F 5126, 250 H6	Shap Cengun, 1510 bytes	
Interface Name	Filter	File Size (in bytes)	File Name	Device Name			
Ethernet1/2	filter_icmp	84340	cap1-ethernet-1-2-0.pcap	ftd1	*		

### **FXOS CLI**

Controleer de opnamedetails in scope-pakketopname:

```
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
Opnamebestanden verzamelen
```

Volg de stappen in het gedeelte Verzamel Firepower 4100/9300 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketvastlegging om het opnamebestand te openen. Selecteer het eerste pakket en controleer de belangrijkste punten

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer opgenomen en getoond.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.
- 4. Op de switch staat een extra VN-tag.

No. Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info							^
1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 -	0x0012	(18)	64 Echo	(ping)	request	id=0x0018,	seq=349/23809	, ttl=64	(no r	
2 2022-08-02 15:46:55.603279688	192.0.2.100	198.51.100.100	ICMP	102	0x0012	(18)	64 Echo	(ping)	request	id=0x0018,	seq=349/23809	, ttl=64	(no r	
3 2022-08-02 15:46:56.627139252	192.0.2.100	198.51.100.100	ICMP	108	0x00db	(219)	64 Echo	(ping)	request	id=0x0018,	seq=350/24065	, ttl=64	(no r	
4 2022-08-02 15:46:56.627140919	192.0.2.100	198.51.100.100	ICMP	102	0x00db	(219)	64 Echo	(ping)	request	id=0x0018,	seq=350/24065	, ttl=64	(no r	
5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb	(459)	64 Echo	(ping)	request	id=0x0018,	seq=351/24321	, ttl=64	(no r	
6 2022-08-02 15:46:57.651186787	192.0.2.100	198.51.100.100	ICMP	102	0x01cb	(459)	64 Echo	(ping)	request	id=0x0018,	seq=351/24321	, ttl=64	(no r	
7 2022-08-02 15:46:58.675153317	192.0.2.100	198.51.100.100	ICMP	108	0x01d6	(470)	64 Echo	(ping)	request	id=0x0018,	seq=352/24577	, ttl=64	(no r	
8 2022-08-02 15:46:58.675154503	192.0.2.100	198.51.100.100	ICMP	102	0x01d6	(470)	64 Echo	(ping)	request	id=0x0018,	seq=352/24577	, ttl=64	(no r	
9 2022-08-02 15:46:59.699152639	192.0.2.100	198.51.100.100	ICMP	108	0x01f4	(500)	64 Echo	(ping)	request	id=0x0018,	seq=353/24833	, ttl=64	(no r	
10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4	(500)	64 Echo	(ping)	request	id=0x0018,	seq=353/24833	, ttl=64	(no r	
11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9	(505)	64 Echo	(ping)	request	id=0x0018,	seq=354/25089	, ttl=64	(no r	
12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9	(505)	64 Echo	(ping)	request	id=0x0018,	seq=354/25089	, ttl=64	(no r	
13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e	(622)	64 Echo	(ping)	request	id=0x0018,	seq=355/25345	, ttl=64	(no r	
14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e	(622)	64 Echo	(ping)	request	id=0x0018,	seq=355/25345	, ttl=64	(no r	
15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc	(700)	64 Echo	(ping)	request	id=0x0018,	seq=356/25601	, ttl=64	(no r	
16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc	(700)	64 Echo	(ping)	request	id=0x0018,	seq=356/25601	, ttl=64	(no r	
17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f	(815)	64 Echo	(ping)	request	id=0x0018,	seq=357/25857	, ttl=64	(no r	
18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f	(815)	64 Echo	(ping)	request	id=0x0018,	seq=357/25857	, ttl=64	(no r	
19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f	(1039)	64 Echo	(ping)	request	id=0x0018,	seq=358/26113	, ttl=64	(no r	
20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f	(1039)	64 Echo	(ping)	request	id=0x0018,	seq=358/26113	. ttl=64	(no r	~
<						,,		(10/					>	
Ename 1: 100 butes on wine (964 bit	(c) 100 but os co	ntured (964 hits)	on interface c	antuno un	1 1 00	00 59 0	a7 bd ba 77 a	00 50	se od e	2 bo 90 26	90.03 Y	. P. V	2	_
Sthemat II Spei Whang OdioSibe	aaisaissiadiaaih	a) Dett Circo bu	77:00 (59:07:h	dib0177100	, 1 00	10 00 0	30 81 00 00 00 6	5 08 00	45 00 0	0 54 00 12	40.00		A.	
VIN-Tag	00.30.30.90.00.0	e), DSC. CISCO D9.	77.00 (38.97.0	u.09.77.0e	00	20 40 0	01 4d 9b c0 0	02 64	c6 33 6	54 64 08 00	9e 67 @·M···	·d ·3dd··	e	
vivi- Tag	- Dinecti	on, Enom Bridge			00	030 00 t	18 01 5d e2 4d	5 e9 62	00 00 0	00 00 c1 a6	0c 00 ···]·F	·b · · · · ·		
A	- Pointer	wif id			00	040 00 (	00 00 00 10 1	1 12 13	14 15 1	6 17 18 19	1a 1b			
00 0000 0000 1010	- Dostina	tion: 10			00	50 1c :	1d 1e 1f 20 2:	1 22 23	24 25 2	26 27 28 29	2a 2b ···· !	"# \$%&'()	)*+	
	- Looped	No.			00	60 2c 3	2d 2e 2f 30 3:	1 32 33	34 35 3	36 37	,/01	23 4567		
	- Rosonwa	d a	• •											
	- Vension													
	= version													
Turner, 002 10 Vintural Latt (0000 00	00 0000 = Source.	0												
Page 10 Victual LAN DELLA DELLA	10: 102													
- Boionitus	IU: 102 Post Effort (dof:	w1+) (0)												
obs = priority:	mible	uit) (0)	2											
0000 0110 0110 - TD: 102	BIDIG	-	' I											
0000 0110 0110 = 1D: 102														
Type: IPV4 (0x0800)	00 0 0 100 Det.	100 51 100 100	_											
Internet Protocol Version 4, Src: 1	92.0.2.100, DSC:	198.51.100.100												
Internet Control Message Protocol														
1														

Selecteer het tweede pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen. Elk pakket wordt 2 keer

opgenomen en getoond.

- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.
- 3. De switch voegt extra poort VLAN-tag **102 in** die de toegangsinterface Ethernet1/2 identificeert.

No.	Time	Source	Destination	Protocol	Length	PD		IP TTL Info						-	^
-	1 2022-08-02 15:46:55.603277760	192.0.2.100	198.51.100.100	ICMP	108 -	0x0012 (1	8)	64 Echo	(ping)	request	id=0x0018,	seg=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 (1	8)	64 Echo	(ping)	request	id=0x0018,	seg=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 (2	19)	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	exeedb (2	19)	64 Echo	(ping)	request	id=0x0018,	seq=350/24065,	tt1=64 (	(no r	
	5 2022-08-02 15:46:57.651185193	192.0.2.100	198.51.100.100	ICMP	108	0x01cb (4	59)	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 (4	(59)	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 (4	70)	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 (4	70)	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 (5	(00)	64 Echo	(ping)	request	id=0x0018,	seq=353/24833,	ttl=64 (	(no r	
1	10 2022-08-02 15:46:59.699153835	192.0.2.100	198.51.100.100	ICMP	102	0x01f4 (5	(00)	64 Echo	(ping)	request	id=0x0018,	seq=353/24833,	ttl=64 (	(no r	
1	11 2022-08-02 15:47:00.723142641	192.0.2.100	198.51.100.100	ICMP	108	0x01f9 (5	05)	64 Echo	(ping)	request	id=0x0018,	seq=354/25089,	ttl=64 (	(no r	
1	12 2022-08-02 15:47:00.723144643	192.0.2.100	198.51.100.100	ICMP	102	0x01f9 (5	05)	64 Echo	(ping)	request	id=0x0018,	seq=354/25089,	ttl=64 (	(no r	
1	13 2022-08-02 15:47:01.747162204	192.0.2.100	198.51.100.100	ICMP	108	0x026e (6	22)	64 Echo	(ping)	request	id=0x0018,	seq=355/25345,	ttl=64 (	(no r	
1	14 2022-08-02 15:47:01.747163783	192.0.2.100	198.51.100.100	ICMP	102	0x026e (6	22)	64 Echo	(ping)	request	id=0x0018,	seq=355/25345,	ttl=64 (	(no r	
1	15 2022-08-02 15:47:02.771209952	192.0.2.100	198.51.100.100	ICMP	108	0x02bc (7	/00)	64 Echo	(ping)	request	id=0x0018,	seq=356/25601,	ttl=64 (	(no r	
1	16 2022-08-02 15:47:02.771211062	192.0.2.100	198.51.100.100	ICMP	102	0x02bc (7	'00)	64 Echo	(ping)	request	id=0x0018,	seq=356/25601,	ttl=64 (	(no r	
1	17 2022-08-02 15:47:03.772258550	192.0.2.100	198.51.100.100	ICMP	108	0x032f (8	315)	64 Echo	(ping)	request	id=0x0018,	seq=357/25857,	ttl=64 (	(no r	
1	18 2022-08-02 15:47:03.772259724	192.0.2.100	198.51.100.100	ICMP	102	0x032f (8	315)	64 Echo	(ping)	request	id=0x0018,	seq=357/25857,	ttl=64 (	(no r	
1	19 2022-08-02 15:47:04.791118519	192.0.2.100	198.51.100.100	ICMP	108	0x040f (1	.039)	64 Echo	(ping)	request	id=0x0018,	seq=358/26113,	ttl=64 (	(no r	
1 2	20 2022-08-02 15:47:04.791119721	192.0.2.100	198.51.100.100	ICMP	102	0x040f (1	.039)	64 Echo	(ping)	request	id=0x0018,	seq=358/26113,	ttl=64 (	(no r	~
<														>	
> En	ame 2: 102 bytes on wire (816 bit	s), 102 bytes cap	otured (816 bits) or	interface ca	pture u0 1	, it 0000	58 97 b	d b9 77 0	e 00 50	56 9d e	8 be 81 00	00 66 X ···· w··	P V · · · · ·	٠f	
> Et	hernet II, Src: VMware_9d:e8:be (	00:50:56:9d:e8:b	e), Dst: Cisco_b9:77	:0e (58:97:bd	:b9:77:0e)	0010	08 00 4	5 00 00 5	4 00 12	40 00 4	10 01 4d 9b	c0 00 ··E··T·	· @·@·M·		
× 80	2.1Q Virtual LAN, PRI: 0, DEI: 0,	ID: 102				0020	02 64 c	6 33 64 6	4 08 00	9e 67 6	18 01 5d	e2 46 ·d·3dd·	· ·g···]	٠F	
	000 E Priority: E	Best Effort (defa	ult) (0)			0030	e9 62 0	0 00 00 0	0 c1 a6	0c 00 0	00 00 00 00	10 11 ·b·····		·: ·	
	0 = DEI: Inelig	gible	3			0040	12 13 1	4 15 16 1	7 18 19	1a 1b 1	c 1d 1e 1f	20 21		1	
	0000 0110 0110 = ID: 102		-			0050	22 23 2	4 25 26 2	7 28 29	2a 20 2	20 20 2e 2t	30 31 #\$%& (	) -+,/(	81	
	Type: IPv4 (0x0800)					0000	32 33 3	4 33 30 3	<i>,</i>			234507			
> In	ternet Protocol Version 4, Src: 1	92.0.2.100, Dst:	198.51.100.100												
> In	ternet Control Message Protocol		21												

### Uitleg

Wanneer een pakketopname op een frontinterface is geconfigureerd, neemt de switch elk pakket tweemaal tegelijk op:

- Na de invoeging van de poort VLAN-tag.
- Na het inbrengen van de VN-tag.

In de volgorde van bewerkingen wordt de VN-tag in een later stadium ingevoegd dan de invoeging van de VLAN-tag in de poort. Maar in het opnamebestand wordt het pakket met de VN-tag eerder weergegeven dan het pakket met de poort VLAN-tag.

Wanneer een opnamefilter wordt toegepast, worden alleen de pakketten opgenomen die overeenkomen met het filter in de invoerrichting.

In deze tabel wordt de taak samengevat:

Taak	Opnam epunt	Interne poort VLAN in opgenomen pakketten	Richtin g	Eigen filter	Opgenomen verkeer
Configureer en controleer een pakketopname met een filter op de voorinterface Ethernet1/2	Etherne t1/2	102	Alleen insprin gen	Protocol: ICMP Bron:192.0.2.1 00 Bestemming: 198.51.100.100	ICMP-echoverzoeken van h 192.0.2.10 naar host 198.51.100.100

## Opnamebestanden van FirePOWER 4100/9300 interne Switch verzamelen

FCM

Volg deze stappen op FCM om interne switch-opnamebestanden te verzamelen:

#### 1. Klik op de knop Sessie uitschakelen om de actieve opname te stoppen:

Overview Interfaces Lo	gical Devices Security Engine	Platform Settings			System To	ools Help admin
Capture Session Filter List						
					C Refresh Capture Session Delete All Ses	isions
Cap1	Drop Count: 0	Operational State: up	Buffer Size: 256 MB		Snap Length: 1518 Bytes	9.8.2
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2	None	34700	cap1-ethernet-1-2-0.pcap	ftd1	⊻	

#### 2. Zorg ervoor dat de operationele status DOWN is - Session\_Admin\_Shut:

Overview Interfaces	Logical Devices Security Engine	Platform Settings				System T	ools Help	ə admin
Capture Session Fiter L	st							
				c	Refresh Capture Session	Delete Al Se	ssions	
a 🕞 cap1	Drop Count: 0	Operational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB		Snap Length: 1518 Bytes		0	68
Interface Name	Filter	File Size (in bytes)	File Name	Device Name				
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	<u></u>			

#### 3. Klik op **Downloaden** om het opnamebestand te downloaden:

Overview Interfaces Logical	Devices Security Engine Flat	onn settings			System 100is	neip aumin
Capture Session Filter List						
				C Ref	resh Capture Session Delete Al Sessions	•
a D cap1	Drop Count: 0 Ope	erational State: DOWN - Session_Admin_Shut	Buffer Size: 256 MB	Sna	ap Length: 1518 Bytes	/88
Interface Name	Filter	File Size (in bytes)	File Name	Device Name		
Ethernet1/2	None	218828	cap1-ethemet-1-2-0.pcap	ftd1	Ł	

In het geval van poort-kanaal interfaces, herhaal deze stap voor elke lidinterface.

#### **FXOS CLI**

Volg deze stappen op de FXOS CLI om opnamebestanden te verzamelen:

1. Stop de actieve opname:

```
firepower# scope packet-capture
firepower /packet-capture # scope session cap1
firepower /packet-capture/session # disable
firepower /packet-capture/session* # commit
firepower /packet-capture/session # up
firepower /packet-capture # show session cap1 detail
Traffic Monitoring Session:
   Packet Capture Session Name: cap1
   Session: 1
   Admin State: Disabled
   Oper State: Down
   Oper State Reason: Admin Disable
   Config Success: Yes
  Config Fail Reason:
  Append Flag: Overwrite
   Session Mem Usage: 256 MB
  Session Pcap Snap Len: 1518 Bytes
  Error Code: 0
  Drop Count: 0
Physical ports involved in Packet Capture:
  Slot Id: 1
   Port Id: 2
```

```
Pcapfile: /workspace/packet-capture/session-1/cap1-ethernet-1-2-0.pcap
Pcapsize: 115744 bytes
Filter:
Sub Interface: 0
Application Instance Identifier: ftd1
Application Name: ftd
```

2. Upload het opnamebestand vanuit het bereik van de opdracht 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:
scn:
          Dest File URI
          Dest File URI
scp:
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
```

ftp://ftpuser@10.10.10.1/cap1-etherne
Password:

In het geval van poort-kanaal interfaces, kopieer het opnamebestand voor elke lidinterface.

## Richtlijnen, beperkingen en beste praktijken voor Interne Switch PacketCapture

Raadpleeg voor de richtlijnen en beperkingen met betrekking tot Firepower 4100/9300 interne switch-opname de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS Chassis Manager* of de *configuratiehandleiding voor Cisco Firepower 4100/9300 FXOS CLI*, hoofdstuk **Problemen oplossen**, paragraaf **Packet Capture**.

Dit is de lijst met best practices op basis van het gebruik van pakketvastlegging in TAC-gevallen:

- Let op richtlijnen en beperkingen.
- Leg pakketten vast op alle poortkanaallidinterfaces en analyseer alle opnamebestanden.
- Gebruik opnamefilters.
- Overweeg de impact van NAT op IP-adressen van pakketten wanneer een opnamefilter is geconfigureerd.
- Vergroot of verlaag de Magnetische Lens die de framegrootte aangeeft voor het geval dat deze verschilt van de standaardwaarde van 1518 bytes. Een kortere grootte resulteert in een hoger aantal opgenomen pakketten en vice versa.
- Pas de **buffergrootte** naar wens aan.
- Let op de **Drop Count** op FCM of FXOS CLI. Zodra de grens van de buffergrootte wordt bereikt, stijgt de teller van de dalingstelling.
- Gebruik het filter **!vntag** op Wireshark om alleen pakketten weer te geven zonder de VN-tag. Dit is handig om VN-getagde pakketten te verbergen in de voorste pakketopnamebestanden.
- Gebruik het filter frame.number&1 op Wireshark om alleen oneven frames weer te geven. Dit is handig om dubbele pakketten te verbergen in de pakketopnamebestanden van de backplane interface.
- In het geval van protocollen zoals TCP, past Wireshark door gebrek kleuringsregels toe die pakketten met specifieke voorwaarden in verschillende kleuren tonen. In het geval van een interne switch wordt het pakket op basis van dubbele pakketten in opnamebestanden

opgenomen, zodat het pakket op een fout-positieve manier kan worden gekleurd en gemarkeerd. Als u pakketopnamebestanden analyseert en een filter toepast, exporteert u de weergegeven pakketten naar een nieuw bestand en opent u het nieuwe bestand.

# Configuratie en verificatie op Secure-firewall 3100

In tegenstelling tot Firepower 4100/9300, legt de switch in de Secure Firewall 3100 vast op de opdrachtregelinterface van de toepassing via de opdracht **Capture <name> switch**, waarin de **switch** Option aangeeft dat de opnamen op de switch zijn geconfigureerd.

Dit is de opnameopdracht met de switch optie:

#### > 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></cr>	

De algemene stappen voor de configuratie van de pakketopname zijn als volgt:

1. Specificeer een toegangsinterface:

Switch Capture Configuration accepteert de **ingangsinterface nameif**. De gebruiker kan namen van gegevensinterfaces, interne uplink, of de beheersinterfaces specificeren:

#### > 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. Specificeer het Ethernet kader EtherType. Het standaard EtherType is IP. De optiewaarden van het **Ethernet-type** specificeren EtherType:

```
> capture capsw switch interface inside ethernet-type ?
802.1Q
<0-65535> Ethernet type
arp
ip
ip6
pppoed
pppoes
rarp
```

sgt vlan

3. Specificeer de overeenkomende voorwaarden. De optie **Capture** match specificeert de matchcriteria:

```
> capture capsw switch interface inside match ?
<0-255> Enter protocol number (0 - 255)
ah
 eigrp
esp
are
icmp
icmp6
iqmp
igrp
ip
ipinip
ipsec
mac
         Mac-address filter
nos
ospf
pcp
pim
pptp
sctp
snp
         SPI value
spi
 tcp
udp
 <cr>
```

4. Specificeer andere optionele parameters zoals de buffergrootte, de pakketlengte, enzovoort.

5. Schakel de opname in. Het commando no Capture <name> switch stop activeert de opname:

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

6. Controleer de opnamegegevens:

- De beheerstatus is ingeschakeld, en de operationele status is ingesteld en actief.
- De grootte van het pakketopnamebestand wordt verhoogd.
- Het aantal opgenomen pakketten in de uitvoer van de show Capture <cap\_name> is niet nul.
- Opname pad **pcapfile.** De opgenomen pakketten worden automatisch opgeslagen in de map /mnt/disk0/packet-capture/.
- Opnameomstandigheden. De software maakt automatisch opnamefilters op basis van de opnameomstandigheden.

enabled

up

Admin State:

Oper State:

#### 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.pcapPcapsize:18838Filter: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. Stop de opnamen indien nodig:

```
> capture capsw switch stop
>show capture capsw detail
Packet Capture info
 Name:
                   capsw
                 1
Session:
 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
                   0
Drop Count:
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
```

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. Verzamel de opnamebestanden. Volg de stappen in het gedeelte **Verzamel Secure Firewall 3100 Internal Switch Capture Files**.

In versie 7.2 wordt de switch-opnameconfiguratie niet ondersteund door het VCC of de FDM. Switch In het geval van ASA-softwareversie 9.18(1) en hoger kunnen internethelefoonopnamen worden geconfigureerd in ASDM-versies 7.18.1.x en hoger.

Deze scenario's zijn gebaseerd op veelgebruikte cases van Secure Firewall 3100 interne switch.

## PacketCapture op een fysieke of poortkanaal-interface

Gebruik de FTD of ASA CLI om een pakketopname op interface Ethernet1/1 of Portchannel1 interface te configureren en te verifiëren. Beide interfaces hebben de naam **vanbinnen**.

#### Topologie, pakketstroom en de opnamepunten



			Cha	ssis	
		Internal Switch		Security Module	
		Pod		FTD/ASA	
192.0.2.100	ICMP echo-request	211/2 S	Uplink	inside	
198.51.100.100	ICMP echo-reply			outside	

## Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface Ethernet1/1 of poortkanaal1:

1. Controleer de naam:

> show nameif		
Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0
> show nameif	Name	Security
Port-channel1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0
2. Een opnamesessie	maken:	

- > capture capsw switch interface inside
  - 3. De opnamesessie inschakelen:

#### > no capture capsw switch stop Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Capsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

> show capture capsw detail
Packet Capture info
Name: capsw
Session: 1
Admin State: enabled
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 /mnt/disk0/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap Pcapfile: Pcapsize: 12653 capsw-1-1 Filter: Packet Capture Filter Info capsw-1-1 Name: Protocol: 0 Ivlan: 0 Ovlan: 0 0.0.0.0 Src Ip: 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 0 Dest Port: 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 In het geval van Port-channel1 wordt de opname op alle lidinterfaces geconfigureerd:

> show capture capsw detail Packet Capture info Session: capsw 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 28824 Pcapsize: Filter: capsw-1-4

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
Dest MAC:	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 F	'ilter Info
Name:	capsw-1-3
Protocol:	0
Ivlan:	0
Ovlan:	0
Src Ip:	0.0.0
Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	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

De poortkanaals lidinterfaces kunnen in de FXOS local-mgmt commando shell worden geverifieerd via de show portchannel summiere opdracht:

```
> 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
_____
                  Protocol Member Ports
Group Port-
            Туре
   Channel
_____
   Pol(U) Eth LACP Eth1/3(P) Eth1/4(P)
1
```

```
LACP KeepAlive Timer:
```

Ethertype:

Dest Port:

0 0

\_\_\_\_\_

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Secure Firewall 3100 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor Ethernet1/1 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.

geval van multi-context, stel het bevel in de admincontext in werking.

2. De oorspronkelijke pakketheader is zonder de VLAN-tag.

No	. Time	Source	Destination	Protocol	Length	IP ID	IP TT	TL Info						^
	1 2022-08-07 19:50:06.925768	192.0.2.100	198.51.100.100	ICMP	102	0x9a10 (39	440) 6	54 Echo (ping)	request	id=0x0034,	seq=1/256, tt	l=64 (no	res	
	2 2022-08-07 19:50:07.921684	192.0.2.100	198.51.100.100	ICMP	102	0x9a3a (39	482) 6	54 Echo (ping)	request	id=0x0034,	seq=2/512, tt	l=64 (no	res	
	3 2022-08-07 19:50:08.924468	192.0.2.100	198.51.100.100	ICMP	102	0x9aa6 (39	590) 6	54 Echo (ping)	request	id=0x0034,	seq=3/768, tt	l=64 (no	res	
	4 2022-08-07 19:50:09.928484	192.0.2.100	198.51.100.100	ICMP	102	0x9afe (39	678) 6	54 Echo (ping)	request	id=0x0034,	seq=4/1024, t	tl=64 (no	re i	
	5 2022-08-07 19:50:10.928245	192.0.2.100	198.51.100.100	ICMP	102	0x9b10 (39	696) 6	54 Echo (ping)	request	id=0x0034,	seq=5/1280, t	tl=64 (no	re i	
	6 2022-08-07 19:50:11.929144	192.0.2.100	198.51.100.100	ICMP	102	0x9b34 (39	732) 6	54 Echo (ping)	request	id=0x0034,	seq=6/1536, t	tl=64 (no	re	
	7 2022-08-07 19:50:12.932943	192.0.2.100	198.51.100.100	ICMP	102	0x9b83 (39	811) 6	54 Echo (ping)	request	id=0x0034,	seq=7/1792, t	tl=64 (no	re .	
	8 2022-08-07 19:50:13.934155	192.0.2.100	198.51.100.100	ICMP	102	0x9b8b (39	819) 6	54 Echo (ping)	request	id=0x0034,	seq=8/2048, t	tl=64 (no	P PE	
	9 2022-08-07 19:50:14.932004	192.0.2.100	198.51.100.100	ICMP	102	0x9c07 (39	943) 6	54 Echo (ping)	request	id=0x0034,	seq=9/2304, t	tl=64 (no	re	
	10 2022-08-07 19:50:15.937143	192.0.2.100	198.51.100.100	ICMP	102	0x9cc6 (40	134) 6	54 Echo (ping)	request	id=0x0034,	seq=10/2560,	ttl=64 (n	io r	
	11 2022-08-07 19:50:16.934848	192.0.2.100	198.51.100.100	ICMP	102	0x9d68 (40	296) 6	54 Echo (ping)	request	id=0x0034,	seq=11/2816,	ttl=64 (n	io r	
	12 2022-08-07 19:50:17.936908	192.0.2.100	198.51.100.100	ICMP	102	0x9ded (40	429) 6	54 Echo (ping)	request	id=0x0034,	seq=12/3072,	ttl=64 (n	io r	
	13 2022-08-07 19:50:18.939584	192.0.2.100	198.51.100.100	ICMP	102	0x9e5a (40	538) 6	54 Echo (ping)	request	id=0x0034,	seq=13/3328,	ttl=64 (n	io r	
	14 2022-08-07 19:50:19.941262	192.0.2.100	198.51.100.100	ICMP	102	0x9efb (40	699) 6	54 Echo (ping)	request	id=0x0034,	seq=14/3584,	ttl=64 (n	io r	
	15 2022-08-07 19:50:20.940716	192.0.2.100	198.51.100.100	ICMP	102	0x9f50 (40	784) 6	54 Echo (ping)	request	id=0x0034,	seq=15/3840,	ttl=64 (n	io r	
	16 2022-08-07 19:50:21.940288	192.0.2.100	198.51.100.100	ICMP	102	0x9fe4 (40	932) 6	54 Echo (ping)	request	id=0x0034,	seq=16/4096,	ttl=64 (n	io r	
	17 2022-08-07 19:50:22.943302	192.0.2.100	198.51.100.100	ICMP	102	0xa031 (41	009) 6	54 Echo (ping)	request	id=0x0034,	seq=17/4352,	ttl=64 (n	o r	
	18 2022-08-07 19:50:23.944679	192.0.2.100	198.51.100.100	ICMP	102	0xa067 (41	063) 6	54 Echo (ping)	request	id=0x0034,	seq=18/4608,	ttl=64 (n	o r	~
<													>	-
>	Frame 1: 102 bytes on wire (816 bits	), 102 bytes capt	ured (816 bits)			0000 b	c e7 12 34	9a 14 00 50	56 9d e8	be 08 00 45	00 ····4····F	V····Е		_
>	Ethernet II. Src: VMware 9d:e8;be (0	0:50:56:9d:e8:be)	Dst: Cisco 34:9a:1	4 (bc:e7:12:3	4:9a:14)	0010 0	9 54 9a 10	40 00 40 01	b3 9c c0	00 02 64 c6	33 ·T··@·@·	·····d-7	3	
>	Internet Protocol Version 4, Src: 19	2.0.2.100. Dst: 19	98.51.100.100		-	0020 6	4 64 08 00	c6 91 00 34	00 01 61	17 f0 62 00	00 dd · · · · 4	···a··b··		
>	Internet Control Message Protocol				2	0030 0	0 00 18 ec	08 00 00 00	00 00 10	11 12 13 14	15			
	0					0040 1	5 17 18 19	1a 1b 1c 1d	1e 1f 20	21 22 23 24	25	··· !"#\$?	6	
						0050 2	5 27 28 29	2a 2b 2c 2d	2e 2f 30	31 32 33 34	35 &'()*+,-	./012345	5	
						0060 3	5 37 55 55	55 55			670000			

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
- 2. De oorspronkelijke pakketheader is zonder de VLAN-tag.

No.	Time	Source	Destination	Protocol	Length	PD	IP TTL Info		^
E.	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 re	ś
	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 re	s
	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 re	5
	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 r	e
	5 2022-08-07 20:41:02.660624	192.0.2.100	198.51.100.100	ICMP	102	0x94a4 (38052)	64 Echo (ping) request	id=0x0035, seq=5/1280, ttl=64 (no r	é 👘
	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 r	é 👘
	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 r	e i
	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 r	e
	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 r	e
	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 i
	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 i
	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 i
	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 i
	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 i
	16 2022-08-07 20:41:13.674903	192.0.2.100	198.51.100.100	ICMP	102	0x9a84 (39556)	64 Echo (ping) request	id=0x0035, seq=16/4096, ttl=64 (no	r i
	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 i
	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	s), 102 bytes cap	tured (816 bits)			0000 bc e7 12	34 9a 2c 00 50 56 9d e8	be 08 00 45 00 ···4·, ·P V····E·	
>	Ethernet II, Src: VMware_9d:e8:be (6	00:50:56:9d:e8:be	), Dst: Cisco_34:9a	:2c (bc:e7	12:34:9a:2c)	0010 00 54 92	96 40 00 40 01 bb 16 c0	00 02 64 c6 33 ·T··@·@· ·····d·3	
>	Internet Protocol Version 4, Src: 19	92.0.2.100, Dst:	198.51.100.100		-	0020 64 64 08	00 58 a8 00 35 00 01 4d	23 f0 62 00 00 dd · · X · · 5 · · M# · b · ·	
>	Internet Control Message Protocol				2	0030 00 00 9e	c8 04 00 00 00 00 00 10	11 12 13 14 15	
6						0040 16 17 18	19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25!"#\$%	
						0050 26 27 28	29 28 20 2C 2d 2e 2f 30	51 52 55 54 55 & ()*+,/012345	
						0000 36 37 55	22 22 22	670000	

## Uitleg

De switch Captures worden geconfigureerd op interfaces Ethernet1/1 of Portchannel1.

In deze tabel wordt de taak samengevat:

Taak	Opnamep unt	Intern filter	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op interface Ethernet1/1	Ethernet1/ E1	None	Alleen inspring en	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.10
Configureer en controleer een pakketopname op interface Portchannel1 met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet1/ 3G Ethernet 1/4	None	Alleen inspring en	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.10

## Packet Capture op een subinterface van een fysieke of poortkanaal-interface

Gebruik de FTD of ASA CLI om een pakketopname op subinterfaces Ethernet1/1.205 of Portchannel1.205 te configureren en te verifiëren. Beide subinterfaces hebben de naam **erin**.

### Topologie, pakketstroom en de opnamepunten



				Cha	ssis		
		Inte	rnal Switch			Security Module	
		Po1.20				FTD/ASA	
192.0.2.100	ICMP echo-request			Uplink	in	side	
		Eth1/2					
	CMP echo-reply				0	utside	
198.51.100.100	)				-		

## Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface Ethernet1/1 of poortkanaal1:

1. Controleer de naam:

> 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. Een opnamesessie	maken:	

- > capture capsw switch interface inside
  - 3. De opnamesessie inschakelen:

#### > no capture capsw switch stop Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

> show capture capsw detail
Packet Capture info
Name: capsw
Session: 1
Admin State: enabled
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 capsw-1-1 Filter: Packet Capture Filter Info capsw-1-1 Name: Protocol: 0 Ivlan: 0 Ovlan: 205 0.0.0.0 Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 0 Dest Port: 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 dit geval wordt een filter met router VLAN **Ovlan=205** gemaakt en op de interface toegepast.

In het geval van Port-channel1 wordt de opname met een filter **Ovlan=205** geconfigureerd op alle lidinterfaces:

<pre>&gt; show capture capsv</pre>	/ 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 I	Jen: 1518
Error Code:	0
Drop Count:	0
Total Physical ports	s 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 H	Filter Info
Name:	capsw-1-4
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0.0
Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	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 H	Filter Info
Name:	capsw-1-3
Protocol:	0
Ivlan:	0
Ovlan:	205
Src Ip:	0.0.0
Dest Ip:	0.0.0
Src Ipv6:	::
Dest Ipv6:	::
Src MAC:	00:00:00:00:00
Dest MAC:	00:00:00:00:00
Src Port:	0

Total Physical breakout ports involved in Packet Capture: 0

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

0 0

Dest Port: Ethertype:

Reading of capture file from disk is not supported

De poortkanaals lidinterfaces kunnen in de FXOS **local-mgmt** commando shell worden geverifieerd via de **show portchannel** summiere opdracht:

> 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 R - Routed S - Switched U - Up (port-channel) M - Not in use. Min-links not met \_\_\_\_\_ Group Port-Type Protocol Member Ports Channel \_\_\_\_\_

1	Pol(U)	Eth LA	ACP Et	ch1/3(P)	Eth1/4(P)		
LACP	KeepAliv	re Timer:					
	Channel	PeerKeepAliveTi	imerFast				
1	Pol(U)	False					
Clust	er LACP	Status:					
	Channel	ClusterSpanned	ClusterDe	etach Clust	erUnitID (	ClusterSysID	
1	Pol(U)	False	False	0		clust	

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Secure Firewall 3100 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor Ethernet1/1.205 te openen. Selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
- 2. De oorspronkelijke pakketheader heeft VLAN-tag 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		^
<b>_</b>	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 re	ts in
	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 re	15
	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 re	is .
	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 r	*e
	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 r	<b>•</b> €
	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 r	۱e
	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 r	۱e
	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 r	۱e
	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 r	۱e
	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	r
	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	r
	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	r
	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	r
	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	r
	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	r
	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	r
	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	r
	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	r v
<								2	Þ
> En	ame 1: 106 bytes on wire (848 bits)	, 106 bytes capt	ured (848 bits)			0000 bc e7 12	2 34 9a 14 00 50 56 9d e8	be 81 00 00 cd 4 P V	
> Eti	hernet II, Src: VMware 9d:e8:be (00	:50:56:9d:e8:be)	Dst: Cisco 34:9a:	14 (bc:e7:12:3	4:9a:14)	0010 08 00 49	5 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····	
~ 80	2.1Q Virtual LAN, PRI: 0, DEI: 0, I	D: 205	-			0020 02 64 c6	5 33 64 64 08 00 06 67 06	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
	000 Bes	t Effort (defaul	t) (0)			0030 f0 62 00	00000008efe 03000	00 00 00 10 11 ·b·····	
	0 = DEI: Ineligit	ole				0040 12 13 14	15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
	0000 1100 1101 = ID: 205				-	0050 22 23 24	1 25 26 27 28 29 2a 2b 20	2d 2e 2f 30 31 "#\$%&"() "+,/01	
	Type: IPv4 (0x0800)				2	0000 32 33 34	1 35 36 37 55 55 55 55	23456700 00	
	Trailer: 55555555								
> In	ternet Protocol Version 4, Src: 192	.0.2.100, Dst: 19	98.51.100.100						
> In	ternet Control Message Protocol								
-									

Open de opnamebestanden voor Portchannel1-lidinterfaces. Selecteer het eerste pakket en controleer de belangrijkste punten:

- 1. Alleen ICMP-echoverdrachtpakketten worden opgenomen.
- 2. De oorspronkelijke pakketheader heeft VLAN-tag 205.

No.	Time	Source	Destination	Protocol	Length	IP ID	IP TTL Info		^
E.	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 re	
	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 re	
	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 re	
	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 re	
	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 re	
	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 re	
	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 r	
	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 r	
	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 r	
	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 r	
	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 r	
	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 r	
	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 r	
	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 r	
	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 r	~
<								>	
> Fra	me 1: 106 bytes on wire (848 bits)	, 106 bytes capt	ured (848 bits)			0000 bc e7 1	2 34 9a 14 00 50 56 9d e8	be 81 00 00 cd 4 P V	
> Eth	ernet II, Src: VMware_9d:e8:be (00	0:50:56:9d:e8:be)	, Dst: Cisco_34:9a	:14 (bc:e7:12:	34:9a:14)	0010 08 00 4	5 00 00 54 41 1f 40 00 40	01 0c 8e c0 00 ··E··TA·@·@·····	
✓ 802	.1Q Virtual LAN, PRI: 0, DEI: 0, I	ID: 205				0020 02 64 c	6 33 64 64 08 00 06 67 00	37 00 01 b0 2c ·d·3dd·· ·g·7···,	
	000 Be: = Priority: Be:	st Effort (defau	lt) (0)			0030 10 62 0	0 00 00 00 8e fe 03 00 00	00 00 00 10 11 ·b·····	
н.	0 = DEI: Ineligi	ble				0040 12 13 1	4 15 16 17 18 19 1a 1b 1c	1d 1e 1f 20 21	
	0000 1100 1101 = ID: 205				2	0050 22 23 2	4 25 26 27 28 29 28 20 20 A 25 36 37 55 55 55 55	20 20 27 30 31 #\$4& () -+,/01	
1	Type: IPv4 (0x0800)				- 2	0000 32 33 3	4 55 50 57 55 55 55 55	25456700 00	
1	Trailer: 55555555								
> Int	ernet Protocol Version 4, Src: 192	2.0.2.100, Dst: 1	98.51.100.100						
> Int	ernet Control Message Protocol								

### Uitleg

De switch neemt op worden geconfigureerd op subinterfaces Ethernet1/1.205 of Portchannel1.205 met een filter dat overeenkomt met router VLAN 205.

In deze tabel wordt de taak samengevat:

Taak	Opname punt	Intern filter	Richtin g	Opgenomen verkeer
Configureer en controleer een pakketopname op subinterface Ethernet1/1.205	Ethernet 1/E1	Buiten VLAN 2015	Alleen insprin gen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.
Configureer en controleer een pakketopname op subinterface Portchannel1.205 met lidinterfaces Ethernet1/3 en Ethernet1/4	Ethernet 1/3G Ethernet 1/4	Buiten VLAN 2015	Alleen insprin gen	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100.

## Packet Capture op interne interfaces

De Secure Firewall heeft 2 interne interfaces:

- in\_data\_uplink1 sluit de applicatie aan op de switch.
- in\_mgmt\_uplink1 biedt een speciaal pakketpad voor beheerverbindingen, zoals SSH naar de beheerinterface of de beheerverbinding, ook bekend als de sftunnel, tussen het FMC en het FTD.

#### Taak 1

Gebruik de FTD of ASA CLI om een pakketopname te configureren en te verifiëren op de uplinkinterface **in\_data\_uplink1**.

Topologie, pakketstroom en de opnamepunten



### Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface in\_data\_uplink1:

1. Een opnamesessie maken:

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

2. De opnamesessie inschakelen:

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

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

```
> show capture capsw detail
Packet Capture info
 Name:
                   capsw
                 1
Session:
                  enabled
 Admin State:
 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
                  0
Error Code:
                   0
Drop Count:
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
```

E	Packet	Capture	Filter	Info
	Name:		Ca	apsw-1-18
	Protoc	col:	0	
	Ivlan	:	0	
	Ovlan	:	0	
	Src Ir	p:	0	.0.0.0
	Dest 1	[p:	0	.0.0.0
	Src Ip	pv6:	:	:
	Dest 1	Lbnę:	:	:
	Src MA	AC:	00	0:00:00:00:00:00
	Dest N	AC:	00	0:00:00:00:00:00
	Src Pc	ort:	0	
	Dest I	Port:	0	
	Ethert	:zype	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 dit geval wordt er een opname gemaakt op de interface met een interne ID **18** die de in\_data\_uplink1 interface op de Secure Firewall 3130 is. De opdracht **switch status** van **show portmanager** in de opdrachtshell van **FXOS local-mgmt** toont de interface-ID's:

#### > 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 \_\_\_\_\_ \_\_\_\_ 1G Full None 0/1SGMII Up Link-Up Up 1G Full None 0/2 SGMII Link-Up Full 1G None Link-Up 0/3 SGMII Up 0/4 SGMII 1G Full None Link-Up Up Down 1G Half None 0/5 SGMII Mac-Link-Down 0/6 SGMII Down 1G Half None Mac-Link-Down Half None 0/7 SGMII Down 1G Mac-Link-Down Half None 0/8 SGMIT Down 1G Mac-Link-Down Full Down 1G 1000\_BaseX 0/9 None Link-Down Down Full 0/10 1000\_BaseX 1G None Link-Down 1000\_BaseX Down 1G Full None Link-Down 0/11 1000\_BaseX Full None 0/12 Down 1G Link-Down 0/13 1000\_BaseX Down 1G Full None Link-Down 0/14 1000 BaseX Down 1G Full None Link-Down Full None 0/15 1000\_BaseX Down 1G Link-Down Full 0/16 1000\_BaseX Down 1GNone Link-Down 1000\_BaseX 0/17 Up 1G Full None Link-Up Full KR2 50G Link-Up 0/18 Up None 25G Full 0/19 KR Up None Link-Up 0/20 KR Up 25G Full None Link-Up 0/21 KR4 Down 40G Full None Link-Down Full 0/22 n/a Down n/a N/A Reset Full 0/23 n/a Down n/a N/A Reset Full 0/24 n/a Down n/a N/A Reset 0/25 1000\_BaseX Down 1G Full None Link-Down n/a Down n/a Full N/A 0/26 Reset 0/27 n/a Down n/a Full N/A Reset 0/28 n/a Down n/a Full N/A Reset 1000\_BaseX Full None 0/29 Down 1GLink-Down Full 0/30 n/a Down n/a N/A Reset Full 0/31 n/a Down n/a 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

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Secure Firewall 3100 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketopnamebestanden om de opnamebestanden voor interface in\_data\_uplink1 te openen. Controleer het belangrijkste punt - in dit geval worden ICMP- echoverzoek en echoantwoordpakketten opgenomen. Dit zijn de pakketten die van de applicatie naar de interne switch worden gestuurd.

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 (repl
-	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 (requ
	3 2022-08-07 22:40:07.684219	192.0.2.100	198.51.100.100	ICMP	102	0x4de8 (19944)	64 Echo (ping) request	id=0x003a, seq=34/8704, ttl=64 (repl
	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 (requ
	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 (repl
	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 (requ
	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 (repl
	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 (requ
	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 (repl
	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 (requ
	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 (repl
	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 (requ
	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 (repl
	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 (requ
	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 (rep
	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 (rec
	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 (rep
	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 (red v
<								>
>	Frame 1: 102 bytes on wire (816 bits	), 102 bytes capt	ured (816 bits)			0000 00 50 56	5 9d e7 50 bc e7 12 34 9a	15 08 00 45 00 ·PV··P·· ·4····E·
>	Ethernet II, Src: Cisco_34:9a:15 (bc	:e7:12:34:9a:15),	Dst: VMware_9d:e7	:50 (00:50:56:	9d:e7:50)	0010 00 54 40	1 93 40 00 <u>40 01</u> 00 1a c0	00 02 64 c6 33 ·TM·@·@· ·····d·3
>	Internet Protocol Version 4, Src: 19	2.0.2.100, Dst: 1	98.51.100.100			0020 64 64 08	3 00 7f 15 <mark>00 3a</mark> 00 21 39	3f f0 62 00 00 dd
>	Internet Control Message Protocol					0030 00 00 8t	a a a a a a a a a a a a a a a a a a a	11 12 13 14 15
						0040 16 17 18	3 19 1a 1b 1c 1d 1e 1f 20	21 22 23 24 25
						0050 26 27 28	8 29 2a 2b 2c 2d 2e 2† 30	31 32 33 34 35 & ()*+,/012345
						0000 36 37 55	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	670000

### Uitleg

Wanneer een switch op de uplink-interface is geconfigureerd, worden alleen pakketten die van de toepassing naar de interne switch zijn verzonden opgenomen. Pakketten die naar de toepassing worden verzonden, worden niet opgenomen.

In deze tabel wordt de taak samengevat:

Taak	Opnamep unt	Intern filter	Richting	Opgenomen verkeer
Configureer en controleer een pakketopname op de uplink-interface in_data_uplink1	in_data_u plink1	None	Alleen inspring en	ICMP-echoverzoeken van host 192.0.2.10 naar host 198.51.100 ICMP-echoantwoorden van host 198.51.100.100 op host 192.0.2.2

### Taak 2

Gebruik de FTD of ASA CLI om een pakketopname op de uplink-interface in\_mgmt\_uplink1 te configureren en te verifiëren. Alleen de pakketten met beheervliegtuigverbindingen worden opgenomen.

### Topologie, pakketstroom en de opnamepunten



#### Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren op interface in\_mgmt\_uplink1:

1. Een opnamesessie maken:

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

2. De opnamesessie inschakelen:

# > no capture capsw switch stop Verificatie

Controleer de naam van de opnamesessie, de administratieve en operationele status, de interfacekaart en de identificatie. Zorg ervoor dat de waarde **Pcapsize** in bytes toeneemt en dat het aantal opgenomen pakketten niet-nul is:

> show capture c	apsw detail	
Packet Capture i	.nfo	
Name:	capsw	
Session:	1	
Admin State:	enabled	
Oper State:	up	
Oper State Rea	son: Active	
Config Success:	yes	
Config Fail Rea	ison:	
Append Flag:	overwrite	
Session Mem Usa	ige: 256	
Session Pcap Sn	ap Len: 1518	
Error Code:	0	
Drop Count:	0	
Total Physical p	oorts involved	in Packet Capture: 1
Physical port:		
Slot Id:	1	
Port Id:	19	
Pcapfile:	/mnt/disk	)/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 00.0.0.0 Ovlan: Src Ip: Dest Ip: 0.0.0.0 Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: 00:00:00:00:00:00 Dest MAC: 0 Src Port: 0 Dest Port: 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 dit geval wordt er een opname gemaakt op de interface met een interne ID 19 die de in\_mgmt\_uplink1 interface is op de Secure Firewall 3130. De opdracht switch status van show portmanager in de opdrachtshell van FXOS local-mgmt toont de interface-ID's:

> connect fxos

KSEC-FPR3100-1 connect local-mgmt

KSEC-FPR3100-	-1(local-mgmt)	show por	tmanage	r switch	status	
Dev/Port	Mode	Link	Speed	Duplex	Loopback Mode	Port Manager
0/1	SGMII	Up	1G	Full	None	Link-Up
0/2	SGMII	Up	1G	Full	None	Link-Up
0/3	SGMII	Up	1G	Full	None	Link-Up
0/4	SGMII	Up	1G	Full	None	Link-Up
0/5	SGMII	Down	1G	Half	None	Mac-Link-Down
0/6	SGMII	Down	1G	Half	None	Mac-Link-Down
0/7	SGMII	Down	1G	Half	None	Mac-Link-Down
0/8	SGMII	Down	1G	Half	None	Mac-Link-Down
0/9	1000_BaseX	Down	1G	Full	None	Link-Down
0/10	1000_BaseX	Down	1G	Full	None	Link-Down
0/11	1000_BaseX	Down	1G	Full	None	Link-Down
0/12	1000_BaseX	Down	1G	Full	None	Link-Down
0/13	1000_BaseX	Down	1G	Full	None	Link-Down
0/14	1000_BaseX	Down	1G	Full	None	Link-Down
0/15	1000_BaseX	Down	1G	Full	None	Link-Down
0/16	1000_BaseX	Down	1G	Full	None	Link-Down
0/17	1000_BaseX	Up	1G	Full	None	Link-Up
0/18	KR2	Up	50G	Full	None	Link-Up
0/19	KR	Up	25G	Full	None	Link-Up
0/20	KR	Up	25G	Full	None	Link-Up
0/21	KR4	Down	40G	Full	None	Link-Down
0/22	n/a	Down	n/a	Full	N/A	Reset
0/23	n/a	Down	n/a	Full	N/A	Reset
0/24	n/a	Down	n/a	Full	N/A	Reset
0/25	1000_BaseX	Down	1G	Full	None	Link-Down
0/26	n/a	Down	n/a	Full	N/A	Reset
0/27	n/a	Down	n/a	Full	N/A	Reset
0/28	n/a	Down	n/a	Full	N/A	Reset
0/29	1000_BaseX	Down	1G	Full	None	Link-Down
0/30	n/a	Down	n/a	Full	N/A	Reset

0/31	n/a	Down	n/a	Full	N/A	Reset
0/32	n/a	Down	n/a	Full	N/A	Reset
0/33	1000_BaseX	Down	1G	Full	None	Link-Down
0/34	n/a	Down	n/a	Full	N/A	Reset
0/35	n/a	Down	n/a	Full	N/A	Reset
0/36	n/a	Down	n/a	Full	N/A	Reset

Om toegang te krijgen tot de FXOS op ASA, voert u de opdracht **connect fxos admin uit**. In het geval van multi-context, stel dit bevel in de admincontext in werking.

#### Opnamebestanden verzamelen

Volg de stappen in het gedeelte Verzamel Secure Firewall 3100 Internal Switch Capture Files.

#### Capture file analyse

Gebruik een applicatie voor pakketopname om de opnamebestanden voor interface in\_mgmt\_uplink1 te openen. Controleer het belangrijkste punt - in dit geval worden alleen de pakketten vanaf het IP-adres voor beheer 192.0.2.200 weergegeven. De voorbeelden zijn SSH, Sftunnel of ICMP echo antwoordpakketten. Dit zijn de pakketten die door de switch van de applicatie naar het netwerk worden verzonden.

No.	Time	Source	Destination	Protocol	Length	IP ID		IP TTL Info
	196 2022-08-07 23:21:45.133362	192.0.2.200	192.0.2.101	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	Øxb7d2	(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	Øxbd9e	(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	Øxbdf2	(48626)	64 Echo (ping) reply id=0x0001, seq=4541/48401, ttl=64
	209 2022-08-07 23:21:48.406312	192.0.2.200	192.0.2.101	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	Øxbea6	(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=1448 TS
	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=1448 TS
	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
<	115 1011 00 07 12·11·55 126700	103 0 3 300	102 0 2 100	TCMD	70	avhfc1	(40000)	64 Echo (ning) ponty id-avagat con-4540/50102 ++1-64
> E	rame 1: 747 bytes on wire (5976 bits	), 747 bytes cap	tured (5976 bi	ts)		0000	a4 53 0e	11 38 2a bc e7 12 34 9a 00 08 00 45 00 ·S··8*·· ·4····E·
> E	thernet II, Src: Cisco 34:9a:00 (bc:	e7:12:34:9a:00),	Dst: Cisco 11	:38:2a (a4:53:0e:11:	:38:2a)	0010	02 d9 4a	3d 40 00 40 06 68 b4 c0 00 02 c8 c0 00 ··J=@·@·h·····
> 1	nternet Protocol Version 4, Src: 192	.0.2.200, Dst: 1	92.0.2.101			0020	02 65 20	71 e6 05 67 1b 2a c5 db e3 6b d4 80 18 ·e q··g· *···k···
> T	ransmission Control Protocol, Src Po	ort: 8305, Dst Po	rt: 58885, Seq	: 1, Ack: 1, Len: 67	77	0030	10 14 27	cc 00 00 01 01 08 0a 08 76 95 7f 91 02 ···································
> T	ransport Layer Security					0040	3d 41 17	03 03 02 a0 22 6a 01 e0 ff cc 98 f9 af =A·····" j······
_						0050	07 40 75	19 a4 d5 df 64 d8 fe 66 8e 9b cc 8d 2f (gudf/
						0060	92 b2 1a	64 e7 20 36 03 8e 48 02 5a 7c 85 30 d4 ····d· 6· ·H·Z ·0·
						0070	he of as	22 94 c1 c1 od of 24 79 b4 15 1c 44 00
						0000	ea ch 43	9e 1f fd a7 70 75 e5 6b a4 f8 2b ee 47
						00a0	2f 86 73	8f b1 e1 b5 c6 57 e3 a8 46 0e cb 26 b7 /·s···· W··F··&·
						ØØbØ	5b c7 e3	09 54 f3 c1 ff 26 d9 87 ea 51 3d 20 08 [···T··· &···Q= ·
						00c0	16 fd cb	f5 4f 91 98 5e 86 15 17 55 68 6f 5d 040^Uho].

#### Uitleg

Wanneer een switch op de uplink-interface voor beheer is geconfigureerd, worden alleen toegangspakketten die vanuit de toepassingsbeheerinterface zijn verzonden, opgenomen. Pakketten die bestemd zijn voor de interface voor toepassingsbeheer worden niet opgenomen.

In deze tabel wordt de taak samengevat:

Taak	Opnamep unt	Intern filter	Richting	Opgenomen verkeer
Configureer en	in_mgmt_	None	Alleen inspringen	ICMP-echoantwoorden van IP-adres voo

controleer een pakketopname op de beheeruplinkinterface (van de beheerinterface naar het netwerk via de interne switch) FTD-beheer 192.0.2.200 op host 192.0.2 Sftunnel van FTD management IP-adres 192.0.2.200 naar FMC IP-adres 192.0.2. SSH van FTD management IP-adres 192.0.2.200 naar host 192.0.2.10

### PacketCapture filters

De interne pakketopnamefilters van de switch worden geconfigureerd op dezelfde manier als het gegevensvlak opneemt. Gebruik de opties **ethernettype** en **overeenkomende** om filters te configureren.

#### Configuratie

Volg deze stappen op ASA of FTD CLI om een pakketopname te configureren met een filter die ARP-frames of ICMP-pakketten aanpast vanaf host 198.51.100.100 op interface Ethernet1/1:

1. Controleer de naam:

<pre>&gt; show nameif</pre>		
Interface	Name	Security
Ethernet1/1	inside	0
Ethernet1/2	outside	0
Management1/1	diagnostic	0

2. Een opnamesessie voor ARP of ICMP maken:

> capture capsw switch interface inside ethernet-type arp

#### > capture capsw switch interface inside match icmp 198.51.100.100 Verificatie

Controleer de naam van de opnamesessie en het filter. De waarde van Ethertype is **2054** in decimaal en **0x0806** in hexadecimaal:

```
> 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 Dit is de verificatie van het filter voor ICMP. IP-protocol 1 is de 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 I	Len: 1518
Error Code:	0
Drop Count:	0

Total Physical ports involved in Packet Capture: 1

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

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

## Opnamebestanden van beveiligde firewall 3100 interne Switch

Gebruik ASA of FTD CLI om switch-opnamebestanden te verzamelen. Op FTD kan het opnamebestand ook via de CLI-**kopieeropdracht** worden geëxporteerd naar bestemmingen die via de gegevens- of diagnostische interfaces kunnen worden bereikt.

U kunt het bestand ook kopiëren naar **/ngfw/var/common** in de expert-modus en downloaden van FMC via de optie **File Download**.

In het geval van poort-kanaal interfaces zorg ervoor dat pakketopnamebestanden van alle lidinterfaces worden verzameld.

#### ASA

Volg deze stappen op om switch-opnamebestanden op ASA CLI te verzamelen:

1. Stop de vastlegging:

#### asa# capture capsw switch stop

2. Controleer of de opnamesessie is gestopt en noteer de naam van het opnamebestand.

```
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
                0
Protocol:
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. Gebruik de CLI-kopieeropdracht om het bestand naar externe bestemmingen te exporteren:

```
asa# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ?
cluster: Copy to cluster: file system
               Copy to disk0: file system
disk0:
disk1:
               Copy to disk1: file system
flash:
               Copy to flash: file system
               Copy to ftp: file system
ftp:
running-config Update (merge with) current system configuration
               Copy to scp: file system
scp:
               Copy to smb: file system
smb:
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

Volg deze stappen om switch-opnamebestanden op FTD CLI te verzamelen en deze naar servers te kopiëren die bereikbaar zijn via gegevens- of diagnostische interfaces:

1. Ga naar diagnostische CLI:

> 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#</pre>
```

2. Stop de vastlegging:

firepower# capture capi switch stop

3. Controleer of de opnamesessie is gestopt en noteer de naam van het opnamebestand:

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 capsw-1-1 Name: Protocol: 0 Ivlan: 0 Ovlan: 0 Src Ip: 0.0.0.0 0.0.0.0 Dest Ip: Src Ipv6: :: Dest Ipv6: :: 00:00:00:00:00:00 Src MAC: Dest MAC: 00:00:00:00:00:00 Src Port: 0 Dest Port: 0 0 Ethertype: 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. Gebruik de CLI-kopieeropdracht om het bestand naar externe bestemmingen te exporteren. firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap ? cluster: Copy to cluster: file system disk0: Copy to disk0: file system disk1: Copy to disk1: file system flash: Copy to flash: file system Copy to ftp: file system ftp: running-config Update (merge with) current system configuration scp: Copy to scp: file system Copy to smb: file system smb: startup-config Copy to startup configuration system: Copy to system: file system Copy to tftp: file system tftp:

firepower# copy flash:/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap tftp://198.51.100.10/
Source filename [/packet-capture/sess-1-capsw-ethernet-1-1-0.pcap]?
Destination filename [sess-1-capsw-ethernet-1-1-0.pcap]?
Copy in progress...C

#### 139826 bytes copied in 0.532 secs

Volg deze stappen om opnamebestanden te verzamelen bij FMC via de optie **Bestand downloaden**:

- 1. Stop de vastlegging:
- > capture capsw switch stop
  - Controleer of de opnamesessie is gestopt en noteer de bestandsnaam en het pad voor het volledige opnamebestand:

```
> show capture capsw detail
Packet Capture info
Name:capswSession:1Admin State:disabledOper 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

      Slot 1d:
      1

      Port Id:
      1

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

      Pcapsize:
      139826

      Filter:
      capsw-1-1

Filter:
Packet Capture Filter Info
Name: capsw-1-1
Protocol: 0
Protocol:
                    0
                    0
Ivlan:
                  0
0.0.0.0
0.0.0.0
Ovlan:
Src Ip:
Dest Ip:
Src Ipv6:
                    ::
                Dest Ipv6:
Src MAC:
Dest MAC:
                    0
Src Port:
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. Ga naar expertmodus en switch naar wortelmodus:

```
> expert
admin@firepower:~$ sudo su
root@firepower:/home/admin
```

4. Kopieert het opnamebestand naar /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. Kies in FMC Apparaten > Bestand downloaden:



#### 6. Kies de FTD, geef de naam van het opnamebestand op en klik op **Downloaden**:

Firewall Management Center Devices / Troubleshoot / File Download	erview	Analysis	Policies	Devices	Objects	Integration	Dep	oloy	Q 🚱	\$	<b>?</b> Ial	o_domain	∖ admin ▼	cisco	SECURE
		Device FPR3100-1 File sess-1-cap	sw-ethernet-	T-1-0.pcap Back	Download			т	hreat De	fense C	U	Packet C	Capture	Packet	Tracer

## Richtlijnen, beperkingen en beste praktijken voor pakketvastlegging in Switch

Richtsnoeren en beperkingen:

- Meervoudige switch-opnamesessies worden ondersteund, maar er kan slechts 1 switchopnamesessie tegelijkertijd actief zijn. Een poging om 2 of meer opnamesessies in te schakelen, resulteert in een fout "ERROR: Inschakelen sessie mislukt, als limiet van maximaal 1 actieve pakketopnamesessies bereikt".
- Een actieve switch Capture kan niet worden verwijderd.
- Switch Captures kunnen niet gelezen worden op de applicatie. De gebruiker moet de bestanden exporteren.
- Bepaalde opties voor gegevensvlak vastleggen, zoals dump, decoderen, pakketnummer,

overtrekken en andere opties worden niet ondersteund voor switch-opnamen.

 In het geval van multi-context ASA, wordt de switch op gegevensinterfaces geconfigureerd in gebruikerscontexten. De switch legt op interfaces in\_data\_uplink1 vast en in\_mgmt\_uplink1 worden alleen ondersteund in de admin context.

Dit is de lijst met best practices op basis van het gebruik van pakketvastlegging in TAC-gevallen:

- Let op richtlijnen en beperkingen.
- Gebruik opnamefilters.
- Overweeg de impact van NAT op IP-adressen van pakketten wanneer een opnamefilter is geconfigureerd.
- Vergroot of verlaag de **pakketlengte** die de framegrootte aangeeft, voor het geval dat deze verschilt van de standaardwaarde van 1518 bytes. Een kortere grootte resulteert in een hoger aantal opgenomen pakketten en vice versa.
- Pas indien nodig de buffergrootte aan.
- Let op de **Drop Count** in de output van de opdracht **show cap <cap\_name> detail**. Zodra de grens van de buffergrootte wordt bereikt, stijgt de teller van de dalingstelling.

# Gerelateerde informatie

- Firepower 4100/9300 Chassis Manager en FXOS CLI-configuratiehandleidingen
- <u>Cisco Secure Firewall 3100 Introductiegids</u>
- <u>Cisco Firepower 4100/9300 FXOS opdrachtreferentie</u>

### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.