Configurazione di NetFlow/IPFIX per l'acquisizione della telemetria sulla SNA

Sommario

Introduzione

Questo documento descrive le best practice e la configurazione di base di Netflow/IPFIX necessarie per Secure Network Analytics (SNA) per il caricamento della telemetria.

Prerequisiti

- Conoscenza SNA Cisco
- Conoscenze NetFlow/IPFIX

Requisiti

- Secure Network Analytics versione 7.2.1 o successive
- Flow Collector in 7.2.1 o versioni successive
- Accesso CLI come root a Flow Collector

Componenti usati

- Ciò dipende completamente dalla progettazione della rete e dai dispositivi selezionati per inviare NetFlow/IPFIX a Secure Network Analytics. La configurazione di NetFlow/IPFIX varia a seconda dell'esportatore. Per informazioni dettagliate sulla configurazione, rivolgersi al team di supporto di ciascun esportatore.

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

conseguenze derivanti dall'uso dei comandi.

Premesse

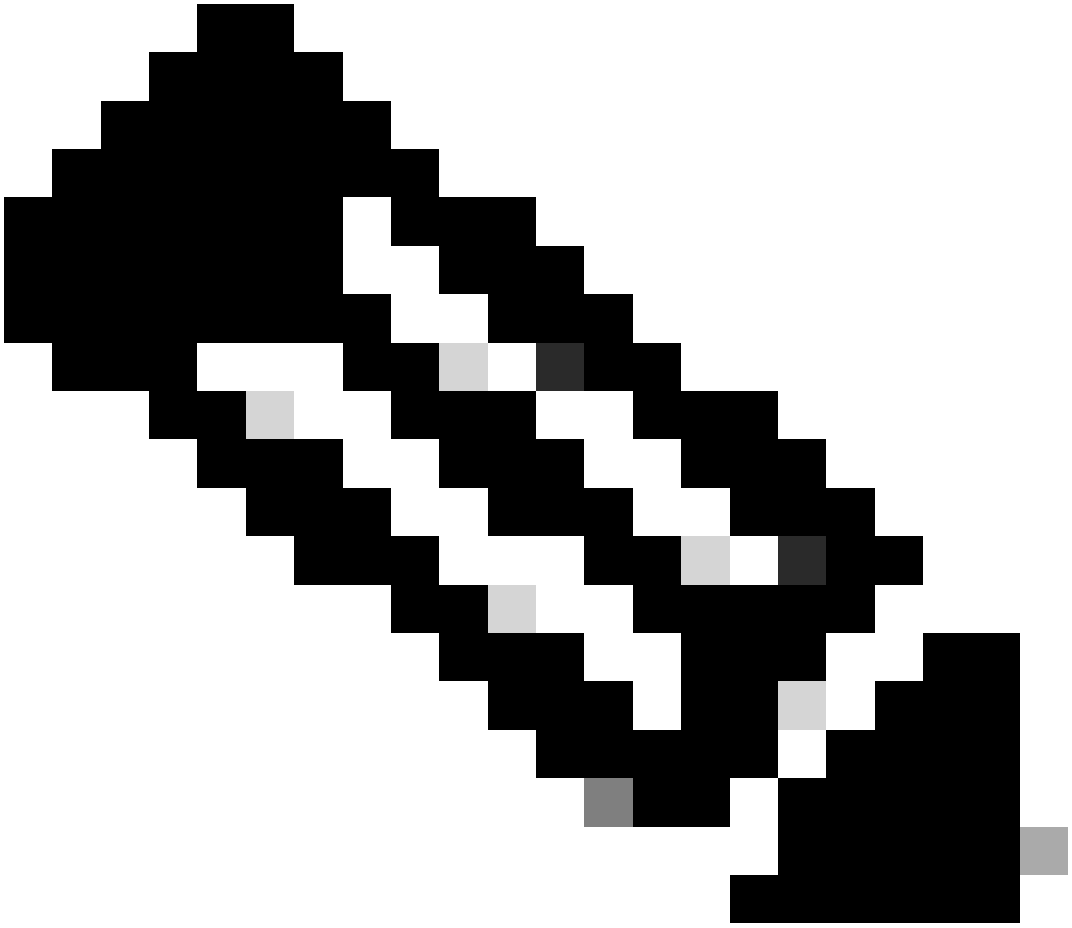
Flow Collector è un'appliance SNA incaricata di raccogliere, elaborare e archiviare i flussi che vengono inviati a Secure Network Analytics. Per NetFlow versione 9 o IPFIX, è possibile includere diversi campi nel modello NetFlow/IPFIX per aggiungere ulteriori informazioni relative al traffico di rete. Tuttavia, sono disponibili 9 campi specifici che devono essere inclusi nel modello NetFlow/IPFIX affinché il Flow Collector possa elaborare tali flussi. Flow Collector non elabora i flussi in ingresso che includono un modello non valido, pertanto SNA non visualizza le informazioni sul flusso di tali esportatori sotto interfaccia utente Web o client desktop.

Configurazione

Campi obbligatori

I campi successivi devono essere inclusi nel modello NetFlow/IPFIX per il caricamento della telemetria. Verificare che questi 9 campi siano inclusi nel modello NetFlow/IPFIX per consentire a Secure Network Analytics di elaborare i flussi in ingresso.

- Source IP Address
- Indirizzo IP di destinazione
- Porta di origine
- Porta di destinazione
- Protocollo di livello 3
- Conteggio byte
- Conteggio pacchetti
- Ora inizio flusso
- Ora fine flusso



Nota: è possibile includere più campi nella configurazione NetFlow/IPFIX, tuttavia i campi precedenti rappresentano i requisiti minimi di Secure Network Analytics per il caricamento della telemetria.

Campi consigliati

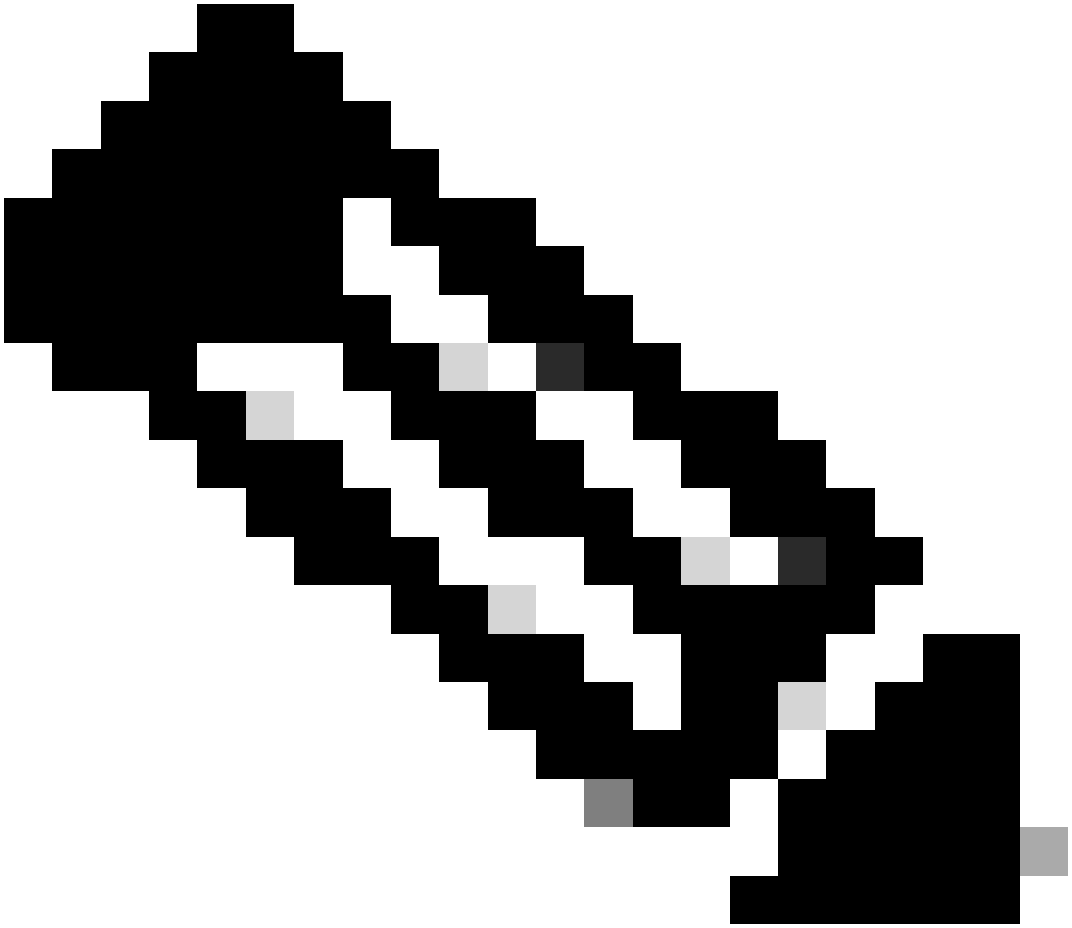
Si consiglia di includere i campi successivi nel modello NetFlow/IPFIX per raccogliere informazioni sull'interfaccia. Questa configurazione è necessaria per visualizzare le informazioni sull'interfaccia, ad esempio il nome e la velocità:

- Ingresso interfaccia
- Uscita interfaccia

Procedure ottimali

Inoltre, le impostazioni successive sono consigliate come best practice per garantire le prestazioni corrette di Secure Network Analytics.

- Imposta timeout attivo su 60 secondi
- Impostare il timeout di inattività su 15 secondi
- Impostare il timeout del modello su 30 secondi



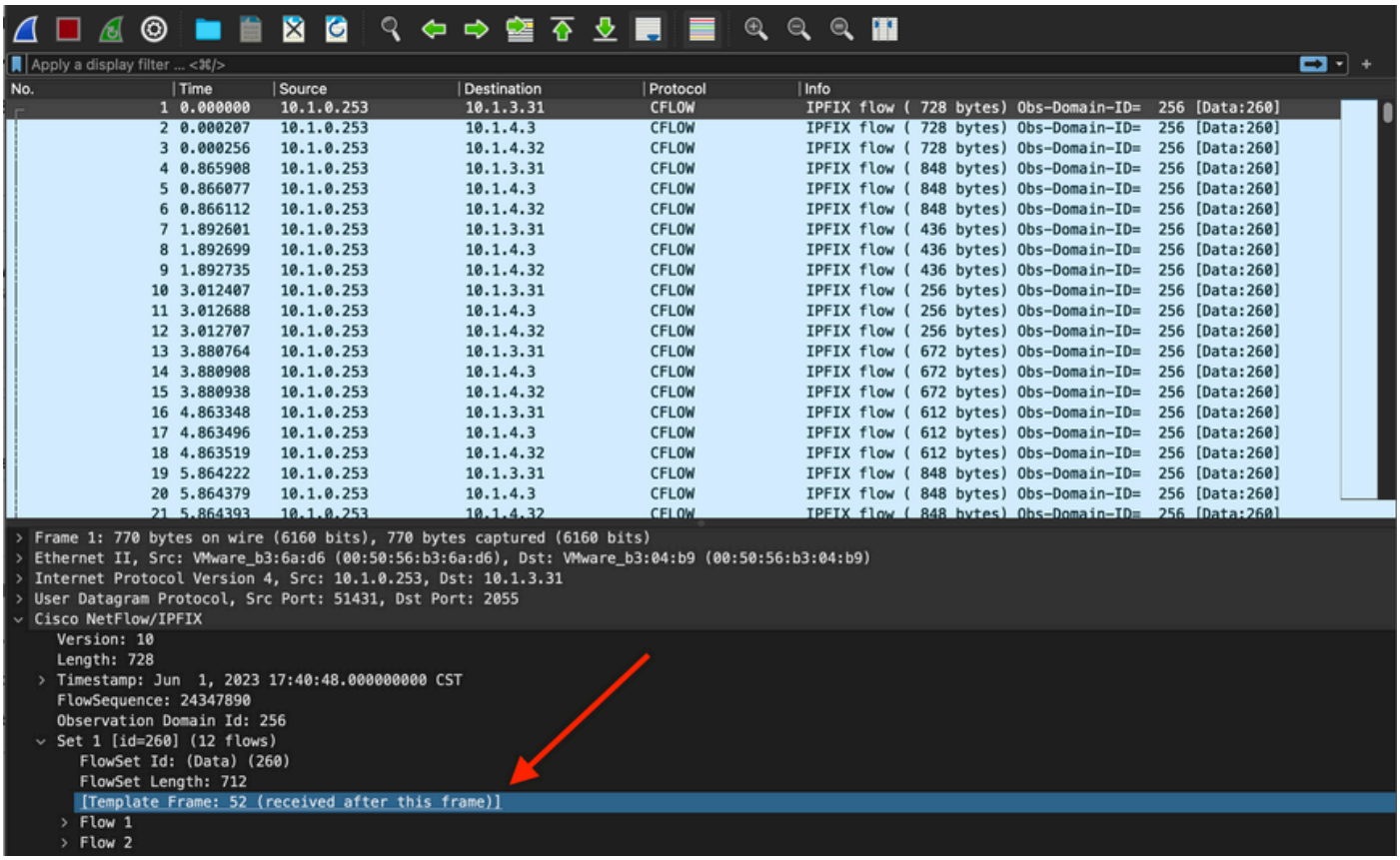
> Nota: la porta predefinita per NetFlow è 2055. Tuttavia, è possibile selezionare un'altra porta. Accertarsi di utilizzare la stessa porta durante il processo lc-ast sui Flow Collector.

Verifica

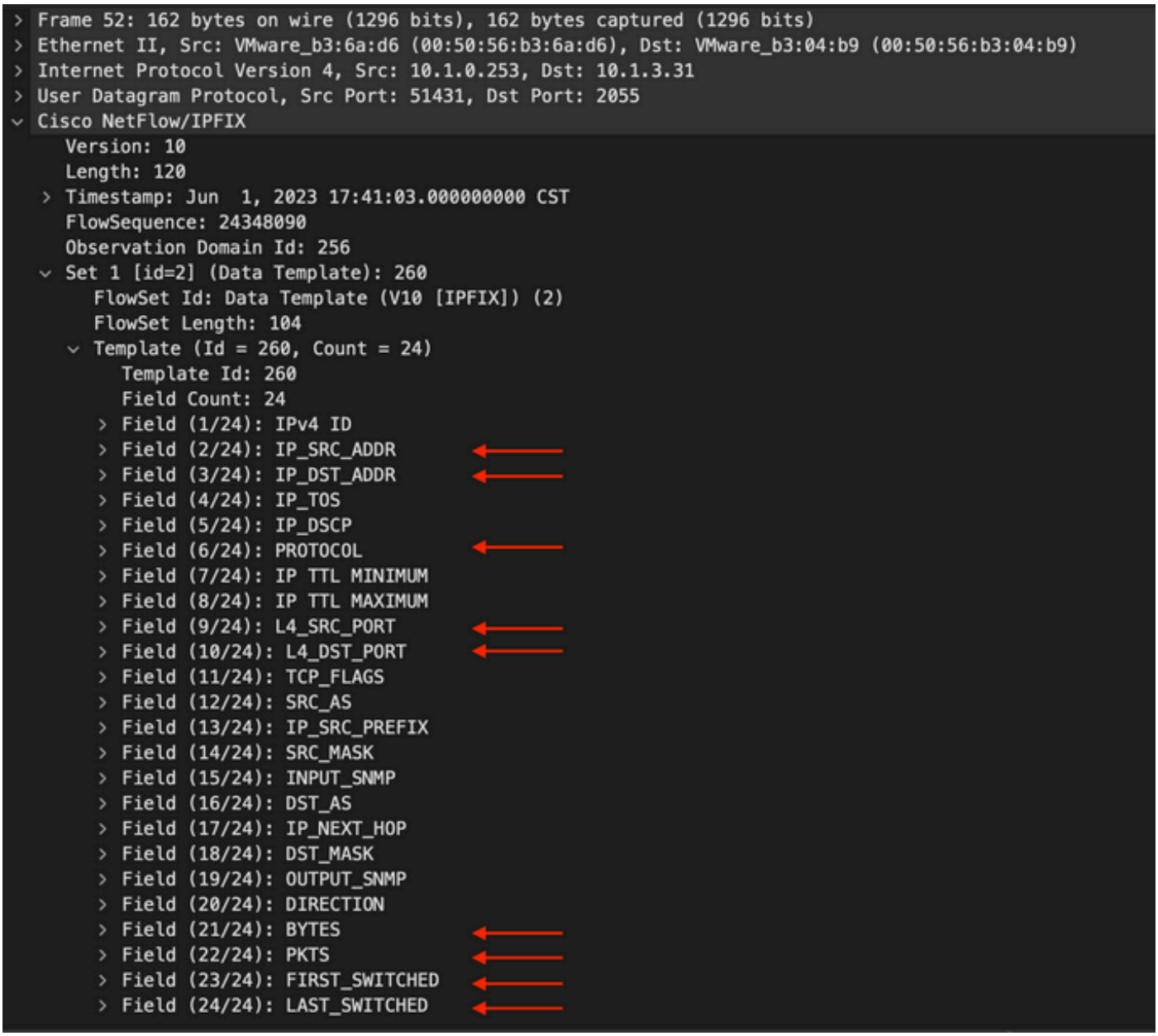
Per convalidare la configurazione del modello NetFlow/IPFIX, è possibile eseguire un'acquisizione di pacchetto tra l'utilità di esportazione e Flow Collector. Accedere al Flow Collector con l'utente root tramite SSH ed eseguire il comando:

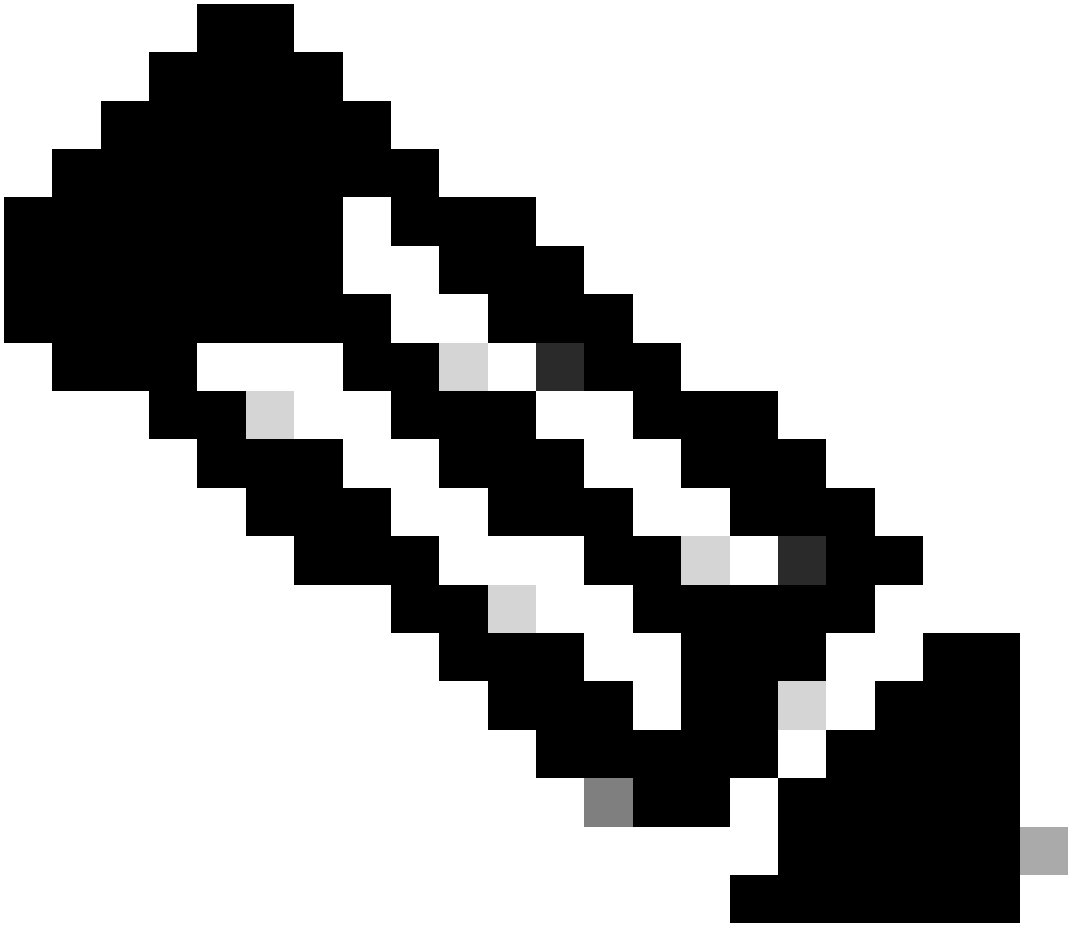
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Usare uno strumento SCP per esportare l'acquisizione del pacchetto dal Flow Collector (situato in /lancope/var/tcpdump) al computer locale e aprirla su Wireshark



- Identificare il frame in cui è stato ricevuto il modello NetFlow/IPFIX e aprirlo per convalidare i campi inclusi nel modello


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



Nota: i nomi dei campi visualizzati possono avere un aspetto diverso in ogni funzione di esportazione. Si tratta solo di un riferimento al modo in cui è possibile convalidare tali campi.

Informazioni su questa traduzione

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