



Cybersecurity Specialist

# **Cyber Security & Ethical Hacking**

## **GIORNO 5 – CISCO CYBEROPS**

---

**Alejandro Cristino  
S13-L5**

# TRACCIA

## Packet Tracer - Explore a NetFlow Implementation

In this Packet Tracer activity, you will do the following:

- Explore an implementation of NetFlow.

<https://itexamanswers.net/25-3-10-packet-tracer-explore-a-netflow-implementation-answers.html>

# Parte 1: Osservare i record di flusso NetFlow – One Direction

**Effettuare il ping del gateway predefinito dal PC-1.**

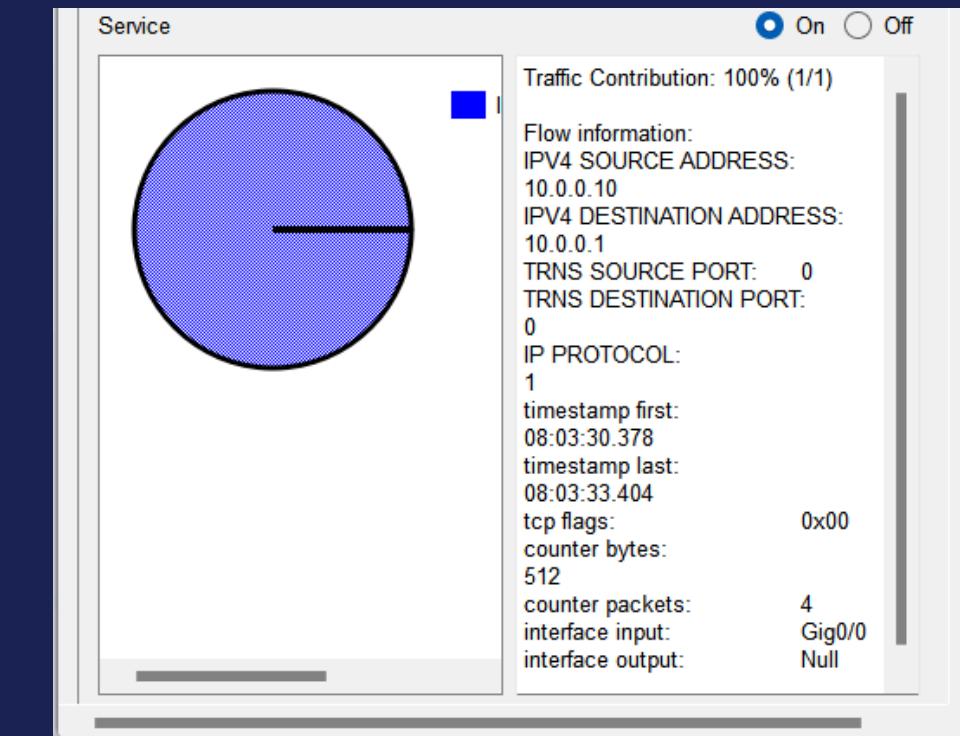
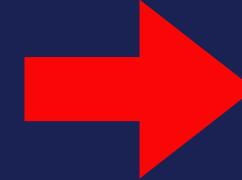
1. Fare clic su PC-1 .
2. Aprire la scheda Desktop e fare clic sull'icona Prompt dei comandi.
3. Immettere il comando ping per testare la connettività al gateway predefinito su 10.0.0.1.
4. Fare clic sul grafico a torta o sulla voce della legenda per visualizzare i dettagli del record di flusso.

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

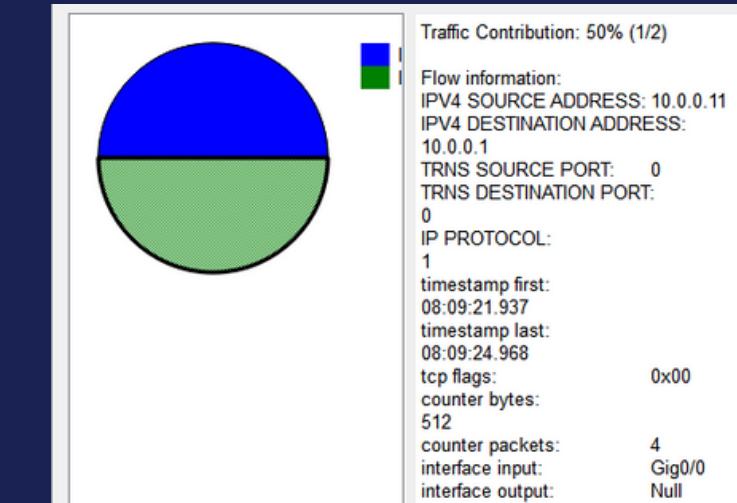
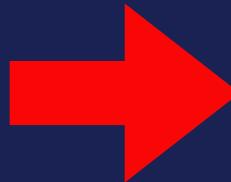


In questo caso, il flusso rappresenta il ping ICMP dall'host 10.0.0.10 a 10.0.0.1. Nel flusso erano presenti quattro pacchetti ping. I pacchetti sono entrati nell'interfaccia G0/0 dell'esportatore.

## Effettuare il ping del gateway predefinito dal PC-1.

1. Fare clic su PC-2 > Desktop.
2. Aprire un prompt dei comandi ed effettuare il ping sul gateway predefinito 10.0.0.1.

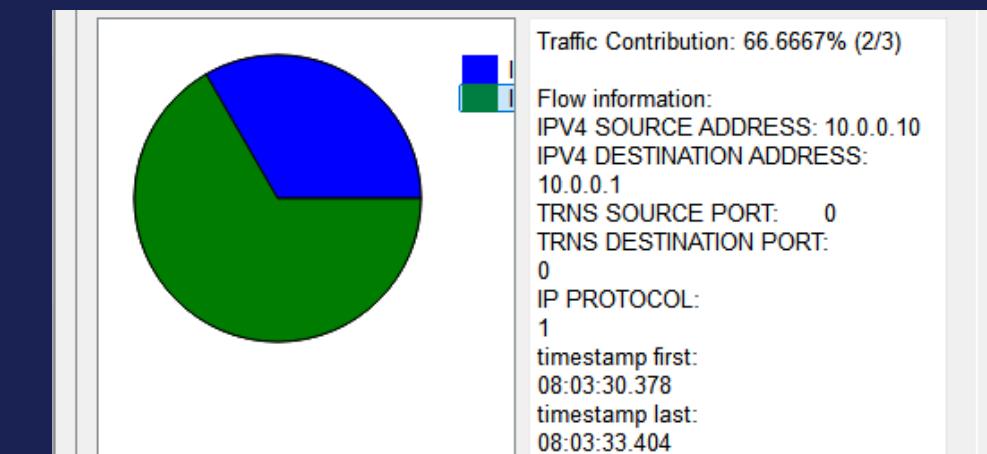
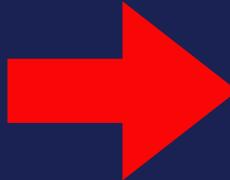
```
Cisco Packet Tracer PC Command Line 1.0  
C:\>ping 10.0.0.1  
  
Pinging 10.0.0.1 with 32 bytes of data:  
  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```



Poiché questo traffico avrà un indirizzo IP di origine diverso, creerà un nuovo record di flusso rappresentato da una nuova porzione codificata a colori del grafico a torta.

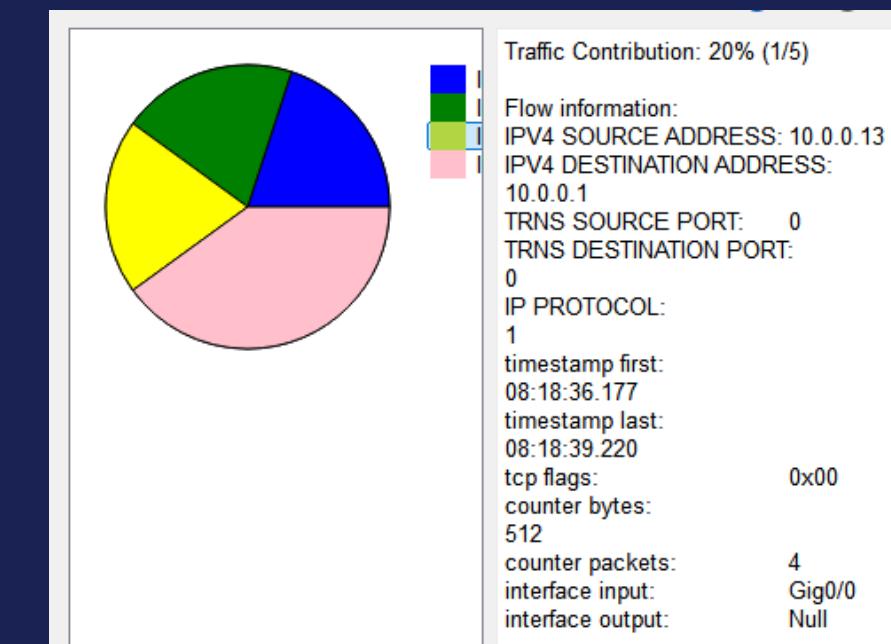
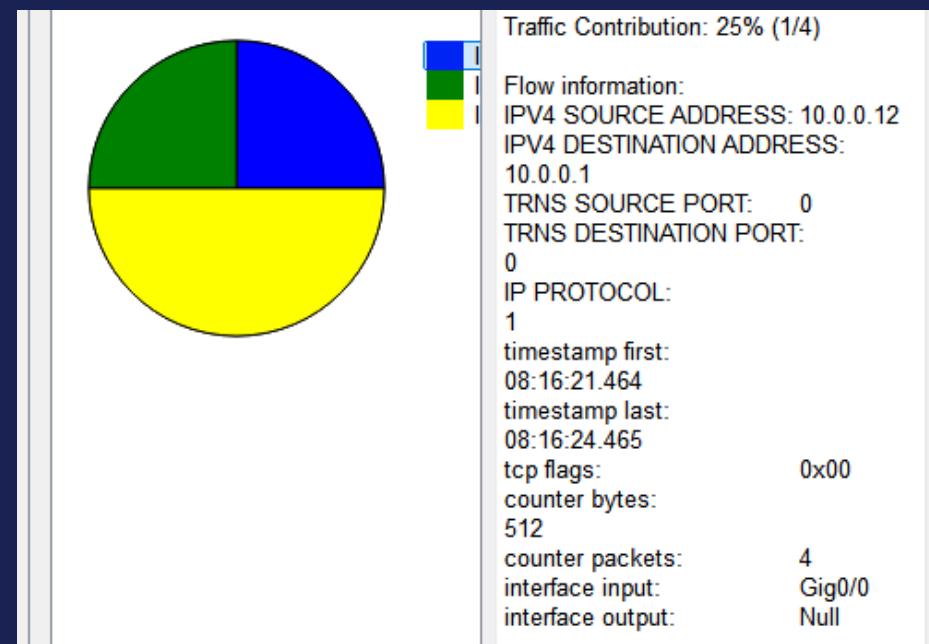
3. Ritornare al PC-1 e ripetere il ping ed effettuare il ping sul gateway predefinito 10.0.0.1.

```
C:\>ping 10.0.0.1  
  
Pinging 10.0.0.1 with 32 bytes of data:  
  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255  
Reply from 10.0.0.1: bytes=32 time<1ms TTL=255
```



I dettagli del flusso originale rimangono gli stessi, tuttavia la quota di traffico rappresentata dal flusso è raddoppiata.

#### 4. Inviare ping da PC-3 e PC-4 all'indirizzo gateway predefinito.



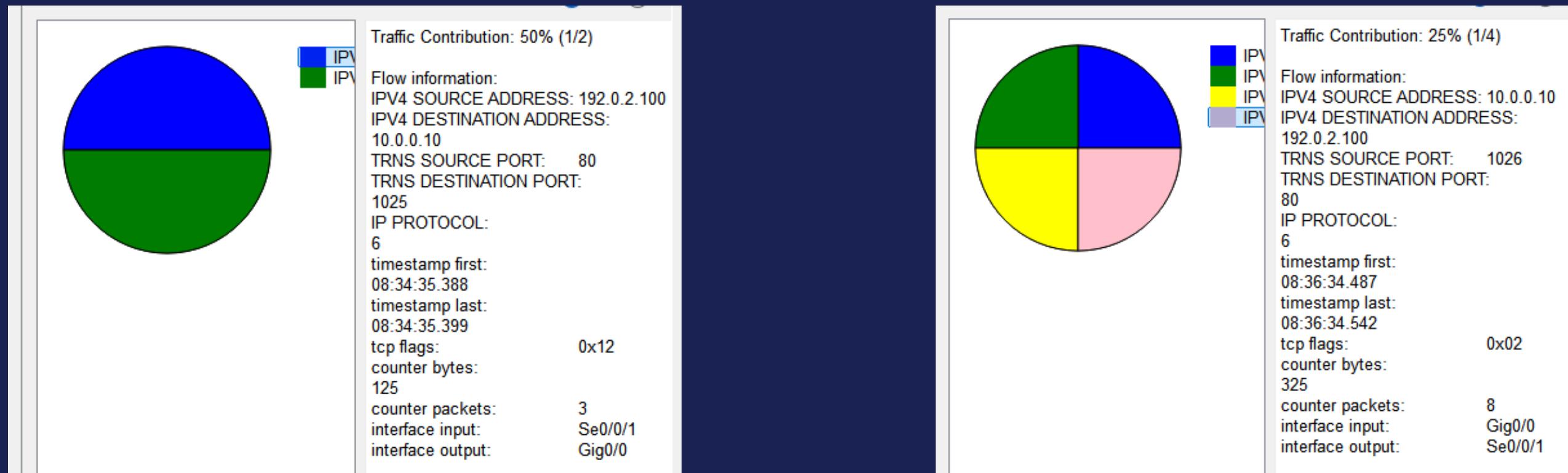
In questo caso, appare un nuovo record per ogni flusso

## Parte 2: Osservare i record NetFlow per una sessione che entra ed esce dal Collector

### Accedere al server Web tramite l'indirizzo IP.

1. Fai clic sull'icona Netflow Collector. Successivamente disattivare e attivare il collector per cancellare i flussi.
2. Nel browser Web per PC-1, immetti 192.0.2.100 e fai clic su Vai . Verrà visualizzata la pagina Web del sito Web di esempio.
3. Dopo un breve ritardo, verrà visualizzato un nuovo grafico a torta nel raccoglitore NetFlow. Vedrai almeno due segmenti di torta per la richiesta e la risposta HTTP. Potresti vedere un terzo segmento se la cache ARP per PC-1 è scaduta.

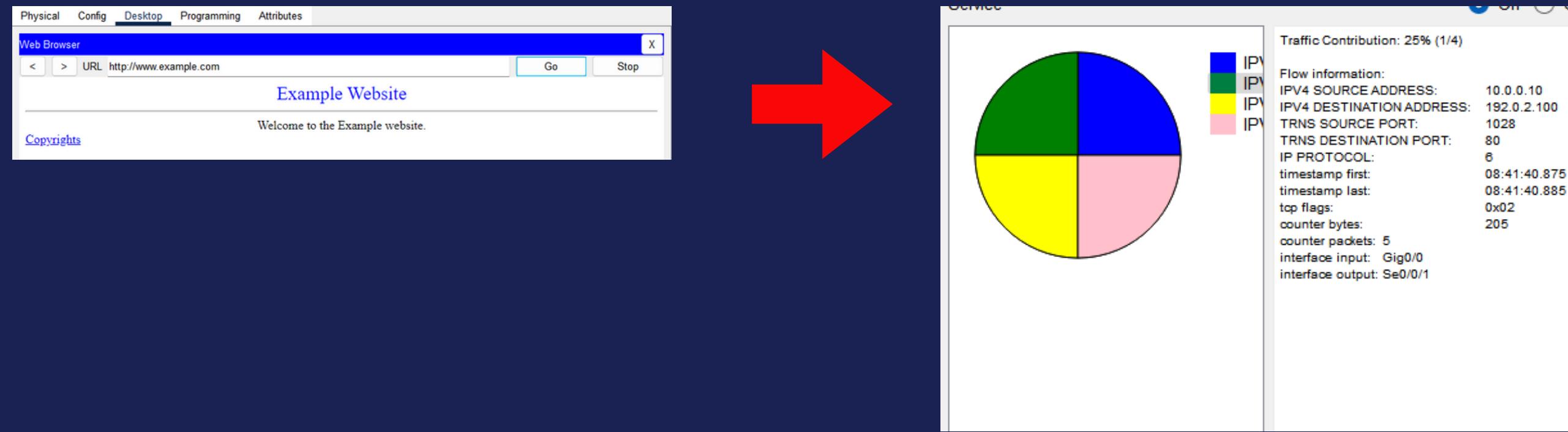
- Fai clic su ciascun segmento di torta HTTP per visualizzare il record e verificare le tue previsioni.
- Fai clic sul collegamento alla pagina Copyright.



Poiché l'host ha aperto una nuova porta sorgente per la nuova richiesta al server Web, sono stati creati due nuovi flussi.

## Accedere al server Web tramite URL.

- Spegnere e riaccendere NetFlow Collector per cancellare i flussi.
- Attivare il servizio NetFlow Collector.
- Su PC-1, immettere [www.example.com](http://www.example.com) nel campo URL.



Dopo aver visualizzato i flussi e ispezionato i record, il valore 6 è per TCP e viene utilizzato per il traffico HTTP sulla porta TCP 80. Il valore 17 è per il traffico UDP e viene utilizzato dai flussi di query e risposta DNS.

# TRACCIA

## Packet Tracer - Logging from Multiple Sources

In this Packet Tracer activity, you will do the following:

- Use Packet Tracer to compare network data generated by multiple sources including syslog, AAA, and NetFlow.

<https://itexamanswers.net/25-3-11-packet-tracer-logging-from-multiple-sources-answers.html>

# Parte 1: Visualizzare le voci del registro con Syslog

## Il server syslog

1. Fai clic su Syslog Server per aprire la sua finestra.
2. Seleziona la scheda Services e seleziona SYSLOG dall'elenco dei servizi mostrato a sinistra.
3. Fai clic su On per attivare il servizio Syslog.
4. Le voci Syslog provenienti dai client syslog verranno mostrate nella finestra a destra. Al momento, non ci sono voci.

The screenshot shows the Cisco IOS XE interface. On the left, a vertical menu lists services: TFTP, DNS, SYSLOG (which is selected and highlighted in blue), AAA, NTP, EMAIL, FTP, and TAC. To the right, there is a table with three columns: Time, HostName, and Message. The table is currently empty, indicating no log entries have been received.

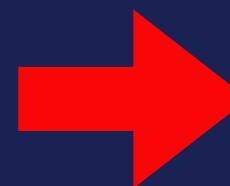
Time	HostName	Message

5. Fare clic su R1 > scheda CLI
6. Premere Invio per ottenere un prompt dei comandi e immettere il comando enable .
7. Immettere il comando debug eigrp packets per abilitare il debug EIGRP. La console della riga di comando si riempirà immediatamente di messaggi di debug.
8. Tornare alla finestra Syslog Server . Verificare che le voci di log appaiano sul server syslog.
9. Dopo aver registrato alcuni messaggi, fare clic sul pulsante di scelta per disattivare il servizio syslog .

```

R1>enable
R1#debug eigrp packets
EIGRP Packets debugging is on
(UPDATE, REQUEST, QUERY, REPLY, HELLO, ACK )
R1#
*Mar 01, 08:03:42.033: EIGRP: Sending HELLO on GigabitEthernet0/1
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01, 08:03:44.033: EIGRP: Sending HELLO on GigabitEthernet0/0
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01, 08:03:45.033: EIGRP: Received HELLO on GigabitEthernet0/0 nbr 192.168.11.1
  AS 1, Flags 0x0, Seq 9/0 idbQ 0/0
*Mar 01, 08:03:47.033: EIGRP: Sending HELLO on GigabitEthernet0/1
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01, 08:03:49.033: EIGRP: Sending HELLO on GigabitEthernet0/0
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01, 08:03:50.033: EIGRP: Received HELLO on GigabitEthernet0/0 nbr 192.168.11.1
  AS 1, Flags 0x0, Seq 9/0 idbQ 0/0
*Mar 01, 08:03:51.033: EIGRP: Sending HELLO on GigabitEthernet0/1
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01, 08:03:53.033: EIGRP: Sending HELLO on GigabitEthernet0/0
  AS 1, Flags 0x0, Seq 10/0 idbQ 0/0 iidbQ un/rely 0/0
*Mar 01 08:03:54.033: EIGRP: Received HELLO on GigabitEthernet0/0 nbr 192.168.11.1

```

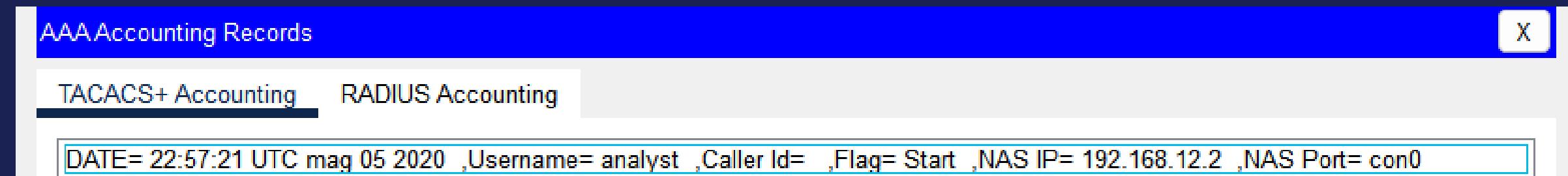


	Time	HostName	Message
1	03.01.1993 08:04:29.152 AM	192.168.11.2	EIGRP: Sending HELLO on ...
2	03.01.1993 08:04:26.639 AM	192.168.11.2	EIGRP: Received HELLO on ...
3	03.01.1993 08:04:26.117 AM	192.168.11.2	EIGRP: Sending HELLO on ...
4	03.01.1993 08:04:24.327 AM	192.168.11.2	EIGRP: Sending HELLO on ...
5	03.01.1993 08:04:22.258 AM	192.168.11.2	EIGRP: Received HELLO on ...
6	03.01.1993 08:04:21.651 AM	192.168.11.2	EIGRP: Sending HELLO on ...
7	03.01.1993 08:04:19.372 AM	192.168.11.2	EIGRP: Sending HELLO on ...
8	03.01.1993 08:04:17.972 AM	192.168.11.2	EIGRP: Received HELLO on ...
9	03.01.1993 08:04:17.292 AM	192.168.11.2	EIGRP: Sending HELLO on ...

EIGRP: invio di HELLO su GigabitEthernet0/0 AS 1, flag 0x0, sequenza 10/0 idbQ 0/0 iidbQ un/rely 0/0 Alcune delle informazioni sono il tipo di pacchetto EIGRP (HELLO), l'interfaccia che ha ricevuto il pacchetto, il numero di sistema autonomo EIGRP, il timestamp del messaggio e l'origine del messaggio.

## Parte 2: Registra l'accesso dell'utente

1. Fare clic su Syslog Server per aprire la sua finestra.
2. Selezionare la scheda Desktop e selezionare AAA Accounting . Lasciare aperta questa finestra.
3. Fare clic su R2 > CLI .
4. Premere Invio per ottenere un prompt dei comandi. R2 chiederà username e password prima di concedere l'accesso alla sua CLI.
5. Torna alla finestra AAA Accounting Records del Syslog Server.



La voce contiene il timestamp in cui si è verificato l'evento, il nome utente e la password utilizzati, l'indirizzo IP di R2 (il dispositivo utilizzato per il tentativo di accesso) e un flag di avvio. Il flag di avvio indica che l'utente analista ha effettuato l'accesso all'ora indicata.

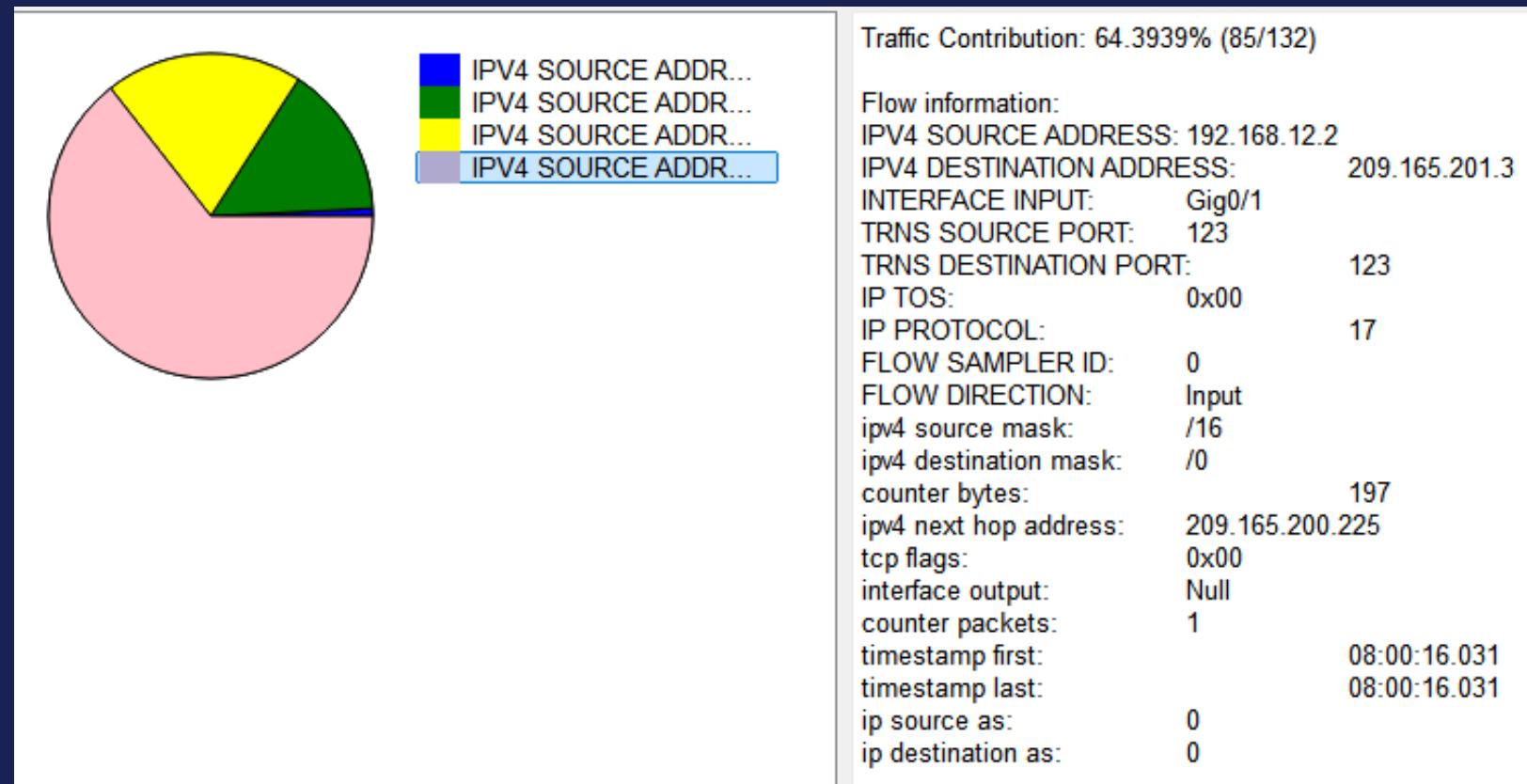
**DATE= 22:59:32 UTC mag 05 2020 ,Username= analyst ,Caller Id= ,Flag= Stop ,NAS IP= 192.168.12.2 ,NAS Port= con0**

È stata aggiunta una nuova voce, ma questa volta il flag Stop indica che l'utente ha effettuato il logout.

# Parte 3: NetFlow e visualizzazione

I server Syslog è anche un collettore NetFlow. Il firewall è configurato come un esportatore NetFlow.

1. Fare clic sul server Syslog per aprire la sua finestra. Chiudere la finestra AAA Accounting Records.
2. Dalla scheda Desktop , selezionare Netflow Collector . I servizi di collettore NetFlow devono essere attivati.
3. Da qualsiasi PC, effettuare il ping del Corp Web Server a 209.165.200.194. Dopo un breve ritardo, il grafico a torta verrà aggiornato per mostrare il nuovo flusso di traffico



I grafici visualizzati variano in base al traffico sulla rete. Altri flussi di pacchetti, come il traffico correlato a EIGRP, vengono inviati tra dispositivi. NetFlow cattura questi pacchetti ed esporta statistiche su NetFlow Collector. Più a lungo NetFlow può funzionare su una rete, più statistiche sul traffico verranno catturate.



Cybersecurity Specialist

# Cyber Security & Ethical Hacking

GRAZIE.