# Packet Tracer — Explore uma implementação NetFlow

## Objetivos

**Parte 1: Observar registros de fluxo NetFlow - Uma direção**

**Parte 2: Observe os registros NetFlow para uma sessão que entra e sai do coletor**

## Histórico/Cenário

Nesta atividade, você usará o Packet Tracer para criar tráfego de rede e observar os registros de fluxo NetFlow correspondentes em um coletor NetFlow. O Packet Tracer oferece uma simulação básica da funcionalidade NetFlow. Não é um substituto para aprender NetFlow em equipamentos físicos. Algumas diferenças podem existir entre registros de fluxo NetFlow gerados pelo Packet Tracer e por registros criados por equipamentos de rede completos.

## Instruções

## Parte 1: Observe os registros de fluxo NetFlow - Uma direção

### Etapa 1: Open the NetFlow collector.

a. No NetFlow Collector, clique na guia **Desktop**. Clique no ícone **Netflow Collecto**.

b. Clique **no botão de** opção Ligado para ativar o coletor conforme necessário. Posicione e dimensione a janela para que ela fique visível a partir da janela de topologia do Packet Tracer

### Etapa 2: Ping o default gateway a partir do PC-1.

a. Clique em **PC-1**.

b. Abra a guia **Desktop** e clique no icone **Command Prompt** .

c. Digite o comando **ping** para testar a conectividade com o gateway padrão em 10.0.0.1.

```
C:\ > ping 10.0.0.1
```

d. Após um breve atraso, a tela NetFlow Collector exibirá um gráfico de pizza.

**Observação**: O primeiro conjunto de pings pode não ser enviado ao NetFlow Collector porque o processo ARP deve primeiro resolver endereços IP e MAC. Se após 30 segundos, um gráfico de pizza não aparecer, faça o ping no gateway padrão novamente.

e. Clique no gráfico de pizza ou na entrada de legenda para exibir os detalhes do registro de fluxo.

f. O registro de fluxo terá entradas semelhantes às da tabela abaixo. Seus carimbos de data/hora serão diferentes.

| Entrada | Valor | Explicação |
|---|---|---|
| Contribuição do tráfego | 100% (1/1) | Esta é a proporção de todo o tráfego representado por esse fluxo. |
| IPV4 SOURCE ADDRESS | 10.0.0.10 | Este é o endereço IP de origem dos pacotes de fluxo. |
| IPV4 DESTINATION ADDRESS | 10.0.0.1 | Este é o endereço IP de destino dos pacotes de fluxo. |

| Entrada | Valor | Explicação |
|---|---|---|
| TRNS SOURCE PORT | 0 | Esta é a porta de origem da camada de transporte. O valor é 0 porque este é um fluxo ICMP. |
| TRNS DESTINATION PORT | 0 | Esta é a porta de destino da camada de transporte. O valor é 0 porque este é um fluxo ICMP. |
| PROTOCOLO IP | 1 | Isso identifica o serviço da Camada 4, normalmente 1 para ICMP, 6 para TCP e 17 para UDP. |
| timestamp primeiro | 00:47:49.593 | Este é o carimbo de data/hora para o início do fluxo. |
| carimbo de data/hora | 00:47:52.598 | Este é o carimbo de data/hora do último pacote no fluxo. |
| flags TCP | 0x00 | Este é o valor do flag TCP. Nesse caso, nenhuma sessão TCP foi envolvida porque o protocolo é ICMP. |
| contador de bytes | 512 | Este é o número de bytes no fluxo. |
| contador de pacotes | 4 | Este é o número de pacotes no fluxo. |
| entrada da interface | Gig0/0 | Esta é a interface do Flow exporter que coletou o fluxo na direção de entrada (na interface do dispositivo de monitoramento). |
| saída da interface | Nulo | Esta é a interface do Flow exporter que coletou o fluxo na direção de saída (fora da interface do dispositivo de monitoramento). O valor é “Nulo” porque este era um ping para a interface de entrada. |

Nesse caso, o fluxo representa o ping ICMP do host 10.0.0.10 para 10.0.0.1. Quatro pacotes de ping estavam no fluxo. Os pacotes inseridos na interface G0/0 do exportador.

**Observação**: Nesta atividade, o roteador de borda foi configurado como um NetFlow Flow exporter . A interface LAN é configurada para monitorar fluxos que entram na rede local. A interface serial foi configurada para coletar fluxos que entram na internet. Isto foi feito para simplificar esta atividade.

Para ver o tráfego que corresponde a uma sessão bidirecional completa, o NetFlow Flow exporter precisaria ser configurado para coletar fluxos que entram e saem de uma rede.

## Etapa 3: Crie tráfego adicional.

a. Clique no **PC-2 > Desktop**.

b. Abra um prompt de comando e execute **ping** no gateway padrão 10.0.0.1.

O que você espera ver nos registros de fluxo do NetFlow collector? As estatísticas do registro de fluxo existente serão alteradas ou um novo fluxo aparecerá no gráfico de pizza?

c. Retorne ao PC-1 e repita o ping para o gateway.

Como esse tráfego será representado? Como um novo segmento no gráfico de pizza ou ele modificará os valores no registro de fluxo existente?

d. Emita pings de PC-3 e PC-4 para o endereço de gateway padrão.

O que deve acontecer com a tela no coletor de fluxo?

## Parte 2: Observe os registros NetFlow para uma sessão que entra e sai do coletor

O NetFlow exporter foi configurado para coletar fluxos que saem da LAN e entram no roteador pela Internet.

### Etapa 1: Acesse o servidor Web por endereço IP.

Antes de continuar, ligue o NetFlow Collector para limpar os fluxos.

a. Clique na guia **NetFlow Collector > Physical**.

b. Clique no botão de energia vermelho para desligar o servidor. Em seguida, clique nele novamente para ligar o servidor novamente. (**Observação**: talvez seja necessário rolar ou diminuir o zoom.)

c. No NetFlow Collector, clique na guia **Desktop**.

d. Clique no ícone Netflow Collector. Clique no botão de opção “On” para ativar o coletor. Feche a janela NetFlow Collector.

e. Antes de acessar um servidor Web a partir do PC-1, prever quantos fluxos haverá no gráfico de pizza? Explique.

A partir do seu conhecimento de protocolos de rede e NetFlow, preveja os valores para as solicitações de página da Web que saem da LAN.

| Campo de registro | Valor | Diretrizes |
|---|---|---|
| Endereço IP de origem | | N/A |

| Campo de registro | Valor | Diretrizes |
|---|---|---|
| Endereço IP de destino | | N/A |
| Porta de origem | 1025—5000 (padrão do MS Windows, que é o que o PT usa. | Este é um valor aproximado que é criado dinamicamente. |
| Porta de destino | | N/A |
| Interface de entrada | | N/A |
| Interface de saída | | N/A |

Preveja os valores para a resposta da página da Web que entra no roteador do exportador NetFlow a partir da Internet.

| Campo de Registro | Valor | Diretrizes |
|---|---|---|
| Endereço IP de origem | | N/A |
| Endereço IP de destino | | N/A |
| Porta de origem | | N/A |
| Porta de destino | 1025-5000 | Este é o valor que foi atribuído aleatoriamente a partir do intervalo de portas efêmeras. |
| Interface de entrada | | N/A |
| Interface de saída | | N/A |

f. Clique no **PC-1 > Desktop**. Feche a janela do prompt de comando, se necessário. Clique no ícone do navegador da web.

g. No Navegador da Web para PC-1, digite 192.0.2.100 e clique em **Ir**. A página Web do site de exemplo será exibida.

h. Após um pequeno atraso, um novo gráfico de pizza aparecerá no coletor NetFlow. Você verá pelo menos dois segmentos de pizza para a solicitação HTTP e resposta. Talvez você veja um terceiro segmento se o cache ARP para PC-1 expirou.

i. Clique em cada segmento de pizza HTTP para exibir o registro e verificar suas previsões.

j. Clique no link para a página Direitos autorais.

O que aconteceu? Explique. (Dica: compare o número da porta no host para os fluxos.)

Compare os fluxos. Além do carimbo de data/hora óbvio, endereço IP de origem e destino, porta e interfaces, diferenças, o que mais é diferente entre os fluxos de solicitação e resposta?

## Etapa 2: Acesse o Servidor Web por URL.

a. Reinicie o NetFlow Collector para limpar os fluxos.

b. Ative o serviço Coletor de fluxo de rede.

c. Antes de acessar o servidor Web por sua URL.
O que você acha que verá na exibição do NetFlow collector?

d. Em PC-1, insira **www.example.com** no campo URL e pressione **Ir**.

e. Depois que os fluxos forem exibidos, inspecione cada registro de fluxo.
Quais valores você vê para o campo de protocolo IP do registro de fluxo? O que significam esses valores?