Modelo de exportação de fluxos bidirecionais baseados no IPFIX

André Proto

UNESP – Universidade Estadual Paulista – Instituto de Biociências, Letras e Ciências Exatas (IBILCE) - Campus de São José do Rio Preto, SP

Era uma vez o IPFIX...

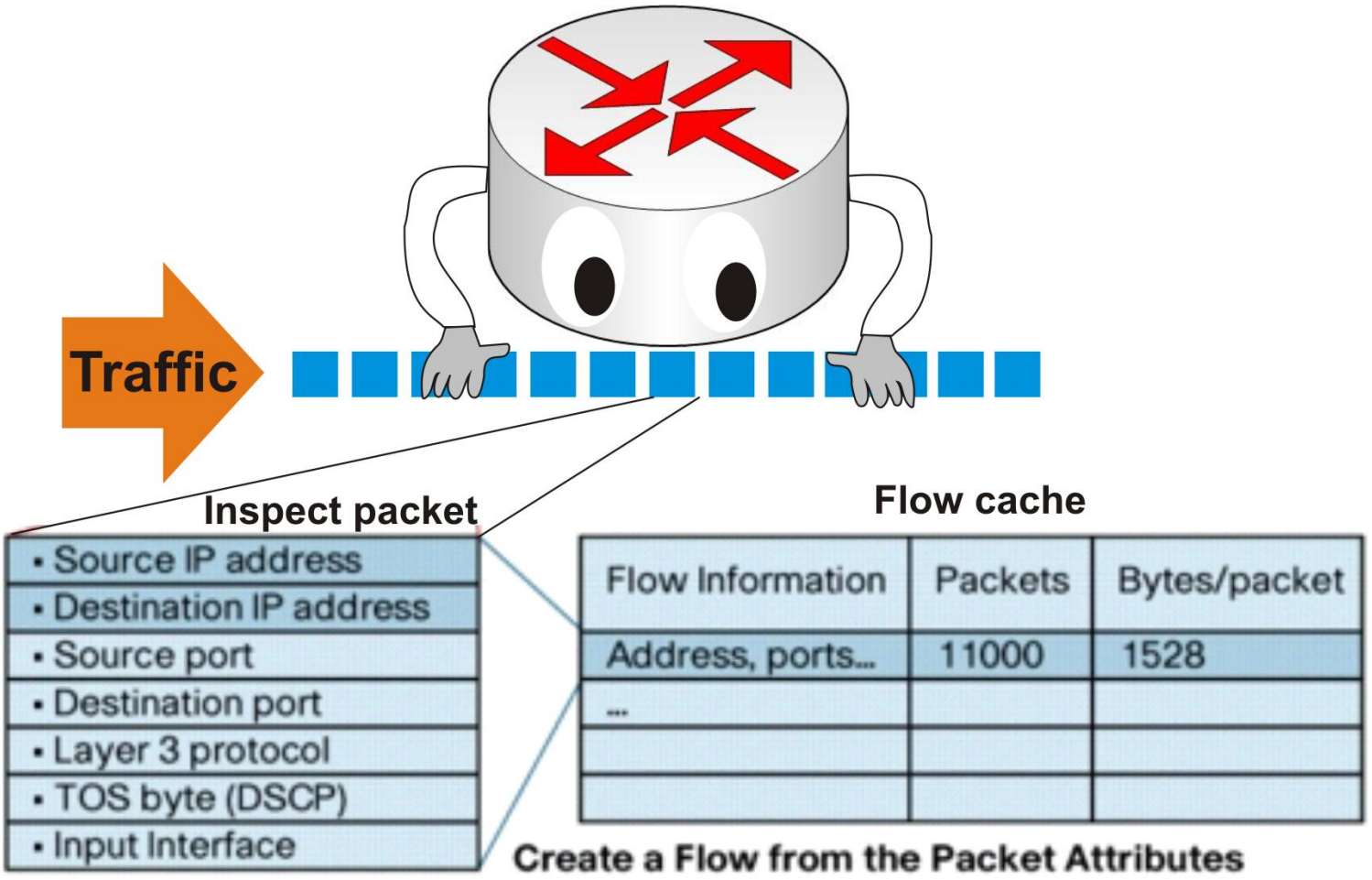
- Desenvolvimento de aplicações necessitavam de medições de tráfego dentro de uma rede de computadores.
- Surge a idéia de análise de fluxos, uma alternativa de análise de tráfego tradicional.
- Diversos protocolos foram propostos dentre eles o *Netflow* pela *Cisco Systems* RFC-3954.
- IETF propôs a criação do padrão IPFIX (*IP Flow Information* Export) RFC-3917.

O que é o IPFIX?

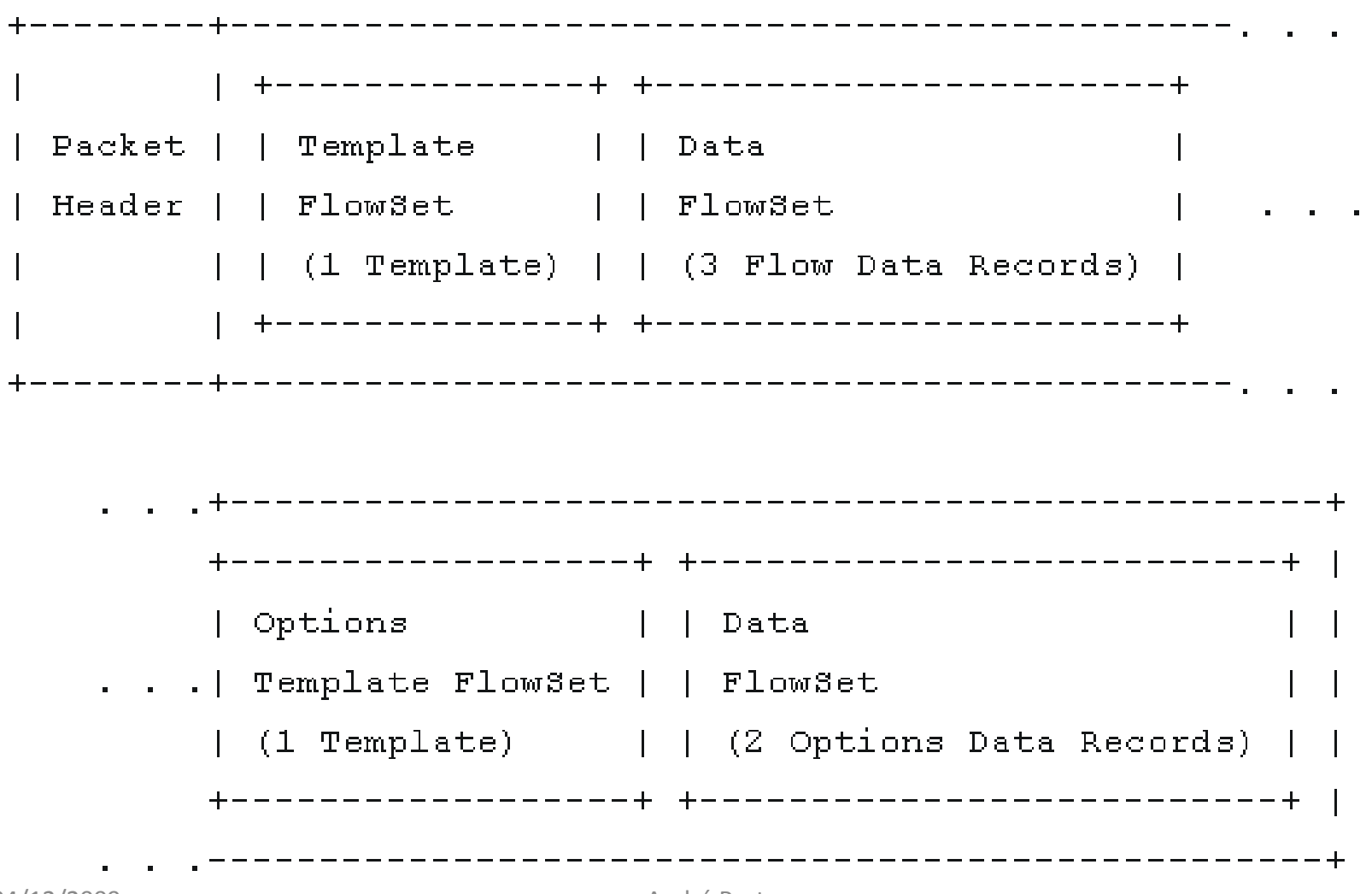
- Especificações para exportação de informações de tráfego.

- **Define algumas terminologias:**
  - ✓ Fluxo de tráfego IP
  - ✓Ponto de observação
  - ✓Processo de medição
  - ✓Processo de exportação
  - ✓Processo de coleta
  - ✓Registro de fluxo
- **Indica possíveis utilizações do modelo:**
  - ✓ Contabilização baseado no uso
  - ✓ Perfíl de tráfego
  - ✓Engenharia de tráfego
  - ✓Detecção de intrusão
  - ✓ Monitoramento de QoS
- **Como distinguir os fluxos;**
  - ✓ Interfaces
  - ✓Campos do cabeçalho IP
  - ✓Campos do cabeçalho de transporte
  - ✓Rótulos MPLS
  - ✓Código DiffService
- **Técnicas para medição e exportação dos dados:**
  - ✓Amostragem
  - ✓Expiração
  - ✓Confiabilidade
  - ✓Segurança
  - ✓Etc.

Exemplo de medição/exportação

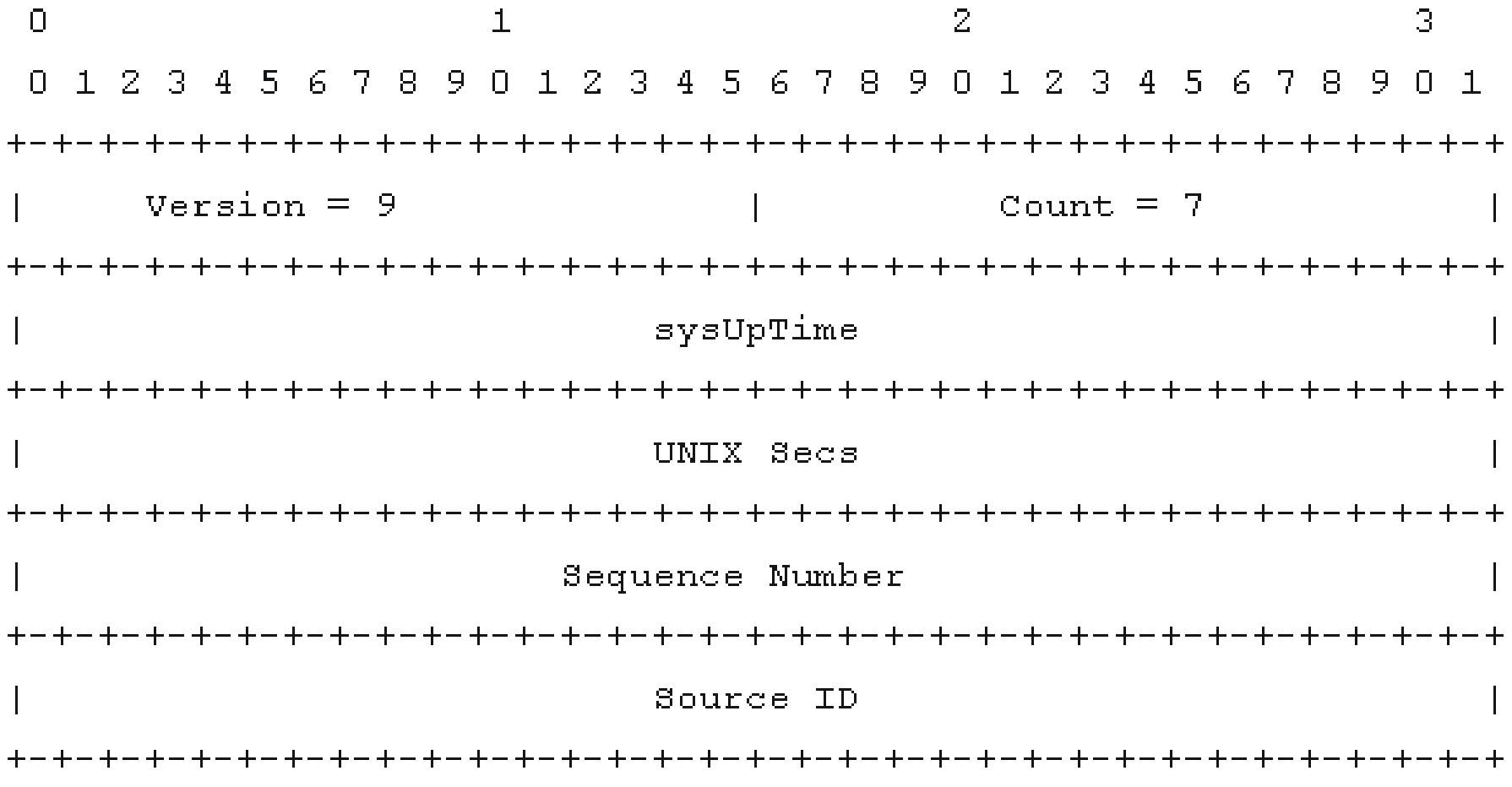


Protocolo *NetFlow v9*



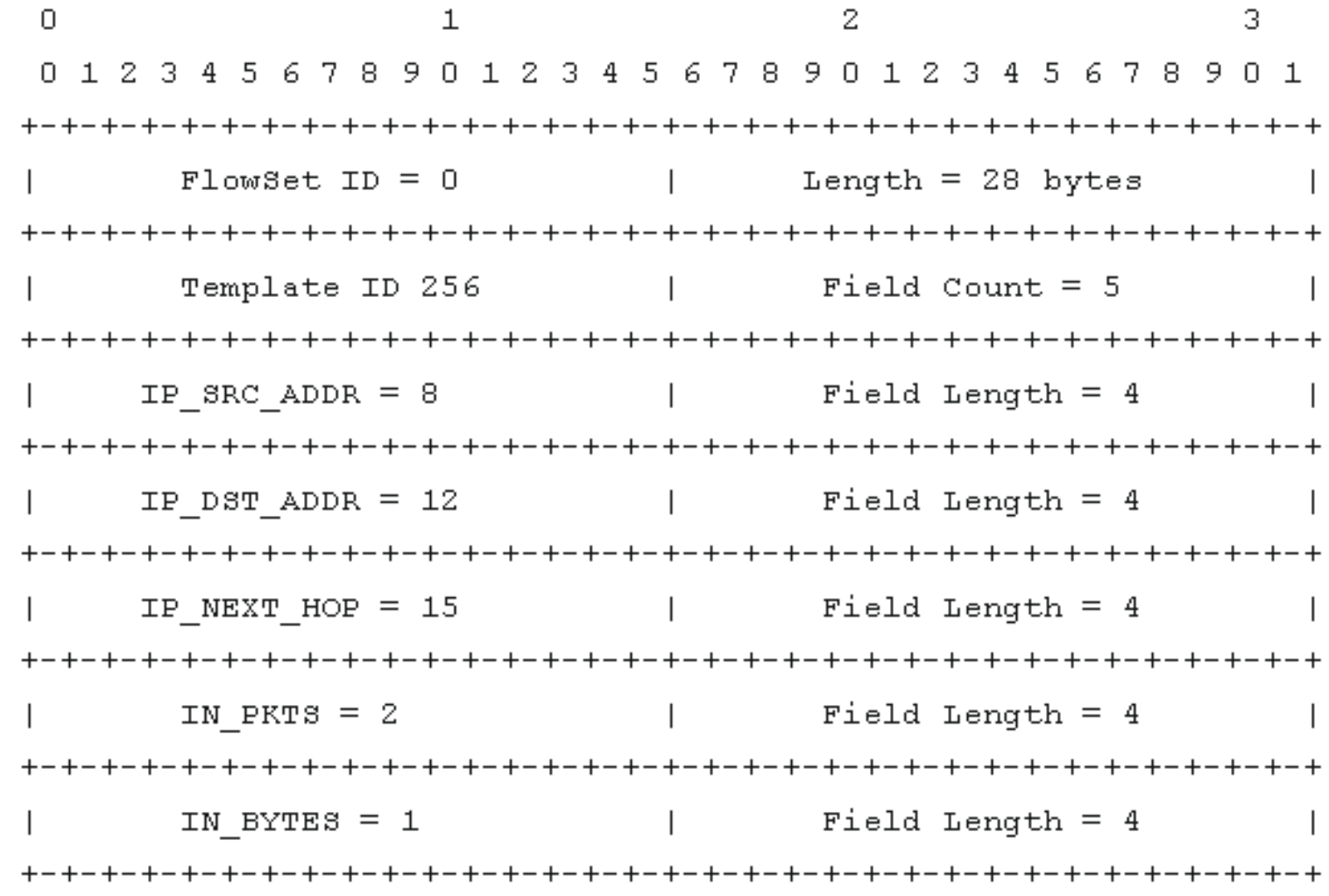
Protocolo *NetFlow v9*

Packet Header



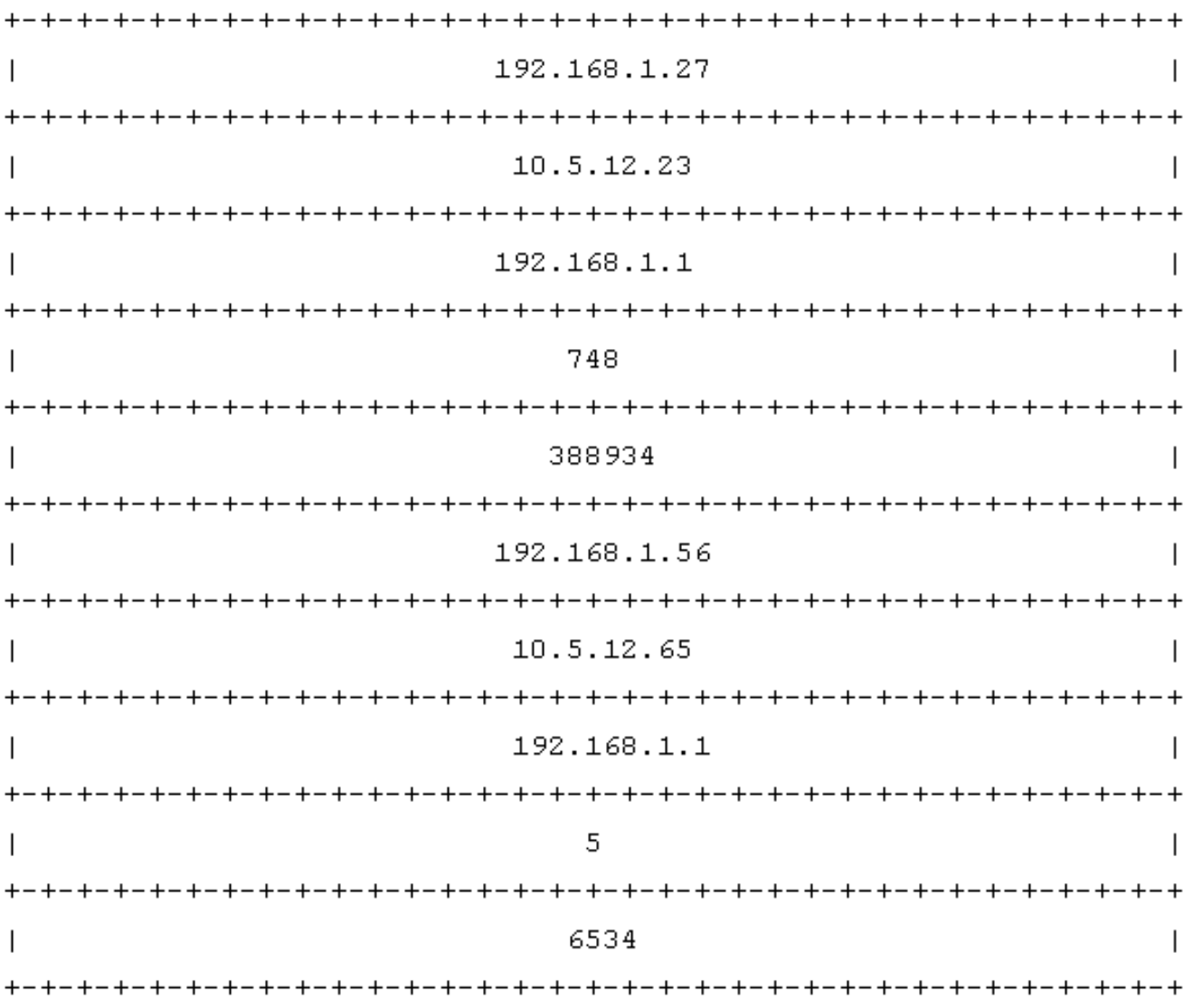
Protocolo *NetFlow v9*

Template FlowSet



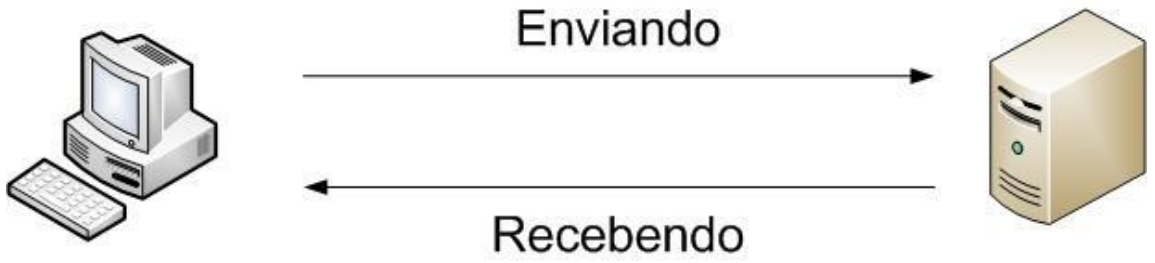
Protocolo *NetFlow v9*

Data FlowSet



Fluxos unidirecionais

- Um fluxo unidirecional representa uma das direções de uma determinada conexão/sessão entre dois hosts.



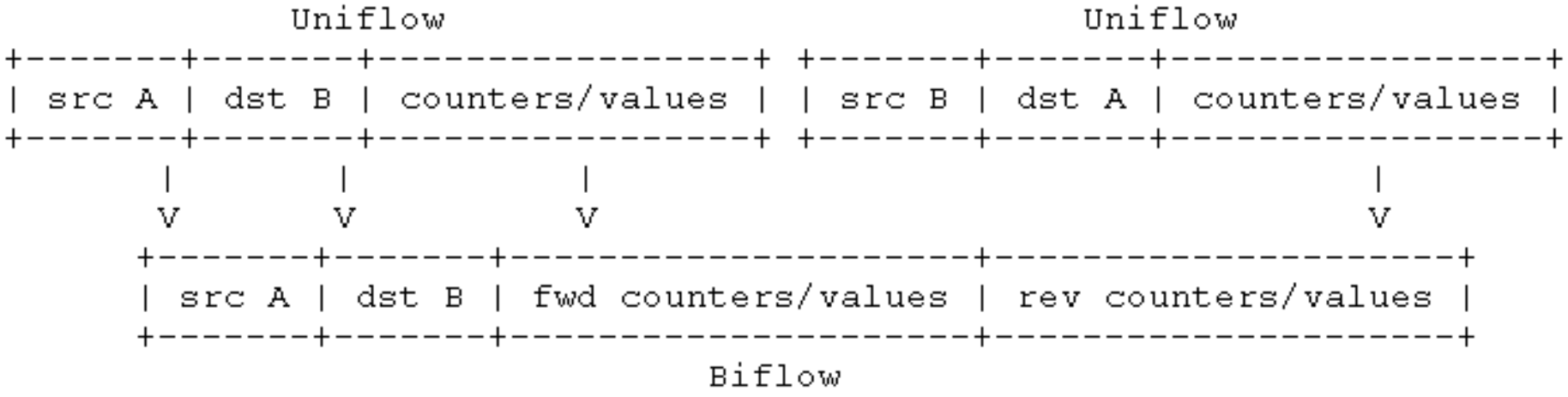
Source	Destination	srcport	dstport	first	TotalBytes	TotalPackets	Protocol
192.168.216.129	192.168.202.9	54616	22	2008-05-06 17:26:57	429323	5201	6
192.168.202.9	192.168.216.129	22	54616	2008-05-06 17:26:57	634087	4044	6

2 rows in set (20.73 sec)

Fluxos Bidirecionais (*Biflow*)

- **Um fluxo bidirecional é um fluxo representando pacotes fluindo entre ambas direções de uma conexão de rede.**

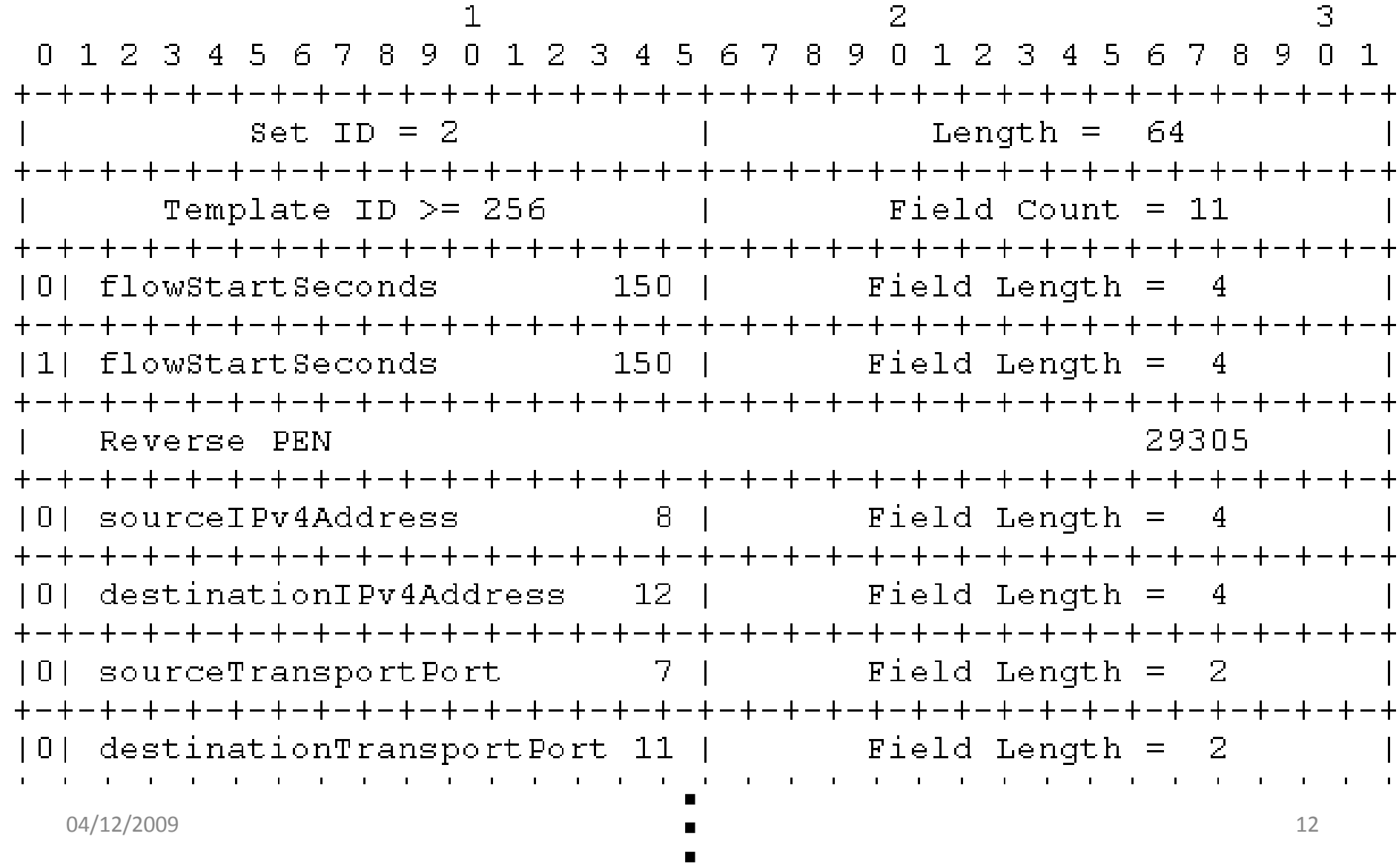
- **Razões para sua existência:**
  - **A maioria das aplicações de rede são bidirecionais;**
  - **Eliminar duplicações de campos do modelo IPFIX.**



Fluxos Bidirecionais (*Biflow*)

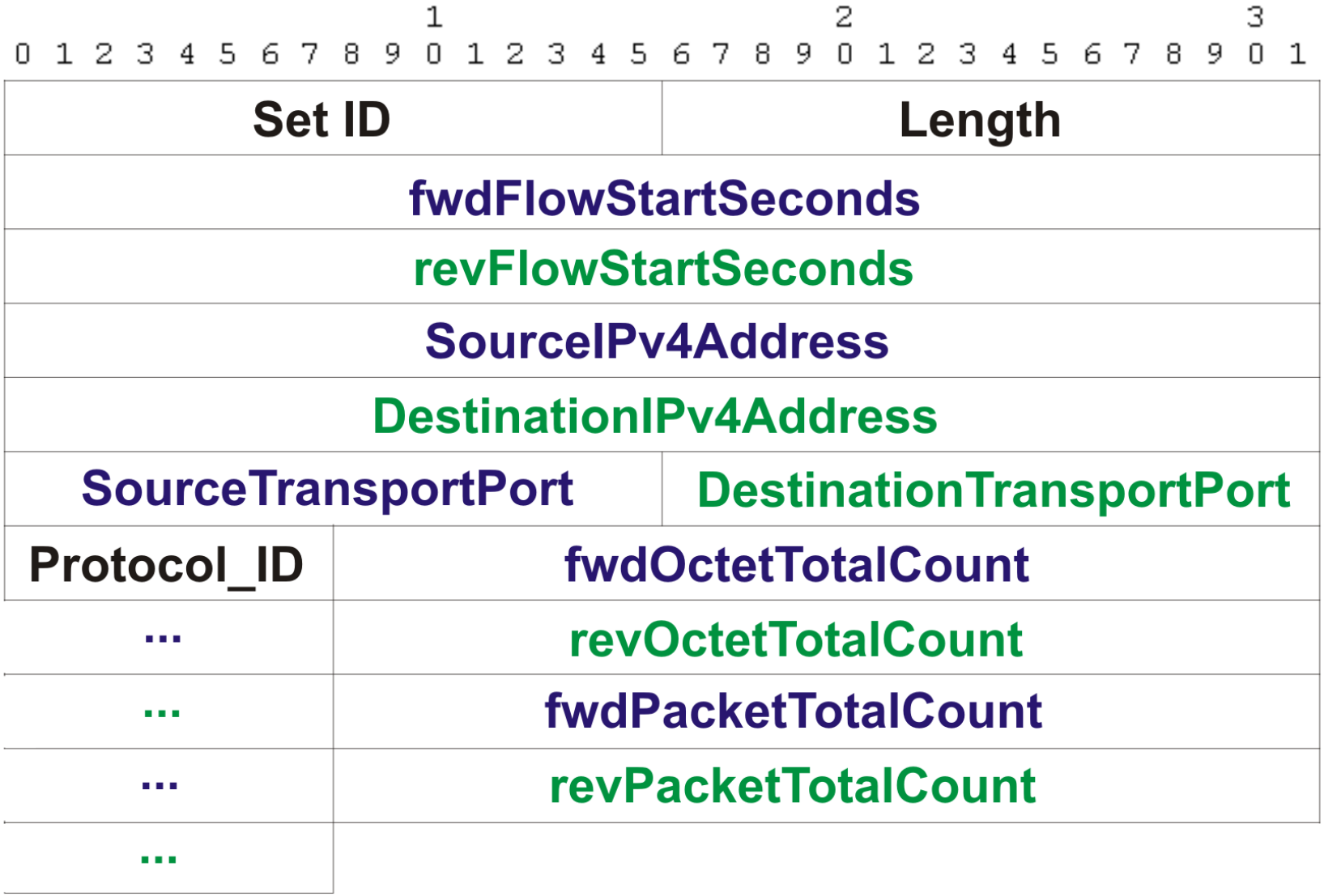
- **Terminologia:**
  - ***Directional key Field***: associado a uma única extremidade do fluxo. Ex.: *sourceIPv4Address*, *destinationTransportPort*.
  - ***Non-directional key field*: não está especificamente associado a alguma das extremidades do fluxo. Ex.: *protocolIdentifier***
  - ***Biflow Source/Destination*:** É a entidade fim identificado pelos campos direcionais de origem/destino em um *BiFlow*.
  - ***Forward direction*:** a direção que representa os pacotes enviados pela origem.
  - ***Reverse direction*:** a direção que representa os pacotes enviados pelo destino.
  - ***Reverse Information Element*:** elemento associado a direção reversa do *BiFlow*.

Exemplo de template do *BiFlow*

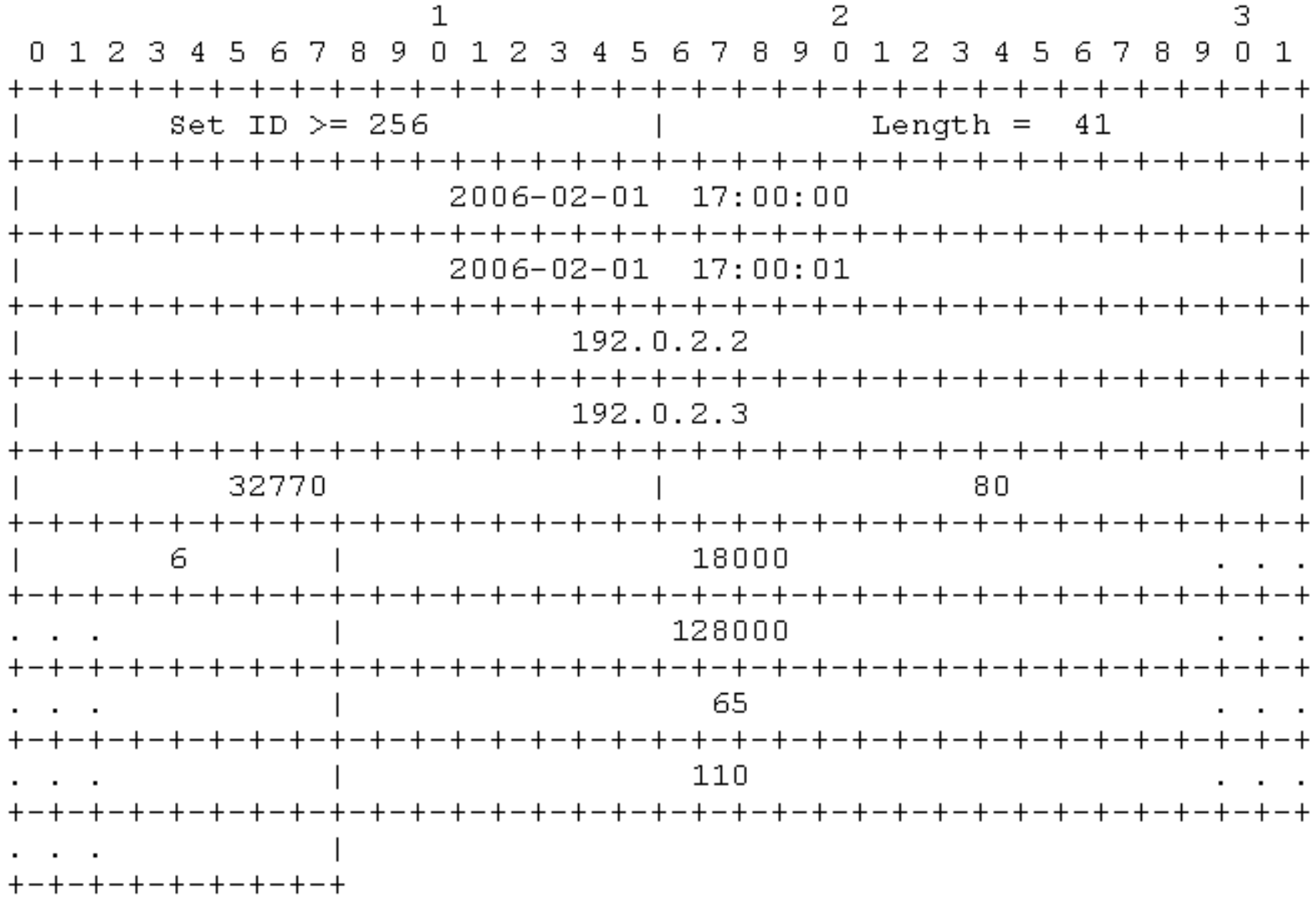


Exemplo de template do *BiFlow*

Exemplo de dados do *BiFlow*

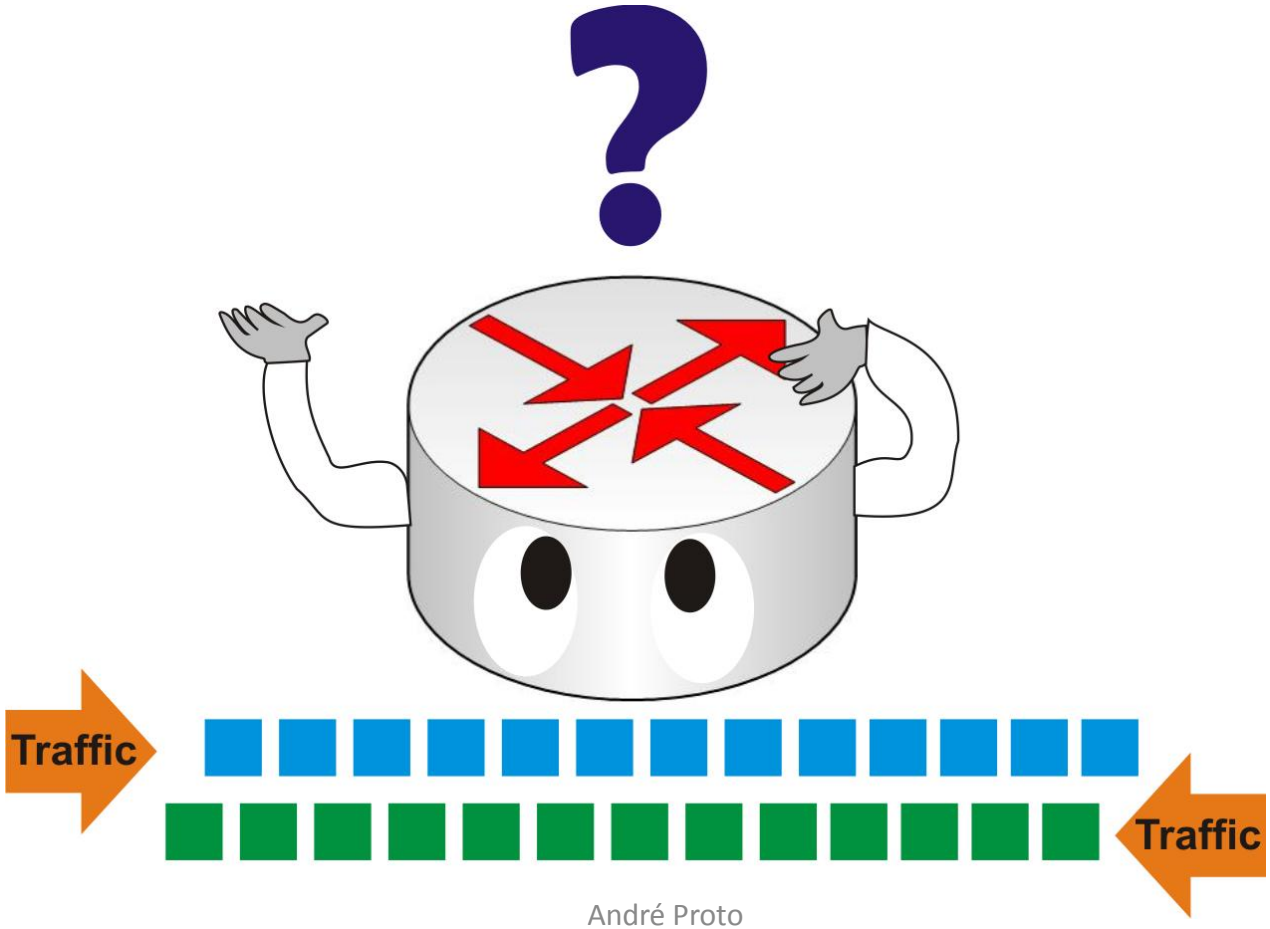


Exemplo de dados do *BiFlow*



Determinar direções no *BiFlow*

Como determinar o IP de origem e destino de um fluxo bidirecional?

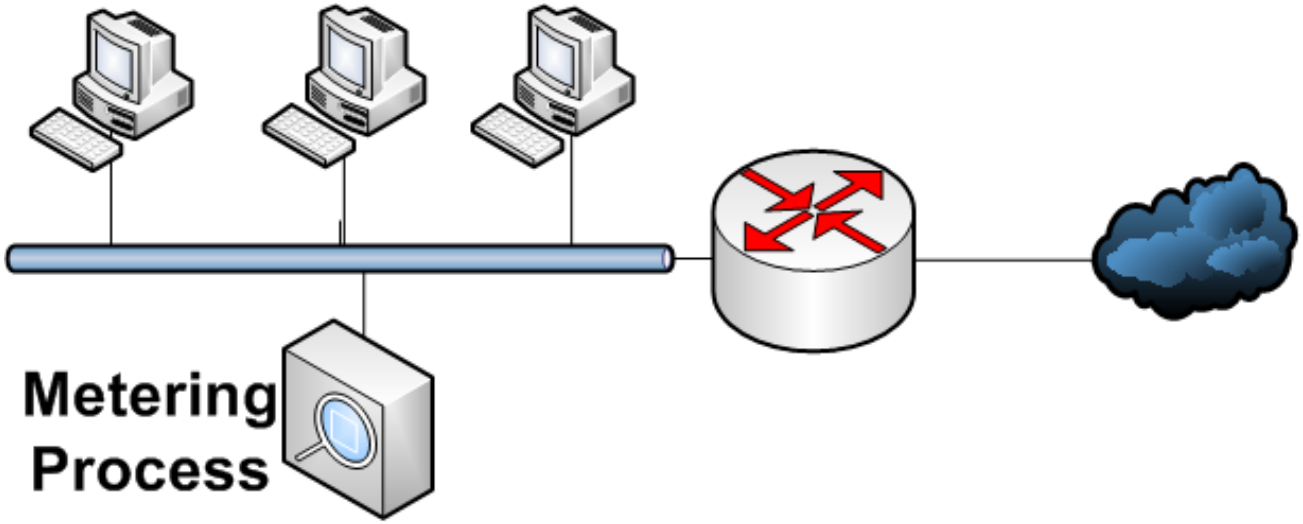


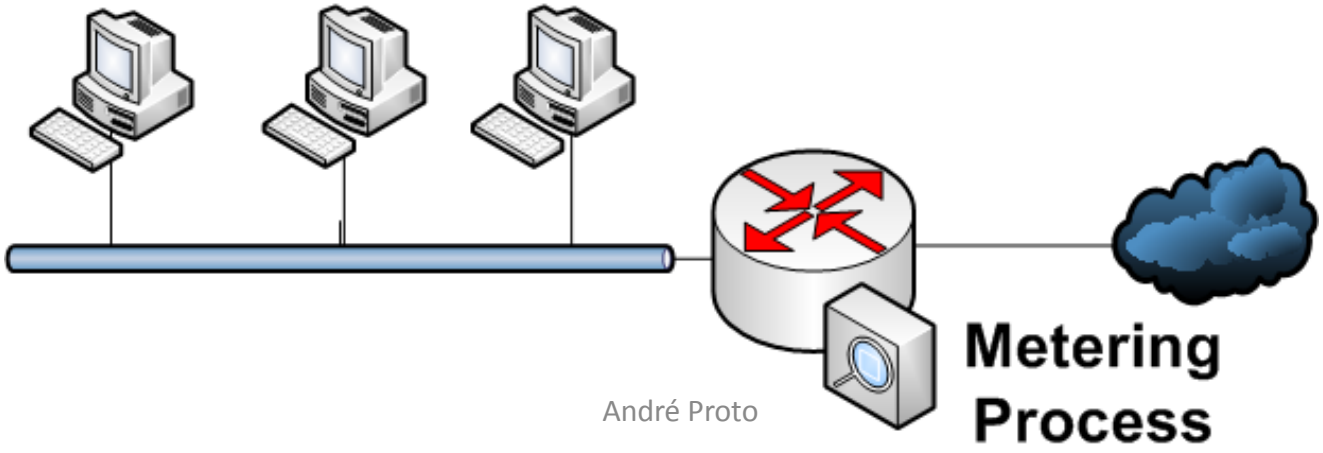
Direções – Primeiro cenário

1. **Determinar origem pelo iniciador da comunicação.**
   - **Assumir que o primeiro pacote passante de uma comunicação seja o iniciador;**
   - **Analisar *flags* dos protocolos de transporte.**
   - **Analisar características do protocolo de aplicação (ex.: *DNS Query/Response*).**

- **Existem problemas quando um novo fluxo é gerado a partir de pacotes de uma comunicação já existente.**

Direções – Primeiro cenário



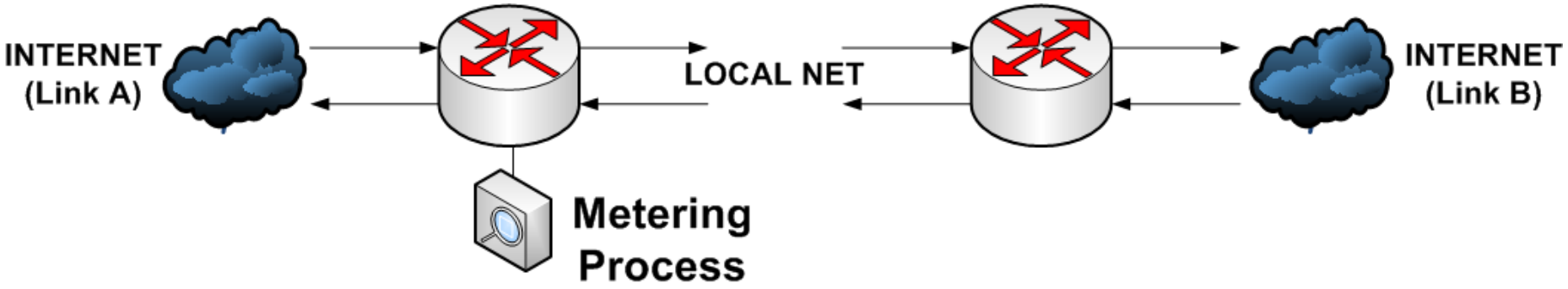


Direções – Segundo cenário

2. Determinar direção baseado no perímetro.

- Cenário em que não é possível determinar a comunicação pelos métodos citados anteriormente.
- Um conjunto de endereços locais deve estar bem definido.

- **Origem é sempre o comunicante externo.**

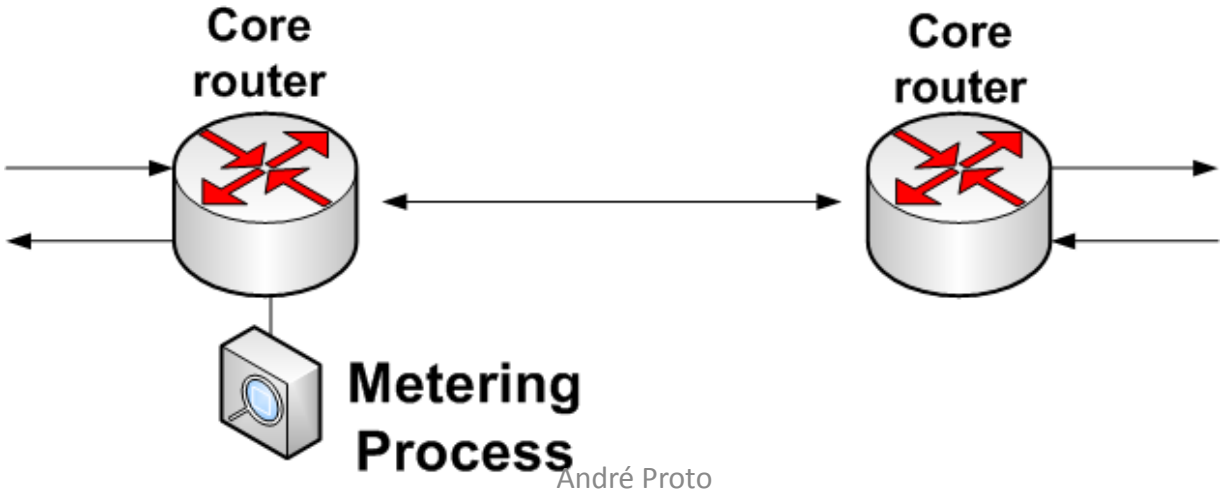


Direções – Terceiro cenário

3. Determinar a direção arbitrariamente.

- Monitoramento em núcleo de redes, em que não há um conjunto de IPs bem definidos.

- **O MP pode definir origem e destino arbitrariamente.**
  - Após definidos, o MP deve manter a decisão até o fim da vida do fluxo.



BiflowDirection Information Element

Value	Name	Description
0x00	arbitrary	Direction was assigned arbitrarily.
0x01	initiator	The Biflow Source is the flow initiator, as determined by the Metering Process' best effort to detect the initiator.
0x02	reverseInitiator	The Biflow Destination is the flow initiator, as determined by the Metering Process' best effort to detect the initiator. This value is provided for the convenience of Exporting Processes to revise an initiator estimate without re-encoding the Biflow Record.
0x03	perimeter	The Biflow Source is the endpoint outside of a defined perimeter. The perimeter's definition is implicit in the set of Biflow Source and Biflow Destination addresses exported in the Biflow Records.

Conclusões e próximos passos

- **Questões ainda pendentes sobre o *BiFlow*:**
  - **Qual custo computacional para determinar a origem e destino?**
  - **É realmente viável?**
- **Próximo passo: Criar e implementar um protocolo baseado no RFC 5103.**

Fim

Obrigado!

- **André Proto**
  - andre.proto@sjrp.unesp.br
  - PGP KeyID: 0xA6FC761A