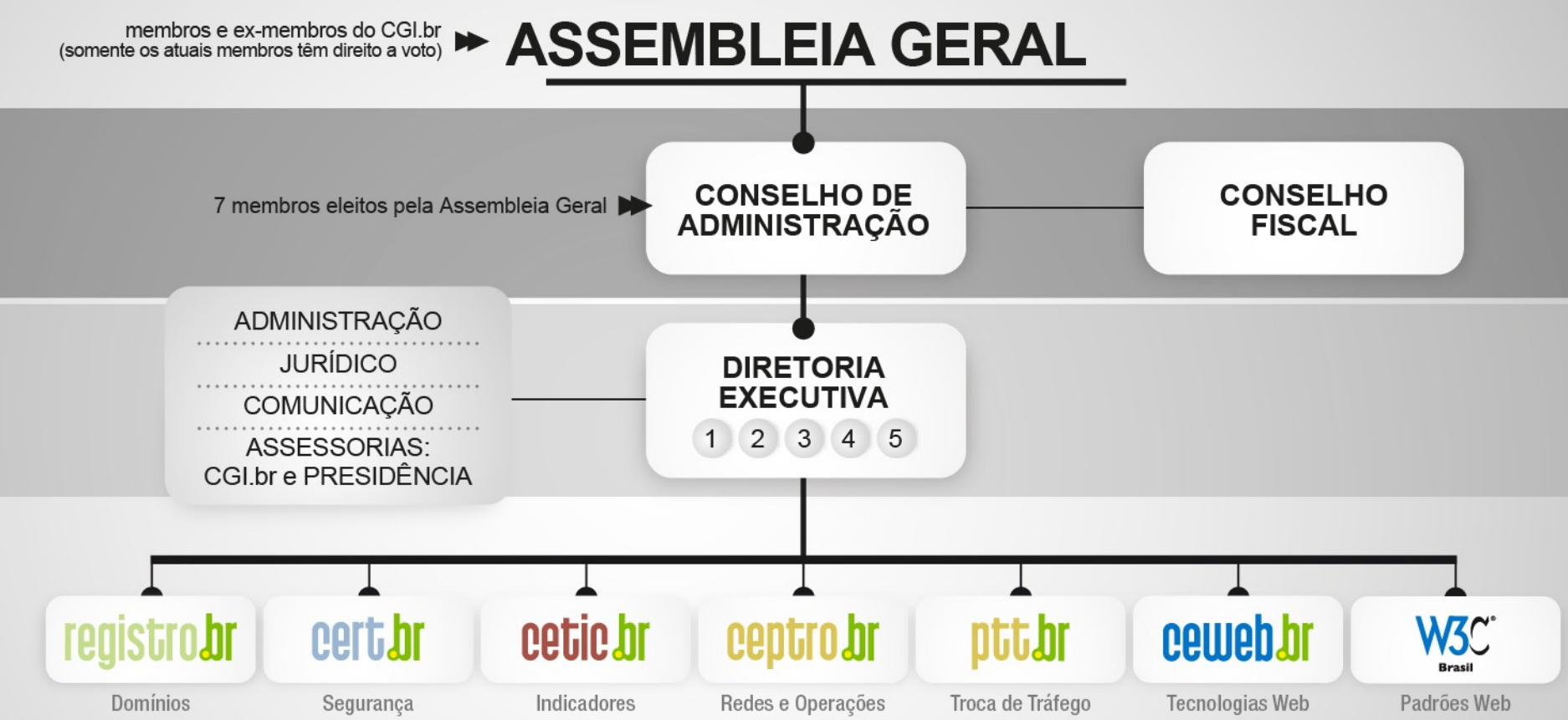

nic.br
Núcleo de Informação
e Coordenação do
Ponto BR
cgi.br
Comitê Gestor da
Internet no Brasil
registro.br cert.br cetic.br ceptro.br ptt.br ceweb.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e SOCIEDADE CIVIL — 10 11 12 13 14 15 16 17 18 19 20 21

Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

nic.br cgi.br | ceptro.br

LACNIC / LACNOG

São Paulo, SP | **22**/05/15

FLOWs
uma introdução muito muito básica...

Antonio Marcos Moreiras

ceptro.br nic.br cgi.br

Introdução ao uso de Flows

➔ O que é Flow?

➔ Para que serve?

➔ Quando é útil?

➔ Como eu utilizo?

O que é Flow?

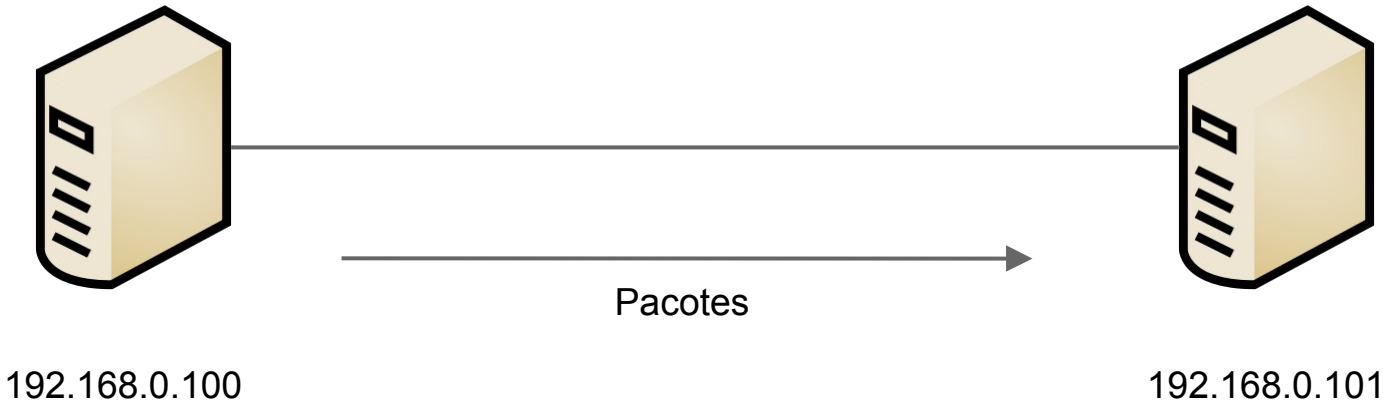
O que é Flow?

➔ No contexto de redes de computadores:

sequência **unidirecional** ou bidirecional de pacotes com características em comum entre uma origem e um destino

O que é Flow?

Exemplo de Flow:



flow: 1 origem:192.168.0.100 destino:192.168.0.101

Para que serve?

Para que serve?

➔ Necessidade de **mais informações** sobre o uso da rede

- O SNMP (p. exemplo, usando Cacti ou MRTG) informa apenas o total do tráfego em uma interface

Para que serve?

➔ Necessidade de um mecanismo **eficiente** de coleta de dados

- A captura de todo o tráfego (usando tcpdump p. ex.) pode ser inviável dependendo da banda

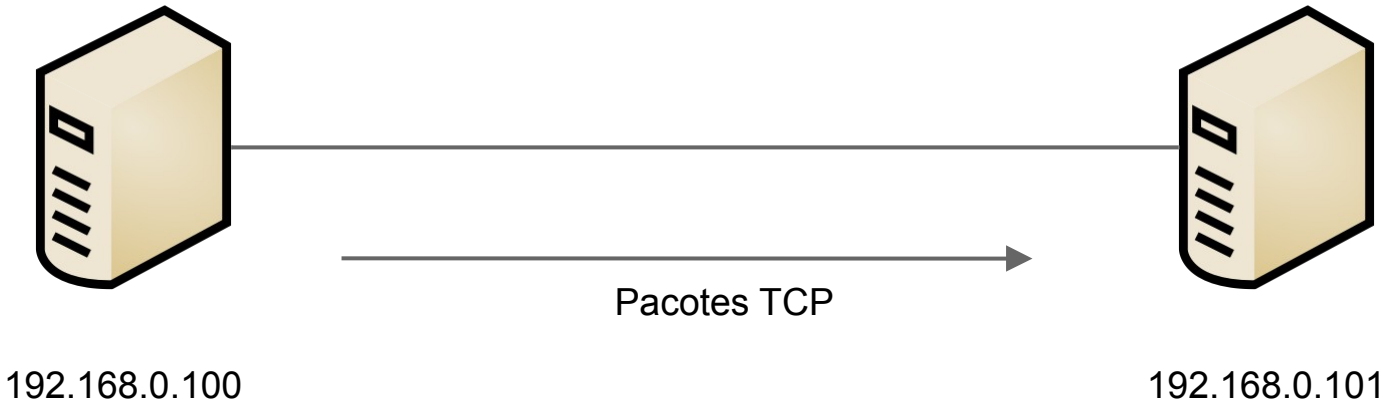
Para que serve?

➔ O que queremos é um meio termo:

- Ao invés de guardar pacote a pacote, agrupar esses pacotes por **características semelhantes**
  - **Origem e destino**
  - **Porta de origem e destino**
  - **Protocolo de camada de transporte**

O que é Flow?

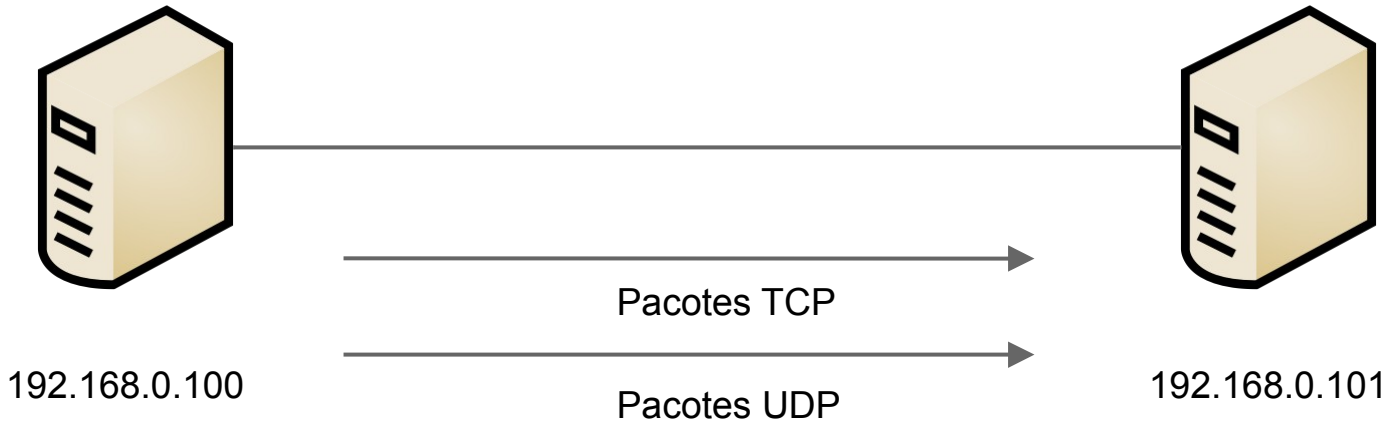
Exemplo de Flow:



flow: 1 origem:192.168.0.100 destino:192.168.0.101 protocolo: tcp

O que é Flow?

Exemplo de Flow:



flow: 1 origem:192.168.0.100 destino:192.168.0.101 protocolo: tcp
flow: 2 origem:192.168.0.100 destino:192.168.0.101 protocolo: udp

Quando é útil?

Quando é útil?

- ➔ Engenharia de tráfego
- ➔ Top Talkers
- ➔ Monitoramento de redes ocultas
- ➔ Lista de IPs maliciosos
- ➔ Análise de dados históricos
- ➔ Violações de política de uso

Como eu utilizo?

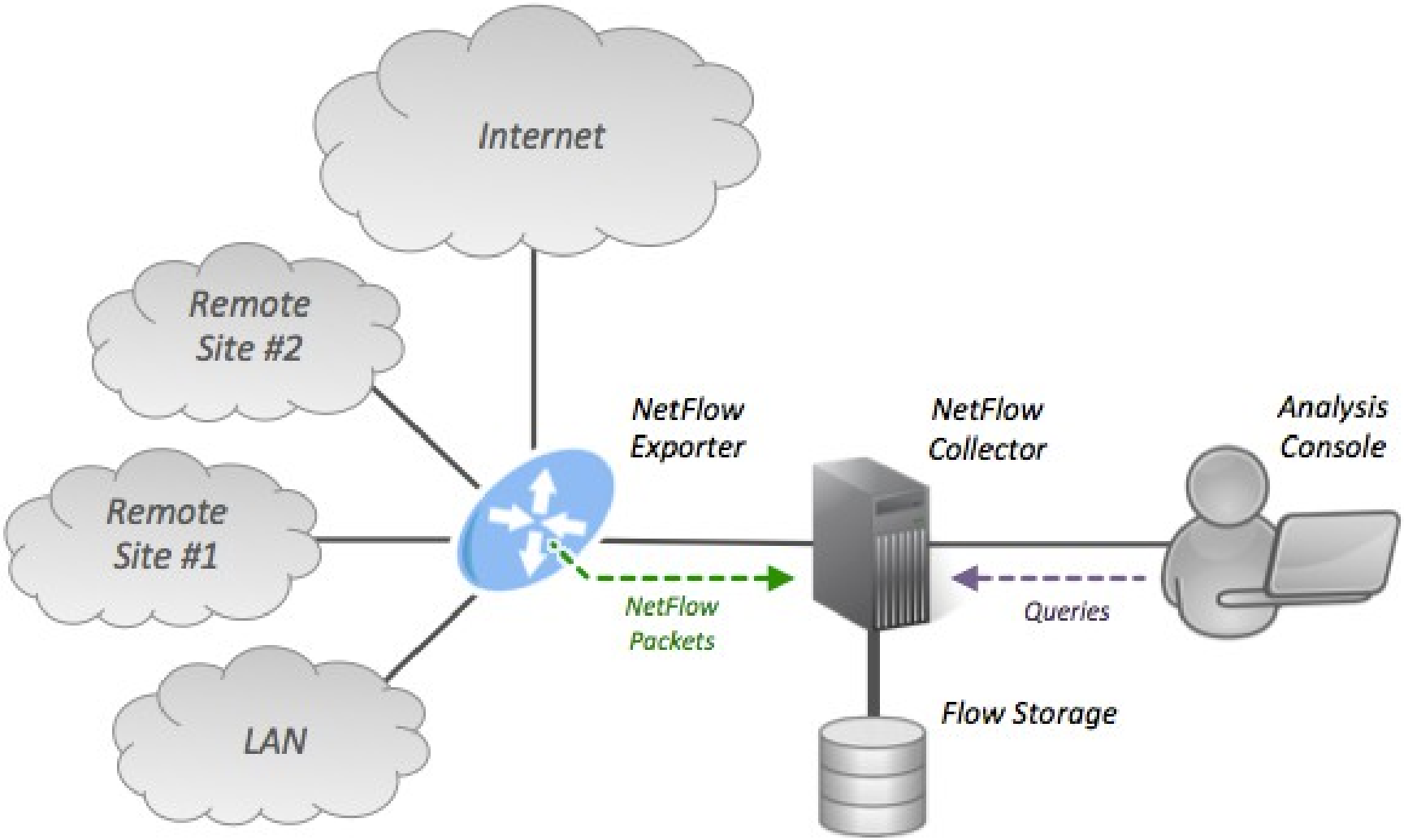
Tipos de Flow

Tipos de Flow

- NetFlow
- IPFIX
- sFlow

Equipamentos necessários

- **Exportador de flows (roteador / servidor)**
  - Equipamento que analisa os pacotes, gera os flows e os envia ao coletor
- **Coletor de flows**
  - Recebe os flows do exportador, armazena e pré-processa os dados
- **Analisador de flows**
  - Analisa os dados armazenados no coletor de flows



fonte: http://en.wikipedia.org/wiki/File:NetFlow_Architecture_2012.png

Ferramentas

- ➔ **nfdump** (coletor e analisador de dados de flow)
- ➔ **nfsen** (frontend para dados coletados via nfdump)
- ➔ **ntop** (monitora NetFlow através do nprobe)
- ➔ **softflowd** (exportador de flows para Linux)

Obrigado

www.nic.br

moreiras@nic.br

22 de maio de 2015

nic.br cgi.br

www.nic.br | www.cgi.br