Universidade Federal do ABC

Gerenciamento e Interoperabilidade de Redes

NetFlow e Syslog

Prof. João Henrique Kleinschmidt

Syslog

- Escreve mensagens de sistema em um log
- Permite a um dispositivo enviar notificações de eventos a coletores de mensagens de eventos (servidores syslog)
- Originalmente desenvolvido para sistemas UNIX, em que mensagens e alertas do SO geradas são armazenadas em um arquivo na forma de mensagens syslog (usa o daemon syslogd)
- Protocolo Syslog definido pela RFC 3164 na tentativa de padronizar mensages syslog
- Vários dispositivos de rede podem gerar mensagens syslog (roteadores, switches, firewalls, etc)
- Mensagens syslog são enviadas a servidores syslog usando UDP (porta 514)

Syslog

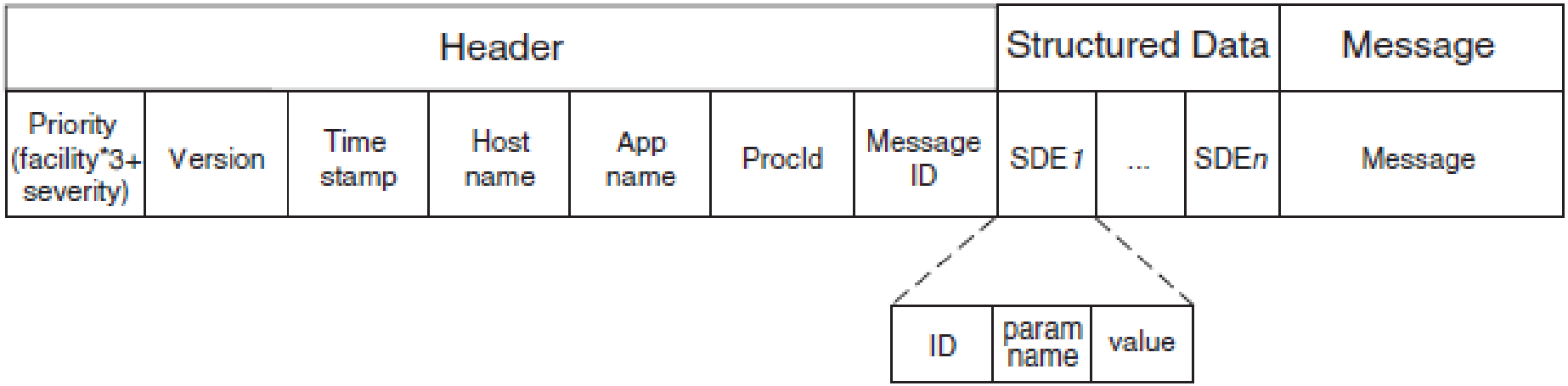
- Exemplos de mensagens syslog (existem diversas variações de mensagens syslog)

```
172.19.209.130  000024: *Apr 12 18:01:55.643: % ENV_MON-1-SHUTDOWN: Environmental
Monitor initiated shutdown
```

```
01:14:11: %IPPHONE-6-REG_ALARM: 25: Name=SEP003094C38724 Load=3.2(2.9)
Last=Initialized
```

```
*Mar  6 22:48:34.452 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
 changed state to up
```

Estrutura da mensagem syslog (IETF)



Ex:

```
<35>1 2006-06-11T22:14:15.003Z mymachine.example.com su – ID58 - 'su root' failed
for wbuchhau on /dev/pts/8
```

Syslog – níveis de facilidade (fonte que gerou os logs)

Facility Values

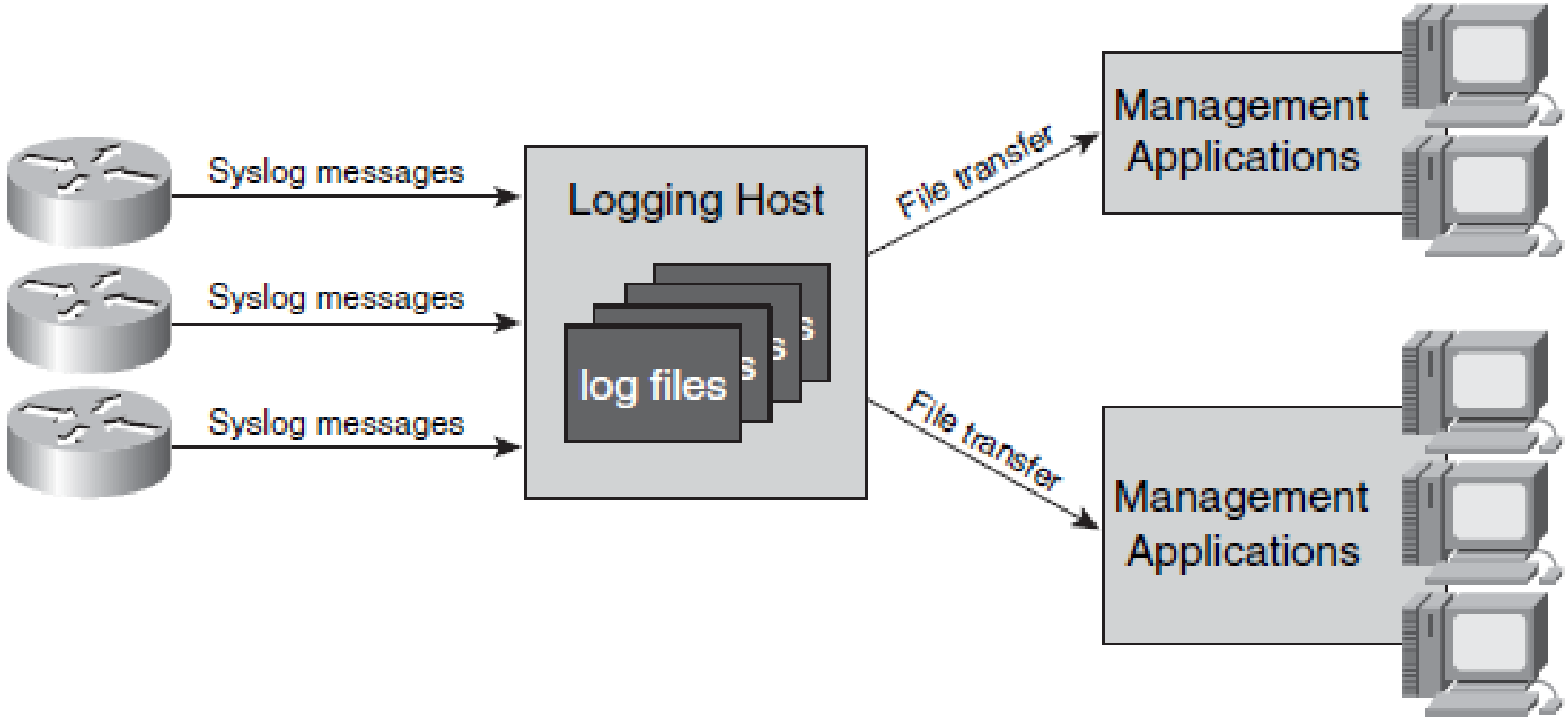
Integer	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages
5	Messages generated internally by Syslogd
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon

Integer	Facility
10	Security/authorization messages
11	FTP daemon
12	NTP subsystem
13	Log audit
14	Log alert
15	Clock daemon
16	Local use 0 **(local0)**
17	Local use 1 **(local1)**
18	Local use 2 **(local2)**
19	Local use 3 **(local3)**
20	Local use 4 **(local4)**
21	Local use 5 **(local5)**
22	Local use 6 **(local6)**
23	Local use 7 **(local7)**

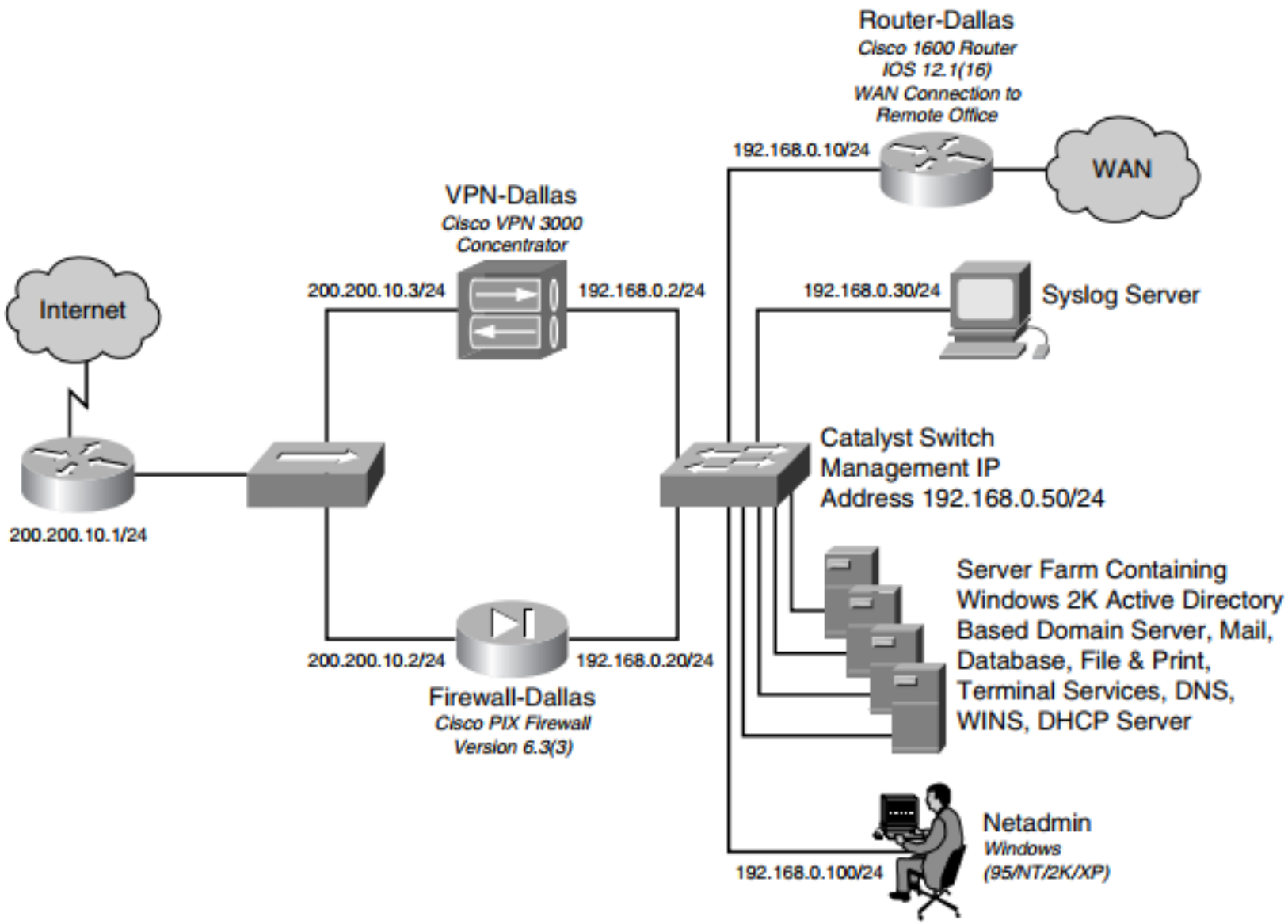
Syslog – níveis de severidade

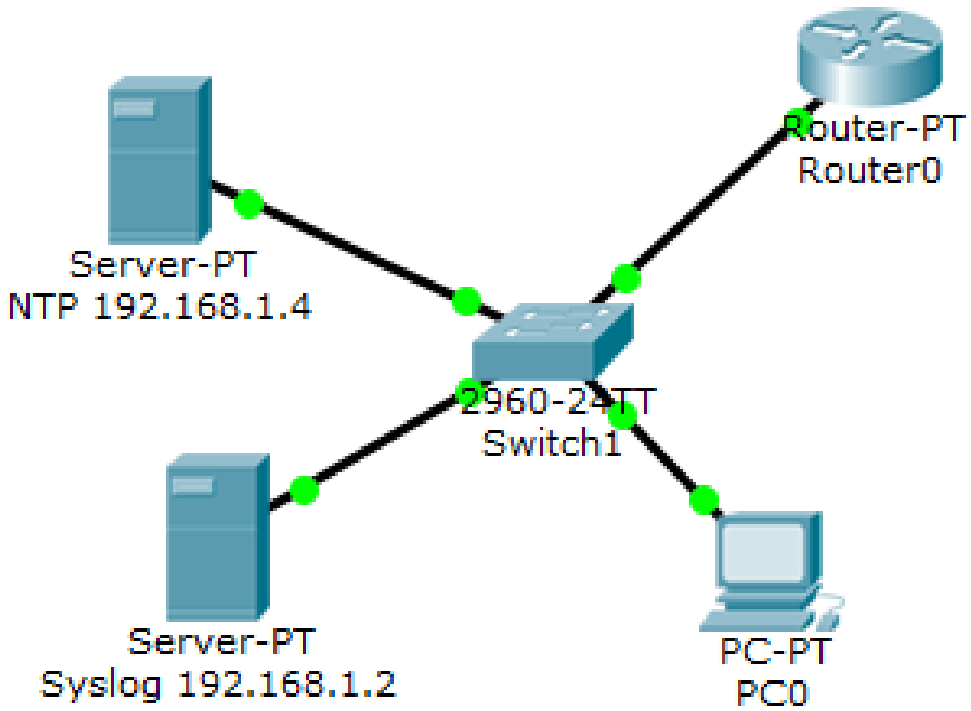
Nível	Significado aproximado
emerg	Situações de pânico
alert	Situações urgentes
crit	Condições críticas
err	Outras condições de erros
warning	Mensagens de alerta
notice	Coisas que podem merecer investigação
info	Mensagens informativas
debug	Somente para depuração

Syslog


Syslog messages
Syslog messages
Syslog messages
Logging Host
log files
File transfer
File transfer
Management Applications
Management Applications

Servidor syslog em um ambiente de rede





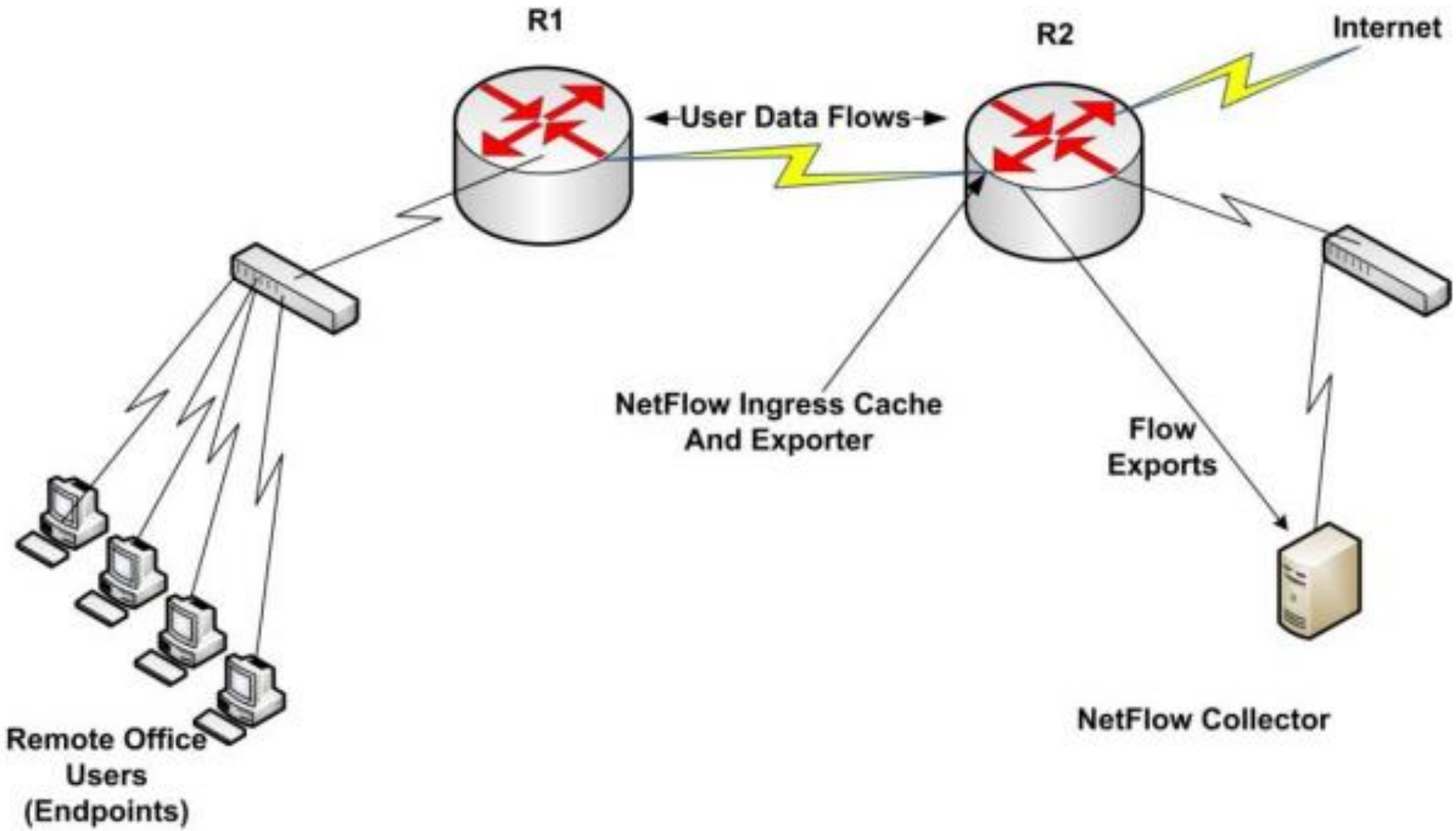
Configuração de syslog e NTP

- Crie a rede e habilite syslog no servidor
- Configure o roteador para enviar eventos de log ao servidor: *logging host 192.168.1.2*
- Gere eventos (como ligar e desligar interface de rede) e verifique as mensagens no servidor syslog
- Para arrumar o timestamp, pode-se usar um servidor NTP. Habilite o servidor NTP e no roteador configure o serviço de timestamps do logging e servidor NTP:
  service timestamps log datetime msec
  ntp server 192.168.1.4
- Verifique a configuração de log e relógio no roteador:
  show logging e *show clock*

Netflow

- Desenvolvido pela Cisco
- IPFIX padronizado pelo IETF baseado na versão 9 do Netflow
- Coleta dados de tráfego de rede
- Netflow comunica informações estatísticas de tráfego de dados IP que “passam” por um roteador
- As estatísticas são dadas para determinados fluxos
- Um fluxo consiste de todo o tráfego que pertence ao mesmo contexto de comunicação

Netflow


R1
R2
Internet
User Data Flows
NetFlow Ingress Cache
And Exporter
Flow
Exports
NetFlow Collector
Remote Office
Users
(Endpoints)

Netflow

- Um fluxo é unicamente identificado pelas seguintes informações:

  - Endereço IP de origem
  - Porta de origem
  - Endereço IP de destino
  - Porta de destino
  - Tipo de protocolo (for example, whether the IP packet carries TCP or UDP)
  - Tipo de serviço (TOS) (byte do protocolo IP que identifica o tipo de serviço, usado para diferenciar categorias de tráfego)
  - Interface de entrada

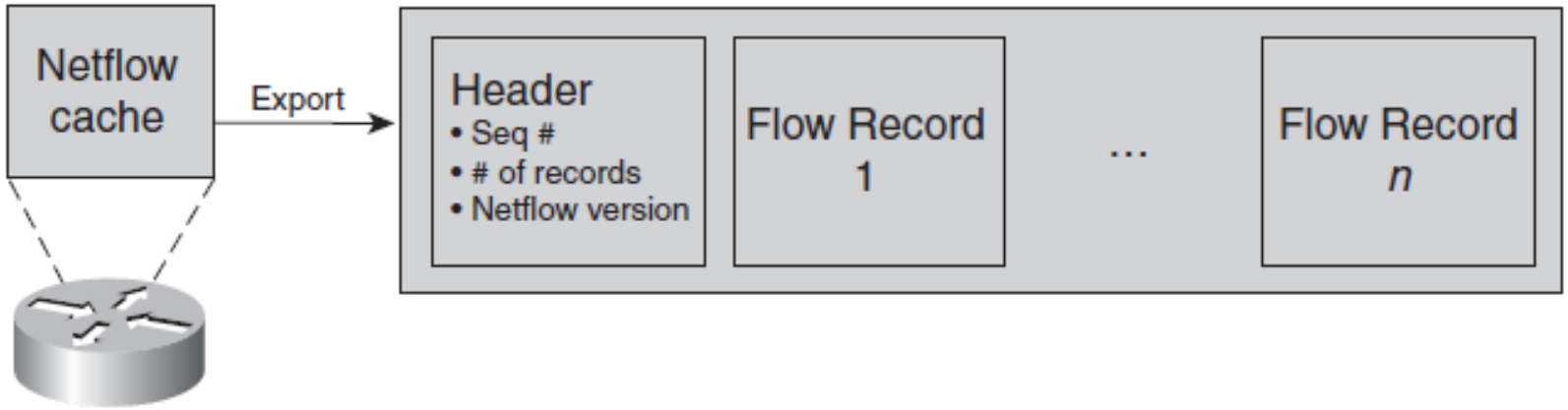
Netflow

- Exemplo de fluxos:

Key Field	Flow 1	Flow 2	Flow 3	Flow 4
Source IP	10.10.1.1	10.10.1.1	10.10.2.1	10.10.3.35
Destination IP	10.10.2.55	10.1.23.1	10.10.2.253	10.10.2.23
Source port	21	8080	21	443
Destination Port	21	8080	21	1122
Protocol	17	6	17	6
ToS	184	184	184	184
IfIndex	1	1	1	1

Netflow

- O protocolo consiste de colocar registros em pacotes Netflow e exportar estes pacotes para um receptor de fluxos, chamado de coletor Netflow

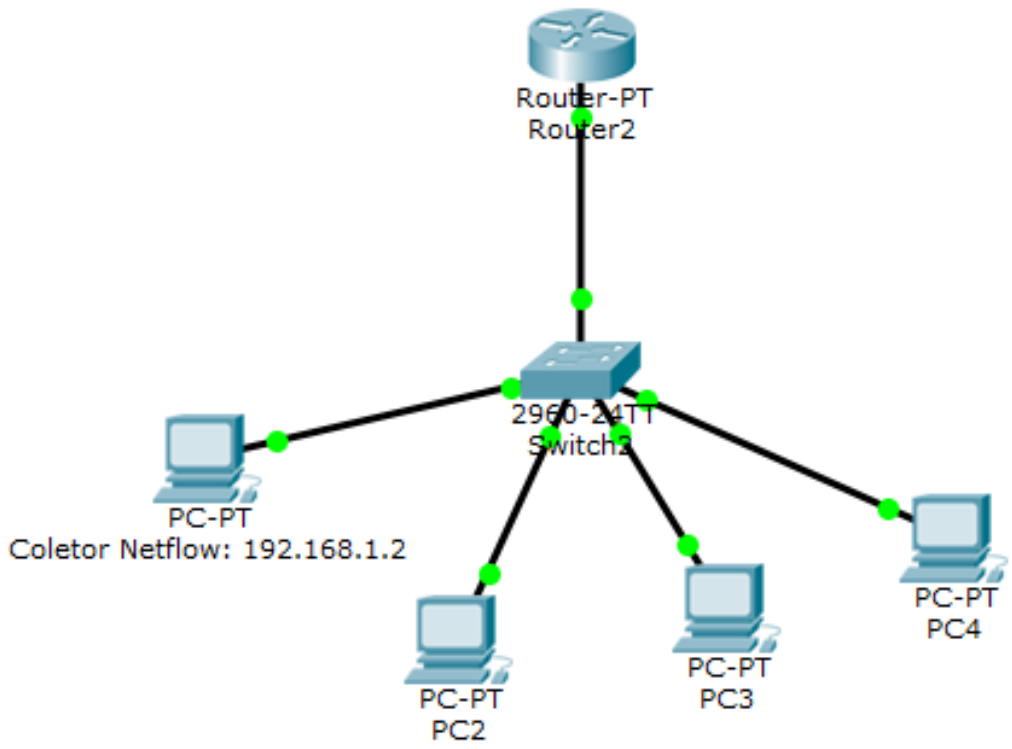


Netflow

- Quando no novo fluxo é detectado, o roteador registra este fluxo no cache Netflow
- Quando um fluxo termina, a entrada no cache expira. A informação do cache é transferida para um registro e preparada para transmissão com o protocolo Netflow.
- Um fluxo é encerrado quando:
  - Não foi detectado tráfego por um certo período (tipicamente 15 segundos ou configurável)
  - Um pacote que indica que o fluxo de dados acabou é detectado (ex: TCP FIN ou RST)
  - Um fluxo ficou ativo por muito tempo (tipicamente 30 minutos ou configurável)

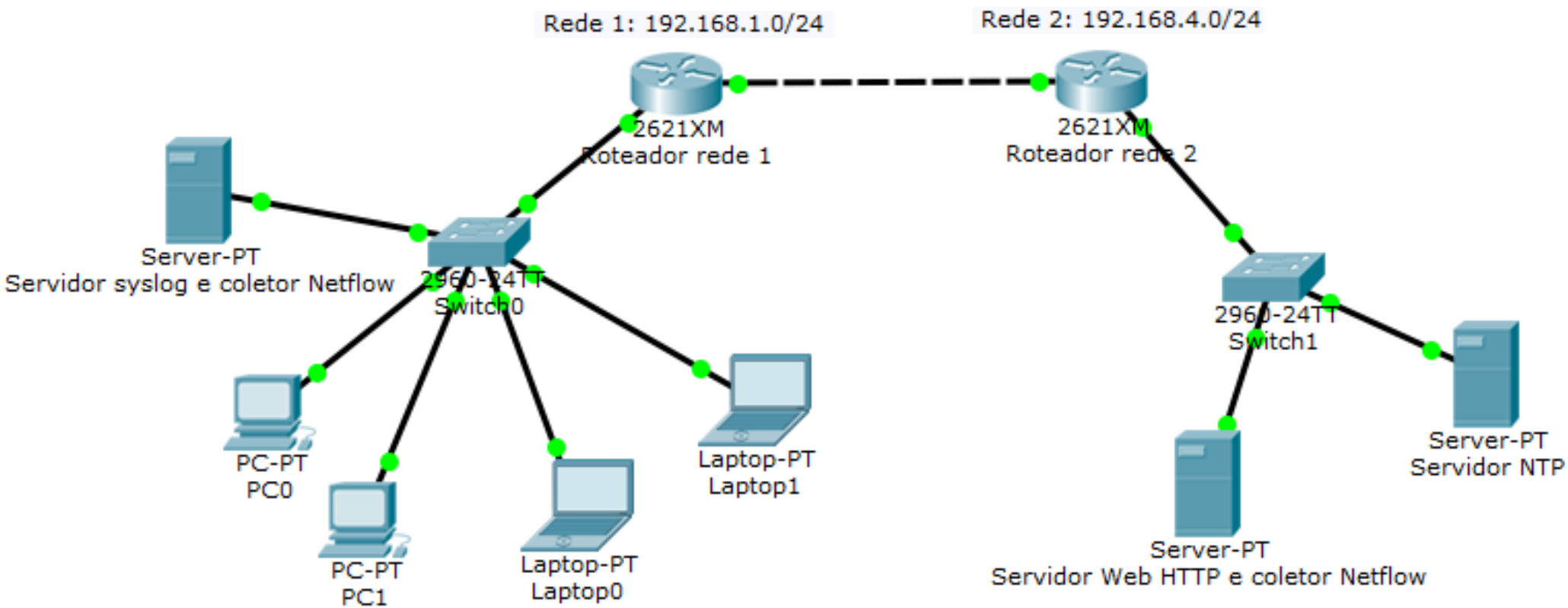
Versões Netflow

- Netflow v5 – versão mais usada com as capacidades discutidas anteriormente
- Netflow v7 – voltado para switches
- Netflow v8 – oferece capacidade de agregação (combinar dados de diferentes fluxos em um registro; ex: todo o tráfego de uma única origem)
- Netflow v9 – versão mais nova. Implementa flexibilidade nas definições de campos chave e não-chave de um fluxo
- IPFIX – padrão IETF baseado na versão 9



Configuração Netflow

- Habilite o Netflow no PC (ou servidor)
- Na interface de rede FastEtherner do roteador habilite o Netflow:
  ip flow ingress
- Configure IP e porta de destino para onde os fluxos serão enviados (o padrão é 9996):
  ip flow-export 192.168.1.2 9996
  ip flow-export version 9 (configura versão do Netflow)
- Para verificar o cache Netflow do roteador:
  show ip cache flow
- Execute ping de vários PCs ao roteador e verifique o coletor Netflow



- A topologia possui 2 sub-redes. Na sub-rede 1, habilite o log e Netflow no roteador e ligue o servidor syslog e coletor Netflow no servidor. A data e hora do roteador devem ser obtidas com o servidor NTP da sub-rede 2. Na sub-rede 2, habilite o servidor HTTP e coletor Netflow. Acesse o servidor Web da sub-rede 2 com os PCs e laptops da sub-rede1. Verifique as estatítiscas do Netflow.