Controlando o Tráfego Peer-to-Peer

Leandro Bertholdo, Andrey Andreoli, Liane Tarouco
CERT-RS / POP-RS / UFRGS
{andrey,berthold, liane}@penta.ufrgs.br
{mell,emerson}@tche.br

Sumário

- Histórico do Peer-to-Peer
- Impactos e riscos
- Mensurando o Problema
- Experiências com P2P

Histórico

- **1998** - Shawn Fanning, estudante da universidade de Massachussets, criou um software conhecido como Napster para facilitar a troca de arquivos mp3 com seus colegas
- **Bloqueio:** Simples, bastava filtrar os IPs dos servidores (64.124.41.0/24)

Histórico

- **2004**: Bearshare, BitTorrent, Earthstation, eDonkey, eMule, KazaA, KazaA Lite, MlMac, SoulSeek, WinMX
- **Bloqueio**: Complexo, quando não impossível – é preciso analisar o protocolo
- Existem implementações que cifram a conexão.

Impactos e Riscos: Viroses

- O maior medo são **vírus/vermes** que venham a utilizar redes P2P
- O primeiro deles foi o Slapper (Linux) em 2002 que contaminou mais de 14.000 servidores Linux (fonte: Symantec)
- Geralmente usado em DDoS

Impactos e Riscos: Viroses

- Uma pesquisa por Kazaa na base de vírus da Symantec retornou 373 resultados

Symantec Security Response - W32.HLLW.Sanker

W32.HLLW.Sanker is a worm that can spread through the Kazaa file-sharing network and through IRC. This worm copies itself into a Kazaa-shared folder under ...

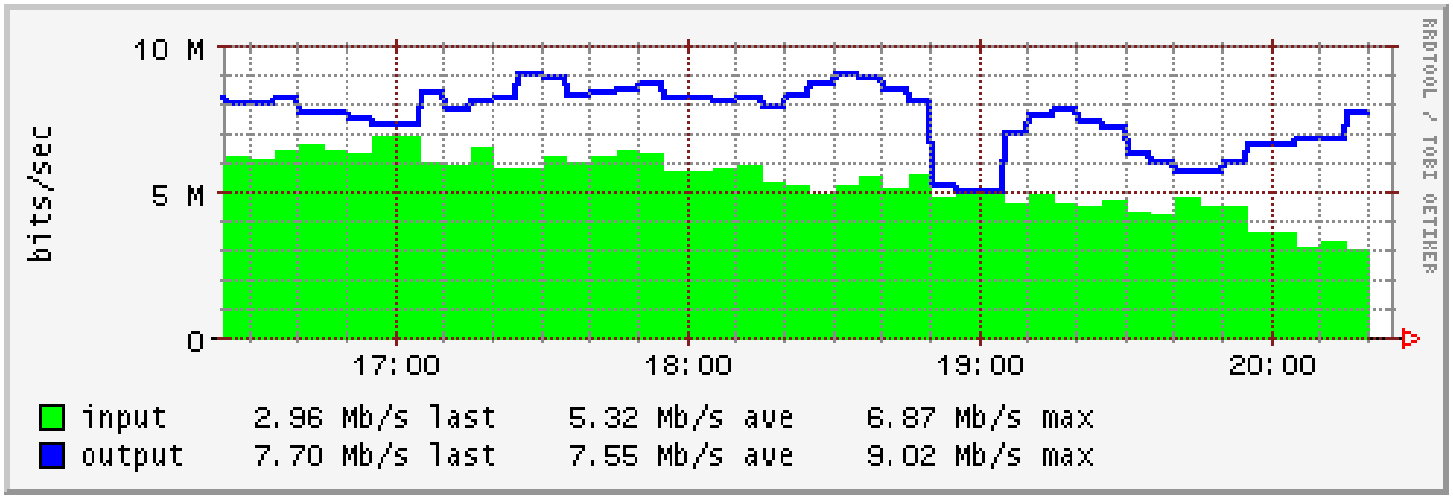
Impactos e Riscos: Recursos da Rede

- Aplicações P2P são grande consumidores de banda (um filme compartilhado geralmente é composto de 2-3 CDROMs em formato mpeg gerando ~2GB)
- Estimativas recentes contabilizam que P2P representa 60% de todo o tráfego da Internet.

→ Resolvemos fazer nossas próprias estatísticas

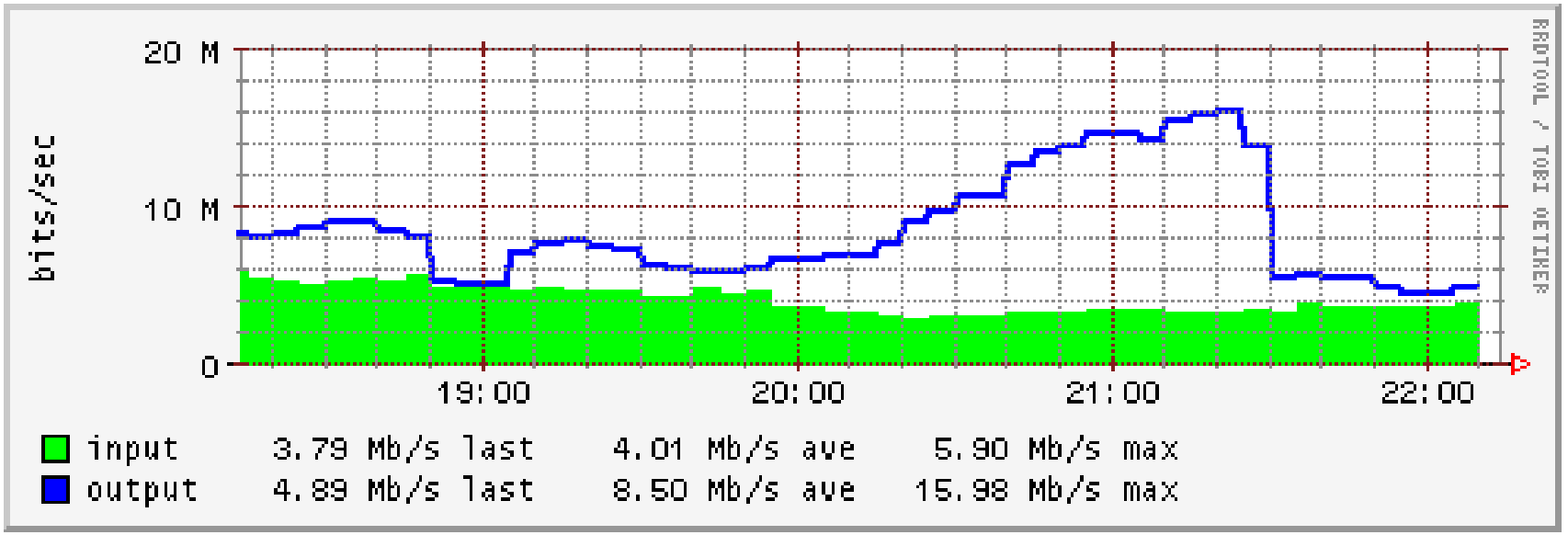
Impactos e Riscos: Recursos da Rede

- Implementado um filtro para aplicações peer-to-peer às 18:45 e retirado as 19h

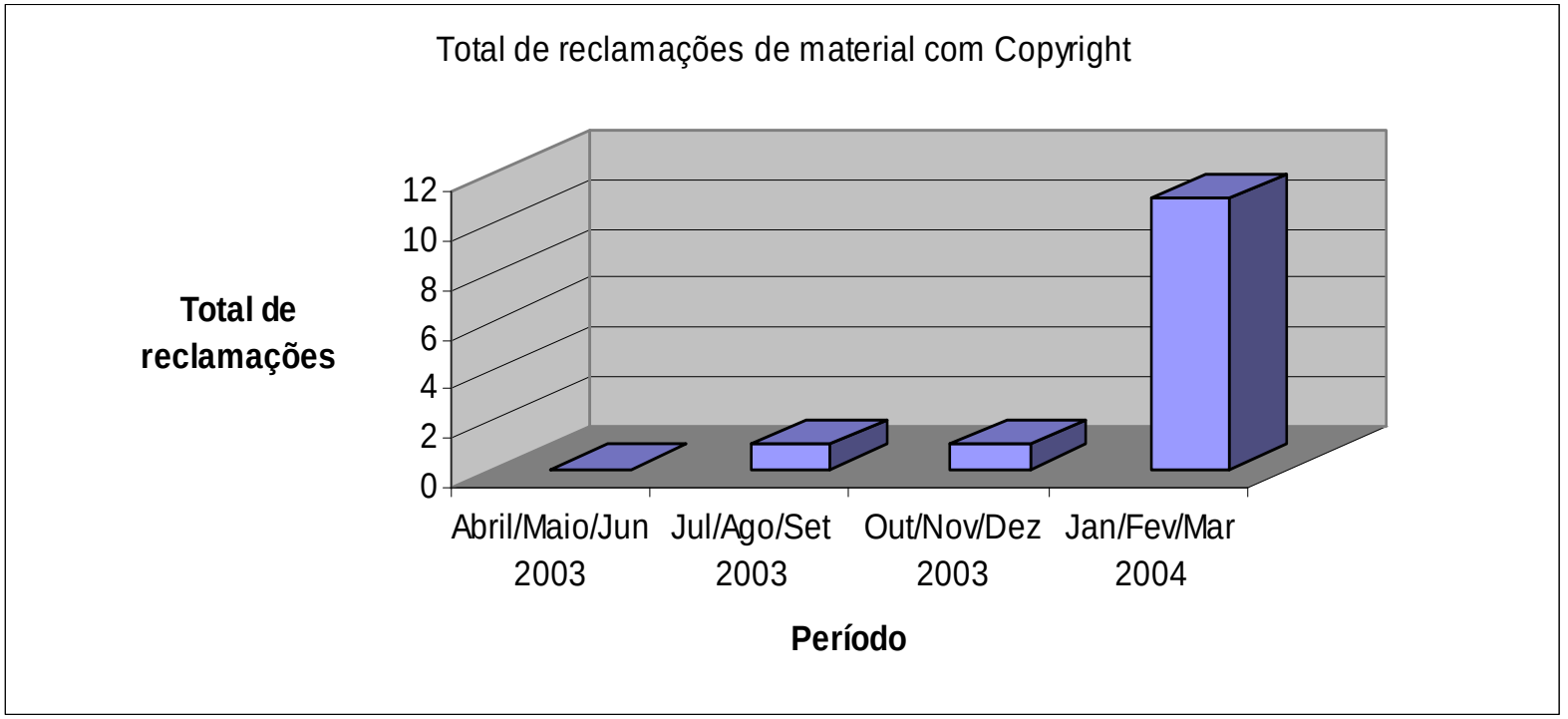


Impactos e Riscos: Recursos da Rede

- 20h: um host disponibilizando vários filmes entra na rede P2P
- 21:30h: o host é retirado da rede



Impactos e Riscos: Violação de Copyright

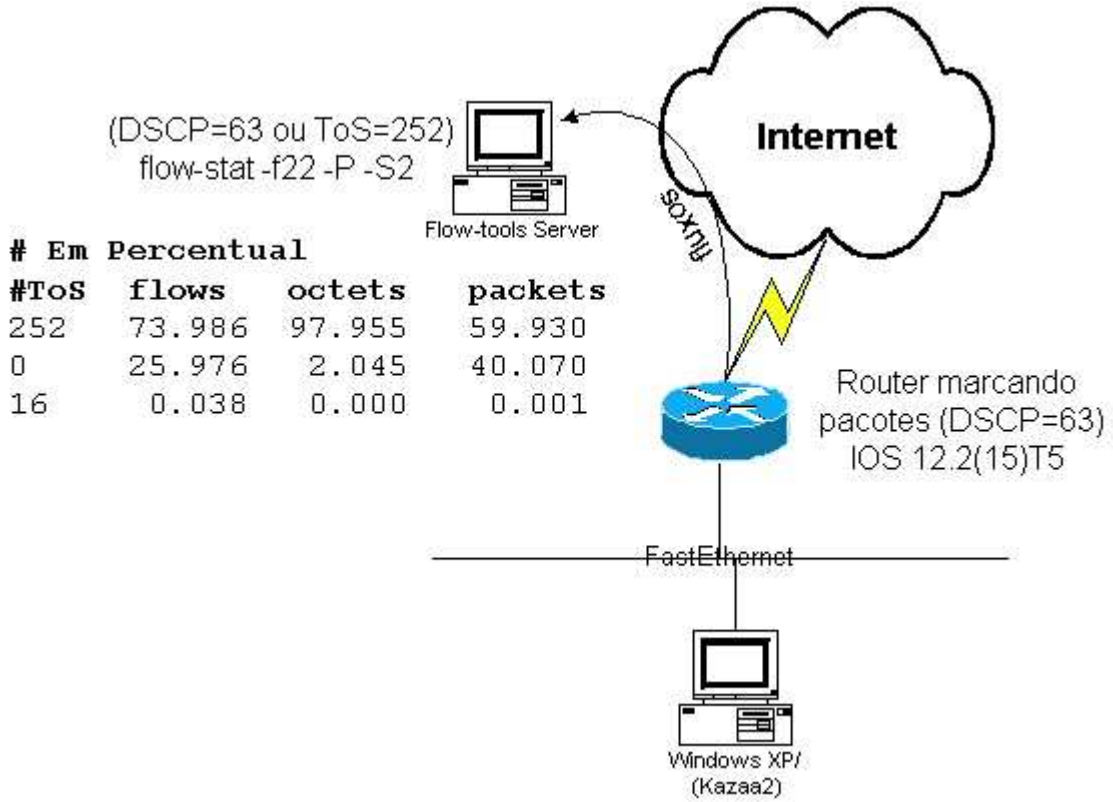


Algumas Universidade Americanas já chegaram a contabilizar 200 reclamações/mês em 2003 (RIAA/MPAA)

Como Mensurar o Problema?

- Para valores confiáveis somente poderíamos mensurar a banda
- Abordagens possíveis
  - Unix rodando SAIF (Statefull Aplication Inspection Filter)
  - Cisco com IOS superior a 12.2(15)]
  - Packeteer e outras soluções comerciais.
- Versões anteriores ao IOS 12.2(15) (2003) usando NBAR eram deficientes

Contabilizando o Tráfego P2P

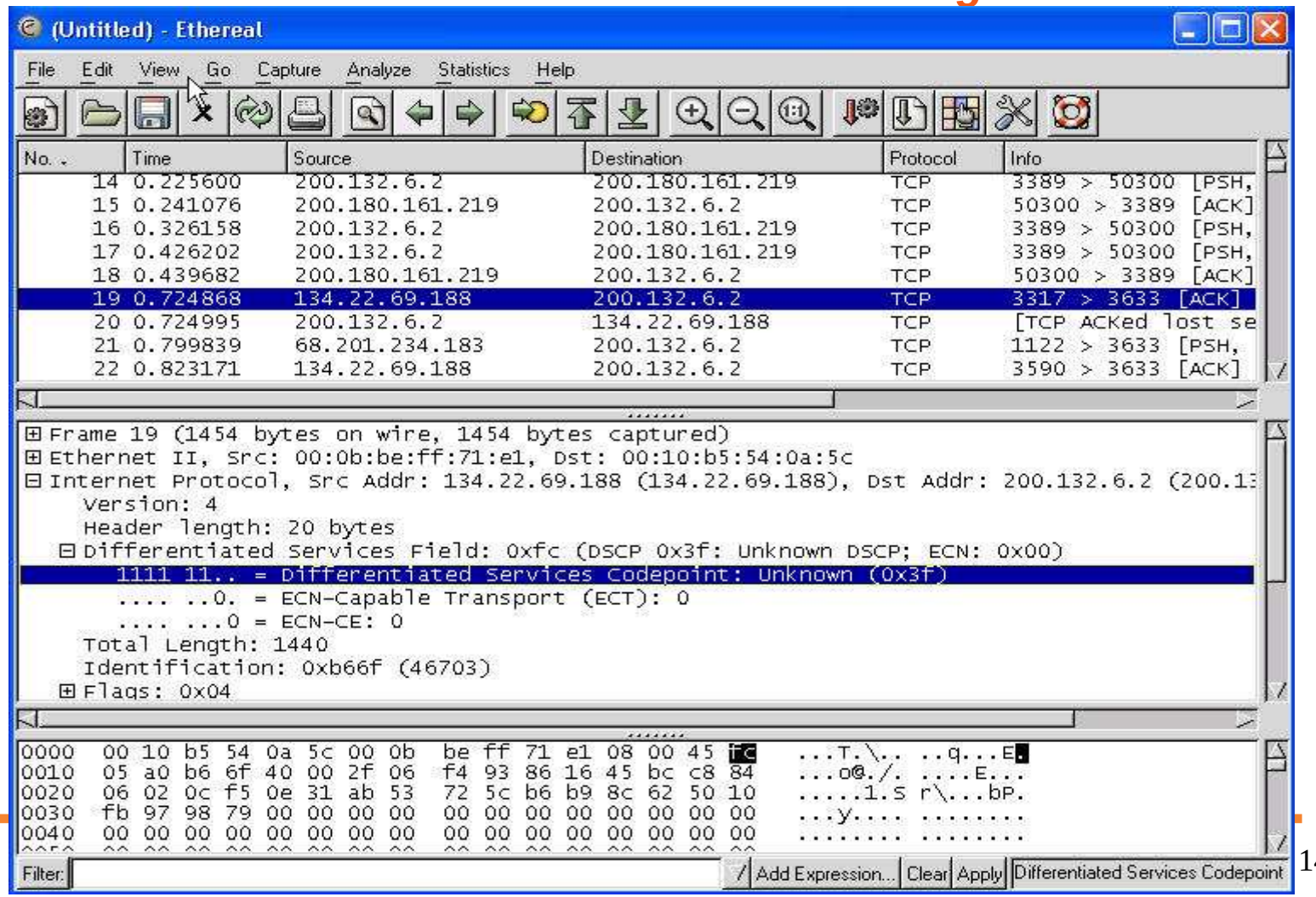



```
# Em Percentual
#ToS   flows    octets    packets
252    73.986   97.955    59.930
0      25.976    2.045    40.070
16      0.038    0.000     0.001
```

Contabilizando o Tráfego P2P – Configuraçao Cisco

```
class-map match-all class-p2p-all
  match any
policy-map marca-p2p
  class class-p2p-all
   set dscp 63
interface FastEthernet0/0
   service-policy input marca-p2p
```

Contabilizando o Tráfego P2P - Ethereal

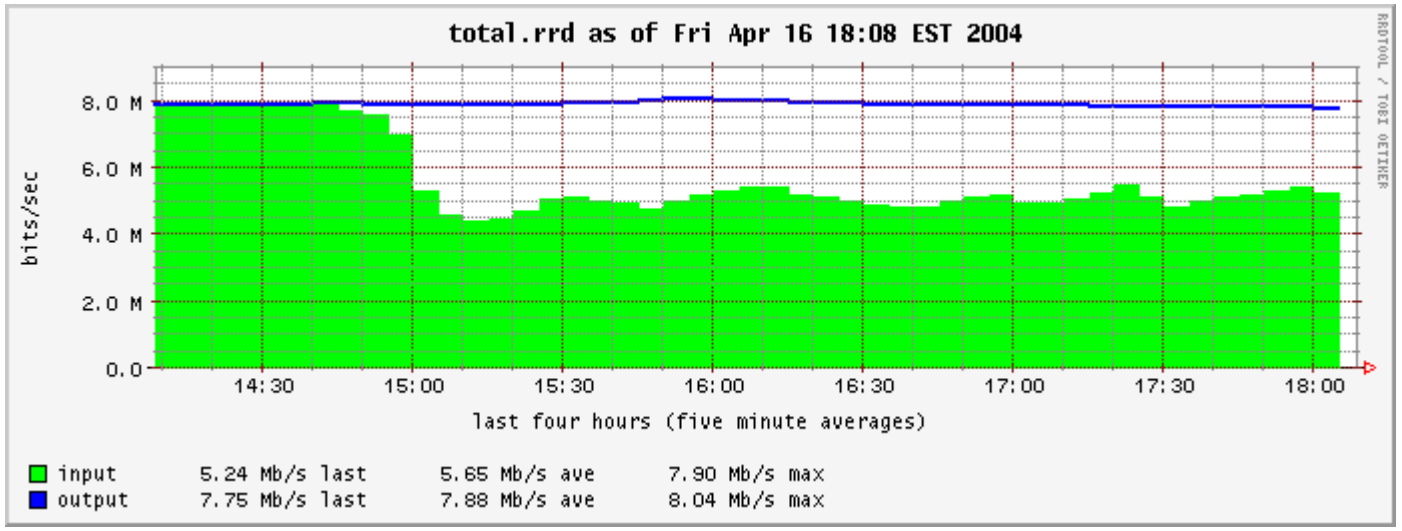


Contabilizando o Tráfego P2P – Netflow

- [root@pampa ft]# flow-cat ft-v05.2004-04-16.02* | flow-stat -f22 -P -S2
- # --- ---- ---- Report Information --- --- ---
- #
- # Fields: Percent Total
- # Symbols: Disabled
- # Sorting: Descending Field 2
- # Name: IP ToS
- #
- # Args: flow-stat -f22 -P -S2
- #
- #
- # ToS flows octets packets
- #
- 252 65.802 97.618 58.292
- 0 34.138 2.382 41.707
- 16 0.060 0.000 0.000

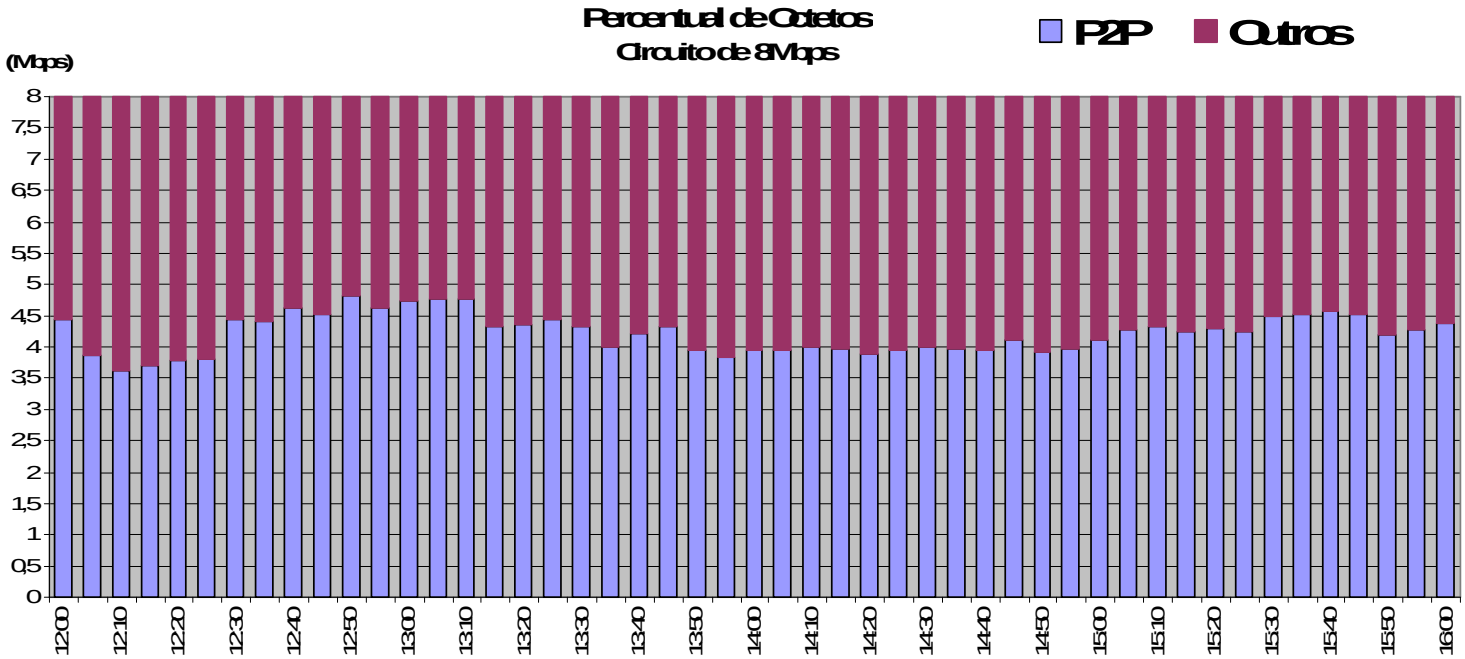
Experiências na Rede Tchê

- Uma instituição com um circuito de 8M havia sofrido 2 aumentos em 1 ano (sem restrição de tráfego P2P)

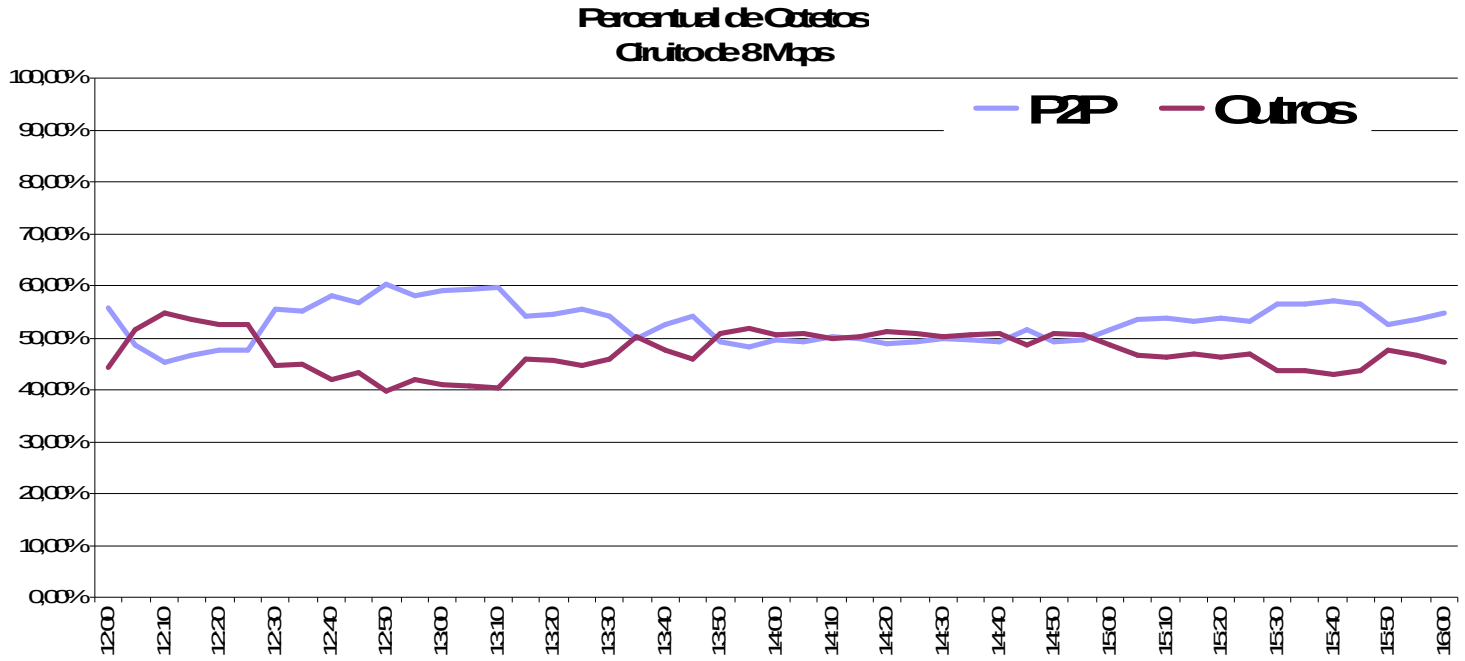


Quantificando o tráfego P2P - Octetos

Durante o horário comercial ~50% do tráfego (octetos) é Peer-to-peer

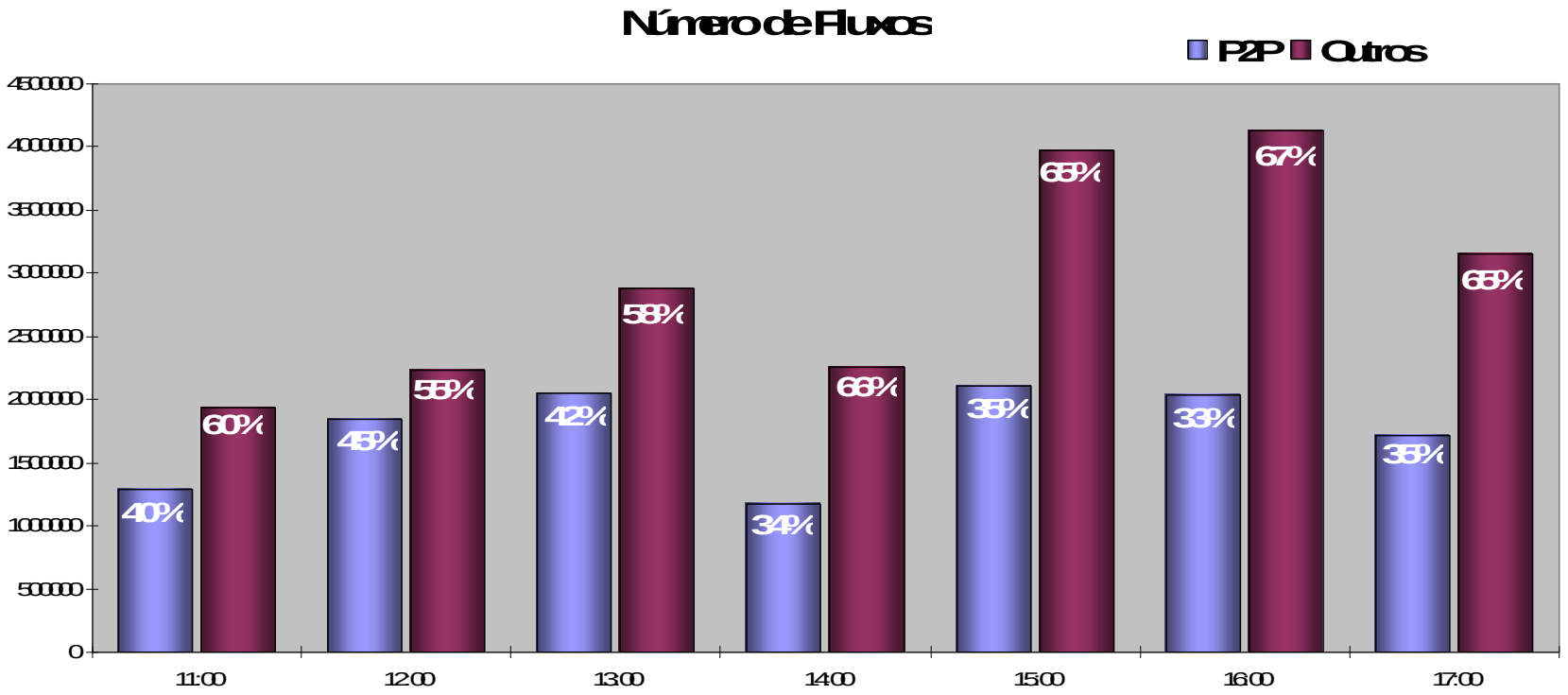


Quantificando o Tráfego P2P - Octetos

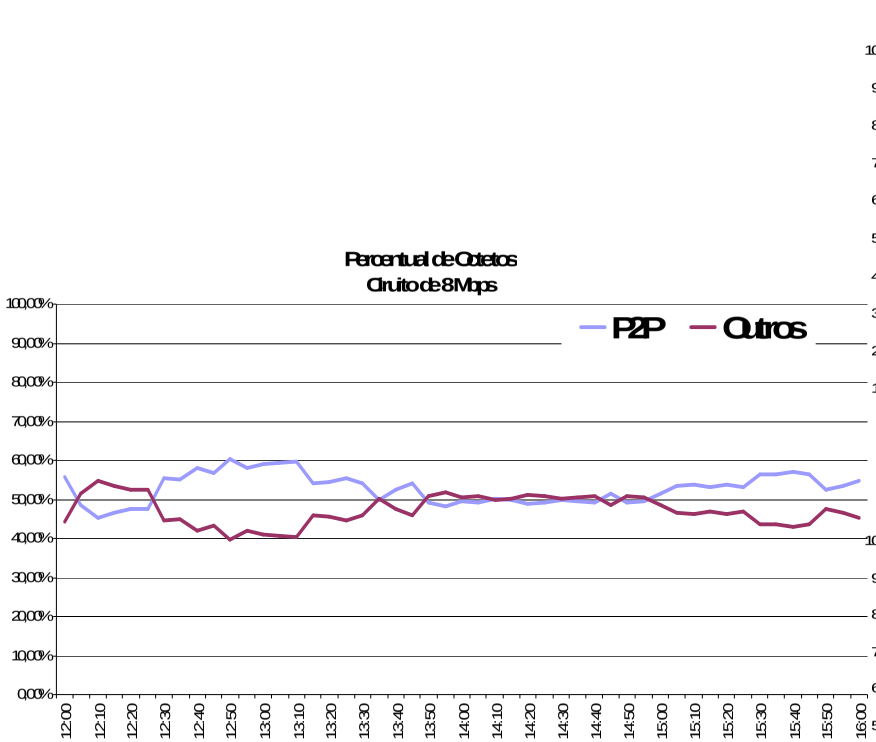


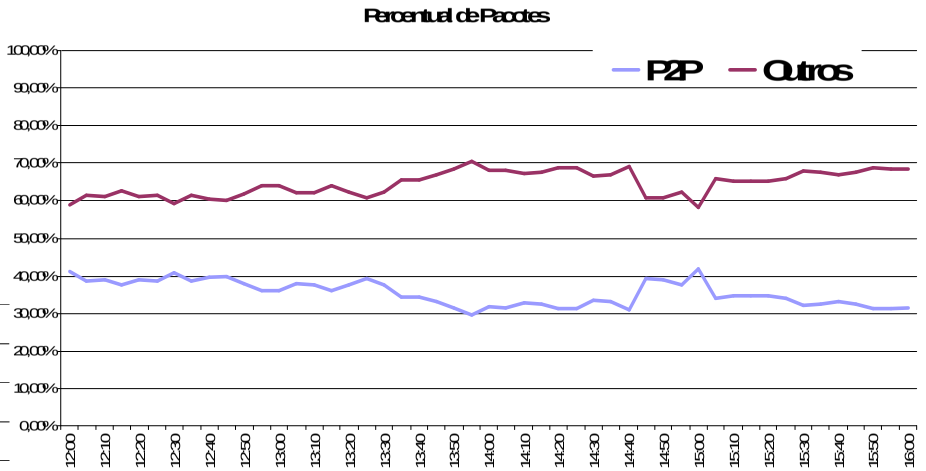
Quantificando o trafego P2P - Fluxos

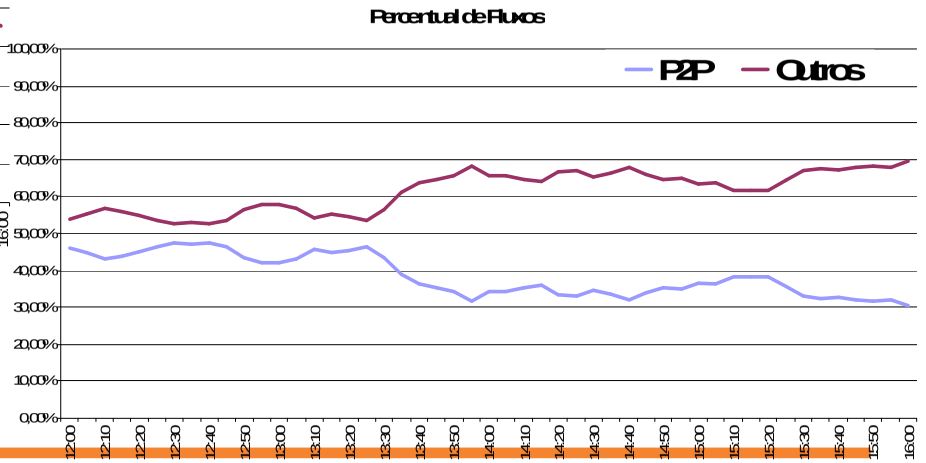
Existe uma relação fluxos X “número de usuários” ?



Relação Percentual bytes, pacotes e fluxos







Experiências

- Decidiu-se não filtrar no backbone
- Os próprios usuários (instituições) tomaram consciência do problema
- Algumas instituições optaram por filtragem direta usando Filtros de Aplicação
- Outras por advertir diretamente os usuários (rrd).

Experiências

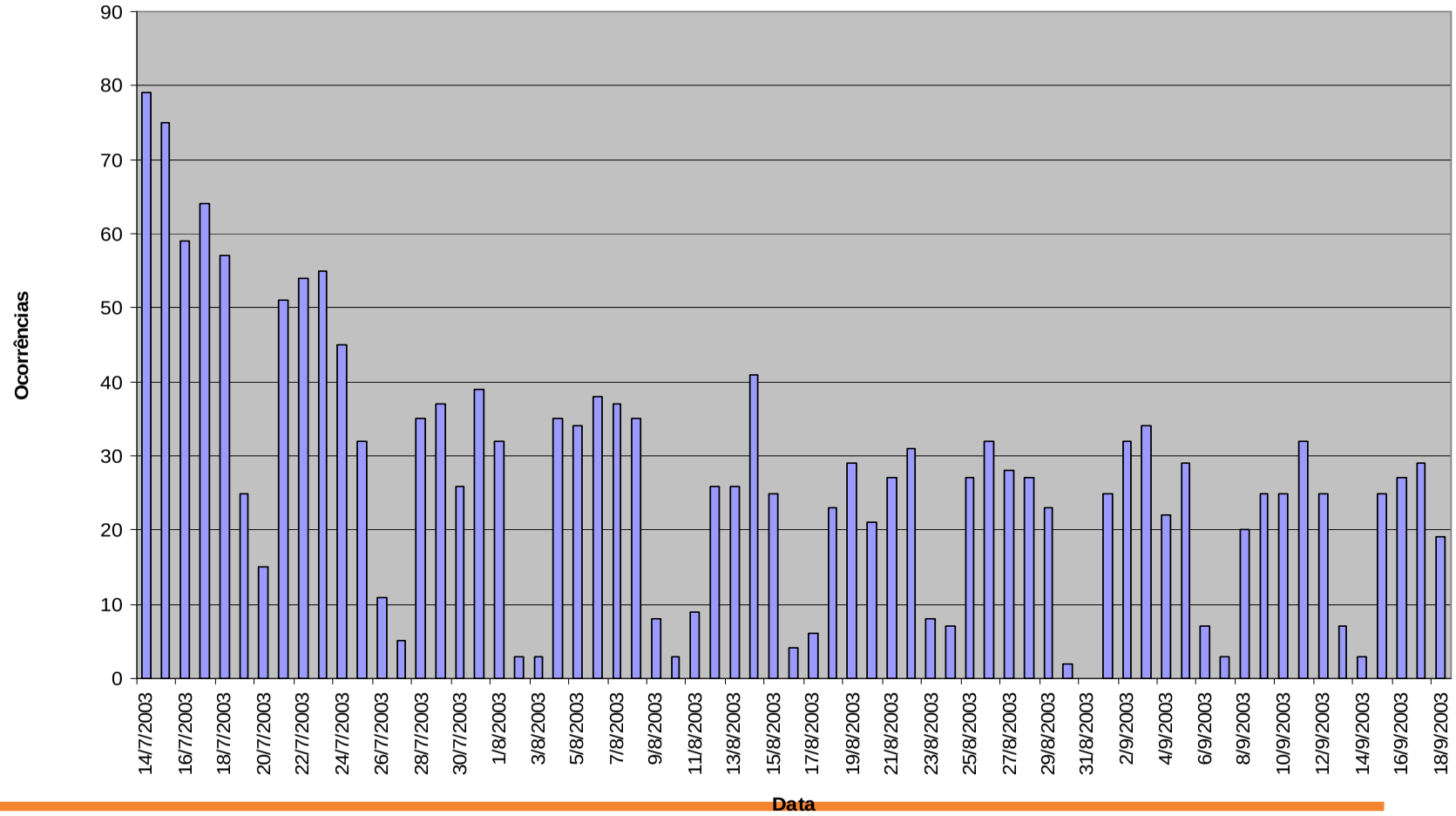
- Difusão de SAIF devido a má implementação do cisco/NBAR

- Nenhuma instituição optou por QoS de aplicações P2P → outros problemas além da banda.

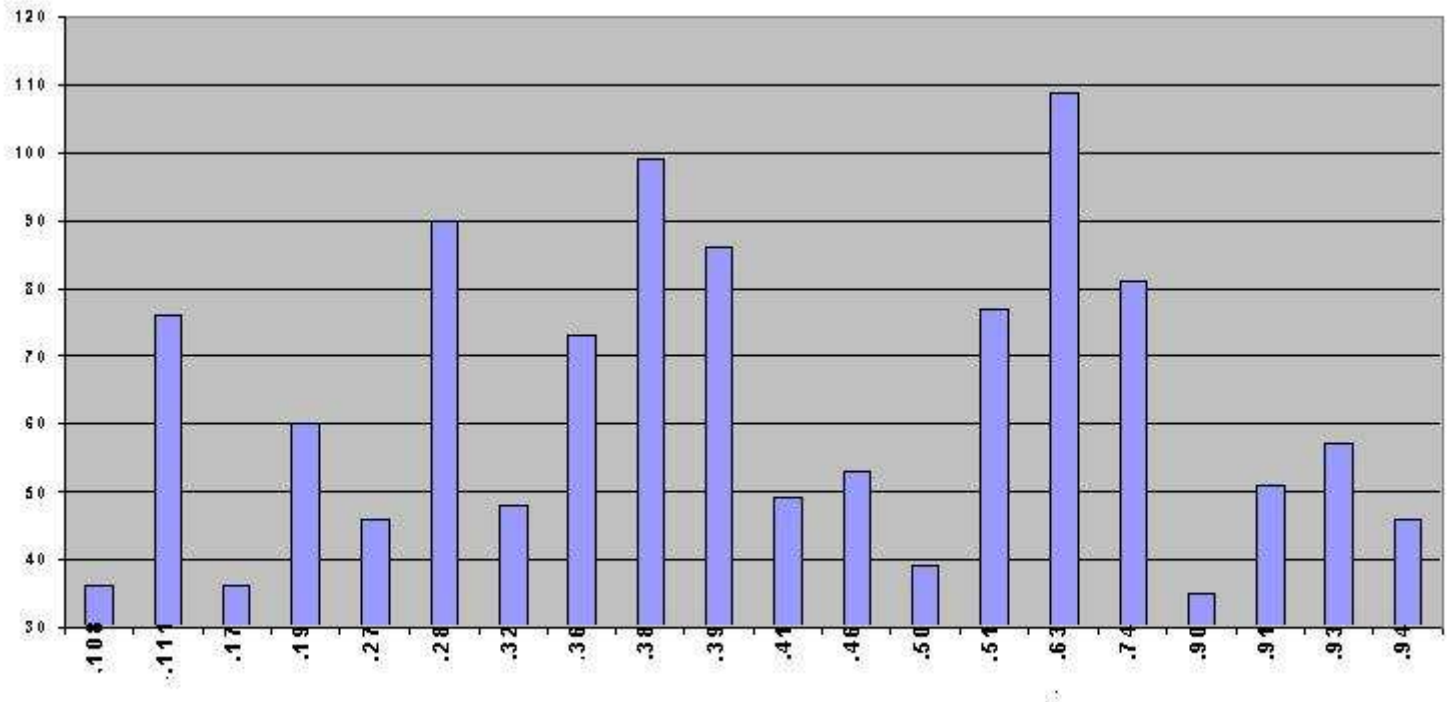
Experiências

- A Universidade Federal do Rio Grande do Sul optou por alertar usuários ao invés de bloqueio
- Utiliza a Firewall
  - Preparada para filtragem (SAIF)
  - Amostra com ngrep 1min a cada hora
  - Emite relatório diário para as unidades sobre o uso
  - Geralmente são os mesmos usuários
  - A mais de 2 anos tenta conscientizar seus usários
  - Teve bons resultados

Experiências na Ufrgs – Ocorrências Diárias



Experiências na Ufrgs – Gráficos por sub-rede



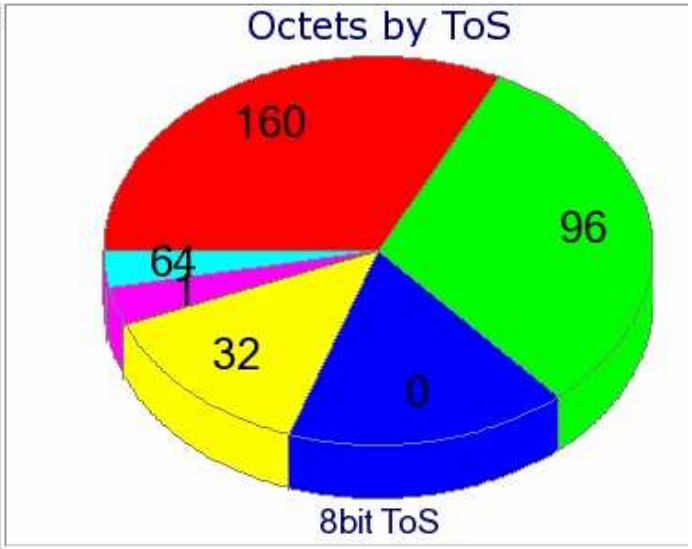
Conclusões e outras abordagens

- Na Rede Tchê a maioria das universidades optou por filtragem
- Algumas universidades como a Florida State University optaram por qualificar os serviços
- Para usuários finais de banda larga o tráfego é livre (ADSL, cable)

Florida State University

Fonte: http://bfs-test.acns.fsu.edu/Network/dscp.shtml

```
#  --- ---- ---- Report Information --- --- ---
#
# Fields:     Percent Total
# Symbols:    Disabled
# Sorting:    Descending Field 2
# Name:       IP ToS
#
# Args:       flow-stat -f22 -P -S2
#
#
# ToS         flows     octets    packets
#
160           16.292    31.575    32.879
96            22.518    30.998    27.200
0             27.135    16.296    17.529
32            14.559    13.332    14.162
1             0.000     3.632     1.523
64            0.396     3.426     1.966
128           18.452    0.644     3.714
12            0.025     0.084     0.903
192           0.612     0.014     0.122
16            0.010     0.000     0.001
20            0.001     0.000     0.000
```



ToS 0 =dscp 0 - P2P
ToS 32 =dscp 8 - Unknown
ToS 64 =dscp 16 - Bulk
ToS 96 =dscp 24 - Humans
ToS 128 =dscp 32 - Network
ToS 160 =dscp 40 - Marked as H323
ToS 192 =dscp 48 - 48
ToS 224 =dscp 56 - 56

Conclusões e Preocupações

- Desde o fastrack até os filtros por aplicações foi impossível o bloqueio. Hoje está sob controle!
- O que fazer quando os usuários P2P começarem a cifrar o tráfego
  - Será que se poderá filtrar?
  - Forçar o uso de criptografia somente para aplicações registradas?
  - Aumentar o controle nas máquinas dos usuários?