

Tráfego e Medidas em Redes IP

*FEUP/MRSC/AMSR
MPR*

Bibliografia

- » Aula preparada com base nos seguintes documentos
 - Joachim Charzinski, “Internet Traffic Measurement and Modelling – Tutorial”
 - Sean McCreary, Caida, “ Internet Measurement – Metrics and Methodologies”
 - Caida Metrics Working Group, “Network Measurement FAQ”
 - V. Paxson, G. Almes, J. Mahdavi, M. Mathis, “Framework for IP Performance Metrics”, IETF RFC 2330
 - ITU-T Rec. I.380, “Internet Protocol data communication service – IP packet transfer and availability performance parameters”
 - Joseph Sloan, “Network Troubleshooting Tools”, O’Reilly

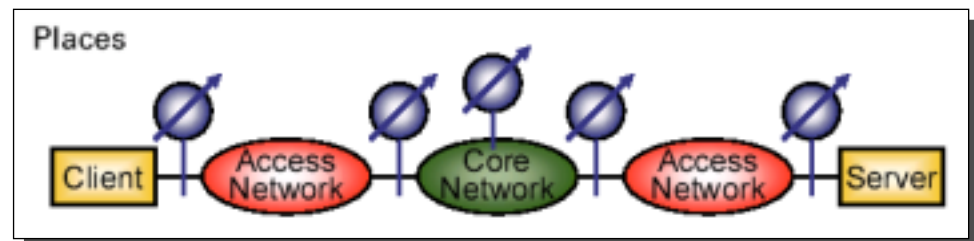
Medidas Activas e Passivas na Internet

◆ Métodos Passivos

- » Observação do tráfego. Medidas sobre tráfego real
- » Traços de pacotes: pré-processados, avaliados off -line
- » Leitura cíclica de contadores

◆ Métodos Activos

- » Geração de tráfego de teste. Detecção desse tráfego
- » Medidas sobre tráfego gerado e detectado
- » Testes de rede e de aplicação



Fontes de Informação

- » Logs de pacotes
 - Ex. pcaplib, tcpdump
- » Logs de fluxos
 - Por ligação TCP ou outros fluxos
- » Dados pré-processados, contadores
 - Valores médios
- » Logs de acesso
 - Registos por sessão
- » Tráfego de teste
 - Medidas de atrasos, perda de pacotes, débitos,
 - desempenho de aplicações

Algumas Ferramentas

- » Traço de pacotes
 - Tcpdump (Paxson)
 - Ethereal

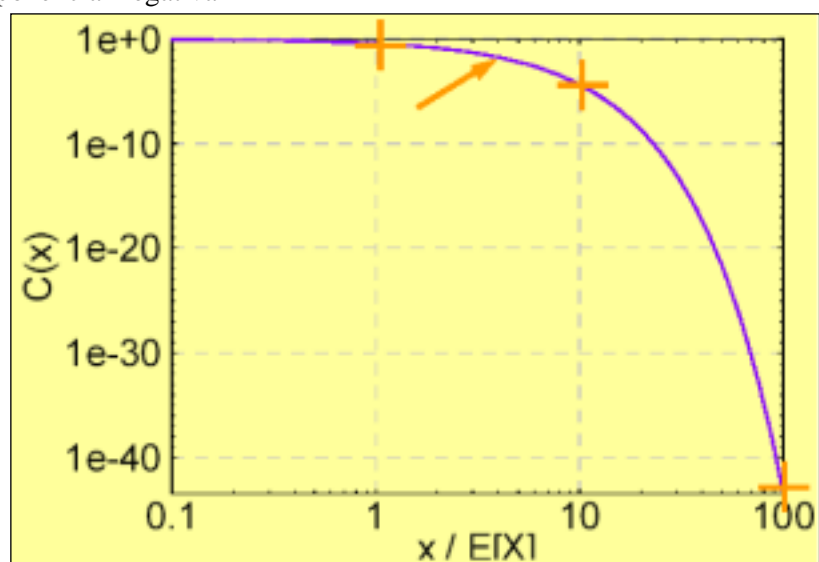
- » Detecção de fluxos
 - OC3mon, CoralReef (www.caida.org)
 - NeTraMet (IETF RTFM)
 - Tcpanaly (Paxson)

- » Ferramentas de teste activo
 - <http://www.ncne.nlanr.net/nimi>

- » Ferramentas de gestão de redes
 - SNMP → obtenção de valores de contadores de rede
 - Sondas RMON

Apresentação de Resultados

- » Função distribuição de probabilidade $F_X(x) = P(X \leq x)$
- » Função de distribuição complementar $F_X^C(x) = P(X > x) = 1 - F_X(x)$
 - Ex. Função exponencial negativa

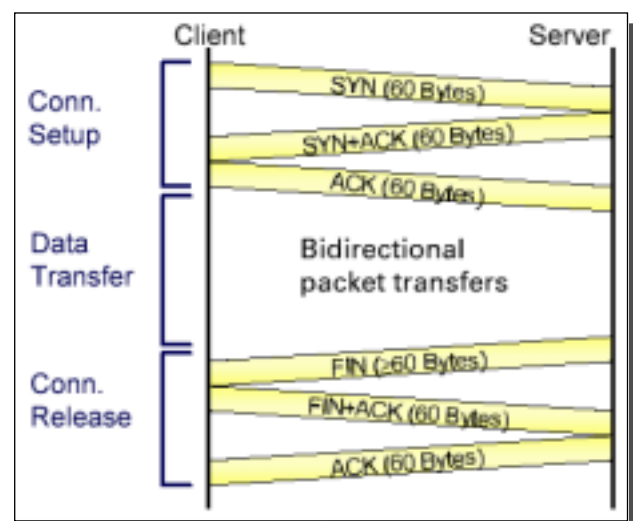


- ◆ Utilizador
 - » Determina início da sessão de acesso
 - » Escolhe e utiliza as aplicações

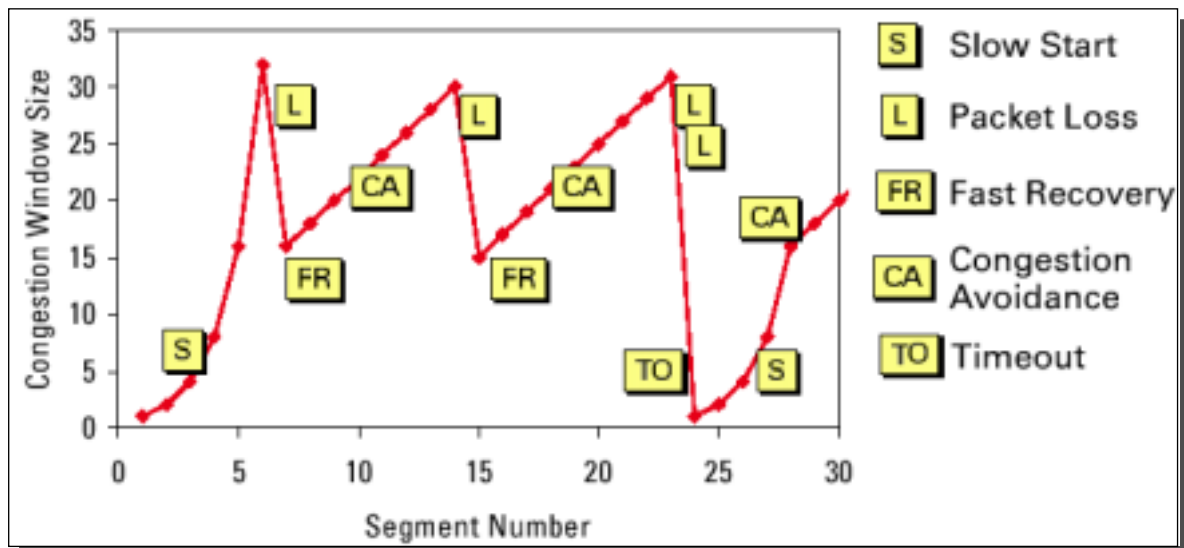
- ◆ Aplicação
 - » Determina tráfego gerado
 - » Tráfego de pacotes devido a
 - Gestão da ligação TCP
 - Confirmações TCP
 - Dados produzidos por protocolos de alto nível
 - Protocolos alto nível

Efeitos do TCP

- ◆ TCP induz padrões de tráfego
- ◆ Gestão da ligação
 - » 3 pacotes para abrir
 - » 3 pacotes para fechar
 - » Tratada nas extremidades
- ◆ Transporte fiável
 - » Utilização de ACKs
- ◆ Controlo de fluxo
 - » Adaptação fluxo
 - » Depende de atraso e perdas

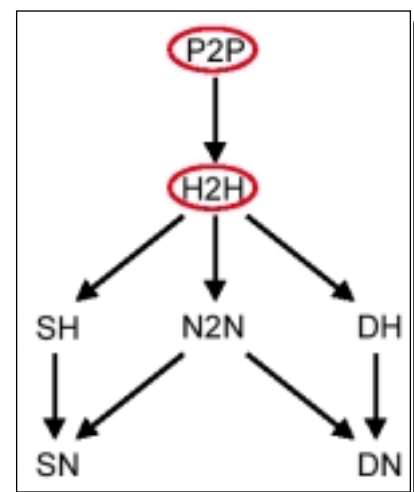


TCP

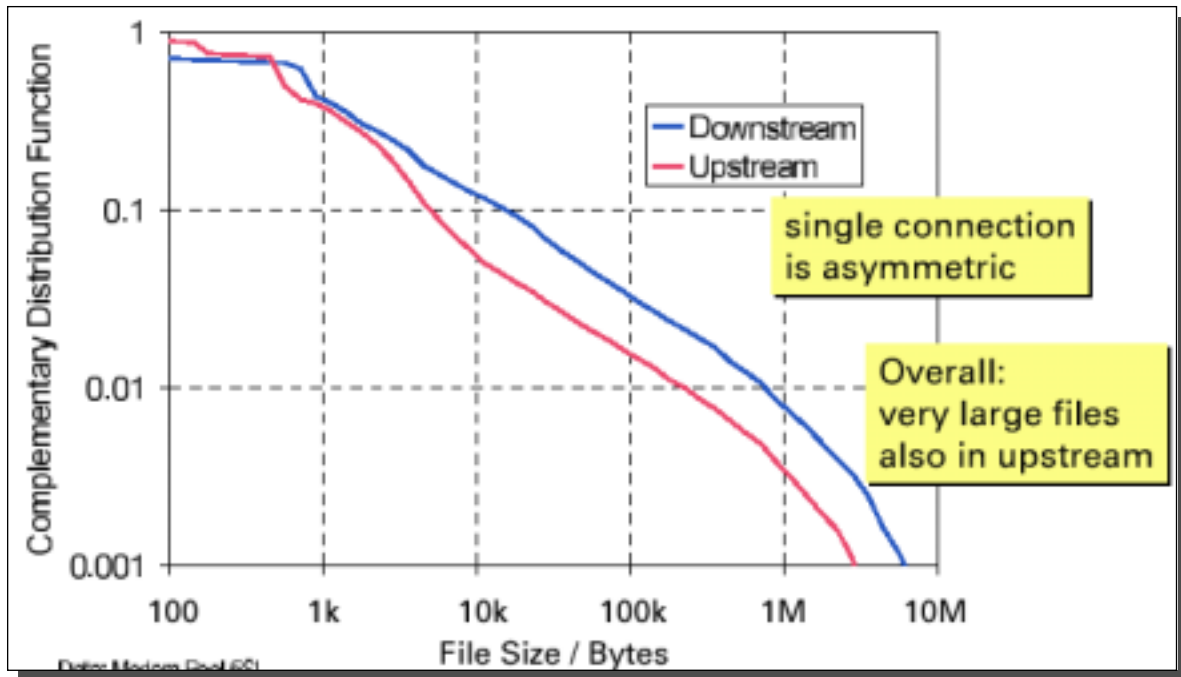


Definição de Fluxo / Relações de Agregação

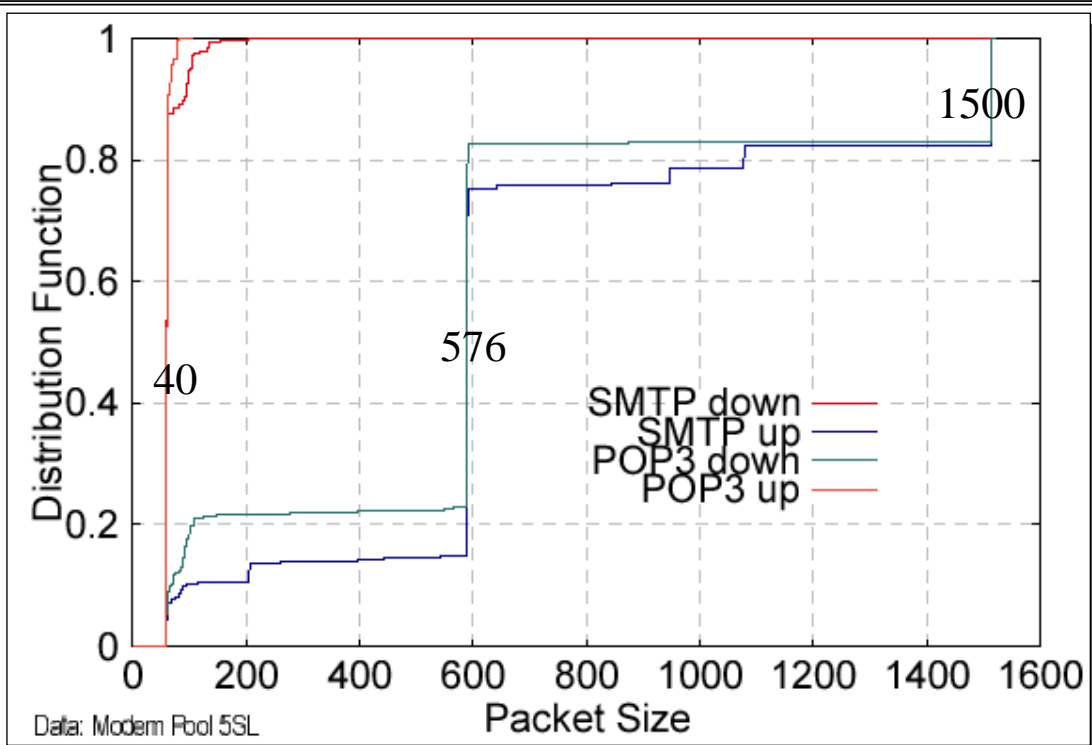
- ◆ Porta a porta (P2P)
 - » Ligação TCP ou relação UDP
 - » Fixos – 2 endereços IP, TOS, protocolo, 2 portas
- ◆ Host a Host (H2H)
 - » Pacotes com o mesmo par de endereços IP
- ◆ Rede a Rede (N2N)
 - » Pacotes com mesmo par de endereços de rede
- ◆ Host de origem (SH)
- ◆ Host de destino (DH)
- ◆ Outros
 - » Aplicação, bidireccional



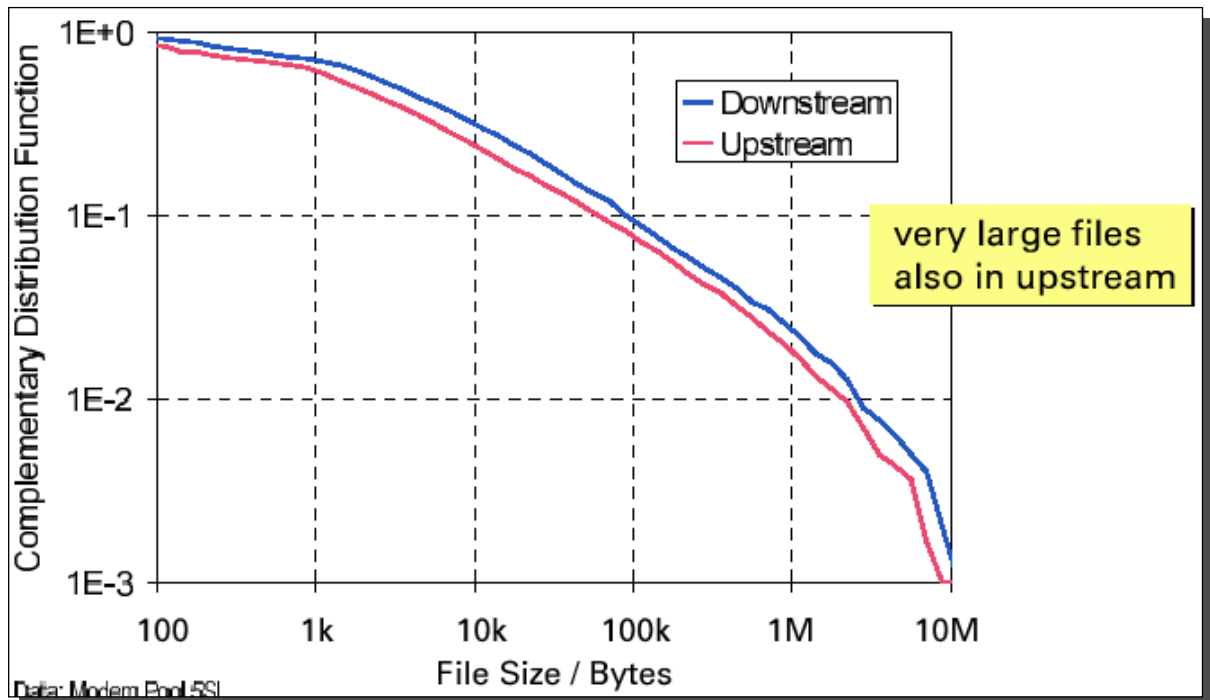
E-Mail – Comprimento das Mensagens



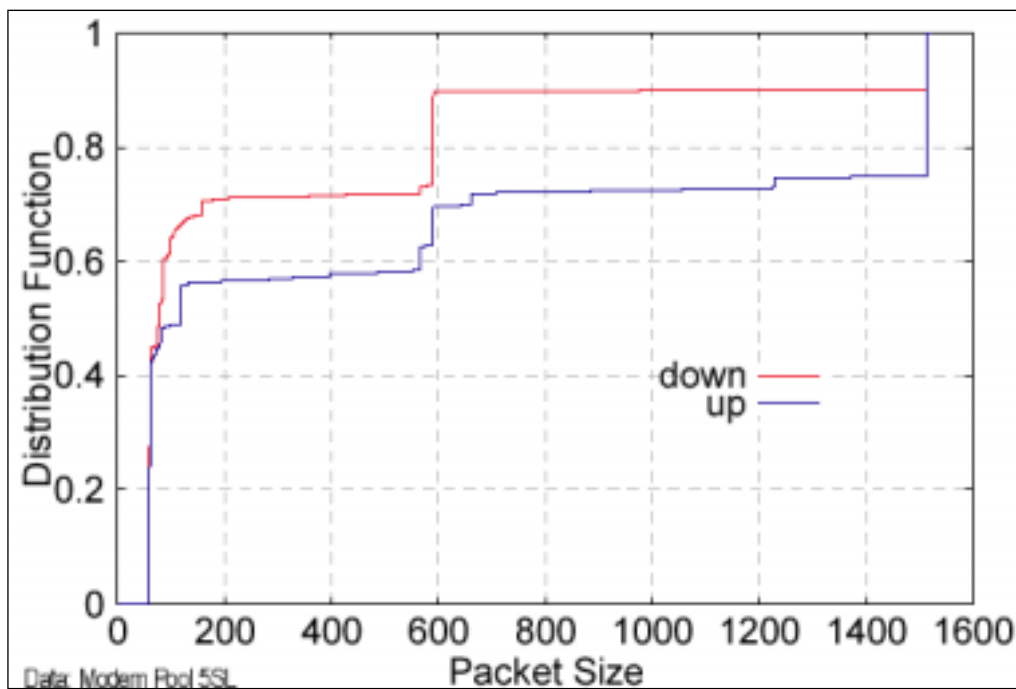
E-Mail – Comprimento dos Pacotes



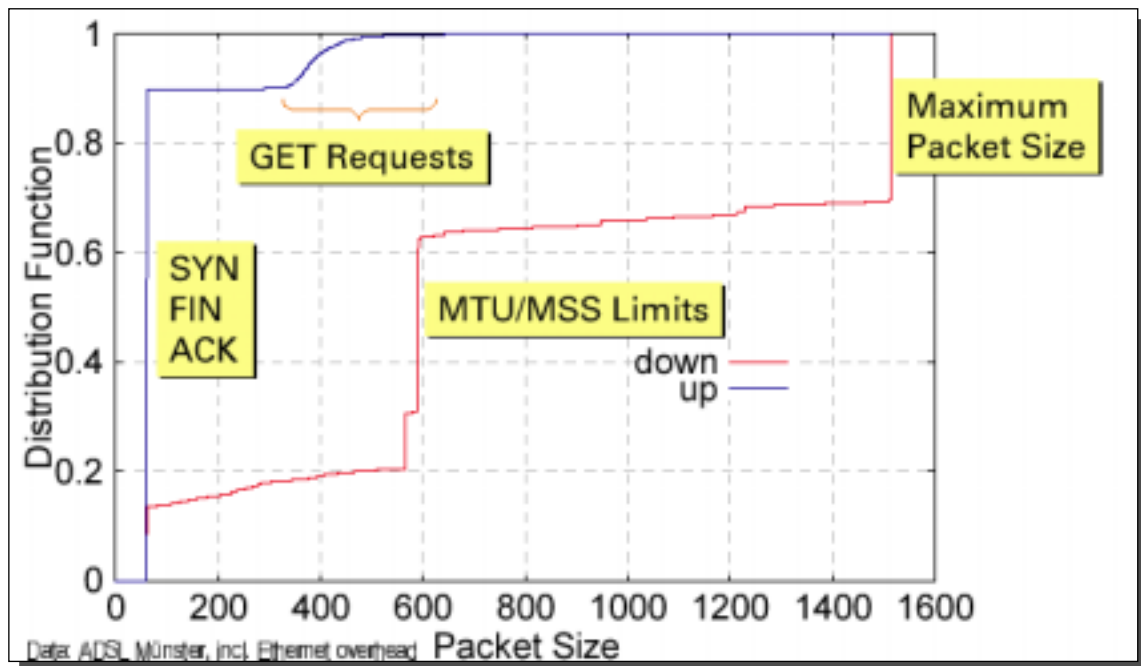
FTP – Comprimento dos Ficheiros



FTP – Comprimento dos Pacotes



WWW – Comprimento dos Pacotes



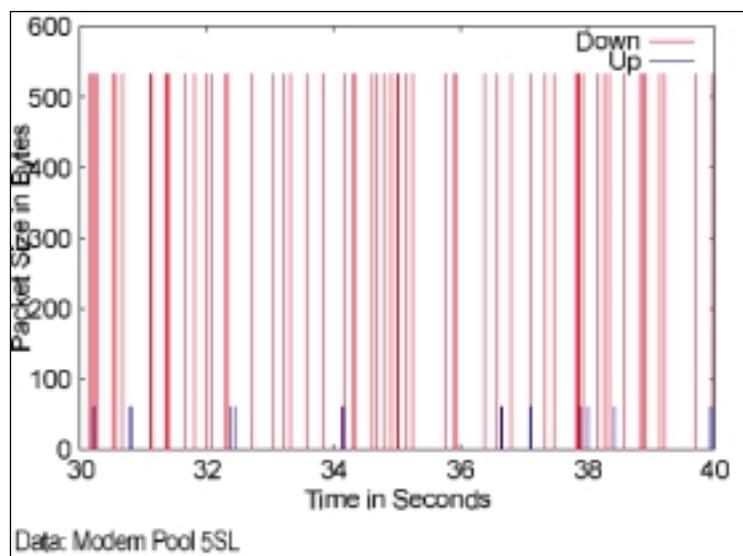
Audio Streaming (Real Audio)

◆ Características

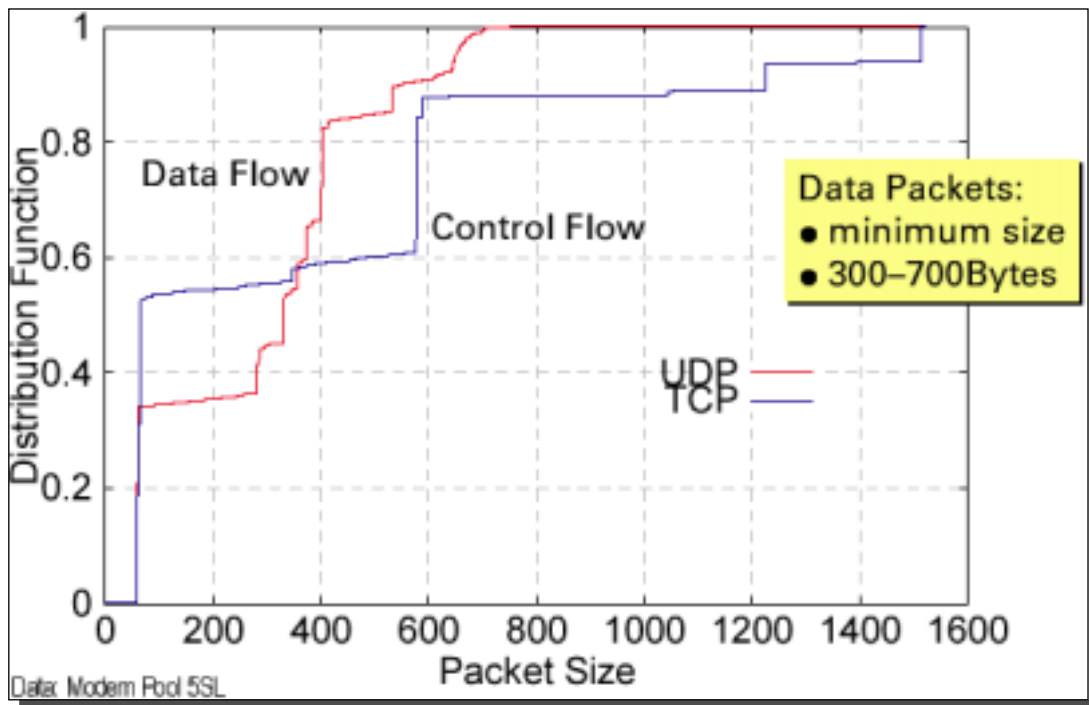
- » Transferência de audio clips
- » Portas → controlo e dados
- » Débito adaptável
 - buffers grandes
 - atraso variaável
 - perda de pacotes

◆ Tráfego

- » Dados
 - UDP
 - Pacotes pequenos
- » Controlo

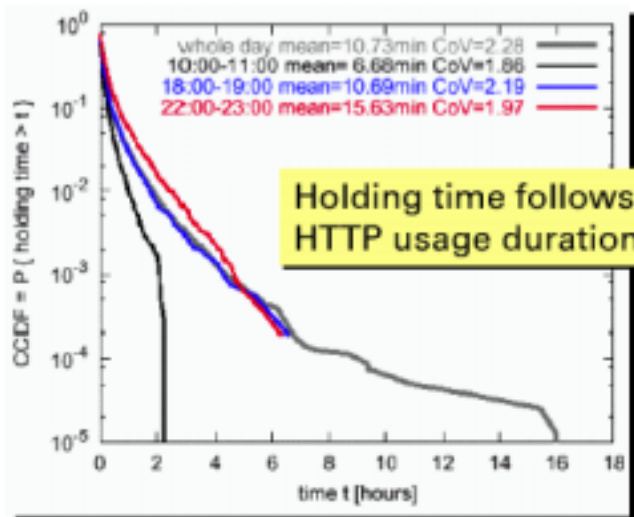


Real Audio – Comprimento dos Pacotes

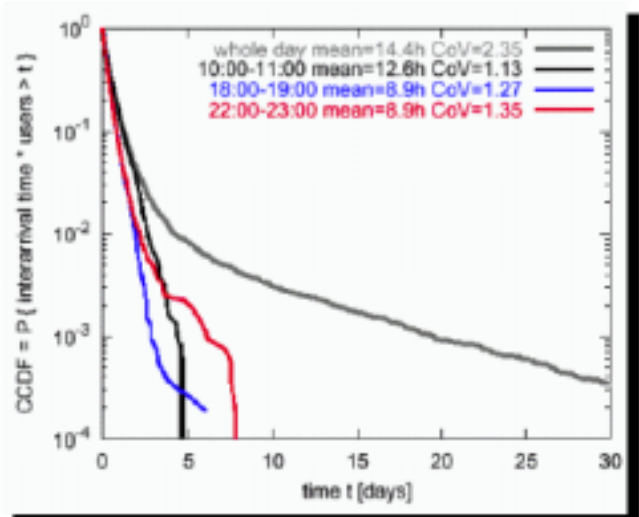


Comportamento do Utilizador Características de Acesso

Holding Time



Cumulative Interarrival Time per User

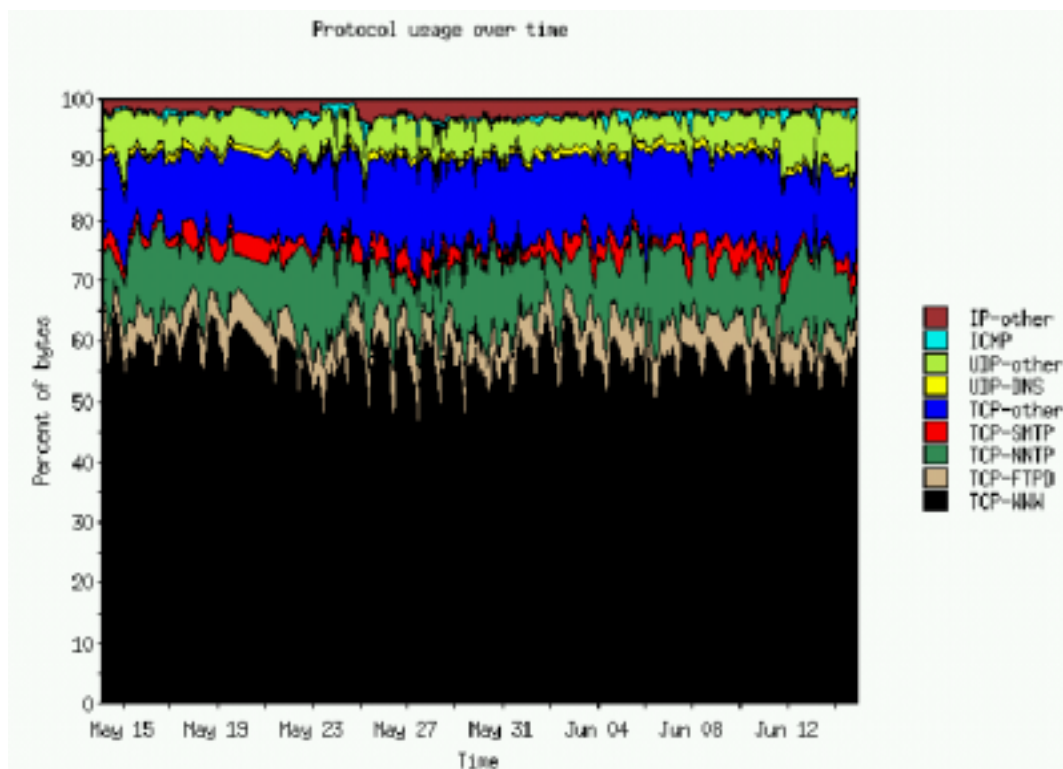


Source: University of Stuttgart

Medidas no Backbone - Tráfego

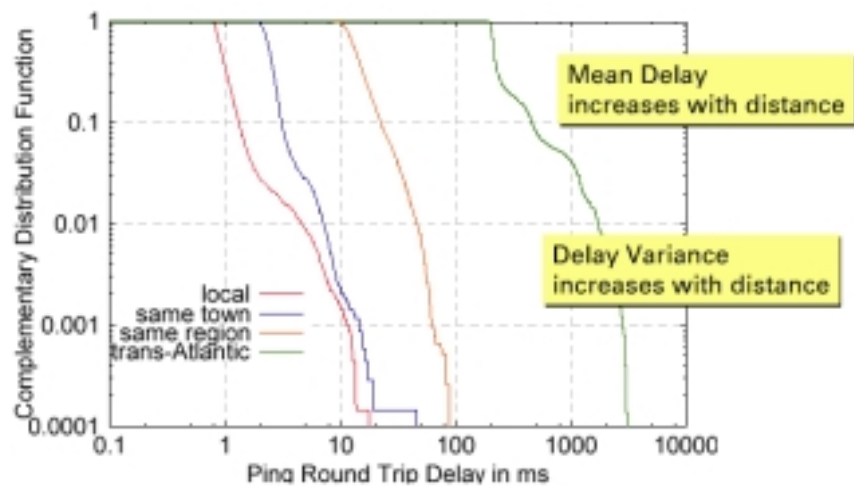
- ◆ Para além do tráfego local
 - » Domain Name Systems (DNS)
 - » Network News (nntp)
 - » Rotas
 - » Gestão da Rede

Mistura de Tráfego Tipo



Características da Rede

- » Ligações Internet
 - Saturadas → probabilidade de perda de pacotes de 4 a 20 %
 - Em estado quiescente → sem perda de pacotes
- » A generalidade dos pacotes consecutivos usa o mesmo caminho
 - retorno pode ser diferente

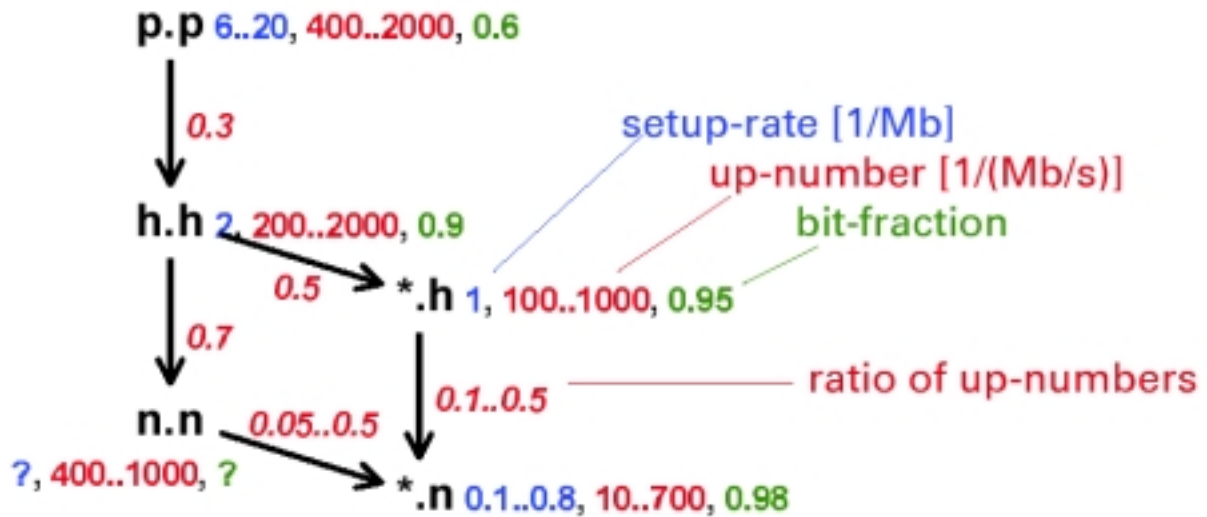


Características dos Fluxos

- ◆ Características normalizadas, que permitem comparação
 - » Taxa de chegada (setup rate)
 - (Novos fluxos por segundo / débito total) = $1 / (\text{volume médio do fluxo})$
 - » Fluxos activos (up-number)
 - Número de fluxos activos por tráfego debitado (fluxo/(bit/s))
 - » Fracção de bit
 - Fracção do tráfego que poderia ser transportado em shortcut

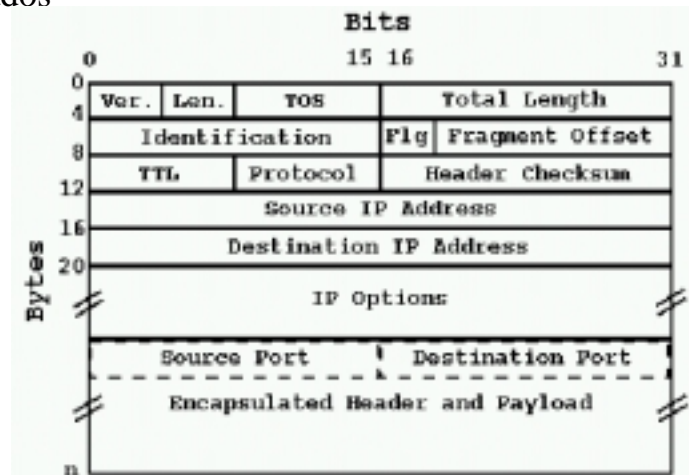
Características dos Fluxos

- » Fracção de Bit
 - melhora significativamente com agregação
- » Up-number
 - Algumas centenas de shortcuts por Mbit/s, forte variação, pouco ganho de agregação



Caracterização de Fluxos

- ◆ Ferramentas trabalham com cabeçalho de pacotes
- ◆ Dados são eliminados
 - » Privacidade
 - » Redução da quantidade de dados



Volume de Tráfego

- ◆ Número de pacotes
 - » Routers e switches → overheads por pacote
- ◆ Número de bytes
 - » Quantidade de dados transportados
 - » Interesse para utilizadores
- ◆ Número de fluxos
 - » Grupos de pacotes com afinidade entre si
 - » Definição de fluxo → depende do objectivo da medida

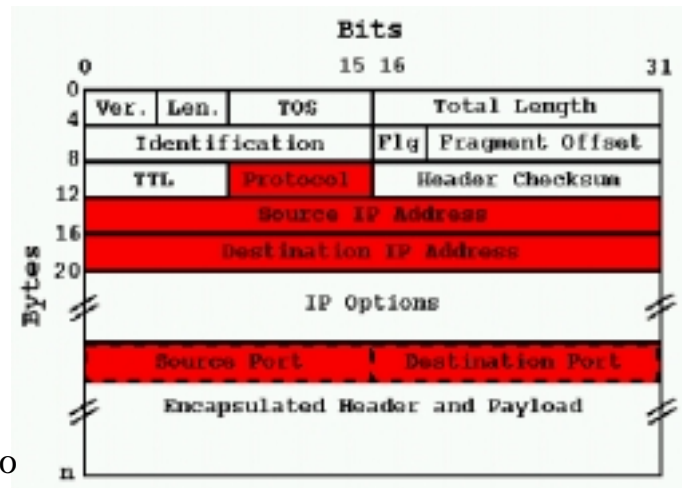
Fluxos

- ◆ Pacotes podem ser agrupados de múltiplas formas
 - » Proximidade temporal
 - Fluxos separados por um intervalo de tempo durante o qual não se observam pacotes
 - Fluxos baseados em timeout
 - Usados para estudo de caches em routers e switches
 - » Por sinalização de transporte
 - Fluxo contém todos os pacotes de uma ligação
 - TCP → todos os pacotes do SYN inicial até ao ACK final
 - Interessante para medidas extremo-a-extremo
- ◆ Pacotes são normalmente *timestamped*
 - » Resolução mínima → ms
 - » Época começa em 00:00:00.00 GMT, Jan. 1, 1970.

Fluxos

- ◆ Fluxos podem ser unidirecionais ou bidirecionais
- ◆ Flutuação das rotas pode desviar tráfego de um fluxo

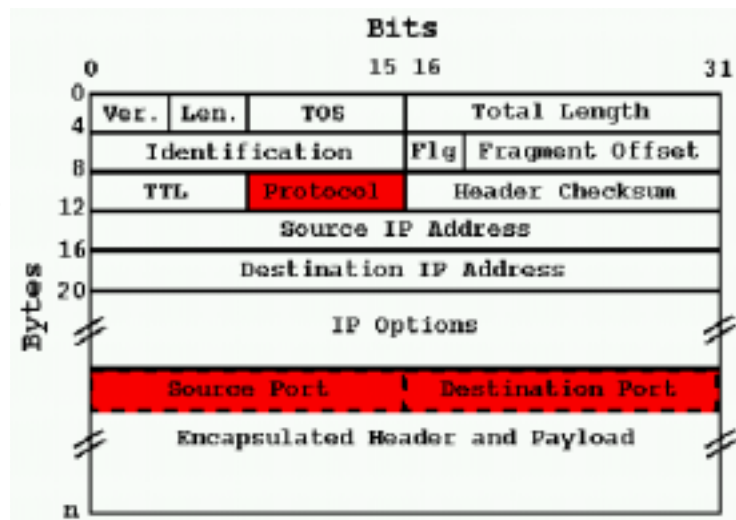
- ◆ Fluxo → vector de 5 dimensões
 - » Source IP Address
 - » Source Port
 - » Destination IP Address
 - » Destination Port
 - » Transport Layer Protocol



- ◆ Às vezes só é usado um subconjunto
- ◆ Nem todos os protocolos usam portas
- ◆ Nem todos os parâmetros são usados simultaneamente

Medida de Aplicações

- ◆ Protocolo de transporte
 - » TCP, UDP, ICMP, IGMP
 - » Utilização do campo *protocolo*
- ◆ Protocolo de aplicação
 - » HTTP, FTP, NNTP, DNS, RealVideo
 - » TCP e UDP usam portas
 - » Utilização das portas bem-conhecidas para descrever os serviços



Utilização das Portas

- ◆ Clientes TCP e UDP usam portas com valor superior a 1023

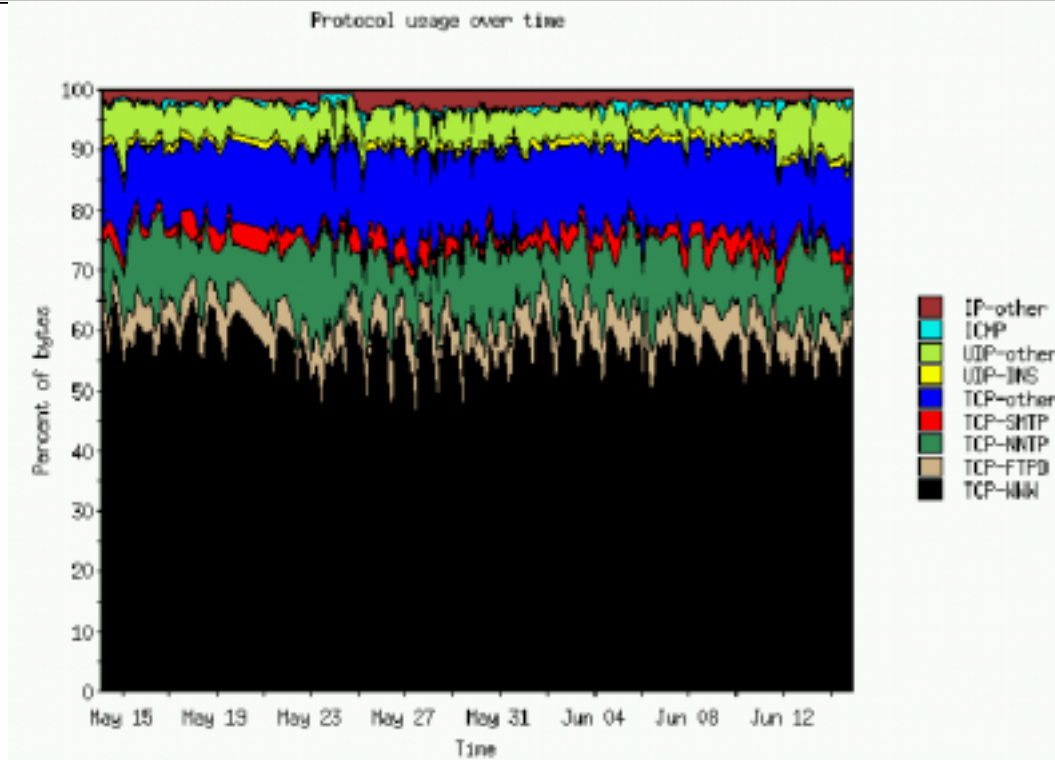
- ◆ Algoritmo identificação de serviço
 - » Para as portas de origem e destino
 - Se porta < 1024 não altera
 - Se porta > 1023, verifica se é um serviço
 - u Se sim, não altera
 - u Se não, substitui por zero

Portas

SRC	DST	Pacotes	Bytes
80	0	185875699	131439625822
0	0	73328126	26121563040
119	0	18383602	17246484519
20	0	13555941	12549586558
0	80	122767195	9724773087

- ◆ Entrada 0,0
 - Servidores em portas não conhecidas
 - Serviço desconhecidos
 - FTP em modo passivo

Mistura Tipo de Tráfego de Aplicação



Localização do Tráfego

- ◆ Topologia
 - » Autonomous System
 - » Prefixo de endereço
 - » Rede/subrede
 - » Host

- ◆ Geografia
 - » Intercontinental
 - » Internacional
 - » Inter-cidade

Topologia

- ◆ Baseado na estrutura hierárquica do espaço de endereços IP
 - » Endereços agrupados a partir da tabela de rotas
 - » Endereços cobertos pela mesma rota estão próximos

- ◆ Tabelas de encaminhamento diferentes → granularidades diferentes
 - » Tabelas de um router local com rota de defeito
 - Distingue entre grupos de endereços internos e externos
 - » Tabelas de routers de backbone → classificam tráfego globalmente
 - » Paths do BGP pode ser usado para agrupar ISPs
 - Autonomous System (AS) de origem usado para representar origem ou destino
 - NextHop AS mostra fluxo de tráfego entre ISP parceiros

Border Gateway Protocol

- ◆ Usado na rede de transporte entre ISPs
 - » Protocolo vector distância
 - » Não conta apenas hops → lista AS atravessados
 - » Lista pode ser muito grande

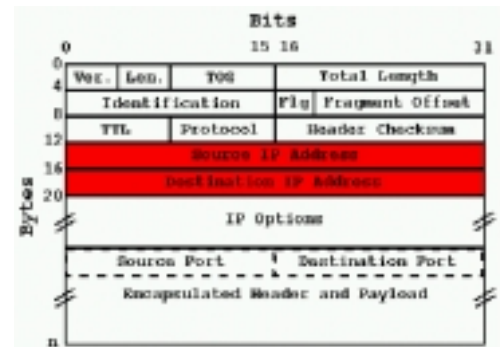
- ◆ Normalmente não há interesse no percurso completo
 - » AS de origem
 - Último AS na lista
 - Identifica ISP responsável por este prefixo

- ◆ Next-Hop AS
 - » Primeiro na lista de AS
 - » Identifica ISP vizinho para o qual tráfego vai ser enviado

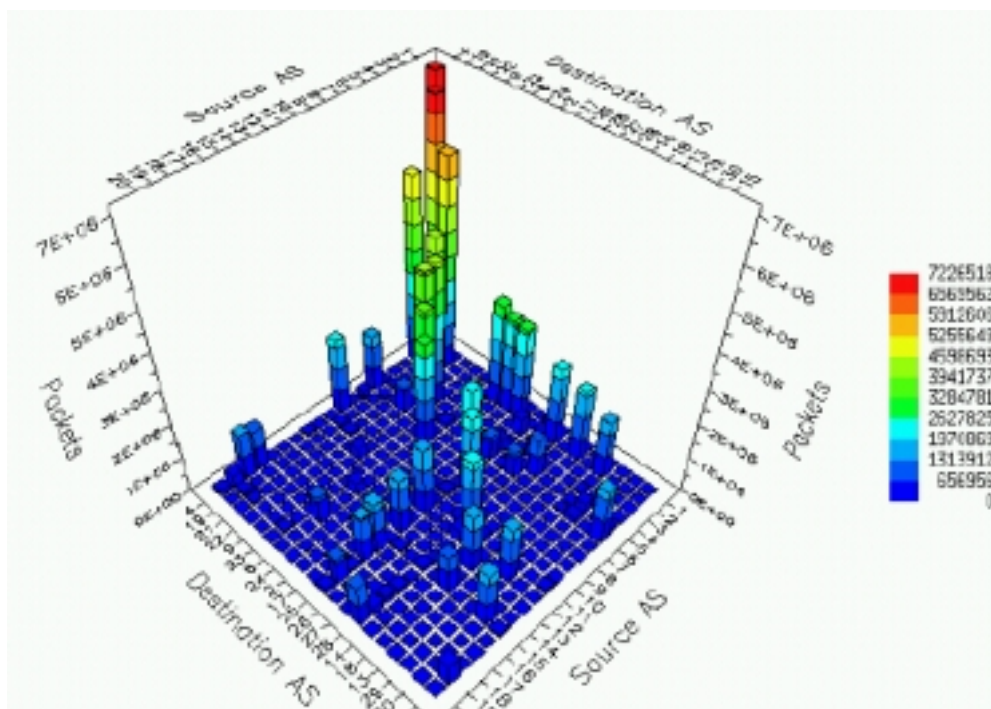
Tabela de Rotas BGP

Network	Path					
- 12.10.175.0/24	3333	1103	6453	701	8074	
- 128.91.0.0	145	10466	55			
- 129.12.0.0	5459	786				
- 129.133.0.0/18	267	1225	1325	1673	3561	

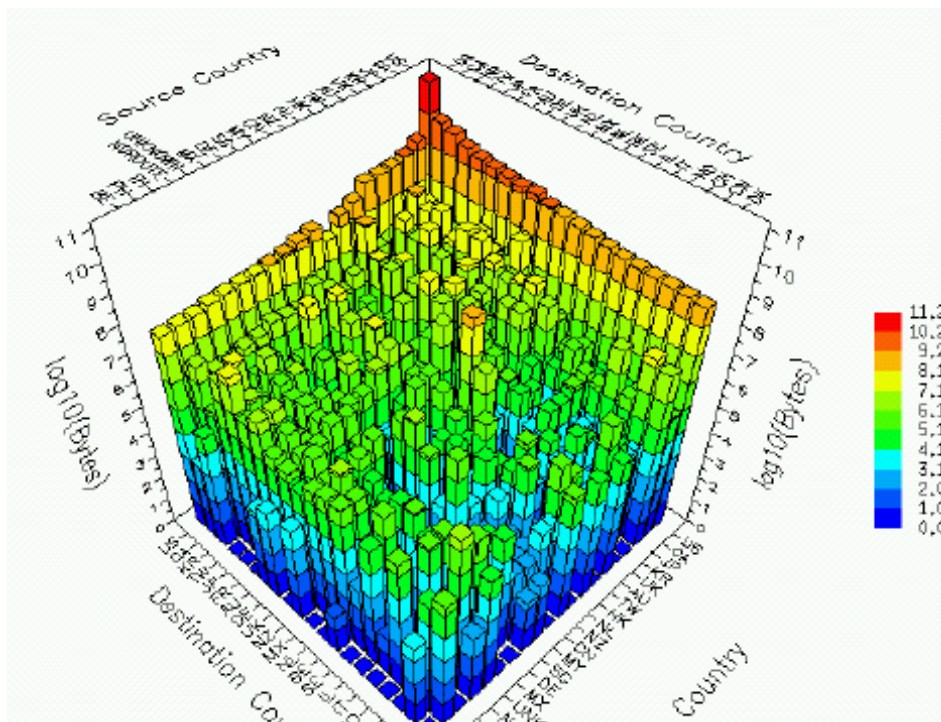
- » Next-hop AS → primeira entrada do trajecto
 - AS do ISP vizinho
- » Origem AS, é a última entrada do Path
 - AS do ISP que anunciou primeiro a rota



Matriz de Tráfego Entre ASs



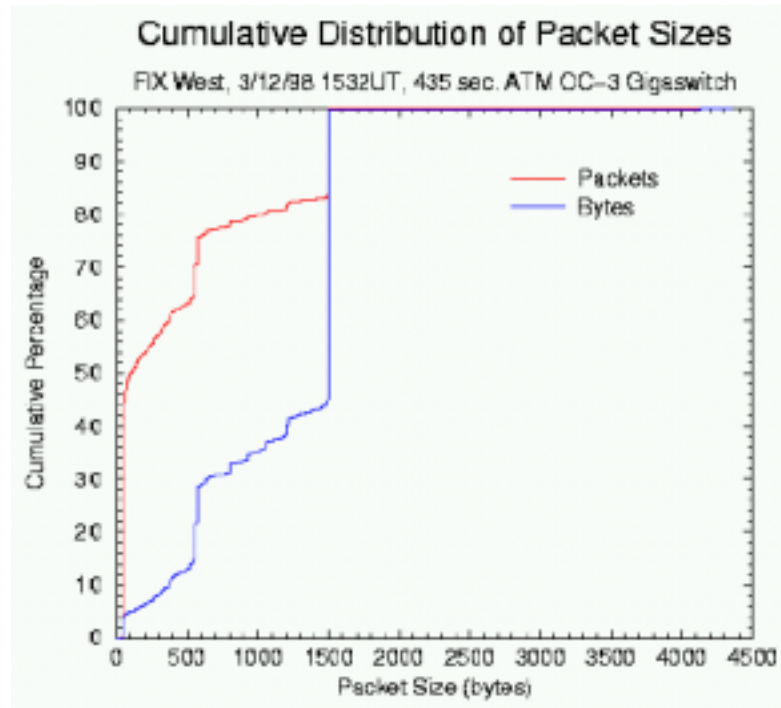
Por País



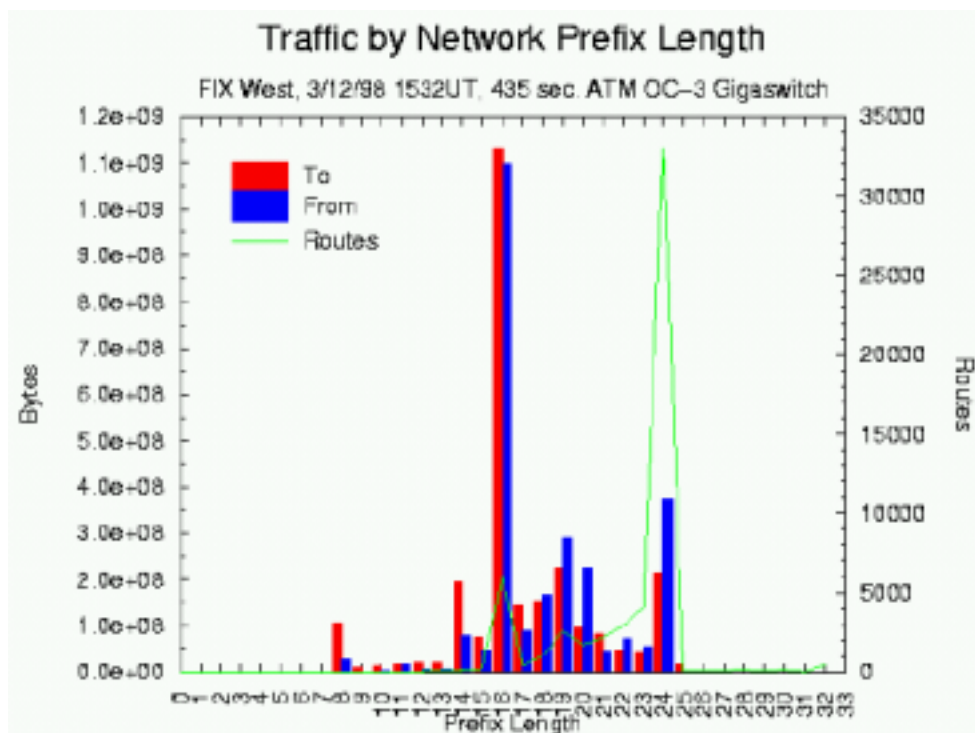
Outras Métricas

- ◆ Histogramas de comprimento de pacotes
 - » Útil para fabricantes de routers e switches
 - » Dimensionamento de buffers
- ◆ Histogramas de tráfego por comprimento de prefixo de endereço
 - » Indicador da eficiência das tabelas de encaminhamento
 - Relação tráfego encaminhado/recursos consumidos

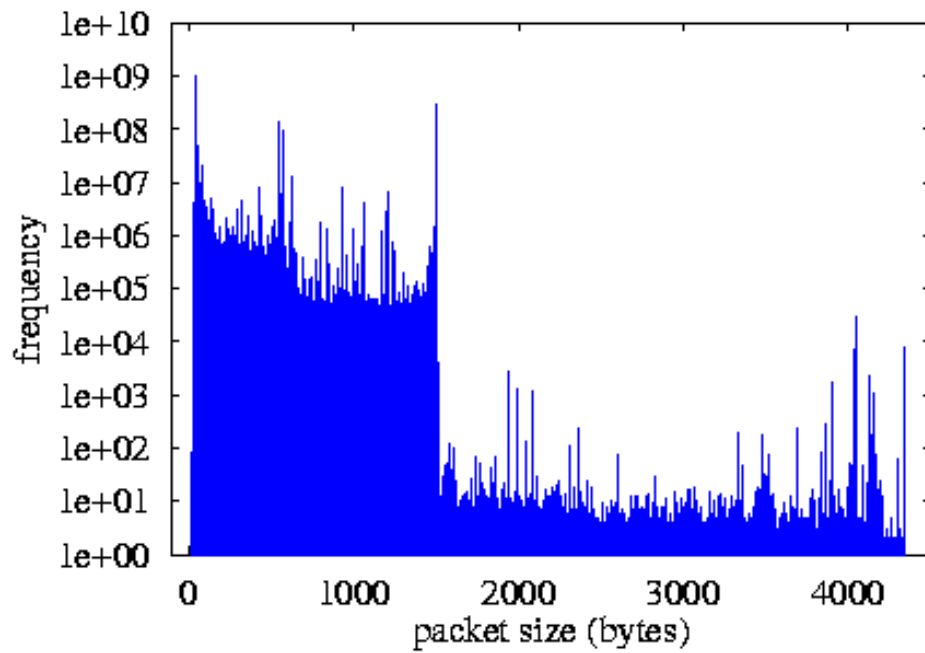
Eficiência de Pacotes



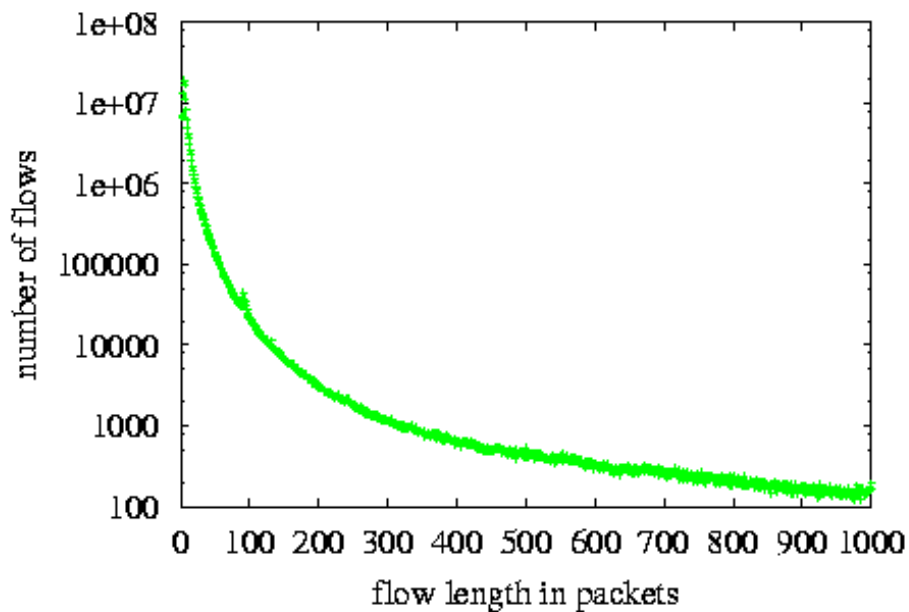
Eficiência da Rotas



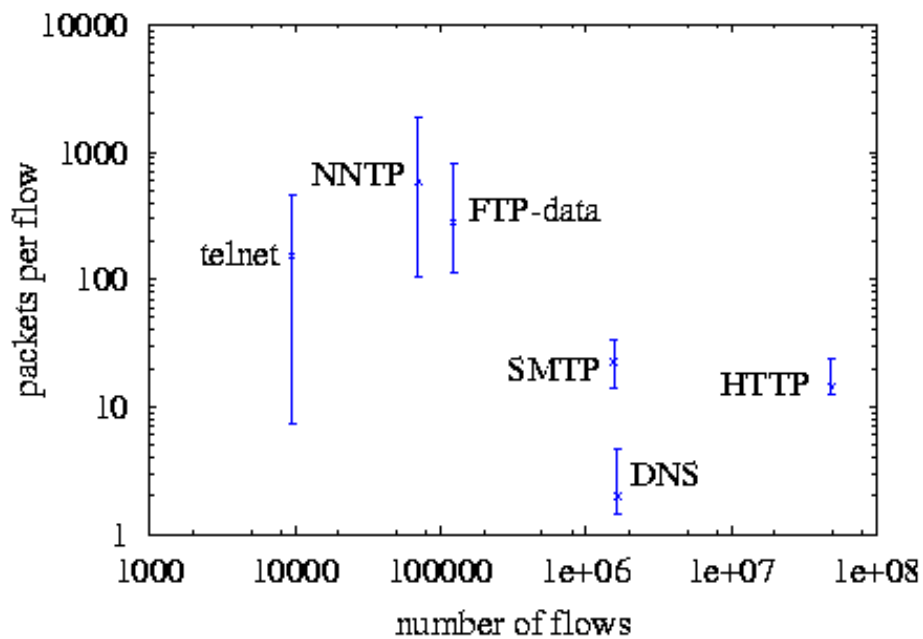
Comprimento dos Pacotes



Comprimento dos Fluxos, em pacotes



Pacotes Por Fluxo - Aplicação



Técnicas de Amostragem

- ◆ Se débito de pacotes → elevado
 - » técnicas de amostragem
- ◆ Técnicas mais usadas
 - » Amostrar pacote $k \cdot N$ (k inteiro, N constante)
 - » Amostragem por tempo
 - mais complexa → mas também usada

Outras Métricas Comuns

- ◆ Métricas de *utilização comum* na Internet
 - » Latência
 - » Perda de pacotes
 - » Disponibilidade
- ◆ Definidas assumindo utilização de ping ou do traceroute
- ◆ Existem definições mais precisas → pouco usadas
 - » IETF IPPM
 - » ITU-T I.380
- ◆ Avaliadas com métodos activos

Latência

- ◆ Latência – tempo de ida e volta de um pacote.
- ◆ Tipos de atraso
 - » A. Tempo de propagação
 - tempo que um bit do pacote demora a atravessar um link
 - » B. Tempo de espera e transmissão
 - Tempo de espera de um pacote na fila + tempo de transmissão do pacote
 - » C. Tempo de resposta do servidor
 - tempo que o servidor demora a processar o pacote de entrada e a gerar o pacote de resposta
- ◆ Componentes da latência
 - » Atraso directo no percurso cliente-servidor. Tipos a, b
 - » Atraso do servidor. Tipo c
 - » Atraso de retorno no percurso servidor – cliente. Tipos a, b
 - pode nao ser o mesmo que o directo
- ◆ Latências de rede tipo – 90 ms (Nova Iorque – Londres)

Latência

- ◆ Medida de latência
 - » utilização de aplicação implementada na pilha to IP do servidor
 - » pouco processamento/ kernel space
 - » ping → utilização mais frequente
 - ISPs usam-no para medir latências. Assumem que c é desprezável
- ◆ Latência não é fixa
 - » varia com a carga
 - carga no servidor
 - congestao da rede → tempo de espera nos routers
 - Mudança de rotas
- ◆ Detecção da variação da latência
 - » Gráficos com medida ao longo do dia → intervalos de 1 a 5 minutos

Perda de Pacotes

- ◆ Internet funciona em best-effort →
 - » Filas grandes, nos routers → pacotes perdidos
- ◆ Pacotes perdidos (definido a pensar no ping ...)
 - » Pacotes perdidos em trânsito entre um cliente e um servidor sobre número de pacotes enviados para o servidor
 - » Medida feita durante um intervalo de tempo
 - » Valor expresso como fracção dos pacotes enviados para o servidor
- ◆ Valores variam de de 0% (sem congestão) até 5 to 15% (congestão severa).
 - » Valores muito altos tornam rede não inusável
 - » Perdas moderadas (1, 2, 3 %) são aceitáveis

Débito

- ◆ Débito de envio informação para a rede.
 - » Medido em
 - bit/s, Byte/s, pacote/s

- ◆ Medido, contando
 - » Número de bytes transportados durante um intervalo de tempo

 - » Sobre TCP ou utilizando fluxo UDP/IP bem comportado

Disponibilidade

- ◆ Capacidade de um dispositivo/serviço permanecer em operação normal
 - » Disponibilidade de serviço (ex. Servidor Web)
 - Teste - descarregar páginas de um servidor Web, usando um browser.
 - » Disponibilidade da máquina
 - Ping do host, verificar recepção de pacotes ICMP
 - » Disponibilidade da rede
 - Fazer traceroute até um host. Verificar se há ligação
- ◆ Em cada um dos casos
 - » Obter valores de latência e perda de pacotes
- ◆ Indisponibilidade é função de latência e perda de pacotes

- ◆ Ex. Rede indisponível quando router do ISP, pingado em intervalos de 1 min,
 - » Latência maior que 10 ms, ou
 - » Perda de pacotes de ping maior que 1%

Disponibilidade

- ◆ Disponibilidade nos ISPs
 - » Figura mensal
 - Indica percentagem de tempo que rede esteve com valores de latencia e perda de pacotes aceitaveis
 - » Disponibilidade de 99,99%
 - serviço indisponível durante 4 minutos, no mês.
- ◆ ISPs
 - » *Podem confundir disponibilidade com acessibilidade* aos hosts
 - » Só começam a contar a indisponibilidade a partir do momento da reclamação
 - » Podem não incluir tempos de manutenção dos equipamentos
- ◆ Outros parâmetros importantes
 - » Mean Time To Repair (MTTR)
 - Tempo de médio de recuperação do serviço, depois de perda de disponibilidade
 - » Mean Time Between Failures (MTBF)
 - Tempo médio entre o início de serviço normal e a próxima perda de disponibilidade

Fiabilidade

- ◆ Probabilidade de se obter uma resposta errada
 - » Pacote corrompido
 - pacotes errados também são considerados como perdidos.

Média, Mediana e Percentil

- ◆ Média – valor interessante, para dados bem comportados

- ◆ Mediana → percentil 50. Melhor valor que média

- ◆ Utilização de percentis → 5%, 95%, 25%, 75%
 - » Eg. Prob(latência < Y) >= 75%
 - » Valor Y, para o qual o percentil é observado

Ping

- ◆ ping
 - » Aplicação simples
 - » Corre em cliente
 - » Ping envia pacotes ICMP echo request para um servidor
 - » servidor envia pacote de ICMP echo reply
 - » Ping calcula tempo de ida e volta
 - » ICMP corre na pilha, no kernel
 - » Ping conta percentagem de pacotes perdidos e latência

- ◆ ping -c 5 xx.yy.com
 -
 - xx.yy.com ping statistics ---
 - 5 packets transmitted, 5 packets received, 0% packet loss
 - round-trip min/avg/max/stddev = 167.401/266.975/366.900/82.312 ms

Ping

- ◆ Ping faz teste de atingibilidade de máquina.
 - » Diferente de ter serviço activo
- ◆ Ausência de resposta pode indicar bloqueio em firewall
- ◆ Mau para teste de routers
 - » routers correm ping com prioridade baixa → latência grande

Traceroute

- ◆ Usado para detectar possível rota
- ◆ traceroute produz a lista de routers até ao destino
- ◆ Imprime latência ou * se não há resposta
- ◆ Só mostra o percurso directo
- ◆ Usa o TTL, que expira, e recebe mensagens de erro ICMP.

Gestão, SNMP

- ◆ Monitorar MIBs através de SNMP

- ◆ MIB-II contém contadores interessantes
 - » ifInOctets
 - Número total de octetos recebidos através de uma interface
 - » ifOutOctets
 - Número total de octetos enviados através de uma interface.

- ◆ Contadores SNMP nunca são postos a zero →
 - » Leitura regular
 - » Diferenças

Wire Time

- ◆ Para um dado pacote
 - » O tempo de chegada de um pacote a um host
 - Instante em que o primeiro bit do pacote chega ao host
 - » Tempo de partida de um pacote de um host
 - Instante em que o último bit do pacote é transmitido para o cabo

Pacotes de Medida

- ◆ Um pacote de medida bem formado
 - » Indica o comprimento correcto e válido (≥ 5) no cabeçalho
 - » Tem cabeçalho válido. Com checksum correcto
 - » Não é um fragmento
 - » Endereços indicados são válidos e verdadeiros
 - » Tem TTL de 255 ou com valor que permita atravessar a rede
 - » Não contém opções
 - » Se existir cabeçalho de transporte, este também é correcto

- ◆ Pacote mínimo
 - » Pacote bem formado
 - » Comprimento de dados = 0

Dezenas de Ferramentas ...

- ◆ Livro do Sloan, Network Troubleshooting Tools
- ◆ www.caida.org