

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA**

**MITIGAÇÃO DE PROBLEMAS DE DESEMPENHO ENTRE
SISTEMAS AUTÔNOMOS COM TRÁFEGO ASSIMÉTRICO
FOCADA NA INFLUÊNCIA NA TOMADA DE DECISÃO DO
BGP**

MÁRCIO AUGUSTO DE DEUS

ORIENTADOR: PAULO HENRIQUE PORTELA DE CARVALHO

TESE DE DOUTORADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPGEE.TD-101/15

BRASÍLIA/DF: SETEMBRO – 2015

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

MITIGAÇÃO DE PROBLEMAS DE DESEMPENHO ENTRE
SISTEMAS AUTÔNOMOS COM TRÁFEGO ASSIMÉTRICO FOCADA
NA INFLUÊNCIA NA TOMADA DE DECISÃO DO BGP

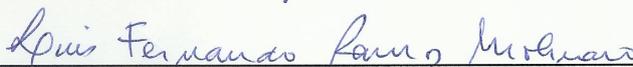
MÁRCIO AUGUSTO DE DEUS

TESE DE DOUTORADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA
FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS
REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE DOUTOR.

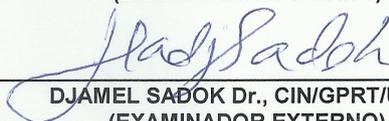
APROVADA POR:



PAULO HENRIQUE PORTELA DE CARVALHO, Dr., ENE/UnB
(ORIENTADOR)



LUÍS FERNANDO RAMOS MOLINARO, Dr., ENE/UnB
(EXAMINADOR INTERNO)



DJAMEL SADOOK Dr., CIN/GPRT/UFPE
(EXAMINADOR EXTERNO)



FLÁVIO HENRIQUE TELES VIEIRA, Dr., EEE/UFG
(EXAMINADOR EXTERNO)



RAFAEL TIMÓTEO DE SOUSA JUNIOR, Dr., ENE/UnB
(EXAMINADOR INTERNO/SUPLENTE)

Brasília, 25 de setembro de 2015.

FICHA CATALOGRÁFICA

DE DEUS, MARCIO AUGUSTO

Mitigação de problemas de desempenho entre sistemas autônomos com tráfego assimétrico focada na influência na tomada de decisão do BGP. [Distrito Federal] 2015.

xiv, 186p., 210 x 297 mm (ENC/FT/UnB, Doutor, Engenharia Elétrica e Telecomunicações, 2015).

Tese de Doutorado – Universidade de Brasília. Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1.Tomada de Decisão

2.Planejamento

3.Internet

4.BGP

I. ENE/FT/UnB

II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

DE DEUS., MARCIO A. (2015). Mitigação de problemas de desempenho entre sistemas autônomos com tráfego assimétrico focada na influência na tomada de decisão do BGP. Tese de Doutorado em Engenharia Elétrica, Publicação PPGEE.TD-101/15, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 186p.

CESSÃO DE DIREITOS

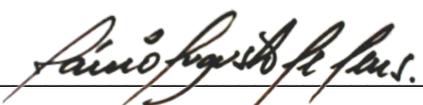
AUTOR: Márcio Augusto de Deus.

TÍTULO: Mitigação de problemas de desempenho entre sistemas autônomos com tráfego assimétrico focada na influência na tomada de decisão do BGP.

GRAU: Doutor

ANO: 2015

É concedida à Universidade de Brasília permissão para reproduzir cópias desta dissertação de mestrado e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor reserva outros direitos de publicação e nenhuma parte dessa dissertação de mestrado pode ser reproduzida sem autorização por escrito do autor.



Márcio Augusto de Deus
SQSW 306 Bloco A, Ap.211 - Sudoeste
70.673-431 Brasília – DF – Brasil.

AGRADECIMENTOS

Em nome de Jesus: a Deus!

A minha esposa Ana Cláudia e minhas filhas Raíssa e Márcia e a minha mãe, D. Maria.

Ao meu orientador, Prof. Paulo Portela e também ao Prof. João Paulo.

Este trabalho é uma prova material de um milagre.

“Quais foram os seus avanços hoje?”
Prof. Dr. Paulo Portela.

SUMÁRIO

1	CONSIDERAÇÕES INICIAIS	1
1.1	INTRODUÇÃO	1
1.2	OBJETIVOS DESTES TRABALHOS	3
1.3	ESTRUTURA DO TRABALHO	4
2	DESCRIÇÃO DE UM PROVEDOR DE SERVIÇOS	6
2.1	RELACIONAMENTOS ENTRE SISTEMAS AUTÔNOMOS BGP	9
2.2	PLANEJAMENTO E CONSTRUÇÃO DE REDES	17
2.3	USO EFICAZ DE RECURSOS	20
2.4	RELAÇÃO COM O MODELO SDN	23
2.5	CONCLUSÃO DESTE CAPÍTULO	27
3	CARACTERIZAÇÃO E DEFINIÇÃO DE SERVIÇO	29
3.1	O TRÁFEGO	31
3.2	A NATUREZA ASSIMÉTRICA DO TRÁFEGO E IMPLICAÇÕES	32
3.3	A BANDA OU VELOCIDADE COMO UM PRODUTO OU SERVIÇO	36
3.4	MODELOS MATEMÁTICOS	38
3.5	ESTIMADORES DE BANDA OU VELOCIDADE	46
3.6	ESTRATÉGIA DE CARACTERIZAÇÃO E CÁLCULO DE BANDA	55
3.7	COMPARAÇÃO ENTRE OS MÉTODOS PARA O CÁLCULO DE BANDA	60
3.8	ESTIMADORES PARA NOVAS APLICAÇÕES	66
3.8.1	O WebRTC	66
3.9	CONCLUSÃO DO CAPÍTULO	67
4	A INTERFERÊNCIA RACIONAL	69
4.1	DESENVOLVIMENTO DE MECANISMOS DE ALGORITMOS DISTRIBUÍDOS	71
4.2	SOLUÇÃO POR ANALOGIA	73
4.3	ANALOGIA ENTRE O PROCESSO DE TOMADA DE DECISÃO	75
4.3.1	A decisão e a recompensa do BGP	76
4.3.2	Definição das estratégias da tomada de decisão	78
4.3.3	Jogo de Soma Zero	79
4.4	CARACTERIZANDO A TOMADA DE DECISÃO	82
4.5	ANÁLISE DA ESTRATÉGIA USADA PELO BGP	83
4.6	MODIFICAÇÃO NA TOMADA DE DECISÃO DO BGP (BÔNUS TRB) OU SOLUÇÃO SEMI-INTRUSIVA	88
4.7	TOMADA DE DECISÃO BASEADA EM CONHECIMENTO ESPECIALISTA	94
4.8	REAGINDO À ESTRATÉGIA DOMINANTE DE FORMA INTUITIVA	95
4.9	ESTABILIDADE DO BGP	97
4.10	ESTABILIDADE DA REDE	99
4.11	CONCLUSÃO DO CAPÍTULO	103
5	APLICAÇÕES DA INTERFERÊNCIA RACIONAL	104
5.1	A ANÁLISE DA TOMADA DE DECISÃO	104
5.2	ENSAIO 1	107
5.3	ENSAIO 2 –USANDO O CONHECIMENTO ESPECIALISTA	117
5.4	ENSAIO 3 – TENTATIVA DE CONTROLE DO TRÁFEGO	125
5.5	ENSAIO 4 – COMPARAÇÃO DOS ESTIMADORES	135
6	CONCLUSÃO E TRABALHOS FUTUROS	140
6.1	PUBLICAÇÃO EM PERIÓDICOS	141
6.2	ARTIGOS PUBLICADOS	141
6.3	ARTIGOS SUBMETIDOS OU AGUARDANDO RESPOSTA	142
7	REFERÊNCIAS BIBLIOGRÁFICAS	143

8 ANEXO I	157
8.1 FERRAMENTA: OMNET ⁺⁺	157
8.2 FERRAMENTA: WEKA	184
8.3 FERRAMENTA: C-BGP	184
8.4 FERRAMENTA: FRACLAB	185
8.5 FERRAMENTA: LABORATÓRIO DE UMA OPERADORA DE TELECOMUNICAÇÕES.....	186

LISTA DE TABELAS

Tabela 3.1 – Teste de aderência com o uso do χ^2	45
Tabela 4.1. Proposta de cálculo do <i>TrB</i>	91
Tabela 4.2 – Tabela RIB.....	100

LISTA DE FIGURAS

Figura 1.1 - Relacionamento entre Sistemas Autônomos.....	10
Figura 1.2 - Relacionamento entre ases em um ponto de troca de tráfego.....	11
Figura 1.3 - Estratificação do processo de tomada de decisão	12
Figura 1.4 - Fluxo de decisão do BGP (Rekter, 2006)	13
Figura 2.1 - Ciclo de planejamento de longo prazo com trilha rápida.	19
Figura 2.2 - Causa raiz para perda de pacotes.	21
Figura 2.3 - Arquivo equinix-chicago.dira.	22
Figura 2.4 - Arquitetura SDN, adaptado de (Alkildiz et al, 2014).	24
Figura 2.5 - Tomada de decisão. Adaptado de (Ghattas, 2013).	27
Figura 3.1 - Tráfego entre os EUA e o Brasil.....	33
Figura 3.2 - Diagrama de uma conexão entre dois nós de comunicação.....	34
Figura 3.3 - Função Fut do equilíbrio entre o TX e o RX.	36
Figura 3.4 - Dilema da banda ou velocidade em bps.....	37
Figura 3.5 - Modelo de conexão de rede simplificado e em camadas de rede.	39
Figura 3.6 - Espectro de Legendre para o tráfego auto-similar.	44
Figura 3.7 - CDF do teste do qui-quadrado para teste de aderência.....	46
Figura 3.8 - Teste real utilizando a ferramenta http://simet.nic.br	48
Figura 3.9 - Curva de Estimção de Banda Passante 108Mbps.	50
Figura 3.10 - Fluxo geral da estratégia de planejamento e curto.....	57
Figura 3.11- Processo inicial de caracterização de tráfego.	58
Figura 3.12 - Computação de banda passante	60
Figura 3.13 - Coletas de uma rede real. Banda Stênico.....	61
Figura 3.14 - Coletas de uma rede real. Banda Kernel.....	62
Figura 3.15 - Coletas de uma rede real. Banda misturas gaussianas	63
Figura 3.15 - Comparação das cdfs da probabilidade de erro.	64
Figura 3.16 - Comparação da economia de banda.....	65
Figura 3.17 - Arquitetura webrtc, em acordo com (webrtc, 2015).....	67
Figura 4.1 - Jogo entre dois ases baseado em estratégia dominante.....	82
Figura 4.2 - Dados reais extraídos de uma rede real	86
Figura 4.3 - Cálculo do raio da Internet - WEKA.	88
Figura 4.4 - Processo parcial de tomada de decisão do BGP	90
Figura 4.5 - Sensibilidade a alterações parametrizadas via BGP.	90

Figura 4.6 - Arquitetura do protocolo.....	91
Figura 4.7a - Processo simulado do BGP sem o TrB.....	93
Figura 4.7b - Processo simulado do BGP com o TrB.....	93
Figura 4.8 - Tempo de convergência com e sem o uso do TrB.....	94
Figura 4.9 - Mecanismo de tomada de decisão especialista.....	94
Figura 4.10 - Tentativa de alteração do tráfego com o uso do <i>Prepend</i>	96
Figura 4.11 - Conexão entre três ases com análise de estabilidade.....	98
Figura 4.12 - Exemplo de rede real - teste de estabilidade.....	99
Figura 4.13 - Código 000x1f3 é relacionado a modificações na RIB AS_PATH.....	101
Figura 4.14 - Todos os eventos coletados.....	102
Figura 4.15 - Eventos coletados por modificação do AS_PATH.....	102
Figura 4.16 - Eventos coletados por modificação do AS_PATH.....	103
Figura 5.1 - Definição de parâmetros de grau de eficácia para a tomada de decisão.....	104
Figura 5.2 - Rede real em teste.....	108
Figura 5.3 - Política de decisão do BGP.....	109
Figura 5.4 - Processo de tomada de decisão para interferência inteligente.....	110
Figura 5.5 - Topologia da rede a partir da informação do BGP.....	110
Figura 5.6 - Caracterização do raio entre ases (número de saltos por ases).....	111
Figura 5.7 - Caracterização do prepend ASN, distância entre Ases.....	112
Figura 5.8 - Caracterização do tráfego → DLD.....	112
Figura 5.9 - Tentativa de modificação do caminho com interferência inteligente.....	113
Figura 5.10 - Processo de alteração do prepend.....	114
Figura 5.11 - Ruptura do encaminhamento de tráfego prepend.....	114
Figura 5.12 - Tráfego modificado.....	115
Figura 5.13 - Efetividade do uso do prepend.....	116
Figura 5.14a - Tráfego, por horário.....	118
Figura 5.14b - Tráfego horário dos Estados Unidos para o Brasil.....	118
Figura 5.14 a - Análise multifractal, espectro de Legendre para o tráfego ingress.....	120
Figura 5.14b - Função de interpolação do expoente de Hölder.....	120
Figura 5.14c - Análise multifractal, espectro de Legendre para o tráfego egress.....	120
Figura 5.14d - Função de interpolação Hölder.....	120
Figura 5.15 - Estrutura da rede em análise (N. U. T. – network under the test).....	121
Figura 5.16 - Política de tratamento dos parâmetros do BGP com prioridades.....	121
Figura 5.17 - Política de tratamento dos parâmetros do BGP com prioridades.....	122

Figura 5.18 - Ciclo completo de tomada de decisão para aplicação em rede real.....	123
Figura 5.19 - Ciclo completo de tomada de decisão do especialista.	123
Figura 5.20 - Percentual de efetividade por grau de experiência do especialista.....	124
Figura 5.21 - CDF do tempo de solução em função da experiência do especialista.	124
Figura 5.20 - Ciclo completo.....	125
Figura 5.22 - Rede sob análise e subrede destino.....	126
Figura 5.23 - Enlace congestionado.	127
Figura 5.23 - Caracterização do Tráfego para algumas das 125 amostras	128
Figura 5.24 - Espectro de Legendre para algumas amostras.	129
Figura 5.25 - Cálculo da Banda Efetiva (E_{bx} = Banda efetiva).	129
Figura 5.26 - Cálculo da banda efetiva para cada um dos casos analisados.....	130
Figura 5.27 - Identificação da fonte do tráfego.	130
Figura 5.28a - Uso do <i>prepend</i>	131
Figura 5.29 - Cálculo da Banda Efetiva.	132
Figura 5.30 - Banda efetiva.	132
Figura 5.31 - Os casos mostrados com economia de banda negativa.....	133
Figura 5.32 - Rede após a alteração com o uso do <i>prepend</i>	134
Figura 5.33 - Perda de pacotes após a alteração.....	134
Figura 5.34 - CDF comparativa dos tempos de solução para os algoritmos	135
Figura 5.35a - Comparação da banda solicitada pelo cliente	136
Figura 5.35b - Percentual de economia de banda Stênico.....	136
Figura 5.36a - Comparação da banda solicitada pelo cliente	136
Figura 5.36b - Percentual de economia de banda.....	137
Figura 5.37a - <i>Boxplot</i> da taxa de perda máx, min, média de pacotes - Stênico.	132
Figura 5.37b - <i>Boxplot</i> da taxa de perda máx, min, média pacotes - Mist. Gaussiana.....	132
Figura 5.37 - CDF da taxa de perda máxima de pacotes - Método de Stênico	139
Figura 5.38 - CDF da taxa de perda máxima de pacotes - Mistura Gaussiana.....	139

LISTA DE EQUAÇÕES

Equação 3.1 - Fator de utilização.	34
Equação 3.2 - Banda média backh.....	39
Equação 3.3 - Banda média distribuição	39
Equação 3.4 - Banda média core.	39
Equação 3.5 - Modelo auto-similar.	40
Equação 3.6 - Limites da variância.	41
Equação 3.7 - Termos do processo auto-similar.....	41
Equação 3.8 - Momentos	42
Equação 3.9 - Hölder	42
Equação 3.10 - Hölder hq.	42
Equação 3.11 - Espectro.	43
Equação 3.12 - Espectro Legendre.....	43
Equação 3.13 - Transformada de Legendre.....	44
Equação 3.14 - Banda Efetiva Kelly	49
Equação 3.15 - Banda Efetica FEP.....	49
Equação 3.16 - Banda Otimizada	50
Equação 3.17 - Banda Otimizada $H > 0.7$	50
Equação 3.18 - Conjunto de Gaussianas	51
Equação 3.19 - Limites do processo $P_p(x)$	51
Equação 3.20 - Limites do processo $P_p(x)$	51
Equação 3.21 - Limites do processo $f_p(x)$	52
Equação 3.22 - Função Geradora de Momentos, por definição	52
Equação 3.23 - Função Geradora de Momentos explicitando $f(z)dz$	52
Equação 3.24 - Função Geradora de Momentos explicitando ρ_i e g_i	52
Equação 3.25 - Termo da Função Geradora de Momentos	52
Equação 3.26 - Termo da Função Geradora de Momentos	52
Equação 3.27 - Função Erro Complementar	52
Equação 3.28 - Banda Efetiva Gaussiana.....	53
Equação 3.29 - Distribuição Gaussiana	53
Equação 3.30 - Banda Efetiva Kernel	53
Equação 3.31 - Banda Efetiva Kernel	54
Equação 3.32 - Expoente de Hölder	54

Equação 3.33 - Banda Efetiva Multifractal - bp_x	55
Equação 3.34 - Banda Efetiva Multifractal (outra forma) - bp_x	55
Equação 4.1 - Definição de grafo	72
Equação 4.2 - Somatório das probabilidades.....	77
Equação 4.3 - Função Utilidade	79
Equação 5.1 - Espectro de Legendre	119
Equação 5.2 - Definição do Espectro de Legendre	119

LISTA DE SÍMBOLOS, NOMECLATURAS E ABREVIACÕES

a	– Fator de escala do tráfego auto-similar
α_q	– Expoente de cascadeamento, caso Multifractal ou DLD
μ	– Média
v	– Variância
$\gamma_k^{(m)}$	– Auto-covariância
$\rho_{G(k)}$	– Coeficiente de auto-correlação
H	– Parâmetro de Hurst
$h(t)$	– Expoente de Hölder
$E(X(t))$	– Esperança do processo estocástico $X(t)$
$R(t_1, t_2)$	– Correlação entre t_1 e t_2
$\zeta(q)$	– Função cascadeamento
q	– Ordem dos momentos, caso Multifractal ou DLD
Ω	– Grau de liberdade de atuação da ferramenta na banda definida por túnel
3G	– Terceira geração de comunicação móvel sem fio
4G	– Quarta geração de comunicação móvel sem fio
ASSINANTE	– Consumidor de serviços prestados pela operadora de telecomunicações
AAA	– <i>Authentication, Authorization and Accounting</i>
ADSL	– <i>Assymmetric Digital Subscriber Line</i>
ATM	– <i>Assynchronous Transfer Mode</i>
BBT	– <i>Bidirectional Traffic Trunk</i>
BER	– <i>Bit Error Rate</i>
BGP	– <i>Border Gateway Protocol</i>
BRAS	– <i>Broadband Router Access Server</i>
CBR	– <i>Constant Bit Rate</i>
CLI	– <i>Command Line Interface</i>
CLIENTE	– Ver assinante
CODEC	– <i>Encoder and Decoder</i>
Diffserv	– <i>Differentiated Services</i>
DCD	– Dependência de Curta Duração – Processos sem memória
DLD	– Dependência de Longa Duração – Processos com memória
DWDM	– <i>Dense Wavelength Division Multiplexing</i>

fBm	– <i>Fractional Brownian Motion</i>
eBGP	– <i>External BGP</i>
ETSI	– <i>European Telecommunications Standards Institute</i>
FEC	– <i>Forwarding Equivalence Class</i>
FGN	– <i>Fractional Gaussian Noise</i>
FIB	– <i>Forwarding Information Base</i>
GTAR	– Gerador de tráfego e análise de <i>QoS</i> na Rede
HMM	– Hora de maior movimento
HTTP	– <i>Hyper Text Transfer Protocol</i>
iBGP	– <i>Internal BGP</i>
IEEE	– <i>Institute of Electrical and Electronic Engineers</i>
IETF	– <i>Internet Engineering Tasking Force</i>
IMS	– <i>IP Multimedia Subsystem</i>
INTERNET	– Rede mundial de computadores que usa o protocolo <i>IP</i>
IP	– <i>Internet Protocol</i>
IS-IS	– <i>Intermediate System to Intermediate System</i>
ITU	– <i>International Telecommunications Union</i>
ITU-T	– <i>International Telecommunications Union (antigo CCITT)</i>
LAN	– <i>Local Area Network</i>
LDP	– <i>Label Distribution Protocol</i>
LDPp	– <i>Label Distribution Protocol peer</i>
LER	– <i>Label Edge Router</i>
LFIB	– <i>Label Forwarding Information Base</i>
LPM	– <i>Least Prefix Match</i>
LSP	– <i>Label Switched Path</i>
LSR	– <i>Label Switch Router</i>
mBm	– <i>Multifractional Brownian Motion</i>
MIB	– <i>Management Information Base</i>
MOS	– <i>Mean Opinion Score</i>
MCP	– <i>Minimum Critical Path</i>
MMW	– <i>Modelo Multifractal baseado em Wavelet</i>
MPLS	– <i>Multiprotocol Label Switching.</i>
MPLS-TE	– <i>MPLS Traffic Engineering</i>
MST	– <i>Minimum Spanning Tree</i>

MWM	– <i>Multiplicative Wavelet Model</i>
NP	– <i>Non Polynomiam</i>
NS	– <i>Network Simulator</i>
OSI	– <i>Open System Interconnect</i>
OSPF	– <i>Open Shortest Path First</i>
P2P	– <i>Peer-to-Peer</i>
P Router	– <i>Provider Router</i> vide LSR
PE Router	– <i>Provider Edge Router</i> vide LER
PoP	– <i>Point of Presence</i>
PPM	– Período de maior movimento
PPP	– <i>Point to Point Protocol</i>
PPS	– <i>Point to Point Protocol</i>
QoS	– <i>Quality of Service</i>
RCS	– <i>Rate Controlled Service</i>
RSVP	– <i>Resource Reservation Protocol</i> (ver <i>IntServ</i>)
RTPC	– Rede de Telefonia pública comutada
RTT	– <i>Round Trip Time</i>
SDH	– <i>Synchronous Digital Hierarchy</i>
SIP	– <i>Session Initiation Protocol</i> .
SLA	– <i>Service Level Agreements</i>
SNMP	– <i>Simple Network Management Protocol</i>
SONET	– <i>Synchronous Optical Network</i>
TCP	– <i>Transmission Control Protocol</i>
T.A.	– Tratamento e Análise
TE	– <i>Traffic Engineering</i>
TIA	– <i>Telecommunications Industry Association</i>
TIER-1	– <i>Classificação mais alta para provedor de serviços Internet</i>
WDM	– <i>Wavelength Division Multiplexing</i>
UDP	– <i>User Datagram Protocol</i>
UMTS	– <i>Universal Mobile Telecommunications System</i>
UPLINK	– Conexão direcionada à subida de tráfego numa comunicação entre dois sistemas hierárquicos entre si
VBR	– <i>Variable Bit Rate</i>
VoIP	– <i>Voice over IP</i>

VPN – *Virtual Private Network*
VTP – *Variance Time Plot*

RESUMO

MITIGAÇÃO DE PROBLEMAS DE DESEMPENHO ENTRE SISTEMAS AUTÔNOMOS COM TRÁFEGO ASSIMÉTRICO FOCADA NA INFLUÊNCIA NA TOMADA DE DECISÃO DO BGP

Autor: Márcio Augusto de Deus

Orientador: Paulo Henrique Portela Carvalho

Programa de Pós-graduação em Engenharia Elétrica

Brasília, setembro de 2015

O objetivo desse trabalho é a proposição de uma estratégia que permita a interferência no processo de tomada de decisão do sistema autônomo (AS) externo.

A proposta é necessária para a otimização de redes onde a assimetria de tráfego é um problema. Devido ao processo de tomada de decisão de um AS ser independente, o tráfego entrante, gerado por um AS externo, não tem como ser controlado diretamente. Devido ao fato de não existirem modelos que possam descrever o comportamento do relacionamento entre sistemas autônomos foi necessária a sua caracterização. Com base nesta caracterização foram aplicados modelos matemáticos e conhecimento especialista de forma a se construir uma estratégia de interferência na tomada de decisão de um AS externo.

Estes procedimentos devem garantir um grau aceitável de estabilidade e efetividade. Caso contrário, resta ao administrador do AS que recebe o tráfego a negociação direta e pessoal com o administrador do AS que envia o tráfego.

A validação desta proposta foi realizada através de uma rede real com presença no Brasil, Venezuela, Colômbia e Estados Unidos. Ao final, após o processo ter sido explicitado, foram mostradas aplicações práticas na otimização dos recursos de operação e no planejamento de longo e curto prazo em ambientes de rede com tráfego assimétrico.

ABSTRACT

PERFORMANCE ISSUES MITIGATION BETWEEN AUTONOMOUS SYSTEMS WITH ASYMMETRIC TRAFFIC FOCUSED ON THE BGP DECISION-MAKING PROCESS

Author: Márcio Augusto de Deus

Supervisor: Paulo Henrique Portela Carvalho

Programa de Pós-graduação em Engenharia Elétrica

Brasília, September 25th 2015

The objective of this work is to propose a strategy to allow interference in the decision-making process of an external autonomous system (AS).

The proposal is required for network optimization where the asymmetry of traffic is a problem. Due to the process of making the decision, the incoming traffic, generated by an external, can not be controlled directly. For these cases it is necessary that actual process is characterized. On the basis of this characterization were applied mathematical models and expert knowledge in order to build the strategy of interference in the decision-making process of an AS external.

These procedures should ensure an acceptable degree of stability and effectiveness. Otherwise, the administrator of the AS which is receiving traffic will be requested to conduct direct and personal negotiation with the administrator of external AS which is sending traffic.

The validation of this proposal was conducted through a real network with presence in Brazil, Venezuela, Colombia and United States. After the process be explained, practical applications in resource optimization of operation and long-and short-term planning in network environments with asymmetric traffic are shown.

1 CONSIDERAÇÕES INICIAIS

1.1 INTRODUÇÃO

O fato de um sistema autônomo – AS ou *Autonomous System* –, conforme definido por (Hawkinson, 1996), ser independente com relação à sua tomada de decisão faz com que a interação entre as diferentes redes constituídas tenha um viés egoísta (Rekhter, 2006). No caso do AS não se observam as necessidades dos ASes vizinhos ou de demandantes que não estejam dentro do mesmo AS.

Quando da concepção das redes de telecomunicações, a simetria está presente em todas as etapas do processo, observa-se que as interfaces de transmissão, canais de comunicação, barramento interno de nós de rede são normalmente concebidos para usar a mesma quantidade de recursos na transmissão e recepção, excetuando-se condições como vistas em acessos ADSL (*Asymmetric Digital Subscriber Line*). A condição relacionada a não observação das necessidades do outro AS, junto ao fato de a maioria da infraestrutura da rede ter sido concebida de forma simétrica, acaba por gerar condições muito desfavoráveis para a otimização global de recursos.

A busca por soluções de otimização de recursos faz parte dos maiores problemas existentes no uso da Internet. O uso dos protocolos de roteamento internos e externos pode ajudar na otimização do uso eficaz dos recursos disponíveis em termos de infraestrutura. No caso específico do BGP – *Border Gateway Protocol* –, o grande desafio é fazer com que o AS vizinho tome uma decisão interna que não o beneficiará diretamente, mas sim, a outros ASes a ele conectados. Isto ocorre, pois o processo de tomada de decisão do BGP não proporciona meios diretos de controle do tráfego entrante a um AS, pois esse tráfego é controlado pelo AS externo ao que está recebendo o tráfego.

Nas redes que formam a Internet na América do Sul, a forte dependência de conteúdo com relação aos Estados Unidos da América gera assimetria de tráfego, efeito que será tratado nesse trabalho. Por outro lado, os recursos de rede, excetuando-se aqueles atuantes no acesso, são construídos para operar em modo simétrico (Wolfgang *et al.*, 2010), gerando dificuldades no controle dos recursos e o seu planejamento de capacidade e operação de rede para uso futuro. A assimetria do tráfego presente nas interconexões entre esses países

gera um ambiente de desbalanceamento. O efeito pode ser medido em função da dificuldade de otimização dos recursos em termos operativos e no planejamento de longo (maior que 12 meses) e curto prazo (até 12 meses).

Nos últimos anos, vários autores vêm abordando o problema. Nos trabalhos (Teixeira *et al.*, 2007) e (Secci, 2011), o encaminhamento de tráfego é tratado com base na possibilidade do seu direcionamento por controles externos. O tráfego na direção de saída do AS é controlado por algoritmos especialistas, dominados pelos IGP's (*Interior Gateway Protocols*). Para esses casos, as redes analisadas possuem características de simetria, pois tratam-se de ambientes na Europa e Estados Unidos da América. Nos trabalhos (Cheng *et al.*, 2014), (Wang *et al.*, 2007) e (Winter, 2012), tentativas de modificação no encaminhamento do tráfego ocorrem por estímulos externos ao AS_{ext} que necessita ser controlado em função de um AS_{int} que necessita controlar. Em todos os casos, a tentativa de se modificar o protocolo BGP ou de se centralizar a tomada de decisão de vários ASes faz com que essas propostas tenham baixa aceitação (Giang Ngo *et al.*, 2013), por não serem compatíveis com os protocolos e tecnologias existentes e por este motivo com prazo de implantação mais longo e custoso também sob os aspectos financeiros.

De acordo com (Rekhter, 2006), o BGP é um protocolo que transporta informação de acessibilidade entre entes BGP. Alguns autores, tais como (Soochang *et al.*, 2014) e (Ning *et al.*, 2014), tratam o BGP como um transportador de políticas muito dependente das estratégias empresariais (Teixeira, 2007). De fato, se para determinado AS pode ser interessante a troca de tráfego entre ASes de mesmo tamanho (*TIERs* ou categorização do AS por abrangência geográfica e número de interconexões diretas), por razões comerciais, pode não ser interessante para os demais. Ao final, caso o BGP não consiga oferecer condições para que a configuração de rede seja modificada, será necessário o contato pessoal entre os administradores. As políticas configuradas no BGP para a tomada de decisão são embasadas em parâmetros com prioridade para comandos internos, ou seja, um AS apenas admite interferência externa se sua política assim o permitir em termos de tomada de decisão. Porém, o princípio de funcionamento de um AS certamente não influencia apenas o tráfego interno a esse AS.

Também, fundamental é a inserção do usuário final na análise, pois segundo (Shenker, 1995) um método para avaliar a arquitetura de uma das redes que compõem a Internet deveria levar em consideração o quão feliz essa arquitetura deixa o usuário final. Ocorre que, no caso de interconexão entre redes, o usuário final pertence a uma rede que não tem como, prioritariamente, interferir no encaminhamento ou na arquitetura de encaminhamento de pacotes.

1.2 OBJETIVOS DESTE TRABALHO

O objetivo deste trabalho é a contribuição na mitigação de processo de tomada de decisão de otimização de recursos de rede. O foco principal é o relacionamento entre sistemas autônomos e o fato de a autogestão ser um fator complicador no processo de encaminhamento de pacotes no caminho reverso. Esse problema se evidencia com mais importância quando o tráfego entre dois ASes ocorre de forma assimétrica, sendo a parte reversa a de maior volume.

O grande desafio para quem toma uma decisão, qualquer que seja esta, é o de se esperar que a decisão tenha o efeito esperado (Shenker, 1995). Para que isso ocorra, é necessário que a tomada de decisão tenha suporte de informações ou que existam modelos que possam ser usados na previsão de determinado comportamento (Takine *et al.*, 2004).

Segundo (Takine *et al.*, 2004), para a utilização de um modelo de comportamento de um sistema físico, faz-se necessário coletar dados referentes a esse sistema e, a partir desses dados, encontrar um procedimento de inferência de parâmetros que exprima as principais características do comportamento que se deseja modelar. Após essa caracterização, um modelo poderá ser inferido de forma a ser possível a predição do comportamento do sistema, independente do tipo de aplicação ou serviço. Essas fases também serão analisadas no desenvolvimento deste trabalho.

O entendimento dos modelos matemáticos é necessário e tem um efeito direto na tomada de decisão. No caso específico de redes de telecomunicações ou de computadores, quando não se compreende a natureza do processo que está por trás dos eventos gerados pela comunicação, compromete-se qualquer tentativa de otimização de rede. Neste caso

também a topologia acaba por ter influência no processo e a sua melhor solução não tem como ser encontrada, pois não se conhecendo a sua natureza não há como se reproduzir uma função que possa representar todas as possibilidades e se chegar àquela que baste para a otimização dos recursos de rede. Desta forma faz-se necessário que os modelos matemáticos possam reproduzir o ambiente a ser melhorado. Após o conhecimento da natureza do tráfego e suas implicações faz-se ainda necessário que sejam feitas considerações específicas para especificidades encontradas. Neste trabalho as redes da América do Sul são analisadas e de forma diferente de análises anteriores, leva-se em consideração aspectos relacionados à assimetria do tráfego. (Winter, 2012).

1.3 ESTRUTURA DO TRABALHO

Este trabalho está dividido em seis capítulos, sendo que, no primeiro capítulo, é apresentado o problema que será analisado, os objetivos a serem atingidos e uma descrição geral do trabalho.

No segundo capítulo, é realizada uma análise dos procedimentos de planejamento em empresas de telecomunicações e suas deficiências, para se chegar a natureza do problema real enfrentado pelas grandes operadoras de telecomunicações. O desconhecimento da natureza do tráfego e portanto, o uso inadequado de modelos que consigam exprimir este comportamento.

Nos capítulos 3 e 4, são apresentadas a base teórica que será utilizada para o processo de tomada de decisão e as bases tecnológicas para infraestrutura de redes de telecomunicações.

No capítulo 5, são realizadas diversas simulações para a análise da proposta de estratégia de tomada de decisão, com análises de rede real que apresentam problemas de tomada de decisão, de desempenho e de uso efetivo dos recursos de transmissão e roteamento. Com relação ao desempenho, o foco será no consumo inteligente dos recursos de transmissão, mostrado pelo grau de eficiência no uso desses recursos e sua relação com o atraso, variação do atraso, complexidade do roteamento e tempo de solução para os problemas apresentados. Ainda nesse capítulo, serão apresentadas estratégias que serão usadas para a

melhoria do desempenho das redes, por meio do mapeamento de alguns processos de tomada de decisão.

Enfim, são apresentadas as conclusões e aplicações imediatas, além de perspectivas de continuidade do trabalho.

2 DESCRIÇÃO DE UM PROVEDOR DE SERVIÇOS

Um sistema autônomo, por definição, não necessita ser um provedor de serviços. Diferentes tipos de organizações podem ter esta função, não necessitando de nenhum tipo de licença de algum órgão regulador para que isto ocorra, bastando apenas uma requisição a um RIR (*Regional Internet Registry*), assim um provedor de serviços de telecomunicações precisa de licença para ser provedor, mas não para ser um sistema autônomo.

Ou seja, no Brasil, na América Latina, nos Estados Unidos da América, o princípio básico de formação de um AS não passa pela regulação da ANATEL (Agência Nacional de Telecomunicações) ou FCC (*Federal Communication Commission*), nos casos brasileiro e americano, respectivamente. Esta condição se repete em diversos outros países. Quando se faz necessária a prestação de serviços de acesso, ou seja, serviços de telecomunicações em conjunto com o acesso à Internet, a regulação ocorre na maioria dos países do mundo. Por outro lado, o Provedor de Serviços não necessita ser um AS para prestar serviços de acesso à Internet.

No Brasil, na Venezuela ou Colômbia, devido à complexidade da operação de um AS, diversos provedores de acesso de menor porte optam por comprar serviços IP de outras operadoras e não possuem um ASN (*Autonomous System Number*). Isto simplifica a operação da rede, pois apenas o roteamento interno será implementado e, uma vez conhecidas as rotas internas, qualquer outro destino será encaminhado através da rota *default* que terá como saída o Provedor de Serviços detentor do AS. Ou seja, não há a necessidade de pessoal treinado para a configuração do BGP.

A restrição vem pelo fato de ser muito difícil que o Provedor de Serviços consiga ter dois acessos por ASes ou provedores distintos. A razão é simples, ao ser um provedor sem AS, os endereços IPv4 ou IPv6 daquele provedor sem o ASN terão que ser anunciados como parte integrante do AS daquele que provê o acesso. Um endereço ou bloco de endereços IP somente poderá pertencer a um único AS, apesar de poder ser anunciado por mais de um, porém com informações de custo diferentes, mas origem única. A operação de um sistema

autônomo é um processo de relacionamento que se traduz em tarefa altamente dependente de relacionamentos pessoais (Wolfgang *et al.*, 2010), isto ocorre devido ao fato do BGP (*Border Gateway Protocol*) expressar, majoritariamente, apenas a vontade unilateral de um AS.

Por este motivo justificando a necessidade de relacionamentos interpessoais quando da tentativa de solução de um problema externo que esteja afetando um sistema autônomo. Alguns autores (Rekhter, 2006) colocam o BGP na categoria de protocolo de roteamento, porém outros o situam em uma condição de divulgador de políticas e informações de rotas (Wang *et al.*, 2007).

O gerenciamento dos processos internos do provedor de serviços é complexo, pois a infraestrutura de rede, baseada em camadas, não tem relacionamento gerencial direto (Akildiz *et al.*, 2014). Ou seja, um problema que ocorre no nível de transporte do DWDM (*Dense Wave Division Multiplexer*) afeta diretamente um roteador, mas o roteador pode não ter sinalização *in-band* ou *out-of-band*, quando usando interfaces Ethernet, para ter conhecimento direto do ocorrido e fazer com que isto reflita diretamente em uma decisão de roteamento.

O *cross-layer* ou interferência entre camadas ainda gera um ambiente complexo para a operação e quanto mais serviços, mais complexo (de Cola *et al.*, 2014). De forma geral, as grandes operadoras usam sistemas para a correlação de eventos coletados via SNMP (*Simple Network Management Protocol*) ou coletas de fluxos (*flow*) para que um serviço possa ser gerenciado, diferentemente de gerenciamento de elementos de rede.

Para que um provedor de serviços possa operar, é necessária uma estrutura mínima com funções de Operações e Projeto de forma separada, ou seja, uma área cuida das novas implantações e modificações em função de crescimento de demanda ou obsolescência tecnológica e outra cuida da operação e manutenção da rede. A operação trabalha por fluxo contínuo e tem a responsabilidade de continuidade, as áreas de projeto, normalmente relacionadas à engenharia, são compostas de planejamento, projeto e implantação

Segundo (Kotler, 1998), o planejamento é condição inequívoca para o estabelecimento de bases para o acompanhamento de qualquer atividade, serviço ou produto. Tem características de continuidade, porém definido por ciclo e deverá gerar as especificações técnicas adequadas às necessidades para o suporte a atividades, serviços ou produtos (Kotler, 1998) oferecidos. Sem uma base de planejamento, não é possível que ocorra um acompanhamento, ou que exista uma linha de base ou referência de forma a ser possível a determinação do que necessita ser mantido ou modificado em razão dos resultados, em comparação com o planejado.

Na definição do que é ter um melhoramento, é importante ressaltar o estabelecimento das necessidades mínimas para o atendimento às condições técnicas e ainda se gerar a linha de base. Utilizando-se a função planejar de forma acurada, pode-se estabelecer uma função objetivo de eficiência operacional que é atingida quando uma atividade, serviço ou produto planejado por uma entidade (empresa ou governo) puder oferecer o que fora concebido utilizando exatamente a quantidade de recursos (materiais ou humanos) para suportar exatamente tal qual definido, seja por acordos de nível de serviço (*SLA - Service Level Agreements*) ou MTBF (*Mean Time Between Failure*) ou qualquer especificação técnica.

A maneira mais simples de se construir modelos matemáticos para previsões é usando valores médios (Barreto, 2007), desconsiderando-se todos os aspectos que se diferenciam destes, no entanto observa-se que o modelo proposto em (Hurst, 1951), em que os valores futuros têm correlação *long tail* determinada pelo ocorrido no passado, ou possuem memória (Kettani *et al.*, 2002).

A conclusão é que o conhecimento obtido por meio da caracterização natural dos processos que dominam o fenômeno é imprescindível para se gerar um bom modelo de previsão, sendo necessário que a caracterização ocorra também de forma constante, pois o modelo baseia-se sempre em dados coletados no passado. Tratando-se de fenômeno natural ou com influência humana, a garantia que um modelo pode ser usado deve ser sempre testada através da caracterização dos mesmos (Takine *et al.*, 2004).

2.1 RELACIONAMENTOS ENTRE SISTEMAS AUTÔNOMOS COM SUPORTE DO *BORDER GATEWAY PROTOCOL* – BGP

A principal característica do BGP é a de não permitir, prioritariamente, que sua tomada de decisão seja influenciada externamente. O problema de relacionamento ocorre devido ao fato do BGP não ser um protocolo especificado para tomar decisões *per se* (Rekther, 2006). De fato, o BGP tem por principal objetivo transportar rotas publicadas por sistemas autônomos de forma descritiva e parâmetros que carregam uma descrição das políticas de um determinado AS.

Esta descrição não tem por objetivo mostrar a um AS externo de que forma está construída a política de roteamento interno de um determinado AS, ao contrário, apenas são encaminhadas a um AS adjacente, as informações que interessam ao AS que as está publicando. Quando as informações não são suficientes para que ocorra o roteamento de forma otimizada faz-se necessário que ocorra a negociação entre os administradores de sistemas autônomos, usando-se o critério da solução de compromisso em bases empíricas. Isto, no entanto, é um processo lento e caro, pois envolve a necessidade de relacionamento constante entre os administradores de sistemas autônomos.

Ao final, tudo pode ser inconclusivo, pois questões financeiras podem levar a uma situação onde o AS de interesse não modifique nenhuma de suas políticas para resolver o problema de outro. Esta condição subjetiva é percebida pela falta de modelos de predição que possam sustentá-la e gerar a confiança da efetividade com melhoria, tendo sido definidas as métricas para acompanhamento (Aitken, Jonathan M.; *et al.*, 2010). O relacionamento entre ASes segue um princípio de autodefinição de tamanho e abrangência. A qualificação de *Tiers* é dada pela abrangência, quantidade de tráfego, quantidade de usuários e conteúdo. Ao final é uma autodefinição e mútuo reconhecimento, assim um *Tier-1* será assim definido se outro *Tier-1* também o assim reconhecer. Um *Tier-2* ou *Tier-3* seguem condições similares, porém uma vez definidos e acolhidos os *Tier-1*, os de segundo e terceiro ou *l*-níveis o serão em acordo com a dependência hierárquica entre os envolvidos, conforme mostrado na Fig.1.1.

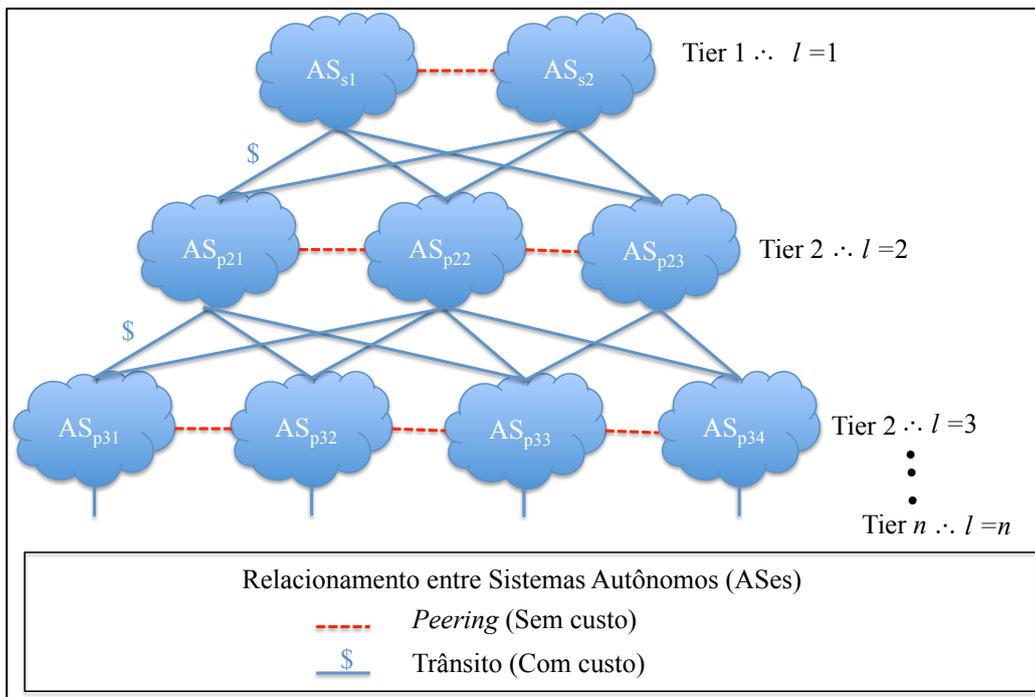


Figura 1.1 – Relacionamento entre Sistemas Autônomos

Ainda na Fig.1.1 observa-se que os relacionamentos entre sistemas autônomos podem ocorrer de duas formas principais, o *peering* e o trânsito. O trânsito tem um significado de venda de acesso a um *Tier-1* por um *Tier-2*, neste caso normalmente o relacionamento é de cliente com provedor. O *peering* é um relacionamento que ocorre normalmente entre *Tiers* de mesmo nível.

Observa-se que nada impede tecnicamente que um *Tier-1* estabeleça uma relação de *peering* com um *Tier-2* ou *Tier-3*. Mas em diversos países, devido a questões de regulação dos serviços de telecomunicações, se um dito *Tier-1* estabelecer um *peering* com um *Tier-2* ou menor, terá que fazer o mesmo para todos. Em todos os casos, uma empresa que atua na Internet sempre divulga suas políticas de interconexão e de entendimento e reconhecimento de nível. Em uma relação de *peering*, normalmente apenas as rotas internas dos sistemas autônomos são repassadas pelas sessões BGPv4 e v6. Isto ocorre quando um provedor quer evitar que um AS de menor porte venda serviços para um outro AS e use uma conexão de *peering* para o encaminhamento deste tráfego.

Em todos os casos de *peering*, o que vale é a negociação direta entre os administradores, portanto mesmo em um *peering* ASes que estejam por trás de um dos ASes pode ser

encaminhado, não existindo nenhuma restrição técnica para que isto ocorra, apenas de política. É importante notar que os acordos de *peering* ocorrem com mais facilidade se já existir uma conexão física. Os NAPs (*Neutral Access Points/Network Access Points*) ou PTT (Ponto-de-troca de tráfego) ou ainda IX (*Internet Exchange*) têm todos a mesma função que é a de gerar um ambiente com um comutador de nível 2 (*Layer Switch 2*) que conecta todos os participantes, conforme pode ser visto na Fig.1.2. Para aqueles que queiram trocar tráfego (*peering*) com todos os participantes, basta que se conectem ao servidor de rotas (*route server*) que estarão trocando rotas com todos os participantes.

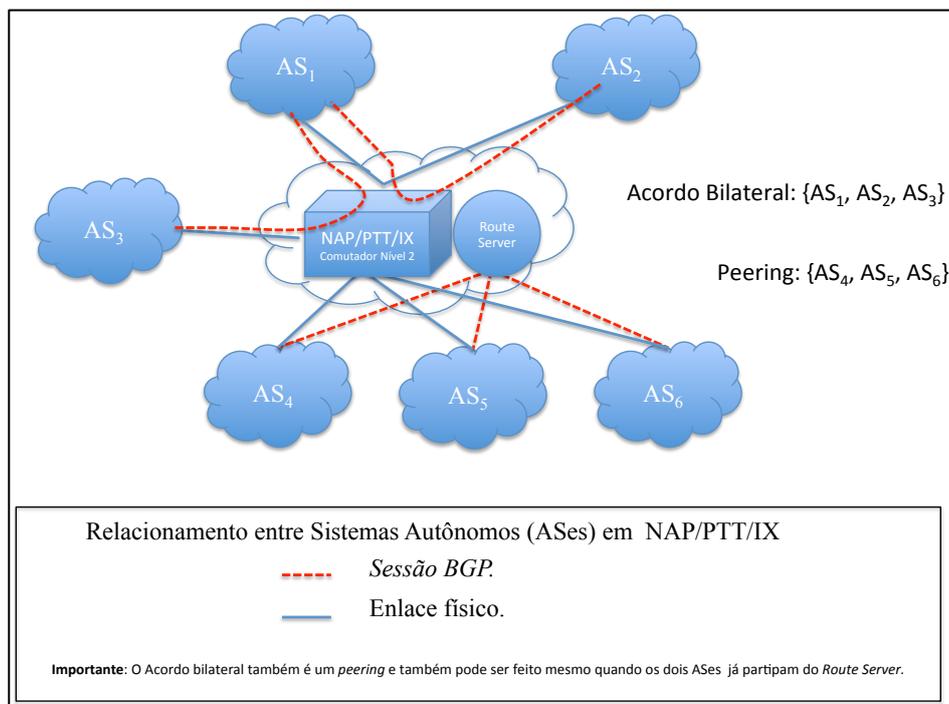


Figura 1.2 - Relacionamento entre ASes em um ponto de troca de tráfego.

Caso não desejem ter conexões de *peering* com todos os participantes, nenhum dos provedores de NAP/PTT/IX obriga esta condição. Para aqueles que tenham por política serem restritivos, pode-se usar os acordos bilaterais, ou seja, usando a mesma infraestrutura do comutador de nível 2, podem fazer conexões diretas, normalmente sem custo, com aqueles mais restritivos entre si. Esta descrição está relacionada apenas a questões de conectividade. Para o encaminhamento de rotas, cada AS pode trabalhar com uma forma distinta de prioridade nos parâmetros que regem o funcionamento do BGPv4 e v6.

Também é possível uma abordagem de estratificação da tomada de decisão em camadas, conforme Fig. 1.3, em que deve ser considerada a construção de uma política de troca de tráfego que será definida em função das necessidades e objetivos que a organização ou empresa tiver para o uso do sistema autônomo. Somente após a definição das políticas, será possível se definir ou se programar o nível tático.

É no nível tático que as ferramentas disponíveis serão usadas com o objetivo de se chegar a melhor decisão. Ou ainda aquela que consiga gerar a melhor eficiência possível de uso de recursos, que seja apenas por reprogramação dos recursos existentes ou ainda a pela realimentação do planejamento de longo prazo com o acréscimo de capacidade. No nível operacional a tomada de decisão poderá ser baseada na existência de problemas anteriores que possam ser usados como base de conhecimento e comparação para se encontrar uma solução adequada e atual para o problema ou ainda através da busca parcial ou cognitiva, quando não existir base de conhecimento com soluções anteriores que possam ser usadas como solução para o problema atual.

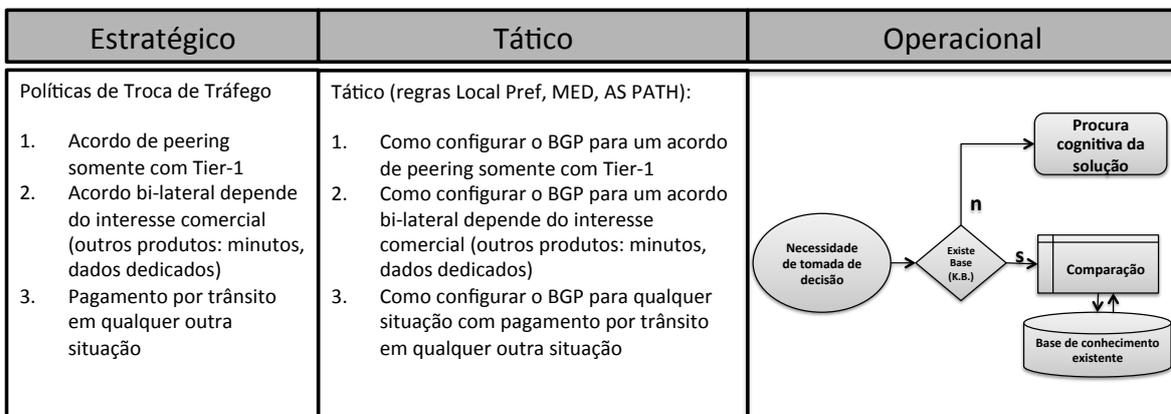


Figura 1.3 - Estratificação do processo de tomada de decisão com base em especificação de políticas, configuração de parâmetros.

No nível estratégico as políticas podem estar relacionadas com vantagens comerciais, menor preço, necessidade de interconexão física com restrições de atraso e perda de pacote, entre outros mecanismos que podem não estar relacionados com aspectos unicamente técnicos. É importante entender que o nível tático é programado seguindo as definições do nível estratégico e o processo de tomada de decisão do próprio BGP.

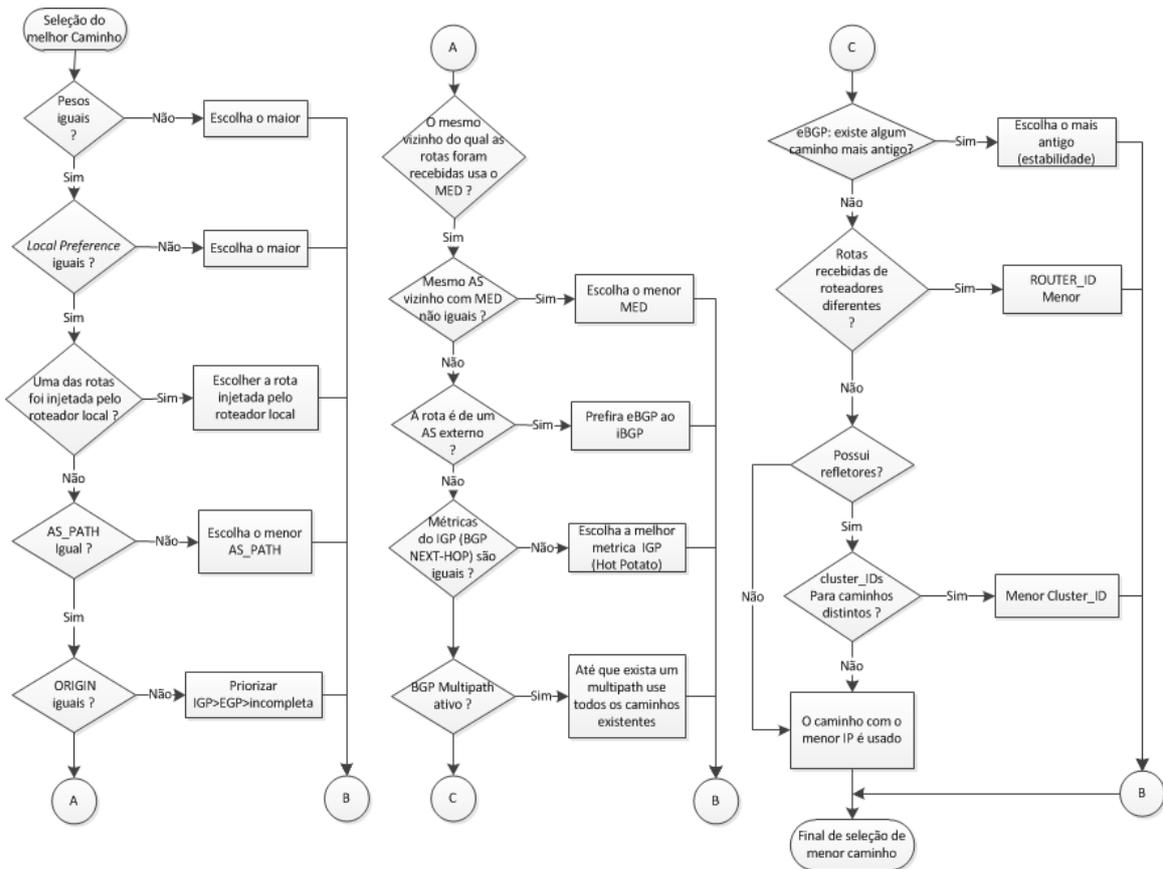


Figura 1.4 - Fluxo de decisão do BGP (Rekter, 2006)

Na Fig. 1.4, são apresentados os mecanismos do BGP que são levados em consideração para tomadas de decisão. O fluxo apresentado denota que quanto mais local, mais prioritário é o parâmetro. No caso, o peso das interfaces tem maior prioridade; em caso de empate, o próximo parâmetro é o LOCAL PREFERENCE; apenas em terceira opção vem o AS-PATH, que, por outro lado, é um parâmetro altamente utilizado para tentativas de influenciar a tomada de decisão de um AS externo ao do próprio domínio.

O parâmetro ORIGIN tem o objetivo de, mais uma vez, dar maior prioridade ao que foi aprendido localmente em detrimento do que foi aprendido externamente, ou seja, nesse ponto o IGP (Interior Gateway Protocol) tem mais prioridade que o EGP (Exterior Gateway Protocol). Por último, as rotas que estão com informação inconsistente ou incompleta.

O objetivo final é tratar mais rápido os aspectos carregados no nível operacional, de forma a devolver para a rede eficácia no uso dos recursos, informação para que a arquitetura da

rede possa ser influenciada de forma coerente e para que, nos próximos ciclos de crescimento, ocorra acerto das condições operacionais *versus* necessidades demandadas; e, ainda, que o nível tático e o estratégico possam, também, ter visão coerente da rede.

A Neutralidade de Rede é um assunto que vem sendo abordado de forma intensa nos últimos anos por diversos agentes. Em (Economides e Tåg, 2012), o assunto é discutido em seus aspectos econômicos e de mercado. O que de fato não poderia ser diferente, pois trata-se de uma condição a ser analisada na camada de estratégia da tomada de decisão, voltada para o negócio e não para os aspectos técnicos.

No trabalho citado, é mostrado um modelo com dois lados do mercado relacionado a Neutralidade de Rede. Um dos lados representa a visão dos provedores de acesso e o outro, dos provedores de conteúdo ou aplicativos.

Uma definição possível para a neutralidade de rede é a não cobrança de tarifas para provedores de conteúdo ou aplicativos em favor dos provedores de acesso. Além disso, há, também, a condição de não diferenciação do tráfego, por parte do provedor de conteúdo, em função do conteúdo ou aplicação. Esta poderia ser uma definição coerente para o termo Neutralidade de Rede. Ainda segundo a análise de (Economides e Tåg, 2012), existem efeitos positivos e negativos para neutralidade. Mas, ao final, trata-se de condição econômica e financeira.

Nesse ponto, é importante voltar ao básico da Internet. A Internet é baseada em padrões abertos; o protocolo que transporta todos os dados é o IP - *Internet Protocol* - (Postel, 1981), que, por definição, é baseado em melhor esforço - *best effort*. Uma operadora de Voz sobre IP ou de conteúdo de vídeo trabalha com aplicações que necessitam de controle de atraso e da variação deste (*jitter*). Portanto, o seu modelo de negócios é baseado em venda de serviços para uma rede que não foi projetada para tal finalidade, em princípio. A priorização dos serviços prestados na Internet é objeto de discussão contínua na comunidade acadêmica.

Em (Choi, 2010), é descrita uma análise em que os decisores políticos e regulatórios deveriam se focar em identificar os efeitos da neutralidade em curto e longo prazos. Um

efeito positivo, segundo os autores, é a possibilidade de se acabar com o monopólio em determinada região por um provedor de acesso, gerando a possibilidade para um duopólio, no mínimo. Por outro lado, em (Economides e Tåg, 2012), é demonstrado que os investimentos de cada um dos lados não podem ser esquecidos sob pena de inviabilizar a continuidade dos serviços básicos.

No Brasil, a regulação dos serviços e Neutralidade de Rede seguem uma discussão pouco voltada para as condições básicas de economia. Ou seja, quando se defende um provedor de conteúdo de menor capacidade ou menor capacidade financeira, o assunto toma, via de regra, uma direção pouco científica. Segundo (Cheng e Savage, 2011), um modelo bem estruturado deve ajudar na competitividade e melhorar as condições de compra do consumidor. Por outro lado, quando se analisa o posicionamento dos provedores de conteúdo, é importante destacar o tipo de concorrência.

No caso específico do provedor de conteúdo, observa-se que a dependência do provedor de acesso é algo natural, devido à natureza de suas funções. Em alguns países, a regulamentação das telecomunicações deixou evidente, incluindo a não possibilidade de competição entre o provedor de serviços de telecomunicações e o provedor de conteúdo ou aplicativos.

No Brasil, quando observado a regulação os serviços de telecomunicações no Brasil através do art. 60 da Lei n.º 9472, nota-se uma defasagem entre a descrição e definição legal para os novos serviços de telecomunicações ancorados no protocolo IP. As operadoras reguladas são responsáveis pelo conteúdo e pelo acesso, necessitando de grandes volumes de investimentos para chegar até o usuário final. Por outro lado, as operadoras não reguladas chegam até o usuário final sem a necessidade de cobrança pelo acesso, fazendo com que os seus preços sejam, em princípio, melhores para o consumidor, pois não precisam dispor de investimento para o acesso de seus clientes à rede.

Uma conclusão é que não existe infraestrutura se não existir um provedor que a faça e, para isso, é necessário um negócio que gere retorno. Portanto, qualquer regulação deve também prever uma concorrência leal nesse sentido, outrossim a balança estaria sendo manipulada para beneficiar um dos lados, nesse caso do provedor de conteúdo. Conforme observado

em (Cheng e Savage, 2011), a neutralidade de rede é algo mais complexo que a vontade de apenas um dos lados em se estabelecer acordos de interconexão ou uso de rede sem pagamentos entre as partes.

Ainda de acordo com (Economides e Tåg, 2012), é importante que qualquer solução regulatória que venha a acontecer de maneira definitiva leve em consideração os três lados (dois tipos de provedores e também o usuário final). Pois interessa ao usuário final ter continuidade e qualidade na oferta de serviços de acesso à Internet. Qualquer vantagem deve ser analisada sob a ótica econômica de curto e longo prazo.

Deve ser observado que provedores de conteúdo não regulados, quando reclamam de isonomia no tratamento do seu tráfego em redes de terceiros, não estão inserindo na discussão o fato que um provedor de acesso de TV a cabo (exclusivamente) esteja sofrendo também uma concorrência. É função do regulador entender as características de cada um dos provedores e, com base na natureza de cada um deles, dar condições iguais nas normas de convivência no mercado. Outrossim, apenas dando vantagem a um dos lados, tem-se o risco de ruptura na continuidade de qualidade na prestação dos serviços.

Ao se comparar uma empresa regional brasileira que fornece serviço de acesso à Internet com uma empresa virtual que fornece conteúdo, é necessário se observar que o tamanho e receitas devam ser comparados no seu aspecto global, não apenas local ou regional. Outro ponto importante é que o mercado local necessita de investimentos locais, sem os quais não existe acesso (Cheng e Savage, 2011). Se a questão é de livre concorrência, conforme definido na Lei que o provedor de conteúdo seja liberado para fazer a sua própria infraestrutura ou se associar a um provedor local ou regional.

Questões relacionadas a neutralidade de rede afetam a tomada de decisão no nível estratégico, pois trata-se da definição de cobranças por interconexão, priorização ou restrições relacionadas a conteúdo ou tipo de serviço ou usuário. No nível tático ou operacional, serão tratadas em acordo com a política definida no nível estratégico, portanto não sofrendo nenhuma alteração em termos práticos ou de relacionamento BGP.

Por outro lado, o modelo de negócios escolhido por cada um dos lados não pode ser objeto de julgamento. Se o modelo de negócios não inclui construir uma rede, que se coloque uma previsão de tecnologia que possa ultrapassar a barreira do incomum e utilizar a Internet de forma equiparável às demais. Caso contrário, é possível que, no limite, determinada empresa resolva distribuir conteúdo que necessite de altíssima quantidade de recursos e querer que as demais empresas gerem a rede para transportá-lo. Nesse caso, quem vai investir para que isso se torne possível, espera ter retorno. A abordagem relacionada à neutralidade de rede, pode vir a modificar todo o princípio de funcionamento da Internet.

2.2 PLANEJAMENTO E CONSTRUÇÃO DE REDES

A função do planejamento está inserida no processo de construção e manutenção das redes de telecomunicações. Dentro desse processo existem entradas, saídas, funções e objetivos. As funções necessitam de entradas de dados para poderem gerar informação que irão gerar suporte ao objetivo. No caso de uma empresa de telecomunicações, está sendo dado por se manter um ou mais serviços como objetivo final.

As demandas de serviço são as demandas por serviços de acordo com especificações de produto (Kotler, 1998) que, por sua vez, devem ser definidas de acordo com as especificações técnicas de determinada tecnologia. Caso isso ocorra, são evitados erros do tipo tempo de propagação nulo, o que normalmente impossibilita a manutenção de determinado serviço.

Na Fig.2.1 é mostrado o fluxo interno de diversas funções que devem compor uma empresa prestadora de serviços na área de telecomunicações ou redes. Por se tratar de uma operação, deve ser observada a existência de um processo contínuo para a manutenção de equipamentos que compõem uma rede de forma que os serviços possam ser suportados em conformidade com sua especificação. Na mesma figura existe uma trilha normal que envolve todo o ciclo de análise da demanda por serviços, contratação e operação. Porém, apenas esta trilha não é o suficiente para se resolver problemas relacionados a otimização de recursos, como proposta formal é inserida uma trilha de operação rápida. Não se trata de uma trilha de resposta reativa a problemas, ao contrário, visa a intervenção com base em análise dos dados extraídos da rede. Estes dados relacionados a tráfego e topologia

dinâmica (gerada pelo protocolo interno de roteamento) são caracterizados e após usados para a tomada de decisão em períodos curtos.

O inventário físico é a base instalada, no caso de redes existentes, de todos os elementos de rede ou suporte que a compõem. O inventário lógico diz respeito às configurações, topologias e modificações nos sistemas que visem a gerar, manter ou modificar os serviços que serão suportados.

A inovação é a entrada que garante continuidade na prestação dos serviços, pois evitará obsolescência e poderá incluir melhoria na prestação dos serviços que estão sendo suportados.

O custo de cada insumo deve ser conhecido de forma que seja possível o cálculo de retorno de investimento ou custo total de uma operação. Após o início da operação, será imprescindível que a rede seja monitorada a partir de amostras que sejam devolvidas ao ciclo de planejamento, de forma a ser possível estabelecimento de linha de base de comparação (PMBOK, 2012).

O ciclo de planejamento deve ser estabelecido para que seja possível, com base nas entradas, a execução dos projetos (PMBOK, 2012), observando que a previsão de recursos deverá também ser alimentada com o tempo de aquisição e construção de rede. Para serviços de telecomunicações, de forma geral, os tempos de construção são longos e podem ser um fator de perda de eficiência, pois, quando o problema de capacidade demanda novas construções ou lançamento de cabos, o tempo despendido pode ser superior a meses ou anos (Submarine, 2013).

Por esse motivo, a previsão de longo prazo deve ter em sua base alguma flexibilidade de forma a ser possível a otimização de recursos. Tanto configurações físicas quanto lógicas devem ser previstas no ciclo de planejamento de longo prazo.

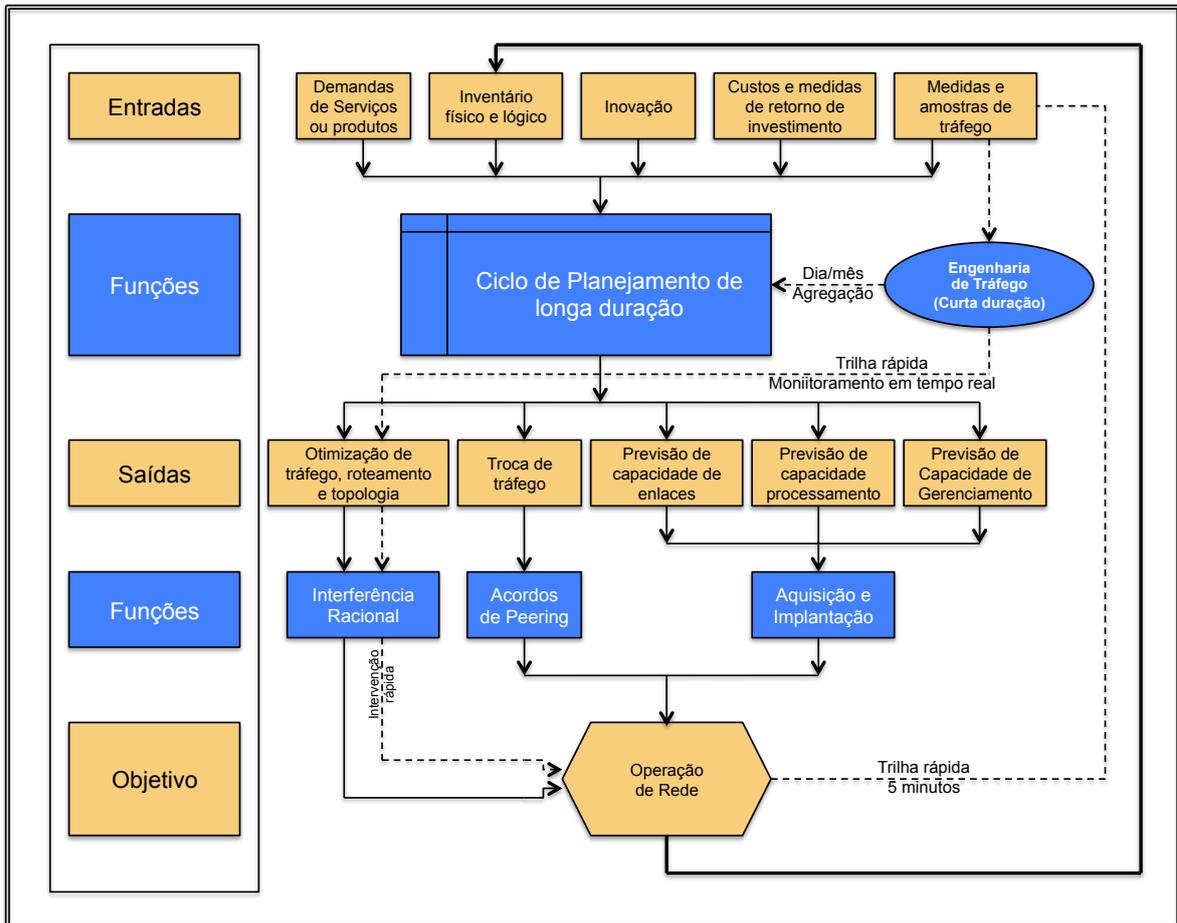


Figura 2.1 – Ciclo de planejamento de longo prazo com trilha rápida.

Como resultado do ciclo de planejamento, a otimização de recursos e topologia deverão ser saídas do processo de longo e, também, de curto prazo (trilha rápida), que pode ser observado na Fig.2.1, de forma a ser possível que os recursos existentes possam ser usados com a melhor eficiência possível.

Ainda como resultado das saídas, em se tratando de redes interconectadas, serão necessários que acordos de troca de tráfego com outras redes sejam estabelecidos e, de forma mais específica, também, acordos de *peering* para enlaces de interconexão de redes na Internet. As demais saídas são as previsões de capacidade, que, por sua vez, irão gerar novos projetos (PMBOK, 2012) e aquisições.

Este trabalho tem um foco na trilha rápida do processo de gerenciamento de uma empresa de telecomunicações. De acordo com (Winter, 2012), a atuação no processo de tomada de decisão das interconexões é de rápido retorno para a configuração e melhoria das

condições de uso da rede. Conforme mostrado na Fig. 2.1, as modificações ocorridas em curto prazo ou em função do retorno gerado pela trilha rápida irão modificar o planejamento do crescimento das redes em longo prazo.

O ciclo de operações é uma atividade contínua, não se enquadrando na definição de projeto (PMBOK, 2012), e, devido a isso, tem a necessidade de controle constante, nesse caso as realimentações ocorrerão em longo e curtíssimo prazo, fazendo com que o sistema atinja um equilíbrio entre as necessidades dos serviços e a quantidade e qualidade dos recursos disponibilizados.

2.3 USO EFICAZ DE RECURSOS

De acordo com (Cheng, 2012), uma questão que precisa ser analisada é o quão eficaz é o uso dos recursos disponibilizados para a formação de uma rede e isso é verificado na distribuição de uso dos recursos que formam a rede. É evidente que a área que é responsável por operar uma rede de telecomunicações tem esse objetivo, porém as informações de monitoração devem transitar em todas as áreas e devem seguir um fluxo, tal como aquele mostrado na Fig. 2.1.

No trabalho de (Wang *et al*, 2007) e (Winter, 2012) são apresentados problemas relacionados a tomada de decisão em situação de necessidade de interferência em ambiente não controlado por políticas, sob domínio do tomador da decisão. Entende-se como política um conjunto de ideias ou regras, usadas dentro de um sistema autônomo, de comum acordo pelos responsáveis pelo mesmo objetivando a sua administração.

Para este trabalho, dentro do ciclo operativo de planejamento, está sendo prevista uma interferência inteligente no processo de otimização de topologia e roteamento, visando principalmente a melhoria das condições de troca de tráfego entre operadoras, mas também à resolução de problemas de interferência em sistemas autônomos (AS), com fonte de tráfego distinto e na existência de assimetria de tráfego. Ainda nos mesmos trabalhos, fica claro que o *backbone* de qualquer grande provedor de serviços de rede Internet é susceptível a perdas. Para que ocorra perda de pacotes, basta que uma ruptura ocorra em um ponto onde a demanda esteja sendo tratada mesmo que de forma eficaz, porém sem

redundância. Mas, sem dúvida, um dos maiores problemas relacionados a perdas em *backbones* é o MTU (*Maximum Transmission Unit*).

Durante a fase de treinamento, todos os protocolos de nível superior deveriam fazer um teste fim-a-fim, antes de encaminhar os pacotes, somente o teste já seria computado como erro, este seria armazenado na MIB de sua interface (*Management Information Base*), porém muitos não fazem o teste completo e encaminham pacotes com MTU maior que o máximo permitido pelas interfaces de nível 2 (Modelo OSI). Na Fig. 2.2, é possível se observar uma coleta indicando a origem de erros coletados. O MTU é causa de 23,3% dos erros enquanto o roteamento gera 71,23% de perdas. Outros erros, relacionados a má formação dos pacotes e problemas nos sistemas de transmissão estão relacionados às causas especificadas em 5,57% dos casos. Essa coleta foi realizada em uma rede de grande operadora internacional em 12/5/2015.

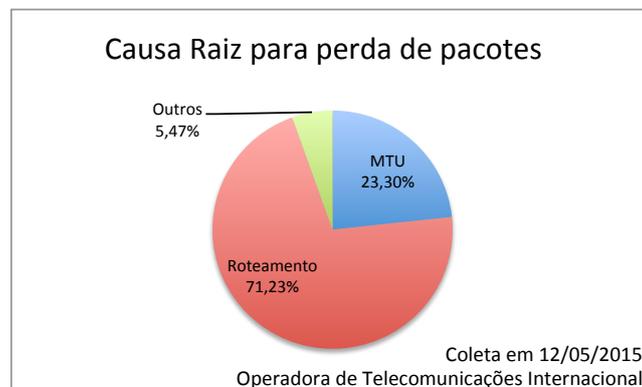


Figura 2.2 – Causa raiz para perda de pacotes.

Na Fig.2.3, é possível se observar que o tamanho máximo de pacote permitido e usual na Internet é inferior a 1.500 bytes. No entanto é comum observar protocolos que tentam usar pacotes com quantidades de *bytes* superiores. Em acordo com (Eittenberger *et al.* 2013), esses protocolos são normalmente usados em aplicações onde o tamanho do pacote gera uma economia substancial no total transmitido quando se compara o cabeçalho (*header*) com o conteúdo (*payload*).

Ainda em acordo com (Albanese *et al.*, 2015), o uso de redes CDN (*Content Delivery Network*), sistemas de *Backup* (cópias de conteúdo) ou vídeo tendem a gerar mais necessidades de uso pacotes com tamanho superior a 1.500bytes. Estas alterações de

tamanho são dependentes do tipo de aplicação e serviços e devem também ser levadas em consideração no processo de análise da tomada de decisão.

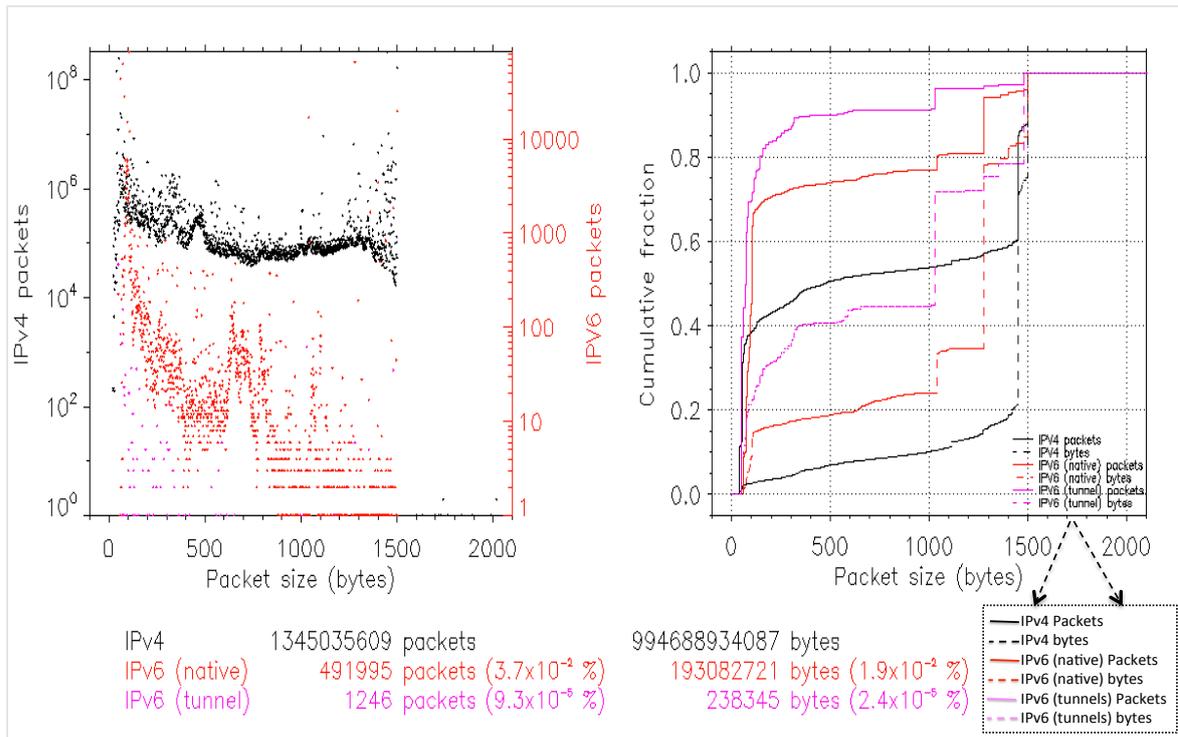


Figura 2.3 - Arquivo equinix-chicago.dirA.20150319-130000.UTC. Coletado em www.caida.org em 14/05/2015.

Ao final, tomar decisões faz parte de qualquer processo humano, incluindo o que ocorre dentro de organizações (Kotler, 1998). Faz-se necessário que a tomada de decisão possa ser vista como algo, além de natural, também possível de ser mensurada dentro de um processo que possa ser mapeado (Bang *et al.*, 2014). O BGP é dominado por tomada de decisão parametrizada por relacionamentos, isso gera a necessidade de entendimento do processo decisório de relacionamento entre empresas.

No trabalho (Epstein e Buhovac, 2014), a estratégia de decisão é relacionada com o grau de recompensa, incorporando condições políticas ao processo, naquele caso aplicado a sustentabilidade, o que também pode ser usado para se comparar com as vantagens de se manter relações de confiança com todos os que estão presentes na Internet. Nesse ponto fica claro que a tomada de decisão em relacionamentos de troca de tráfego, na prática, não leva em consideração apenas a melhor condição técnica relacionada com o atraso, número de saltos, variação do atraso e perdas de pacotes. A mitigação de problemas relacionados a desempenho entre sistemas autônomos (ASes) é um problema político. Em (Hall *et al.*,

2014), o relacionamento para o atingimento de metas de desempenho e sobrevivência é tratado como fundamental, chegando ao ponto de ser comparado com a necessidade de se “colaborar com o inimigo”.

Quando a mitigação de algum problema de desempenho ocorre por assimetrias o problema assume uma importância maior em termos de relacionamentos políticos, mais especificamente no caso do BGP (Winter, 2014). A solução para o problema, ou até mesmo a sua mitigação, não está sob controle do proprietário do recurso, assim o seu grau de influência na tomada de decisão é secundário; apesar de ser o mais interessado, não tem controle sobre a própria tomada de decisão.

Apesar de todos esses aspectos que dificultam a mitigação dos problemas, é interessante notar que na grande maioria dos sistemas autônomos, conforme será mostrado em estudo específico relacionado ao uso do *prepend* (AS-PATH), boa parte dos partícipes na Internet têm interesse em colaborar. Assim, o desenvolvimento de estratégias para a otimização no uso de recursos convém e pode ser usada (Winter, 2012).

Na Fig. 2.1, é apresentado um fluxo de curto prazo. Esse fluxo é responsável por monitorar e levar a rede a um ajuste que conduza todo o processo à maior eficácia no uso dos recursos. O controle de tráfego é um desafio importante na operação de redes Internet, assumindo nesse trabalho um alto grau de relevância.

2.4 RELAÇÃO COM O MODELO SDN

De acordo com (Verdi *et al.*, 2006), o modelo SDN (*Service Delivery Network*) evidencia o serviço como o mais importante fator a ser considerado na concepção, construção e operação dos ambientes de prestação de serviços.

Na Fig. 2.4, é apresentado um modelo de arquitetura SDN (*Software Defined Networks*) que pode retratar esta tentativa crescente em se automatizar o controle e o gerenciamento completo das redes (Akildiz *et al.*, 2014). O modelo é descrito em três camadas, aplicação, controle e plano de dados. Na camada de aplicação são apresentados os serviços e especificadas as interfaces para o usuário final, neste caso um demandante por um

equipamento virtualizado, como exemplo um roteador. O plano de controle é sustentado por uma aplicação que irá possibilitar o compartilhamento de uma infra-estrutura física que é descrita na camada do plano de dados. Nessa arquitetura, a proposta inclui a possibilidade de aplicações comerciais serem capazes de acessar os recursos de rede para a configuração de serviços diretamente, além das aplicações SDN para processos de engenharia de tráfego, virtualização, garantias de qualidade, monitoração e roteamento.

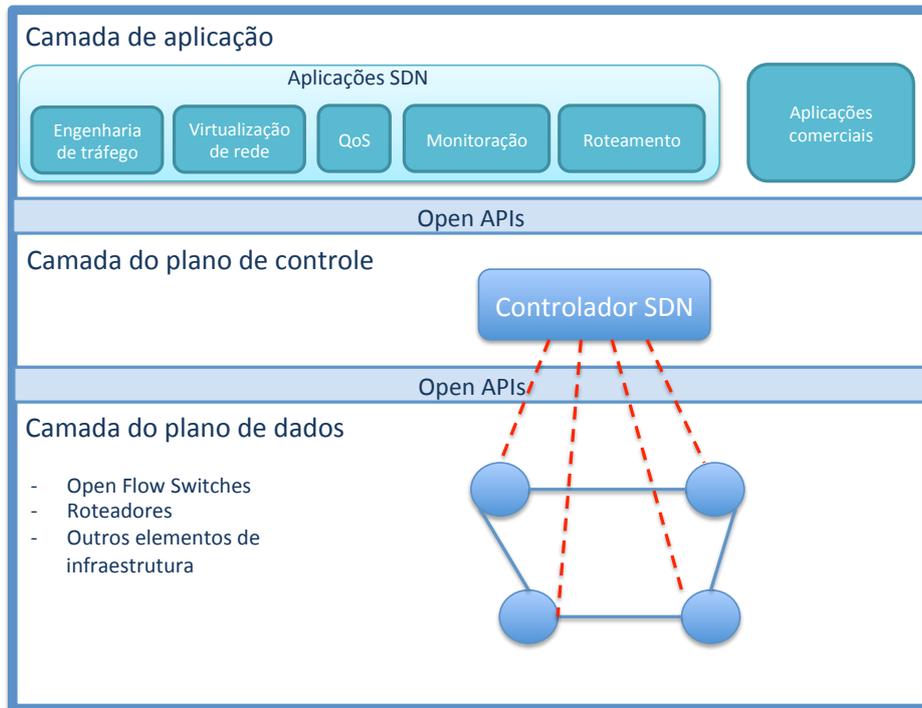


Figura 2.4 – Arquitetura SDN, adaptado de (Alkildiz *et al.*, 2014).

Um aspecto importante a ser abordado é o fato de a arquitetura não substituir o processo de tomada de decisão. A automatização de um processo manual carregará todos os aspectos funcionais e operacionais do mesmo (Fisher, 2014). Por este motivo, é necessário que o processo de automatização possua um processo de inteligência e filtragem de opções (Ghattas *et al.*, 2014). Em um ambiente de tomada de decisão, o excesso de informação também pode ser um problema tão grande quanto à sua falta (Ratnan *et al.*, 2014). A arquitetura SDN pode ser usada para a melhoria das condições gerais do conhecimento e rapidez no controle das informações, porém não irá melhorar o processo de tomada de decisão se este não estiver adaptado ao oferecimento dos requisitos necessários.

Dentro do processo de gerenciamento das interconexões entre sistemas autônomos, o uso da arquitetura SDN é importante para a efetivação rápida, porém essa arquitetura não pode ser vista como simples incorporação da automatização de qualquer processo. A filtragem das opções é fundamental. Na Fig.2.3, é apresentado um fluxo considerando essa necessidade.

Um ponto importante nessa abordagem é a tentativa de substituição dos processos manuais por processos automatizados. O grau de automatização, uma das bases do modelo, é muitas vezes usado para a definição do grau de sucesso na sua implementação. No entanto, o sucesso do modelo, ainda segundo (Verdi *et al.*, 2006), está relacionado não apenas com a automatização mas pela sua concepção, mesmo que manual de funcionalidades que atendam às necessidades dos usuários ou clientes. A SDN pode ajudar na solução do problema de assimetria de tráfego, pois o gerenciador de uma rede presente no Brasil poderia ter a possibilidade de ter um roteador virtual nos Estados Unidos da América e assim poder controlar o seu tráfego de forma mais direta mais próximo da origem, caso a origem esteja neste mesmo país. Desta forma, o tráfego entre os Estados Unidos da América e o Brasil estaria presente dentro do AS sendo controlado pelas mesmas políticas.

Em (Winter, 2012), é observada uma tentativa de solução para a necessidade do usuário de manipular seu fluxo de dados que consiste em modificar o protocolo inserindo um parâmetro de preferência por origem a ser considerado pelo BGP. O processo definido por (Winter, 2012) pode ser considerado um processo de tomada de decisão distribuído, pois não há um único ponto onde os parâmetros são analisados e em que se define como cada nó de roteamento irá encaminhar os pacotes. No trabalho de (Wassim *et al.*, 2014), é inserida uma solução baseada na centralização da tomada de decisão, gerando um serviço específico de controle centralizado do BGP pela operadora. Por outro lado, em (Bekkers *et al.*, 2011), é evidenciado que probabilidade de sucesso de uma nova tecnologia ou modificação desta tem relação muito forte com a compatibilidade. Ainda segundo (Bekkers *et al.*, 2011), no caso de qualquer modificação em um padrão ou protocolo altamente difundido, as chances de sucesso diminuem quando uma solução exige grandes alterações.

Em (Akyildiz *et al.*, 2014), é observado que a simples substituição do processo manual por um procedimento automatizado não deve ser o objetivo de nenhum sistema, pois a automatização de qualquer processo que seja falho muito provavelmente também falhará. Antes de se propor qualquer alteração nos modelos existentes, é necessário uma análise detalhada das vantagens de se modificar as características atuais, levando-se em consideração se a tomada de decisão ocorrerá de forma distribuída ou centralizada. De acordo com (Verdi *et al.*, 2006), o modelo SDN traz diversas bases que permitem o foco no serviço e no usuário final, porém é importante que o processo que estiver sendo mapeado tenha sido muito bem descrito sob o ponto de vista das expectativas que os usuários possuem sobre o mesmo, além disso deverá ser caracterizado matematicamente por um modelo que possa ser usado para previsões futuras.

O grau de dificuldade de se encontrar uma solução para um problema também pode ser relacionado com a quantidade de entradas em um sistema de tomada de decisão (Charnes *et al.*, 1978). O uso de parametrização para o estudo da tomada de decisão é um ponto de partida interessante para que a decisão possa ser estudada, por outro lado é necessário que a metodologia possa convencer que sua aplicação irá gerar resultados melhores com o seu uso. Ainda em (Charnes *et al.*, 1978) é observado que diversas características naturais, tais como o valor econômico, apresentam características duais ou que representam mais de um parâmetro.

Por este motivo, ao gerente do processo é cabido se contentar com a relativização da eficiência. Ou seja, mesmo quando, em função de uma necessidade de atingimento de metas, ficar claro que é necessário determinado investimento, nem sempre a solução que irá ser considerada pelo tomador de decisão (ou gerente) será esta.

O grau de satisfação (Charnes *et al.*, 1978) está relacionado a diversas caracterizações de atividades naturais, como exemplo a escolha de uma rota pelo roteador com o auxílio do BGP. Essa escolha pode ser influenciada pela política interna do AS e esta pode estar relacionada a condições de desempenho, mas também de concorrência. Sem dúvida, são condições que se contrapõem e em muitos casos o uso da programação não linear será obrigatório, pois não há, nesses casos, outra forma de se caracterizar o processo.

Na Fig. 2.5, ainda é importante notar que é necessário que se faça uma análise da possibilidade de se alcançar uma meta. Se para o tomador de decisão a função custo econômico, bem como o desempenho (atraso, *jitter* e perda de pacotes), tem importância mas fatores relacionados com a concorrência entre empresas é também importante, ao final, a caracterização tem a sua complexidade aumentada.

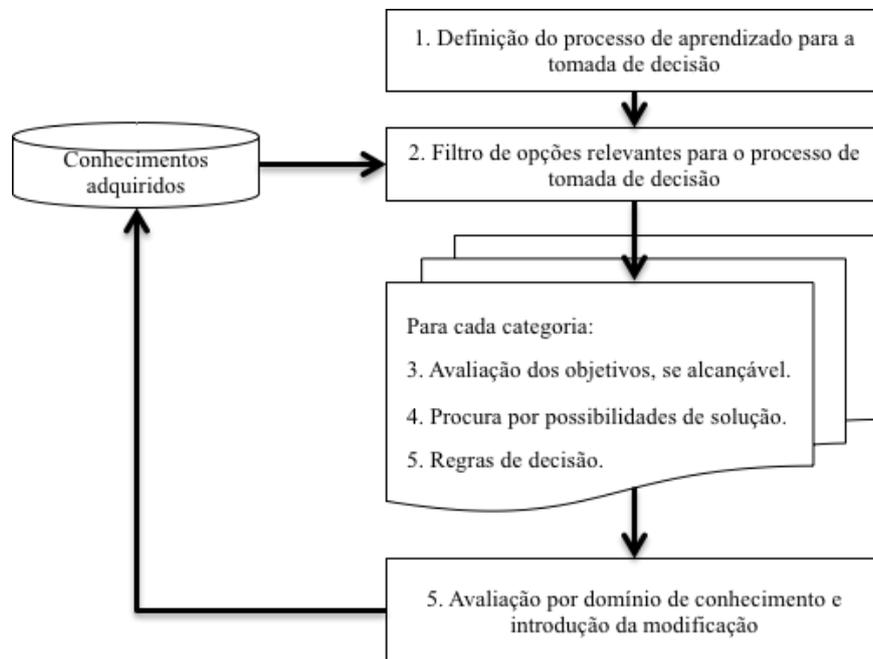


Figura 2.5 – Tomada de decisão. Adaptado de (Ghattas, 2013).

2.5 CONCLUSÃO DESTE CAPÍTULO

O planejamento de uma rede de telecomunicações deve levar em consideração os aspectos construtivos da rede sob o ponto de vista técnico, porém sem deixar de lado os aspectos econômicos. Nesse capítulo, o ciclo de planejamento foi analisado de forma a identificar as principais ações na fase de planejamento, quando a rede pode ainda não existir, passando pelas fases de projeto e implantação quando o planejamento de rede é de longo prazo.

Algumas redes de telecomunicações (satélite, empresas de cabos ópticos submarinos internacionais) podem precisar de anos para terem um projeto concluído, daí a necessidade do planejamento de longo prazo refletir às expectativas técnicas e econômicas. Porém, mesmo quando o planejamento é eficaz, devido a mudanças naturais em termos de novos

serviços, movimentação de demandas de clientes ou novas tecnologias, entre outros, faz-se necessária uma constante monitoração com possibilidade de alterações em curto prazo, de forma a reestabelecer a eficácia no uso dos recursos de rede.

No próximo capítulo, as definições relativas a caracterização do tráfego, definição do tipo de serviço e como utilizar estas informações para melhorar o processo de tomada de decisão serão apresentadas.

3 CARACTERIZAÇÃO E DEFINIÇÃO DE SERVIÇO

A diversidade de serviços presentes na Internet é dicotômica, por um lado essencial para o crescimento e abrangência, pelo outro um excelente desafio para a engenharia e racionalização do uso de recursos. Segundo (Postel, 1980) a Internet é um ambiente que foi desenvolvido para ser usado, basicamente com pacotes de dados (Kleinrock, 1960) e principalmente baseado em “melhor esforço” e hoje a melhor opção de comunicação no sentido da unificação dos serviços em uma única rede. De acordo com (Courcoubetis *et al.*, 2014), os benefícios que a integração dos serviços possibilita são ligados ao crescimento e à facilidade de desenvolvimento de novos serviços (Xu *et al.*, 2014). Para (Droms *et al.*, 2014), este crescimento pode ocorrer baseado em protocolos existentes ou com a criação ou modificação de protocolos, mas não pode deixar de ser compatível com aqueles existentes em algum nível, pois, de outra forma, o sucesso do novo serviço pode ser comprometido.

Exemplos de compatibilidade e inovação são os serviços Skype (Skype, 2014) e NetFlix (Netflix, 2014) em que a condição da rede é sempre testada de forma que o serviço possa ser adaptado às condições momentâneas da rede, podendo ser com o sem vídeo para o Skype e variando de baixa a alta resolução para o Netflix, porém sem deixar de ser compatível com os protocolos utilizados pelos serviços. Segundo (Fallon e O’Sullivan, 2014), a adaptação traz uma condição diferente daquela conhecida nos sistemas de telecomunicações, onde o operador de rede detém o controle completo da qualidade fim-a-fim.

Ainda segundo (Fallon e O’Sullivan, 2014), a inteligência do processo é dada em função da sua própria deficiência, ou característica básica, que é a de não garantir o atendimento a todos os usuários ao mesmo tempo. Aliás, condição que também é dada para as redes legadas, porém com a diferença do bloqueio na entrada. De acordo com (Brewka *et al.*, 2014), o fato de não se bloquear o acesso do usuário ao serviço na entrada traz a impressão da disponibilidade completa, para qualquer serviço. De acordo com (Brewka *et al.*, 2014), o não compartilhamento é um erro, pois a essência de uma rede é o compartilhamento e, se não há compartilhamento por parte dos usuários, não tem como haver comunicação. Em

(Ghezzi, 2014), observa-se que um dos maiores problemas encontrados quando do acesso a redes de comunicação é a correta adequação do grau de serviço e de qual tipo de serviço e requisitos serão necessários para suportá-los.

Por um lado, o provedor de serviços pode estar cometendo um erro ao induzir o usuário pensar de forma simplificada. Por outro lado, a informação relacionada a velocidade do acesso ou consumo de bits ou bytes de informação, pode não ter significado para o usuário final. De acordo com (Go *et al.*, 2014), quando um serviço móvel fornece a informação de quantidade de bytes ou de velocidade (quantidade de bits por segundo), apenas considerando a bilhetagem ou cobrança do serviço através de uma conta, o usuário do serviço tem dificuldade de entendimento com relação ao serviço contratado.

Segundo (Ravindranath *et al.*, 2014) vender bits por segundo ou quantidade de bytes não denota diretamente qualidade. Apesar disso, quando um provedor de serviços planeja a sua rede é imprescindível que o conhecimento do funcionamento de cada um dos serviços, do nível de serviço acordado e quantidade de usuários distribuídos geograficamente. Além disso, a caracterização do funcionamento da rede é também fundamental, de forma a ser possível se reproduzir o comportamento em simulações e com isso poder melhorar o nível de assertividade no planejamento de recursos físicos.

A busca por modelos matemáticos que sejam adequados deve ser contínua. No momento diversos trabalhos, como em (Leland, 1994) e (Barreto, 2007), demonstram que o modelo de Poisson não tem aplicação coerente para estimativas futuras ou planejamento de redes de pacotes, sendo o modelo Auto-Similar e o Multifractal ou de Dependência de Longa Duração – DLD – (Behdin, 2013) mais adequados, contudo novos estudos demonstram a necessidade do conhecimento da “impressão digital” por aplicação e por usuário, conforme demonstra (Petkov, 2013) em uma abordagem de estimativa do parâmetro de entropia, ligando este a cada aplicação.

Uma característica abordada por esses autores diz respeito a não apenas trabalhar com o conhecimento do tráfego agregado, mas principalmente conhecer a fonte para melhorar o conhecimento, sempre mais próximo da origem, das necessidades de cada usuário. Para o planejamento de recursos do lado do provedor, diversos trabalhos recentes denotam a

possibilidade de uso do modelo Auto-Similar e Multifractal ou de DLD com resultados promissores (Barreto, 2007).

O objetivo deste capítulo é entendimento dos modelos que melhor representam o comportamento do tráfego. Através desse entendimento pode-se caracterizar e utilizar a base matemática para previsões em planejamento de longo ou curto prazo.

3.1 O TRÁFEGO

Da mesma forma que em uma abordagem de um sistema de tráfego de veículos, onde o conhecimento da movimentação dos veículos irá definir a necessidade de novos recursos de infraestrutura, em um sistema de telecomunicações ou redes Internet pode ser usada uma abordagem parecida. Observando as distâncias envolvidas, número de faixas, quantidade de cruzamentos entre vias e sistemas de comutação (sinais de trânsito, viadutos, pontes, entre outros) respectivamente pode-se visualizar um paralelismo entre as distâncias dos nós, banda ou velocidade em bits por segundo e quantidade de interfaces, poder de processamento de pacotes.

De qualquer forma, o conhecimento do comportamento natural deve ser o principal dado de entrada para que se encontre um modelo matemático que possa explicar o comportamento do processo natural, de forma coerente. De acordo com (Takine, 2004), sem isso, o modelo não pode existir. De acordo com o trabalho (Garcia-Dorado *et al.*, 2011) o grande desafio no caso da Internet é que o modelo não pode ser estático, dada a grande quantidade de novos serviços que nascem a cada dia e que influenciam diretamente o comportamento das redes que a compõem.

E mais ainda, não pode ser um modelo simplista, que apenas leve em consideração um crescimento linearizado ou ainda seja levado a consequência mais imediatista de superdimensionamento. De acordo com o trabalho (Bitar *et al.*; 2014), em qualquer caso, sub ou superdimensionamento são prejudiciais, pois não geram base para que o planejador possa calcular a quantidade de recursos é de fato necessária para o correto suporte ao produto ou serviço comercializado.

Por outra abordagem, uma grande vantagem das redes Internet é a capacidade de integração de serviços multimídia. Porém em (Bitar *et al.*; 2014) esta mesma vantagem é questionada sob o ponto de vista de planejamento de recursos quando não se pode determinar de fato se os recursos estão de fato sendo aproveitados, porém inquestionável em termos de integração e novas possibilidades de serviços.

De acordo com a abordagem *per flow* apresentada em (García-Dorado *et al.*, 2011), em termos de caracterização, o que foi vivenciado na Internet, caso ocorresse em sistemas de transporte seria algo parecido com integrar em uma mesma pista o trem, o avião, o navio, a nave espacial e também o automóvel pessoal. De uma forma geral não poderia ser realizado no sistema de transporte público, mas o foi na Internet. Quando no trabalho de (Kleinrock, 1962) a comutação por pacotes foi desenvolvida não se sabia onde ou como poderia ser usada. Seguindo toda a evolução da comunicação por pacotes, tem-se um momento em que o conhecimento para a caracterização do tráfego se faz necessária. Esse conhecimento é importante para a qualidade dos serviços e possibilidade de planejamento e operação.

3.2 A NATUREZA ASSIMÉTRICA DO TRÁFEGO E IMPLICAÇÕES

Em (Woodward *et al.*, 2013), para o caso dos enlaces de dados, tem-se uma condição de assimetria a ser estudada em relação ao seu uso em interconexões. Apesar da maioria dos padrões especificarem ou considerarem o uso simétrico dos recursos disponíveis entre as interfaces dos nós de redes interconectadas, percebe-se que nem sempre isso é possível. De acordo com (Adibi *et al.*, 2013) é possível notar que no acesso existe a possibilidade do uso assimétrico - *ADSL – Asymmetric Digital Subscriber Line* ou nas tecnologias emergentes incluindo aquelas de acesso móvel, onde o encaminhamento de dados para o lado do usuário é sempre maior.

De acordo com (Haucap e Heimeshoff, 2014), não apenas por este motivo, mas também devido a concentração de conteúdo em determinados ASes nos Estados Unidos. Isso pode ser verificado na Fig. 3.1 onde é mostrada a diferença entre o *inbound* e o *outbound* no

tráfego entre os Estados Unidos da América (EUA) e a América do Sul através de medidas de tráfego real realizadas em provedor internacional.

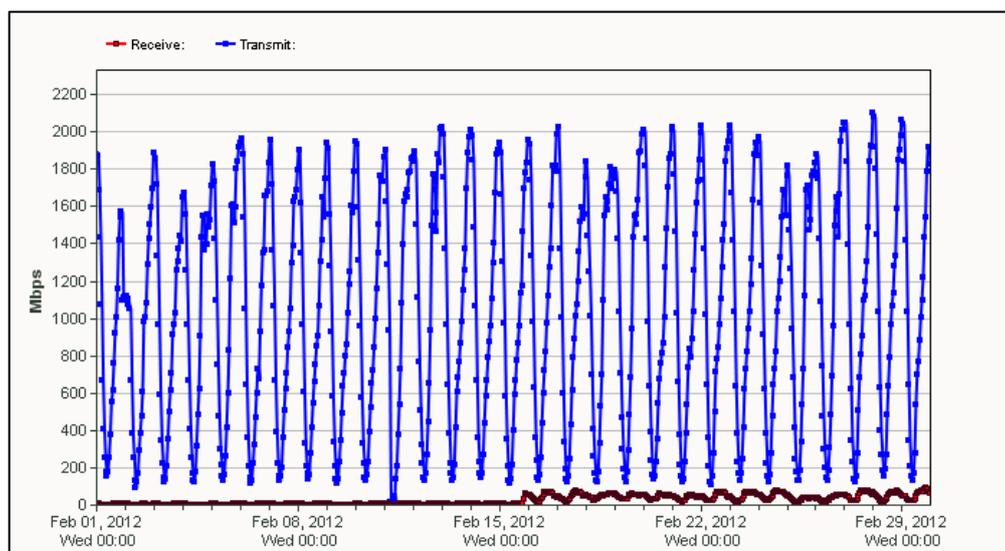


Figura 3.1 - Tráfego entre os EUA e o Brasil, valores divididos por n , em que $n > 1$ devido a acordo de não declaração de origem NDA - non-disclosure agreement . maio, 2012.

O tráfego mostrado na Fig.3.1 é uma amostra similar àquela encontrada em (Taquq *et al.*, 1997). De acordo com (Winter, 2012), a tomada de decisão para a modificação da topologia com assimetria, que estiver sendo descrita pela tabela de roteamento Internet, dependerá fortemente de decisão externa. Todas as amostras aqui apresentadas foram testadas e são compatíveis com a distribuição Gaussiana.

O uso assimétrico dos recursos de banda, poderia ajudar na solução do problema da assimetria do tráfego. Com base no trabalho de (Chamania e Jukan, 2014), os recursos de banda de transmissão e recepção em situação diferente da simetria, poderiam ter utilizações diferentes daquelas em uso pelos padrões IEEE (1000BaseX, 10GBaseX, 40GBaseX, 100GBaseX) ou ITU (SONET/SDH). Para esses casos a alteração da utilização do espectro poderia ser flexível e configurável. Isso poderia fazer com que um enlace de 10Gbps (10Gbps TX e 10Gbps RX) pudesse trabalhar em por demanda inteligente.

Dessa forma, em alguns momentos poderiam ser usadas características de assimetria. Nesse caso, apenas diferenciando-se do ADSL devido a inteligência que seria necessária para manipular a banda em função da demanda de TX ou de RX. Para isso a abordagem

uma abordagem similar a encontrada em (de Cola *et al.*, 2014) entre camadas – *cross layer*, seria necessária. Pois nessa situação, o tráfego presente no nível 3 do modelo OSI teria uma influência direta no nível 1 e 2 do mesmo modelo.

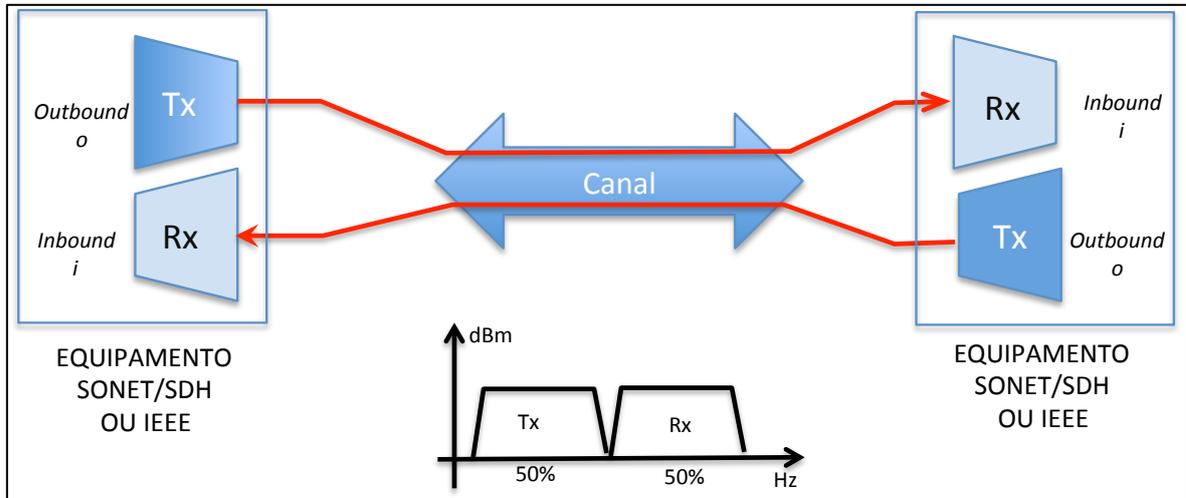


Figura 3.2 - Diagrama de uma conexão entre dois nós de comunicação com utilização simétrica do canal.

Na Fig. 3.1. tem-se uma representação de equipamento com uso simétrico de recursos de transmissão e recepção. Nesse caso, quando existe qualquer desbalanceamento entre a quantidade de informação em bits que está sendo transmitida na direção contrária o fator de utilização total - F_{ut} - será prejudicado.

O F_{ut} é definido como a diferença entre o percentual transmitido com o recebido nas direções inbound e outbound, aqui levando em consideração apenas a interface.

$$F_{ut} = \left(\frac{o}{i + o} \right) - \left(\frac{i}{i + o} \right) \quad (3.1)$$

O F_{ut} é será nulo quando o sistema estiver em equilíbrio, tenderá para o desequilíbrio *inbound* ou *outbound* sempre que o tráfego for maior em um dos sentidos.

Em (Chamania e Jukan, 2014) é testada a possibilidade de se alterar dinamicamente a definição de utilização de banda do canal em função da caracterização e predição de uso futuro daquele enlace, envolvendo todos os nós correspondentes a essa conexão fim-a-fim.

Na Fig.3.3 (b) tem-se uma condição onde o tráfego deixou de ser simétrico, com *inbound* na interface superior à capacidade da mesma, desta forma o excedente é perdido caso não seja possível acomodá-lo ou adapta-lo ao canal. A proposta deste trabalho, descrita de forma análoga em alguns aspectos em (Chamania e Jukan, 2014) leva em consideração o uso de um processo de predição interface-a-interface. Esse processo será melhor detalhado a seguir, com a possibilidade de alteração dinâmica do uso do canal fim-a-fim.

A solução levaria a um nível de otimização constante dos recursos, atualmente, fixos nos casos de interfaces simétricas. Observa-se que essa condição de otimização somente seria válida se novos padrões fossem inseridos para a redefinição dos processos de comunicação de interfaces simétricas.

Essa proposta, assim como aquela descrita por (Chamania e Jukan, 2014), leva em consideração a necessidade de se modificarem padrões. Dessa forma, faz com que sua aplicação não ocorra até que seja provado sua viabilidade econômica. Outro ponto importante é a necessidade de que um processo de coleta e processamento de dados ocorra em tempo real de forma a possibilitar a predição de uso.

Essa necessidade significa que o uso específico somente ocorrerá se existir um protocolo fim-a-fim em todo o caminho em que as interfaces estiverem conectadas de forma a modificar todo o perfil dos canais que estiverem envolvidos na conexão do enlace em questão.

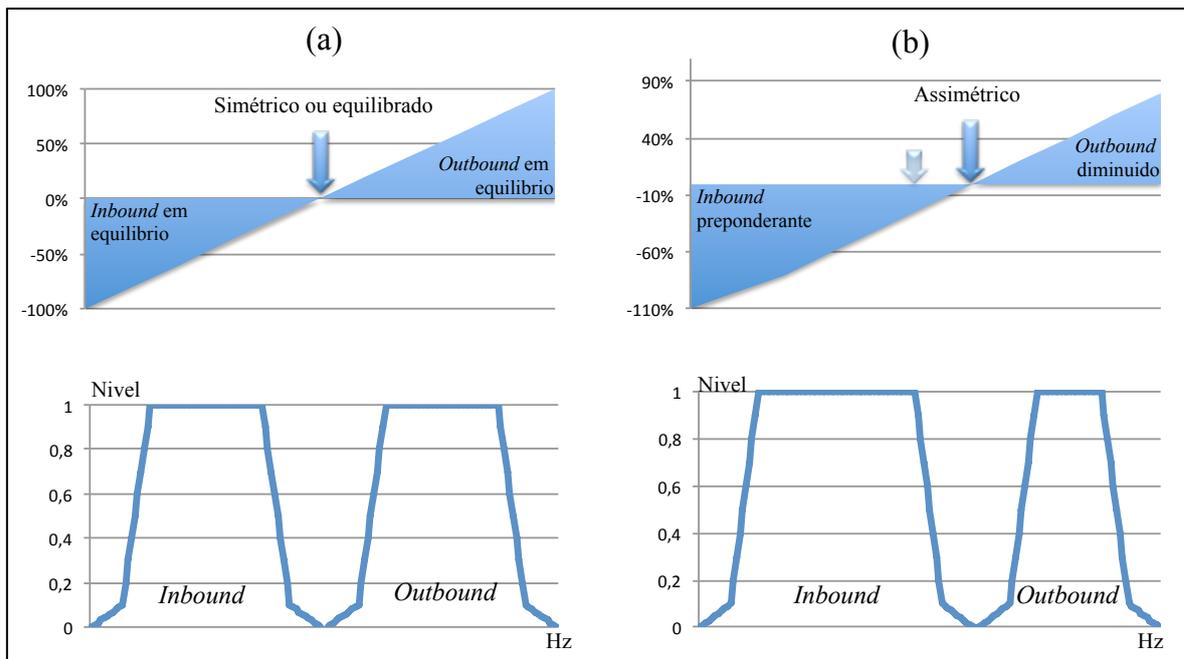


Figura 3.3 - Função Fut do equilíbrio entre o TX e o RX nos sentidos inbound e outbound e a largura de banda dos canais de TX (outbound) e RX (inbound) para os casos (a) simétrico e (b) assimétrico do uso da banda total disponível.

Por outro lado, nesse trabalho a tomada de decisão não será tomada com base na possibilidade efetiva de modificação de padrões. O principal objetivo é auxiliar nas relações que determinam as interconexões entre sistemas autônomos.

3.3 A BANDA OU VELOCIDADE COMO UM PRODUTO OU SERVIÇO

Em (Stênico, 2013) e (Kelly, 1996), são realizados ensaios sobre a definição de banda efetiva. Conforme descrito em (Swift e Dagli, 2013) e (Stênico, 2013), um grande problema que todas as operadoras de telecomunicações enfrentam é a definição de um produto ou serviço que esteja baseado na definição de banda ou velocidade em *bps* (bits por segundo) ou *bytes*. Mas conforme definido por (Kelly, 1996), a grande pergunta, em primeiro lugar, é como definir banda ou velocidade.

Seria apenas uma razão entre a quantidade de bits e um intervalo de tempo? É uma questão interessante a ser abordada, observado-se que em um caso simples, a banda ou velocidade em *bps* pode variar em 100% apenas em função do intervalo de tempo escolhido. Na Fig. 3.4 tem-se um diagrama para auxiliar no entendimento.

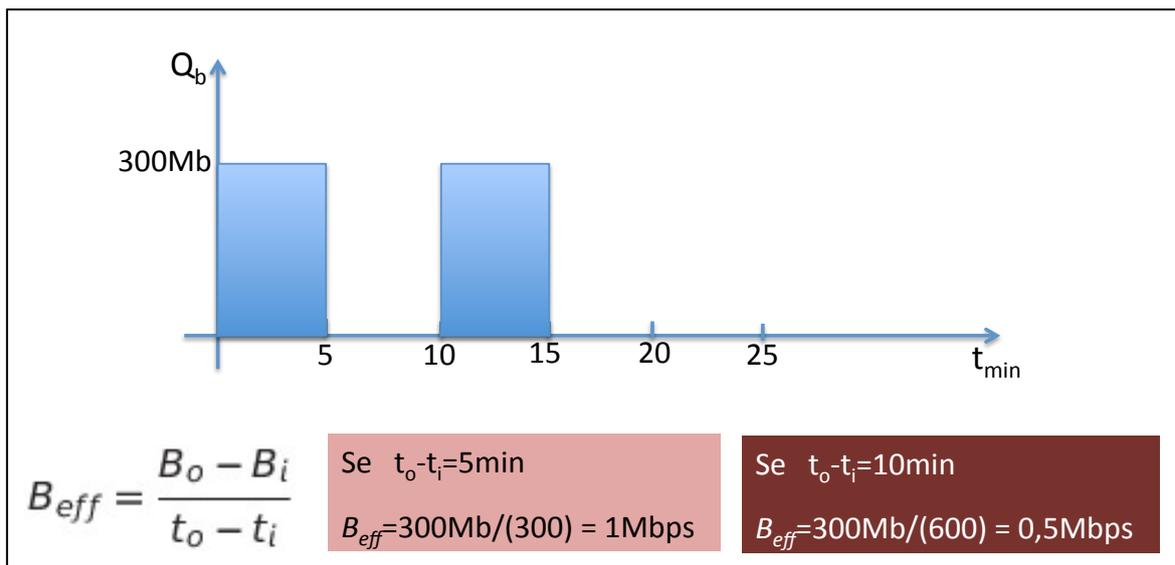


Figura 3.4 - Dilema da banda ou velocidade em bps.

Para este caso em específico, diversos autores (Kelly, 1996) ou (Norros, 1995) contribuíram de forma significativa para melhorar o entendimento da necessidade de conhecer o comportamento do tráfego, de forma a melhor definir banda ou velocidade.

De acordo com (Ravindranath *et al.*, 2014), outra grande dificuldade é o próprio usuário do serviço que não tem nenhum parâmetro para saber exatamente o que está sendo contratado, pois não tem como saber *a priori* quantos bytes possui uma página *html* que esteja sendo requisitada, ou até mesmo qual foi o CODEC de voz (ITU G.711, G7xx) e qual é a sua necessidade de recursos que será requisitada. Dessa forma, o que sobra é uma situação onde não se conhece o que está sendo fornecido e tampouco o que está sendo comprado. Uma outra solução, de acordo com (Kelly, 1998) é a contagem da quantidade de bytes e uma especificação da quantidade de bytes que poderão ser consumidos em um determinado ciclo (semanal ou mensal), esses coletados de uma MIB (*Management Information Base*) usando o protocolo SNMPv3 (*Simple Network Management Protocol*).

Em (Gómez *et al.*, 2014) é mostrado que o usuário pode ser levado a confundir o conceito de banda (ou até mesmo do serviço), pois quando se define quanto de banda está sendo oferecido por produto, normalmente um serviço 2,5G, 3G [3GPP, IMT2000, UIT] ou 4G [LTE, WiMAX] para o móvel com taxas comerciais aparentes que na descrição comercial variam entre 384kbps a 100Mbps. Ainda, de acordo com (Aroussi e Mellouk, 2014) é

possível, tendo uma referência inicial, supor que um serviço que ofereça uma banda de 384kbps terá um desempenho pior que aquele que pode oferecer 100Mbps, porém afirmações em termos de qualidade não se sustentam sem que o tipo de serviço que irá utilizar a rede seja conhecido.

Ainda referenciando os serviços existentes nos mercados brasileiro, americano e europeu observa-se uma estruturação com base em premissas de uso irrestrito para os casos de acessos fixos e quantidade de *bytes* para o móvel, ficando ainda mais fácil entender a dificuldade de se planejar sistemas móveis que possam atender a usuários que realmente se movimentam e geram tráfego de aplicações que podem não ser as mesmas que foram usadas quando do dimensionamento do sistema.

Finalizando, a grande dificuldade de se definir banda ou velocidade juntamente com o fator de mobilidade, adicionado à incerteza do tipo de serviço que irá usar a rede, faz com que seja muito difícil para o planejador ter confiança nos seus cálculos. Um cenário não interessante para um ciclo de planejamento é a incerteza do modelo que está sendo usado, pois, caso os recursos planejados sejam insuficientes o cliente final não terá como usar a rede e se os recursos forem além da necessidade do produto especificado, a empresa não terá resultados financeiros interessantes para a manutenção do negócio (Kotler, 1998).

3.4 MODELOS MATEMÁTICOS

De acordo com (Takine *et al.*, 2004), um modelo matemático deve expressar, com a máxima exatidão possível, o comportamento natural de um processo. Ou seja, não é o modelo matemático que força o funcionamento do processo natural. À medida que as imperfeições do modelo são conhecidas, minimiza-se o erro em previsões, maximizando-se a assertividade do processo de planejamento.

3.4.1 - O modelo simplificado

Em (García-Dorado *et al.*, 2014) uma abordagem simplificada para o problema da previsão é apresentada utilizando-se a banda média por usuário, em que cada usuário recebe um valor médio de utilização que pode ser expresso em *bits* por segundo ou *bytes* acumulados.

No modelo de (García-Dorado *et al.*, 2014), a taxa de reutilização do recurso (DSLAMs, Roteadores ou enlaces) deve ser considerada individualmente. Na Fig. 3.5 é apresentado um exemplo para o cálculo do acesso entre o usuário e o DSLAM (Multiplexador de linhas digitais assimétrico), *backhaul* que é conexão entre o DSLAM e o BRAS (*Broadband remote access server*) ou servidor de acesso remoto para acessos) e *backbone*.

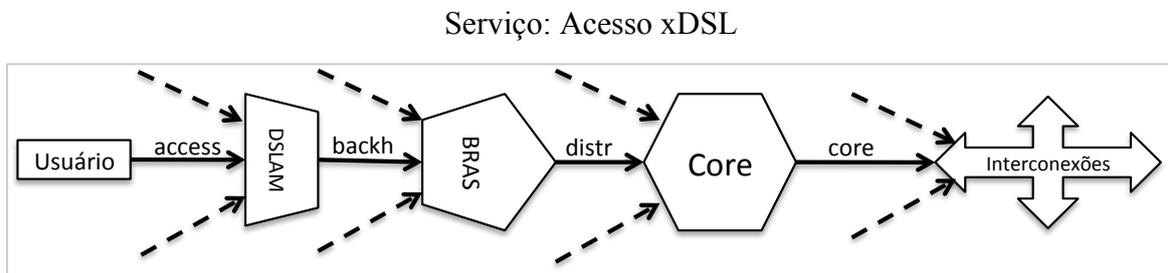


Figura 3.5 - Modelo de conexão de rede simplificado e em camadas de rede.

Da mesma forma que aquela apresentada em (García-Dorado *et al.*, 2014), a condição mais simplificada para este caso é o uso de uma banda média única à partir da conexão {backh} até o {core}. Nesse caso o dimensionamento dos enlaces é realizado apenas com base em uma banda ou velocidade média do acesso que gera um cálculo simples. Neste exemplo, define-se $B_{\{.\}}$ como a banda do enlace que está sendo calculado. Para n usuários, m enlaces de *backhaul* que é basicamente uma conexão entre o elemento concentrador do acesso (nesse caso um DSLAM) e k enlaces de distribuição que chegam aos pontos centrais da rede para serem escoados internamente ou ainda externamente através de enlaces de interconexão:

$$B_{\{backh\}} = n * B_{\{média\}} \quad (3.2)$$

$$B_{\{distr\}} = \sum_1^m B_{\{backh\}} \quad (3.3)$$

$$B_{\{core\}} = \sum_1^k B_{\{distr\}} \quad (3.4)$$

Para este modelo, é simples verificar que há pouca informação que esteja relacionada com o serviço ou produto, ou seja, toda a informação de tráfego está contida na banda média do usuário.

Essa simplificação pode facilitar por um lado a forma de se calcular a necessidade de banda de dados (comumente chamada de velocidade), mas mesmo assim ainda não resolve a questão relacionada a processamento. Para este caso, mesmo para uma situação

simplificada, é necessário que se conheça um pouco mais quais serão os serviços que irão trafegar na rede e no mínimo, definir o tamanho médio do pacote que irá trafegar na rede.

Com essas informações, melhora-se a possibilidade de se definir um nó com capacidade de encaminhamento de pacotes compatível com a demanda. Em (Cisco, 2014), a capacidade de processamento é definida de forma empírica relacionando-se diretamente a capacidade de encaminhamento de pacotes, sendo, os valores informados pelo fabricante e que são descritos em pacotes por segundo ou *pps*.

Outra informação fundamental para o dimensionamento, mesmo que simplificado, é o interesse de tráfego, ou de onde e para onde o tráfego irá escoar. Com isso será possível que uma matriz de interesse de tráfego seja especificada.

3.4.2 - O modelo de autosimilar

De acordo com (Leland, 1994), a caracterização da dependência de longa duração, segue as seguintes regras, para a caracterização de um processo estocástico, além do fato de poderem ser explicados por uma distribuição Gaussiana:

Para $1/2 < H < 1$, o processo tem dependência de longa-duração.

Para $H \leq 0,5$, este processo possui dependência de curta duração ou independência.

Para esses casos e observando a equação 3.5, pode-se verificar que todos os momentos de ordem n de $X(t)$, se existirem, terão um comportamento respeitando uma determinada lei de potência em função do tempo:

$$E|X(t)|^n = E|X(1)|^n |t|^{nH} \quad (3.5)$$

Os processos auto-similares com incrementos estacionários (H-sssi) são modelos executáveis de processos com incrementos estacionários. É possível que a melhor característica de um processo auto-similar seja a simplicidade de sua representação, pois o processo todo é controlado apenas pelo parâmetro (H) Hurst. Por outro lado, esta simplicidade de acordo com (Clegg, 2006) gera um grande problema, pois dificilmente na natureza serão encontrados processos que sejam exatamente auto-similares.

De acordo com (Leland, 1994), a auto-similaridade implica que, de acordo com a equação 3.5 pela qual todo momento de ordem n (se existir) será controlado por um único parâmetro H . Na maioria das vezes os modelos auto-similares, com parâmetro único definido, somente poderão ser aplicados em escalas grandes. Este comportamento foi verificado, no caso em estudo, em escalas de 1 e 5 minutos.

Dois modelos podem generalizar os processos auto-similares com relação à escala, o processo forte assintoticamente auto-similar de segunda ordem e o processo assintoticamente auto-similar de segunda ordem. O processo chamado de forte assintoticamente auto-similar de segunda ordem quando as variâncias de seus processos agregados seguem a seguinte condição na equação 3.6.

$$\lim_{m \rightarrow \infty} v(X^{(m)}) \sim m^{-\beta}, \quad \text{com } H = 1 - \frac{\beta}{2} \quad (3.6)$$

O processo assintoticamente auto-similar de segunda ordem tem suas características definidas quando a relação em 3.7 é válida somente assintoticamente. É mostrado em (Vieira, 2006) uma definição em termos de universo restritivo para cada um dos processos auto-similares.

$$\lim_{m \rightarrow \infty} \rho^{(m)}(k) = \frac{1}{2} \left\{ |k+1|^{2H} + |k-1|^{2H} - 2|k|^{2H} \right\} \quad (3.7)$$

Os processos auto-similares podem ser usados como ferramenta para a caracterização de tráfego em redes de pacotes, principalmente relacionadas a tráfego em nível de agregação elevado.

Apesar do modelo de Poisson (Barreto, 2007), ainda em uso atualmente, não satisfazer às necessidades dos planejadores em termos de previsão coerente com , também não é aceitável que se passe a utilizar novos modelos que não possam se provar melhor adaptados às necessidades das novas redes, incluindo as preocupações relativas aos serviços, cada vez mais menos previsíveis. Nesse trabalho serão trabalhados os conceitos relativos à identificação do tipo de tráfego que circula pela *internet*, mas sem dúvida esta também é uma preocupação a ser levada em consideração. Não é interessante que se mencione o ato de planejar sem o conhecimento do comportamento dos serviços que estão

fazendo uso dos recursos, desta forma não existe nenhuma possibilidade de acertos sem o profundo conhecimento do tipo de tráfego em movimento na rede.

3.4.3 - O modelo de Multifractal ou DLD

Um processo Multifractal ou de Dependência de Longa Duração – DLD - não apresenta restrição com relação à uniformidade nas suas variações e tem os seus momentos estatísticos definidos por (Abry, 2002):

$$E|X(t)|^q = E|X(1)|^q |t|^{\zeta(q)} \quad (3.8)$$

onde, $\zeta(q)$ é a função cascadeamento. Esta função apresenta um comportamento não-linear para diferentes momentos de q , caracterizando a multifractalidade ou a DLD.

Em (Abry, 2002) é descrito um método para a detecção de ocorrência de multifractalidade em um processo estocástico. Basicamente, nesse método, é verificado o comportamento da função $\zeta(q)$ em relação aos momentos estáticos q . Nesse caso basta que a função seja não-linear para que o comportamento seja confirmado como Multifractal ou de DLD.

Para se estimar os valores da função $\zeta(q)$ é necessária a determinação do expoente de cascadeamento α_q de acordo com a equação 3.9, fazendo uso do método diagrama LD - *Logscale Diagram* - (Abry, 2002) e (Veitch, 2007) do q -ésimo momento.

A presença de multifractalidade pode ser detectada também analisando o comportamento do expoente de Hölder h_q (Hölder em relação aos momentos estatísticos q). O expoente assume a seguinte forma:

$$h_q = \frac{\alpha_q}{q} - \frac{1}{2} \quad (3.9)$$

ou ainda similarmente,

$$h_q = \frac{\zeta(q)}{q} \quad (3.10)$$

Em (Abry, 2002) é descrito o método diagrama linear multiescala (*Linear Multiscale Diagram*), utilizado para determinar a ocorrência de multifractalidade em um processo.

Nesse método, avalia-se o comportamento da curva obtida com a estimativa do expoente de Hölder h_q e caso o seu comportamento seja não-horizontal é constatado a multifractalidade. Nos casos onde um único h_q controla todo o processo e explosividade (*burstness*) o Hölder equivale ao parâmetro de Hurst H .

Desta forma, quando expoente de Hölder h assume características próprias de uma função $h(t)$, esta altamente irregular, pode-se afirmar que este é um processo estocástico, podendo ser chamado de Multifractal ou de DLD.

A grande variação de $h(t)$ torna extremamente complexa a tarefa de caracterizar as variações em termos de tempo desta função, sendo melhor que a sua caracterização seja estatística. A caracterização estatística pode ser feita através do espectro Multifractal da função $h(t)$. São usados dois tipos de análise espectral: o espectro Multifractal de Hausdorff e o espectro Multifractal de Legendre conforme mostrado em (Seuret, 1995) e (Seuret, 2000). O espectro Multifractal de Hausdorff é a função $D(a)$ que corresponde à dimensão de Hausdorff do conjunto de pontos $t \in IR$ onde $h(t) = a$, onde a é o valor máximo assumido por $h(t)$, assim:

$$D(a) = \dim(t \in IR : h(t) = a) \quad (3.11)$$

onde $\dim(S)$ é a dimensão de Hausdorff do conjunto S .

O espectro de Legendre remete a uma das características dos processos DLD à partir do qual o comportamento das chamadas funções de partição seguem uma lei polinomial com expoente $\zeta(q)$:

$$\int |X(t + \tau) - X(t)|^q dt \approx |\tau|^{\zeta(q)}, \tau \rightarrow 0, \quad q \in IR \quad (3.12)$$

Desta forma o espectro Multifractal ou DLD de Legendre pode ser calculado através da transformada de Legendre de $\zeta(\tau)$, conforme equação 3.13.

$$D(h) = \min_q(qh - \zeta(q) + 1) \quad (3.13)$$

Cascatas multiplicativas são exemplos de processos multifractais, conforme mostrado em (Melo, 2004) e (Erramilli, 2001), é apresentado um modelo de tráfego chamado de cascata multiplicativa, este é capaz de verificar se amostras de tráfego possuem estatísticas multifractais. É mostrada uma escala de tempo θ a partir da qual um traço de tráfego apresenta características monofractais. Nessa mesma linha, para escalas ainda menores que θ , as estatísticas multifractais são encontradas, esta é a escala de tempo limitante (*cutoff scale*).

Na Fig. 3.6. é apresentado um espectro de Legendre calculado através da ferramenta FRACLAB 2.0 (Véhel, 2006) para um traço de tráfego caracterizado como auto-similar. Observa-se nesse exemplo que o expoente de Hölder varia muito pouco em todo o espectro cuja função é côncava em quase toda a sua extensão.

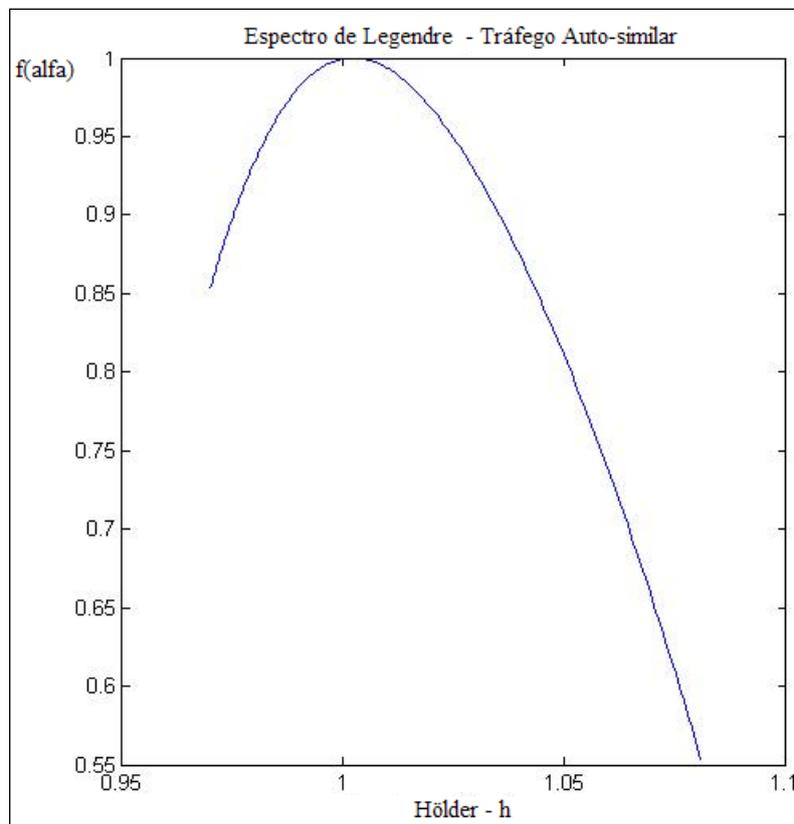


Figura 3.6 - Espectro de Legendre para o tráfego auto-similar, amostra real obtida em rede IP de uma operadora de Telecomunicações do Brasil.

O modelo de Cascata Multiplicativa caracteriza traços de tráfego em escala de tempo maiores ou iguais a θ usando um processo fBm. Nas escalas menores que θ pode ser usado o método da cascata multiplicativa semi-randômica com parâmetro p , para o tráfego avaliado igual a 0,65. Nesse caso são derivadas expressões para o planejamento de capacidade e controle de admissão, essas derivadas da teoria dos Grandes Desvios (Vieira, 2006). A definição dessas expressões tem como requisito a computação dos diversos momentos do tráfego em análise. Em (Vieira, 2006), o modelo Cascata Multiplicativa é utilizado para executar um sistema de fila que tem o seu mecanismo avaliado quando o fluxo que alimenta este sistema apresenta estatísticas com comportamento Multifractal ou DLD.

Tabela 3.1 – Teste de aderência com o uso do χ^2

Evento	Hurst		Hölder	Qui-Quadrado
	Variance time-plot	Kettani-Gubner		Distribuição Gaussiana
1	0,87	0,974	1,049	40,233
2	0,916	0,86	0,835	41,376
3	0,937	0,789	0,588	61,731
4	0,87	0,901	0,832	30,251
5	0,743	0,571	0,751	47,413
6	0,938	0,583	0,48	68,273
7	0,973	0,509	0,63	60,374
8	0,872	0,825	0,661	35,476
9	0,547	0,793	1,031	61,579
10	0,592	0,559	0,964	32,316
11	0,733	0,53	0,453	33,859
12	0,528	0,628	0,377	51,917
13	0,632	0,862	0,675	66,292
14	0,659	0,557	0,756	37,94
15	0,828	0,947	0,637	66,42
16	0,719	0,559	0,917	52,543
17	0,751	0,67	0,556	36,184
18	0,603	0,827	0,695	62,155
19	0,894	0,491	0,653	59,007
20	0,832	0,493	1,065	65,217
21	0,719	0,525	0,913	63,797
22	0,522	0,45	0,711	63,155
23	0,978	0,959	0,823	54,362
24	0,665	0,597	1,053	59,958
25	0,766	0,567	0,559	43,07
26	0,652	0,5	0,377	62,36
27	0,612	0,891	0,742	30,299
28	0,584	0,737	0,618	33,95
29	0,548	0,867	0,778	58,393
30	0,633	0,612	0,663	54,913
31	0,578	0,865	0,501	42,111
32	0,605	0,65	0,386	53,78
33	0,677	0,533	0,5	59,146
34	0,965	0,829	0,997	40,841
35	0,596	0,713	0,587	57,216
36	0,975	0,734	0,749	57,623
37	0,813	0,753	1,033	49,568
38	0,803	0,556	0,662	68,306
39	0,896	0,922	0,341	50,307
40	0,826	0,648	0,44	31,628
41	0,931	0,633	0,916	68,048
42	0,698	0,539	0,653	57,924
43	0,823	0,719	0,472	63,276
44	0,626	0,688	0,716	34,388
45	0,594	0,722	0,731	40,703
46	0,846	0,791	0,92	34,656
47	0,765	0,825	0,447	54,379
48	0,663	0,755	0,641	31,03
49	0,608	0,736	0,479	48,286
50	0,728	0,899	0,497	68,003

Em (Melo, 2004) foram avaliadas escalas de tempo limitante (*cutoff scale*) θ e verificou que para traços de tráfego IP a ordem é de 1 (um) milissegundo, o tempo de um RTT (*Round Trip Time*). Neste trabalho as amostras de tráfego são testadas sempre para a determinação do grau de aderência ao modelo Multifractal ou DLD.

Para a análise do grau de significância foi aplicado o método do χ^2 – Qui-quadrado – (Chwif e Medina, 2006) como forma de verificar o grau de similaridade das distribuições encontradas. Este teste baseia-se no cálculo dos desvios entre as frequências acumuladas observadas em cada classe e as frequências teóricas nas mesmas classes.

Apenas como exemplo do trabalho efetuado para todas as amostras de tráfego utilizadas neste trabalho, na Tabela 3.1 é possível se concluir que o teste de aderência condiz e pode ser aceito para uma distribuição Gaussiana.

Na Fig. 3.7 é possível se analisar a CDF relativa a 125 amostras usadas durante a execução de coletas de dados para uso no sistema de tomada de decisão de uma operadora de Telecomunicações Internacional.

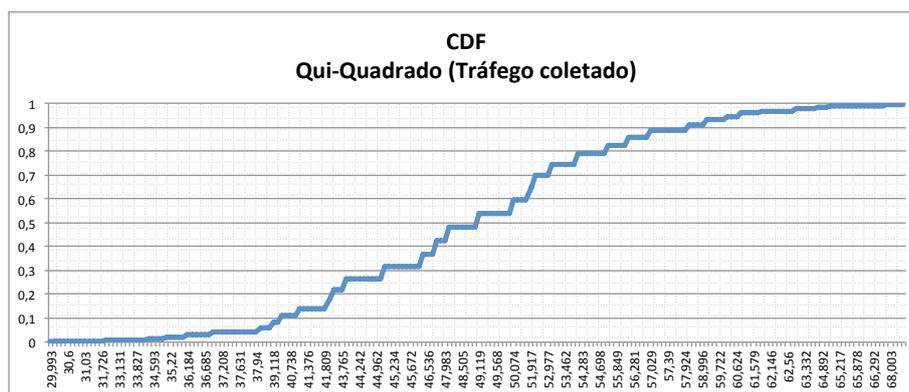


Figura 3.7 – CDF do teste do qui-quadrado para teste de aderência.

3.5 ESTIMADORES DE BANDA OU VELOCIDADE

Conforme mostrado na Fig. 3.8. a determinação da banda, ou de forma mais comum velocidade, utiliza métodos que não conseguem mostrar o comportamento real da taxa de

chegada ou de saída de pacotes em uma determinada interface para qualquer escala de tempo.

De fato o grande problema é que todos os sistemas atuais usam esta mesma estratégia para a determinação da banda que é utilizada e isso faz com que claras discrepâncias sejam verificadas quando da operação das redes que estão presentes na Internet.

Um fato interessante é o cálculo de qualidade do acesso à Internet proposto pelo NIC.BR, conforme observa-se em (NIC.BR, 2014) com o uso da ferramenta Simet. Na Fig. 3.7 são apresentados resultados com o uso da ferramenta proposta.

Os testes indicam que as medidas são realizadas em uma escala de tempo de milissegundos, enquanto todas as medidas utilizadas como padrão na Internet para enlaces no centro (*backbone*) são realizados em uma escala de minutos (Claise, 2004).

O cálculo simples leva a erro, pois o simples acúmulo da informação em uma MIB (Presuhn, 2002), não é o suficiente para também se acumular o comportamento da taxa entre chegada de pacotes, o que irá resultar em interpretações errôneas caso o modelo utilizado não esteja prevendo esta condição. De forma tal que o modelo matemático que estiver sendo usado para o cálculo da banda (ou velocidade) deverá expressar o real comportamento em qualquer escala de tempo.

Os processos que são usados pelas operadoras parecem não coincidir com os modelos utilizados pelo NIC.BR, ANATEL (Agência Nacional de Telecomunicações) entre outras, confirmando-se esta condição, observa-se que o modelo de planejamento e logo após o de operação pode estar levando às redes a uma condição de inviabilidade operacional devido ao não atendimento a condições que sejam especificadas (ou que vierem a ser) pelo órgão regulador.



Resumo dos Resultados
Velocidade: 0 kbit/s
Latência: 34.02 ms
Perda de Tráfego: 11.00%
Banda Contratada: 10.00 Mbit/s

CEP: 70673-431 Banda contratada: 10.00 Mbit/s Local de acesso: Não informado
Data: 06/03/14 02: IP: null Servidor: PTT Metro de Brasília - 30.85ms

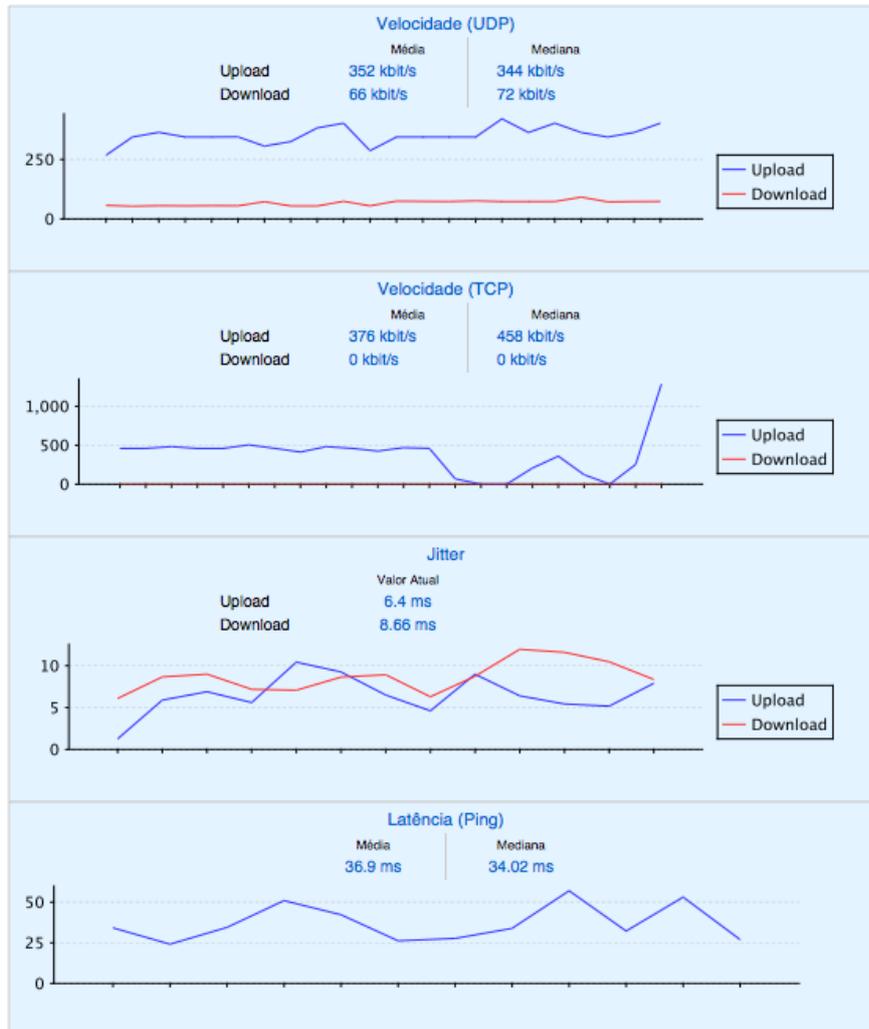


Figura 3.8 – Teste real utilizando a ferramenta <http://simet.nic.br>

Conforme também já demonstrado, a caracterização do tráfego IP pode ser bem descrita com o uso de modelos auto-similares ou multifractal, esses serão usados aqui para o conceito de banda efetiva e possibilidade de estimativas que levem em consideração o comportamento natural dos processos.

Nesse trabalho serão utilizados alguns estimadores de banda, principalmente aqueles com resultados mais expressivos e confirmados em outros trabalhos em termos de efetividade, tal como encontrado em (Stênico, 2013) e em (Swift e Dagli, 2013).

4.5.1 – Estimador de Banda Efetiva de Kelly

Os estimadores de banda efetiva, usam um conceito introduzido por (Kelly, 1996), com uma relação direta entre o tamanho do *buffer* e das escalas de tempo relacionadas com a possibilidade de trasbordo ou taxa de perda de pacotes. O objetivo aqui é mostrar o comportamento real do tráfego, tentando capturar o máximo de informação que possa ajudar a se chegar a um modelo que represente o processo natural ou original, incluindo perdas, tempo entre chegada de pacotes, entre outros. O conceito está mostrado na Equação 3.14 onde $X[0,t]$ é a quantidade de bits que chegam em um intervalo $[0,t]$ e também assumindo que $X[0,t]$ possui incrementos estacionário. A letra b é o tamanho do *buffer* e o t tempo ou sua escala, BP é a capacidade em *bits* por segundo.

$$BP(b, t) = \frac{\log E[e^{bX[0,t]}]}{bt} \quad \therefore 0 < b, t < \infty \quad (3.14)$$

4.5.2 – Estimador de Banda Efetiva FEP ou *Fractal Envelope Process*

Com base nessa teoria, diversos estimadores de banda foram propostos e avaliados quanto a sua eficácia e complexidade de avaliação. Em (Fonseca, 2005) uma avaliação do modelo de estimador *FEP* (*Fractal Envelope Process*) foi realizada com resultados muito promissores, sendo indicada para uso em redes de alta velocidade que necessitem de estimadores em tempo real (quase real). O grau de acerto está relacionado com o tipo de estimador do parâmetro de *Hurst*.

O estimador *FEP* também pode ser considerado como uma evolução do modelo proposto por (Norros, 1995) e é definido pela equação 3.58, onde o *buffer* é aqui representado pela letra b , a letra a representa a média, o H é o parâmetro de *Hurst* o σ representa o desvio padrão das amostras, o P_{loss} representa a probabilidade da perda de dados por transbordo do *buffer*. Esta equação vale para o intervalo: $0,5 < H < 1$.

$$BP = \bar{a} + b^{\frac{H-1}{H}} * (\sqrt{-2 * \ln(P_{loss})} * \sigma)^{\frac{1}{H}} * H(1 - H)^{\frac{1-H}{H}} \quad (3.15)$$

Os resultados para os casos onde a banda possui dependência de longa duração e cujos processos podem ser caracterizados pelo parâmetro de Hurst são aqueles com melhores resultados para este modelo (Fonseca, 2005).

Na Fig. 3.8 pode-se observar uma grande dependência do tamanho do *buffer*, nesse caso foram traçadas curvas de 0,5 segundos até 5 minutos. Pode-se notar que o H aqui representa de forma bem clara o grau de agregação e explosividade (*burstness*), isso é quanto mais próximo de 1 (um) maior a necessidade de banda para um mesmo tamanho de *buffer*.

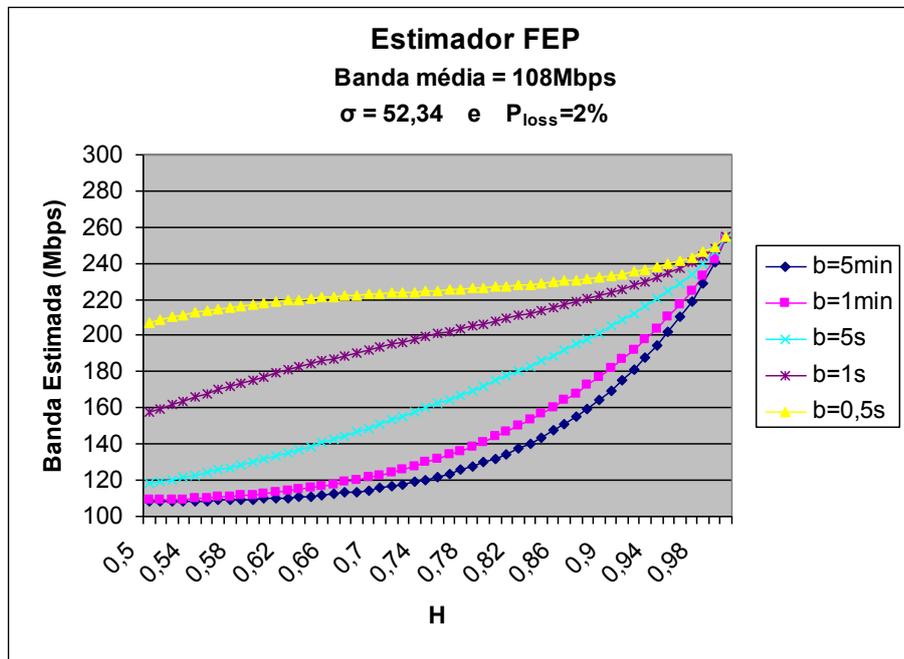


Figura 3.9 – Curva de Estimação de Banda Passante 108Mbps.

Após a análise dos gráficos mostrados na Fig. 3.9, nota-se que existe uma dependência muito forte do tamanho da memória de curta duração (*buffer*) quando o H está mais próximo de 0,5 (meio), sendo que para H mais próximos de 1 (um) existe uma independência com relação a esta memória de curta duração (Taqq *et al.*, 1997).

Em (Perlingueiro, 2005) mostrou de forma empírica que o estimador FEP possui uma tendência a superestimação, por este motivo um método de correção foi proposto em função do parâmetro de Hurst e de acordo com as equações 3.16 e 3.17.

$$BP_{op} = \frac{2}{5} \frac{BP}{\sqrt{b'L}} \quad \text{quando } 0 < H \leq 0.7 \quad (3.16)$$

$$BP_{op} = \frac{2}{75} \frac{BP}{\sqrt{b'L}} \quad \text{quando } H > 0.7 \quad (3.17)$$

Onde BP_{op} é a nova banda otimizada, b' é o *buffer* normalizado $b'=b/b_0$ and b_0 é o menor tamanho de *buffer* considerado. A letra L indica o máximo fator de rajada(*burst*).

4.5.3 – Estimador de Misturas Gaussianas de Banda Efetiva.

Este método é descrito também por (Gonçalves e Vieira, 2013) e é usado para modelar series de tráfego usando o modelo de mistura gaussiana. Em (Resch, 2010) o método é descrito como um agrupamento de densidade de probabilidades gaussianas individuais. Se difere do modelo Kernel e da Banda Efetiva DLD em função dos parâmetros necessários para a sua descrição. É necessário se determinar a *pdf* para cada uma das gaussianas que descreverem o processo e para cada uma das gaussianas deve-se calcular o coeficiente de ponderação, a média e a matriz de covariância.

Na equação 3.18. é apresentada a função densidade de probabilidade do modelo, esta pode ser ainda resumida como uma soma ponderada de funções gaussianas, pois uma série de tráfego possui apenas uma dimensão, sendo a matriz de de covariância podendo ser descrita por um único valor. Neste caso, c é o conjunto de gaussianas ρ_i , σ_i e μ_i os quais correspondem, respectivamente ao coeficiente de ponderação, o desvio padrão e a média de uma gaussiana i .

$$f(x) = \sum_{i \in c} \rho_i \frac{1}{\sigma_i \sqrt{2\pi}} \exp \left[-\frac{(x-\mu_i)^2}{2\sigma_i^2} \right] \quad (3.18)$$

A sua *pdf* terá um crescimento e decaimento suave $-\infty$ até $+\infty$, diferente do tráfego que assume valores apenas positivos e possui um limite superior. Este conhecimento se faz necessário como forma de se evitar superestimação (Gonçalves e Vieira, 2013). Em todos os casos tratados neste trábaho isto não é um problema, pois o antes do inicio da metodologia o perfil de tráfego necessita de uma semana de coletas para conhecimento prévio do perfil de tráfego. Pode definir pelas equações 3.19. e 3.20.

$$P_p(x) = P(X = x | 0 \leq X \leq m) \quad (3.19)$$

$$P_p(x) = \frac{P(X=x)}{P(0 \leq X \leq m)} \quad 0 \leq x \leq m \quad (3.20)$$

$$f_p(x) = \frac{f(x)}{\int_0^m f(x)dx} \quad 0 \leq x \leq m \quad (3.21)$$

Onde m é o valor máximo que o processo pode assumir. A função geradora de momentos $\Lambda(b,t)$ do processo deve ser determinada, como no processo já se assume uma escala de tempo a denotação passa a ser $\Lambda(b)$ apenas.

Por definição,

$$\Lambda(b) = E[e^{bX}] = \int_{-\infty}^{\infty} e^{bX} f_p(x)dx \quad (3.22)$$

logo,

$$\Lambda(b) = \int_0^m e^{bX} \frac{f(x)}{\int_0^m f(z)dz} dx \quad (3.23)$$

logo,

$$\Lambda(b) = k \sum_{i \in C} \rho_i e^{\left[\frac{(\sigma_i b)^2}{2} + b\mu_i\right]} g_i(b) \quad (3.24)$$

onde,

$$k = \frac{1}{2 \int_0^m f(x)dx} \approx \frac{1}{2} \quad (3.25)$$

$$g_i(b) = -\operatorname{erfc}\left(\frac{(\sigma_i b)^2 + \mu_i}{\sigma_i \sqrt{2}}\right) + -\operatorname{erfc}\left(\frac{-m + (\sigma_i b)^2 + \mu_i}{\sigma_i \sqrt{2}}\right) \quad (3.26)$$

A função *erfc* é a função erro complementar, definida na equação 3.27.

$$\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} e^{-t^2} dt \quad (3.27)$$

A banda efetiva por mistura gaussiana é definida na equação 3.28. sendo desconsiderados os limites relativos aos valores superiores e inferiores pode-se calcular a banda efetiva fazendo $k = \frac{1}{2}$ e $g_i(b) = 2$.

$$BP_x(b, t) = \frac{1}{bt} \ln \left[k \sum_{i \in C} \rho_i e^{\left[\frac{(\sigma_i b)^2}{2} + s \mu_i \right]} g_i(b) \right] \quad (3.28)$$

4.5.4- Estimador de Kernel de Banda Efetiva

Este método é descrito também por (Gonçalves e Vieira, 2013). Em (Bowman, 1997) são observados métodos para estimação da função densidade de probabilidade (*pdf*) de uma variável aleatória forma não-paramétrica. Caso um processo $X(t)$ seja estacionário, independente e identicamente distribuído (i.i.d.) na escala de tempo t , é possível se estimar sua *pdf* utilizando o método de Kernel e sua banda efetiva a partir de sua *pdf*. Em cada ponto, as estimativas de densidade de probabilidade são encontradas com o uso método de Kernel. Isto ocorre à partir da soma ponderada de funções de probabilidade. Para que o método seja utilizado é necessário que o processo tenha sido caracterizado e possua grau de aderência adequado à uma distribuição Gaussiana, conforme equação 3.29.

$$f_t(x) = \frac{1}{n} [\sum_{i=1}^n k_h(x - x_i)] \quad (3.29)$$

Partindo da definição da banda efetiva de (Kelly, 1996) a banda efetiva pode ser escrita conforme equação 3.30.

$$BP_x(b, t) = \frac{1}{bt} \ln \left[\int_{-\infty}^{\infty} e^{b\tau} f_t(\tau) d\tau \right] \quad (3.30)$$

Como o método de Kernel gera um grande número de parâmetros para se determinar a *pdf* de uma variável aleatória, para facilitar estima-se numericamente a *pdf* do processo $X(t)$, com escala de tempo t , tendo como resultado um vetor $x[i]$ de pontos e um vetor $p[i]$ com

respectivas densidades de probabilidade. Então é possível se aproximar a banda efetiva através da equação 3.31.

$$BP_x(b, t) = \frac{1}{bt} \ln\left[\sum_{i=1}^M e^{bx[i]} p[i]\right] \quad (3.31)$$

onde M é o número de pontos estimados. Nesse caso o número de pontos estimados deve ser grande e $x[i]$ deve cobrir toda região onde está concentrado a maior parte da densidade de probabilidade, ou seja $\int_{x[1]}^{x[M]} f_t(x) dx \approx 1$, para $x[1]$ o menor e $x[M]$ o maior valor.

4.5.5 – Estimador de Banda Efetiva de Stênico

Em (Stênico, 2013) é apresentado um estimador de banda efetiva que experimentalmente consegue melhor capturar características naturais do processo de tráfego em mais de uma escala de tempo, pois baseia-se no modelo DLD (fBm). A ideia principal é a de se encontrar um parâmetro global, similar ao de Hurst, porém que capture as características multifractais ou de variação em qualquer escala de tempo, isso é, qualquer que tenha sido a escala de tempo em que uma amostra tenha sido capturada após a retirada de parâmetros, seria possível uma estimativa da banda efetiva. Os parâmetros para este caso são o Hölder - h - ou de escala global, média, variância, tamanho de buffer e taxa de decaimento assintótica do tamanho da fila.

O parâmetro ou expoente de Hölder pode também ser interpretado como uma generalização do parâmetro de escala global H_{EG} e o α e o β são parâmetros da distribuição beta.

$$H_{EG} \triangleq h \triangleq H = 1 - \frac{1}{2} \log_2 \frac{(\alpha+\beta)(\alpha+\beta+1)}{(\alpha+1)\alpha} \quad (3.32)$$

Assim a banda efetiva DLD - BP_x - poderá ser escrita através da função geradora de momento $X(t)$ em termos dos parâmetros θ e δ , $E[X(\delta)] = \mu \cdot \delta$ e a variância como $var[X(\delta)] = \sigma^2 \delta^{2H_{EG}}$ e escrevendo diretamente o resultado:

$$BP_x = \frac{1}{\theta\delta} \mu\delta\theta + \frac{\sigma^2 \delta^{2H_{EG}} \theta^2}{2} = \mu + \frac{\theta\sigma^2}{2} \delta^{2H_{EG}-1} \quad (3.33)$$

ou ainda:

$$BP_x = \mu + \frac{\theta\sigma^2}{2} \delta^{((2-\log_2 \frac{(\alpha+\beta)(\alpha+\beta+1)}{(\alpha+1)\alpha})-1)} \quad (3.34)$$

Observando-se que na Equação 3.34 tem-se θ representando a taxa de decaimento assintótica da distribuição do tamanho da fila e δ a escala de tempo. Em (Stênio, 2013), a BP_x foi testada com bons resultados para uma fonte de tráfego DLD.

3.6 ESTRATÉGIA DE CARACTERIZAÇÃO E CÁLCULO DE BANDA

A diversidade de estimadores de banda demonstra a dificuldade em se definir banda, conforme já analisado, pois esta definição encontra um caminho difícil pois quando se analisam amostras de pacotes que são encaminhados em escalas de tempo distintas, para uma mesma quantidade, dependendo do modelo o valor da banda efetiva pode ser alterado.

A definição de banda para este trabalho irá diferenciar banda passante de banda efetiva, sendo a efetiva definida pelo cálculo da banda passante em função de requisitos de qualidade de serviços. Ou seja, a banda efetiva é a banda passante observados critérios de qualidade.

O objetivo de uma rede de uma operadora de telecomunicações é o de oferecer serviços adequados às necessidades dos assinantes e em absoluto manter as características acordadas durante todo o período de prestação de serviços. Desta forma, não é interessante que a rede tenha as suas características alteradas constantemente sem que para isso exista a garantia que o ambiente sofrerá instabilidades.

Um grande problema é se definir, em função dos parâmetros apresentados em 3.4 e 3.6, quais são os melhores períodos de atuação, de forma que o amortecimento da instabilidade ocorra de forma a contribuir com a otimização.

Uma proposta para a solução do problema apresentado é a possibilidade da separação do tráfego. Para a definição da separação será usado o conceito do *DiffServ - Differentiated Services* - (Nichols, 1998). O passo mais importante da estratégia é definir qual será o melhor modelo a ser aplicado em função da necessidade de predição. O modelo apresentado na Fig.4-1 engloba as funções de planejamento de crescimento de rede em longos períodos. Porém, a proposta apresentada aqui está relacionada com a possibilidade da utilização em curtos períodos, levando-se em consideração o retorno imediato das novas configurações imediatamente após a análise e inferência dos parâmetros estatísticos capturados.

Na fase de tratamento e análise (T.A.) são efetuadas as coletas de dados através dos sistemas disponíveis podendo ser *Netflow* (Cisco, 2007) ou ainda coletas efetuadas diretamente nas interfaces de rede dos roteadores. A fase de classificação é importante para a análise possa ser efetuada de forma diferenciada, isso é, cada aplicação deve ter as suas amostras separadas de forma a ser possível uma análise por tipo de serviço. Na fase de análise os parâmetros H , H_{EG} ou $h(t)$, α , β , θ , média e variância, desvio padrão ou qualquer outro necessário são calculados ou inferidos.

Após a finalização da fase T.A. os parâmetros são inseridos em um estimador de banda onde é determinada a necessidade por tipo de aplicação ou serviço. Com base nessa informação os túneis serão configurados através de uma ferramenta que fará a tradução das novas configurações em comandos diretos nos elementos de rede.

As função de otimização é também alimentada pela fase de estimação de banda, porém somente irá atuar na rede em longos períodos, após uma fase de simulação onde poderão ser detectadas novas necessidades de ampliação de recursos de rede (aumento de capacidade de transmissão, aumento da capacidade de processamento). Esta fase também é sensível à necessidade de aumento de capacidade por novas demandas de serviços e também por novos tipos de serviços. Nesse caso a rede será realimentada por novas definições de parâmetros de desempenho que afetarão diretamente a fase de otimização de recursos.

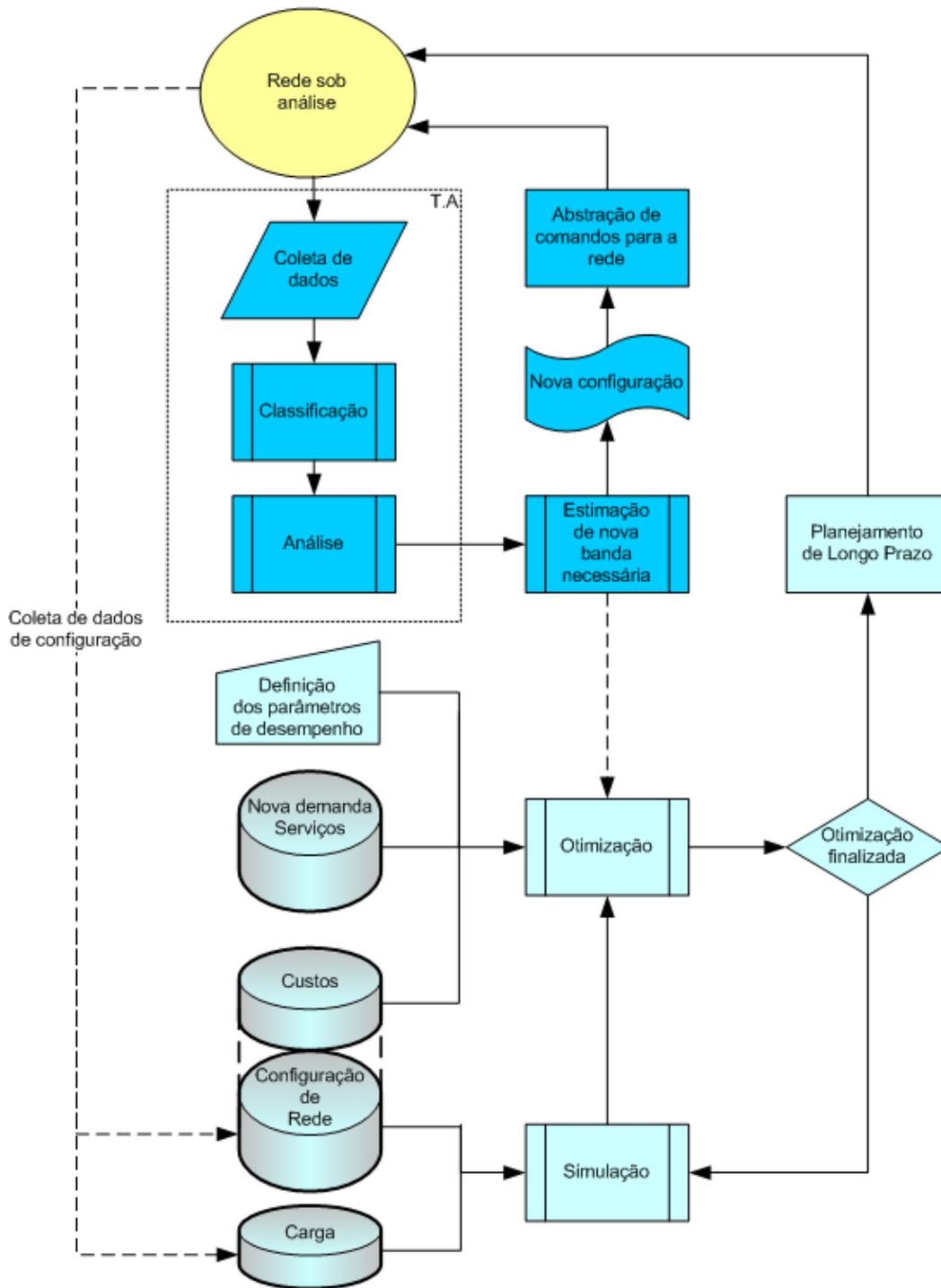


Figura 3.10 – Fluxo geral da estratégia de planejamento e curto(início via fase T.A.) e longo prazo.

Para que o processo de otimização possa existir os custos de rede deverão ser compatíveis com as necessidades de crescimento e apenas se for atingida a viabilidade econômica é que o processo terá continuidade.

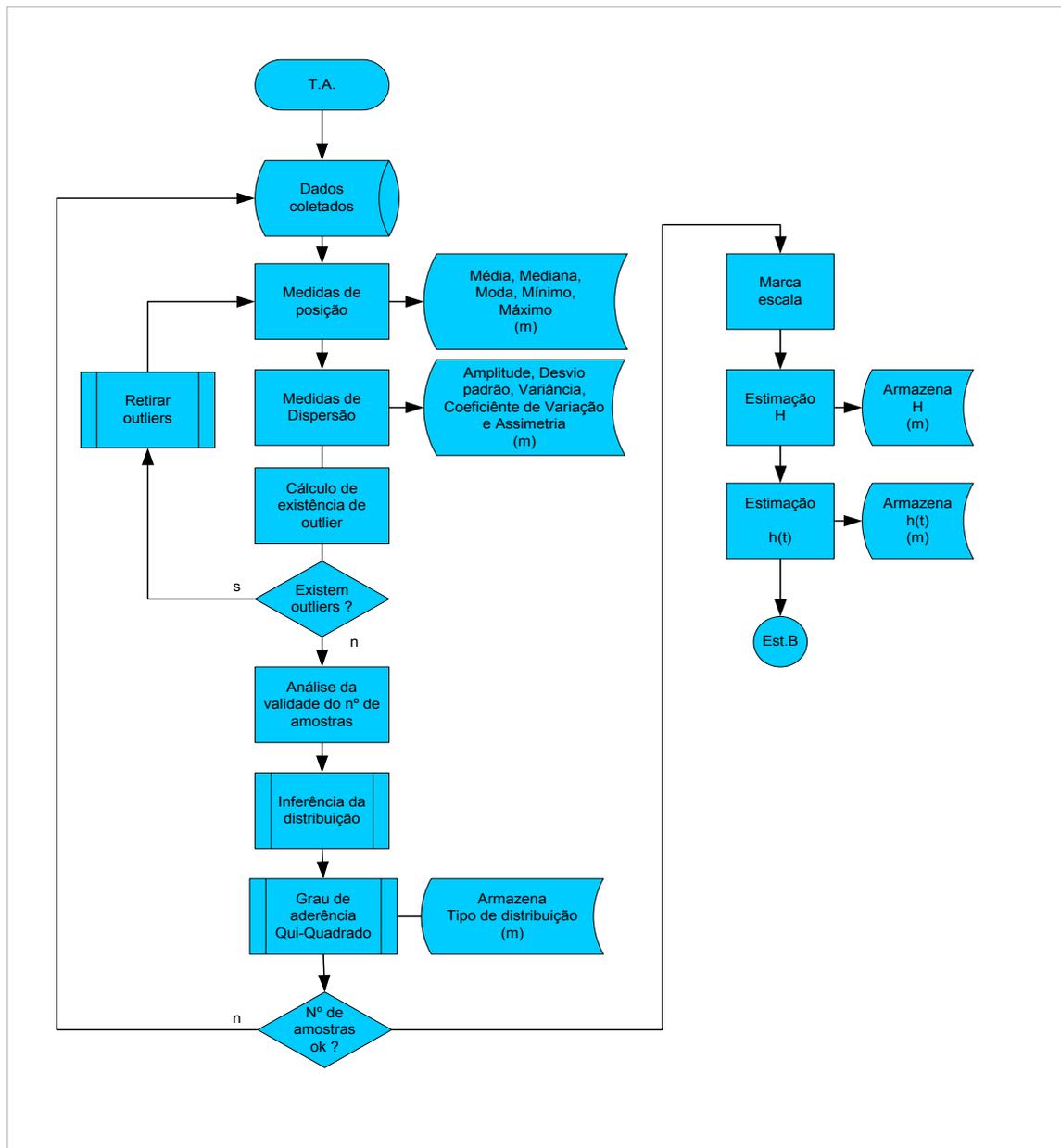


Figura 3.11– Processo inicial de caracterização de tráfego.

No processo de simulação são testadas as possibilidades de falha no processo de otimização e caso sejam positivos para a empresa, terão continuidade com a aprovação para a aquisição e implantação dos novos recursos.

Este trabalho está direcionado para a possibilidade de modificação da configuração da rede durante a sua operação. Para que isso seja possível será usado o fluxo apresentado na Fig.

3.11 nesse caso a fase T.A. (tratamento e análise) será o início seguido pelas funções de estimação, nova configuração e abstração dos comandos na rede

Pseudocódigo “A” para a proposta de planejamento e realimentação rápida

De T.A.

Coleta de dados e armazenamento para uso imediato

$i \leftarrow 0, k \leftarrow$ Classificação dos dados “todas as amostras”

Repetir

 Selecionar a amostra a_i

 Diferenciar

 Armazenar a amostra na base separada

$i = i + 1$, até k

Medidas de posição (média, máximo, mínimo)

Medidas de dispersão (amplitudes, v, σ)

$i \leftarrow 0, k \leftarrow$ Existem outliers “todas as amostras”

Repetir

 Selecionar a amostra a_i

 Retirar

 Armazenar a amostra na base separada

$i = i + 1$, até k

Inferência do tipo de distribuição

Determinação da escala de trabalho

$H \leftarrow$ Estimação do parâmetro de *Hurst*

H_{EG} ou $h(t) \leftarrow$ Estimação do parâmetro global ou expoente de Hölder

Vai para Pseudocódigo B

Um ponto importante com relação às medições é a relação da sua validade com os pontos distantes que podem ser erros de medida ou *outliers* (Chwif, 2006), esses são na verdade medidas realizadas que devem ser desprezadas. Isso evitará que sejam tomadas decisões com base em erros ou medidas de eventos completamente descorrelacionados com os processos sob medida.

Na Fig. 3.11, após os dados terem sido coletados são efetuados os cálculos de medida de posição (média, mínimo, máximo), logo após são feitas as medidas de dispersão representadas pelo desvio padrão ou variância, coeficientes de variação e assimetria. Caso existam *outliers* esses deverão ser retirados. A análise seguinte está relacionada com a inferência do tipo de distribuição, esta será realizada através do teste do Qui-quadrado. Esta informação será armazenada. Nesse momento os parâmetros para a caracterização do tipo de tráfego serão inferidos através de no mínimo duas técnicas distintas. A estrutura

em quadros (*framework*) aqui apresentada pode utilizar qualquer modelo, desta forma não de acordo com a evolução dos métodos de computação de banda poderão ser utilizados outros modelos que se mostrem mais eficazes. O cálculo de banda é apresentado na Fig. 3.12 e é representado por B_p .

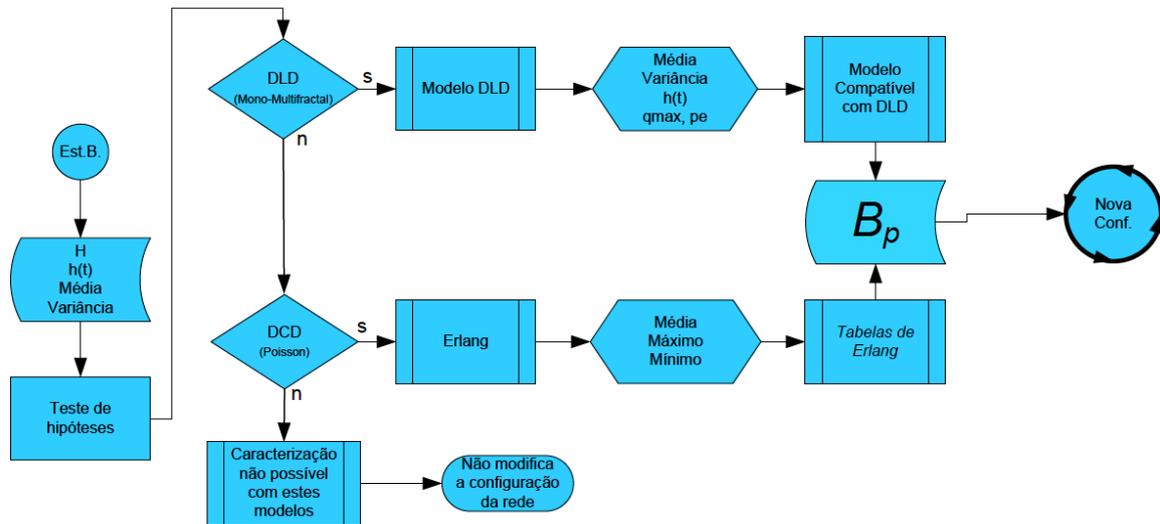


Figura 3.12 – Computação de banda passante

Pseudocódigo “B” para determinação da banda passante.

De Pseudocódigo A

Testar o grau de aderência a uma distribuição Gaussiana

Testar $h(t)$ e H

Se $h(t)$ não é constante

Se $H > 1$ e $H < 0,5$

Ir para o passo 20

Modelo auto-similar ou monofractal

Usar os valores (H , média, σ) para a estimação da banda $\leftarrow B_p$

Modelo um dos modelos multifractais

Usar os modelos aderentes às coletas caracterizadas para a calculo da banda

Retorno para a rede

3.7 COMPARAÇÃO ENTRE OS MÉTODOS PARA O CÁLCULO DE BANDA.

Usando como base o processo de escolha do melhor estimador de banda, uma coleta das estimativas de banda com o uso do estimador multiractal (Stênico, 2013) será comparado com simulações de 125 destas coletas e seus efeitos em cada um dos casos. Na Fig. 3.13 é

mostrado uma comparação entre a banda solicitada e aquela efetivamente usada no processo de provisionamento da rede de uma operadora de telecomunicações internacional. Pode ser observado que o estimador, para as amostras analisadas, tem um grau de acerto excelente, sempre economizando ou minimizando o efeito do *overprovisioning*, muito comum em operadoras de telecomunicações americanas.

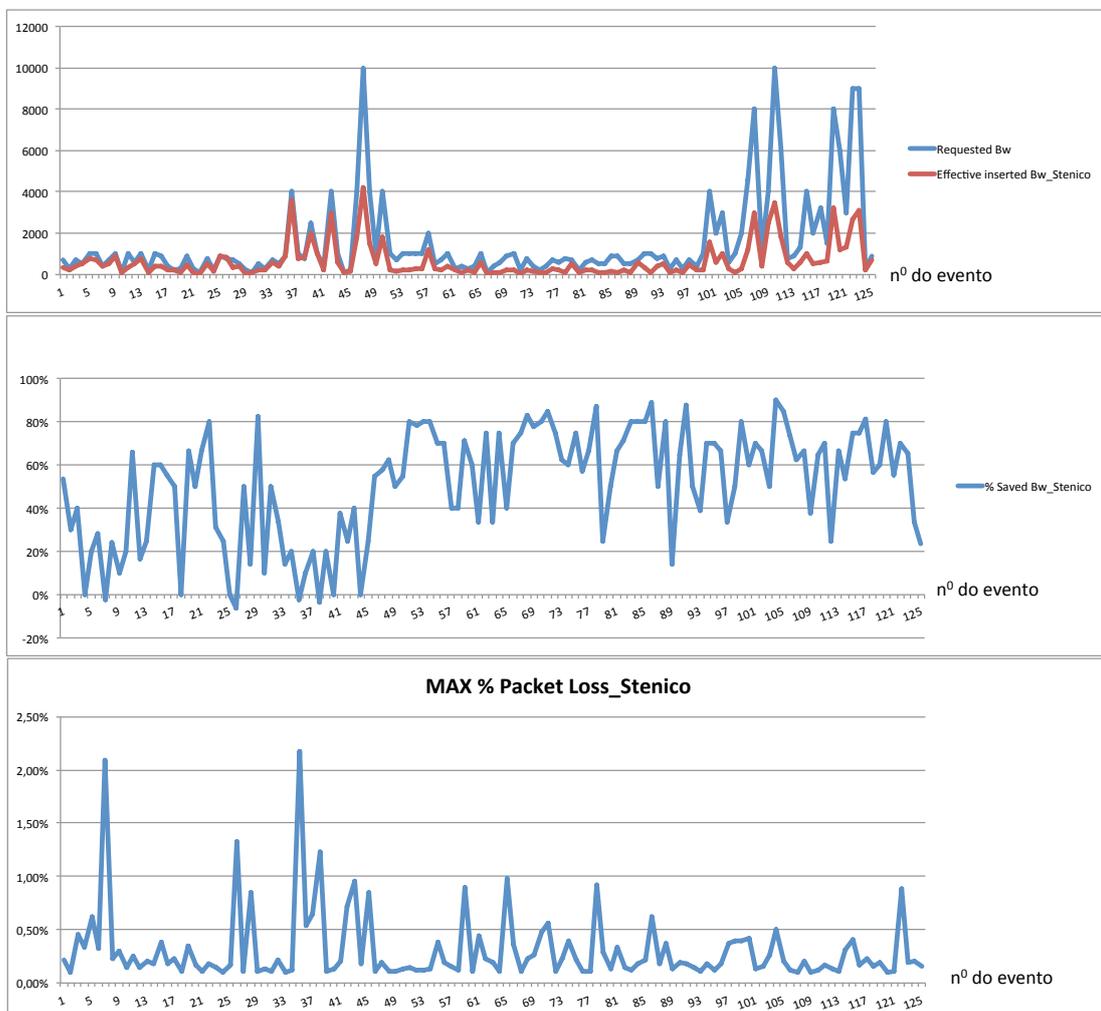


Figura 3.13 – Coletas de uma rede real. Banda requisitada e implantada, economia e perda de pacotes para o estimador de Stênico - DLD (Stênico, 2013).

A taxa de erro, ficou dentro do nível de serviço estabelecido para pacotes que é abaixo de 1%, excedendo este valor apenas uma vez em 125. É importante lembrar também que por se tratar de uma rede real, outros fatores também influenciam a perda de pacotes, incluindo o MTU.

Na Fig. 3.14. é feita uma simulação com o uso o OMNET⁺⁺ (Varga, 2015) , porém usando o tráfego das 125 amostras coletadas de forma a ser possível uma comparação mais próxima do ambiente real, uma vez que seria mais difícil e pouco seguro a comparação dos métodos na rede real.

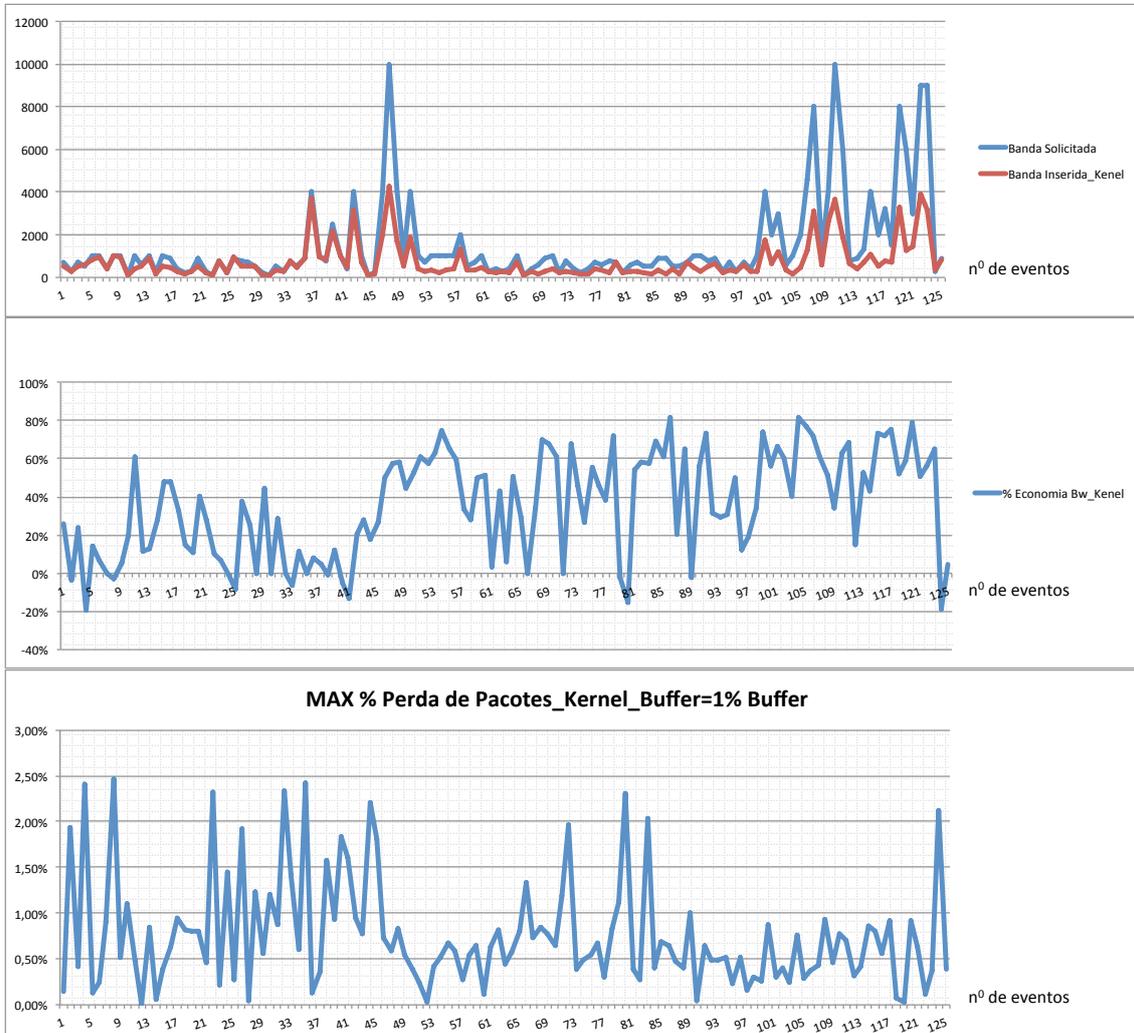


Figura 3.14 – Coletas de uma rede real. Banda requisitada e implantada, economia e perda de pacotes para o estimador de Kernel.

É possível observar que as estimativas em alguns casos ficam aquém do necessário para suprir a demanda. À princípio, isto poderia passar como um efeito positivo em contrapartida ao *overprovisioning*. Mas na prática se revela um fator adicional a ser combatido pois aumenta a probabilidade da perda de pacotes.

A mesma comparação é também realizada na Fig. 3.15. para o método de estimação de banda efetiva por misturas gaussianas. Com as amostras usadas o efeito foi melhor que do método de Kernel.

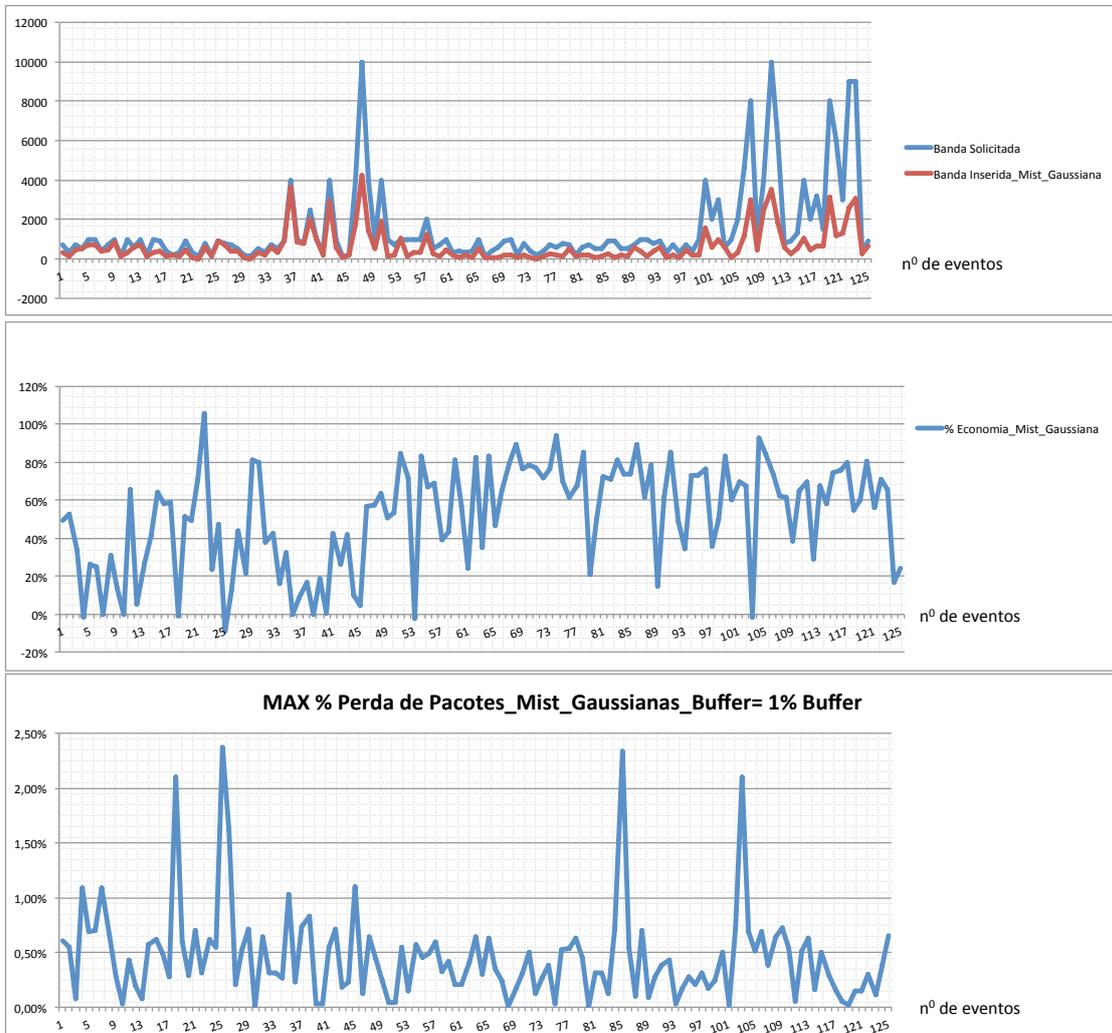


Figura 3.15 – Coletas de uma rede real. Banda requisitada e implantada, economia e perda de pacotes para o estimador de misturas gaussianas.

Na Fig. 3.16 é mostrada a comparação entre a CDF para os 125 eventos, cada um correspondente a um traço tráfego real. É possível notar que o melhor desempenho na simulação foi o do método das misturas gaussianas, porém o método de Kernel não pode ser desprezado, pois obteve resultados interessantes em termos de economia de banda, apesar de aquém dos dois outros métodos testados, ainda possível de ser usado sob supervisão. Ou seja, aumentou a probabilidade de perda devido ao compromisso em diminuir o *overprovisioning*.

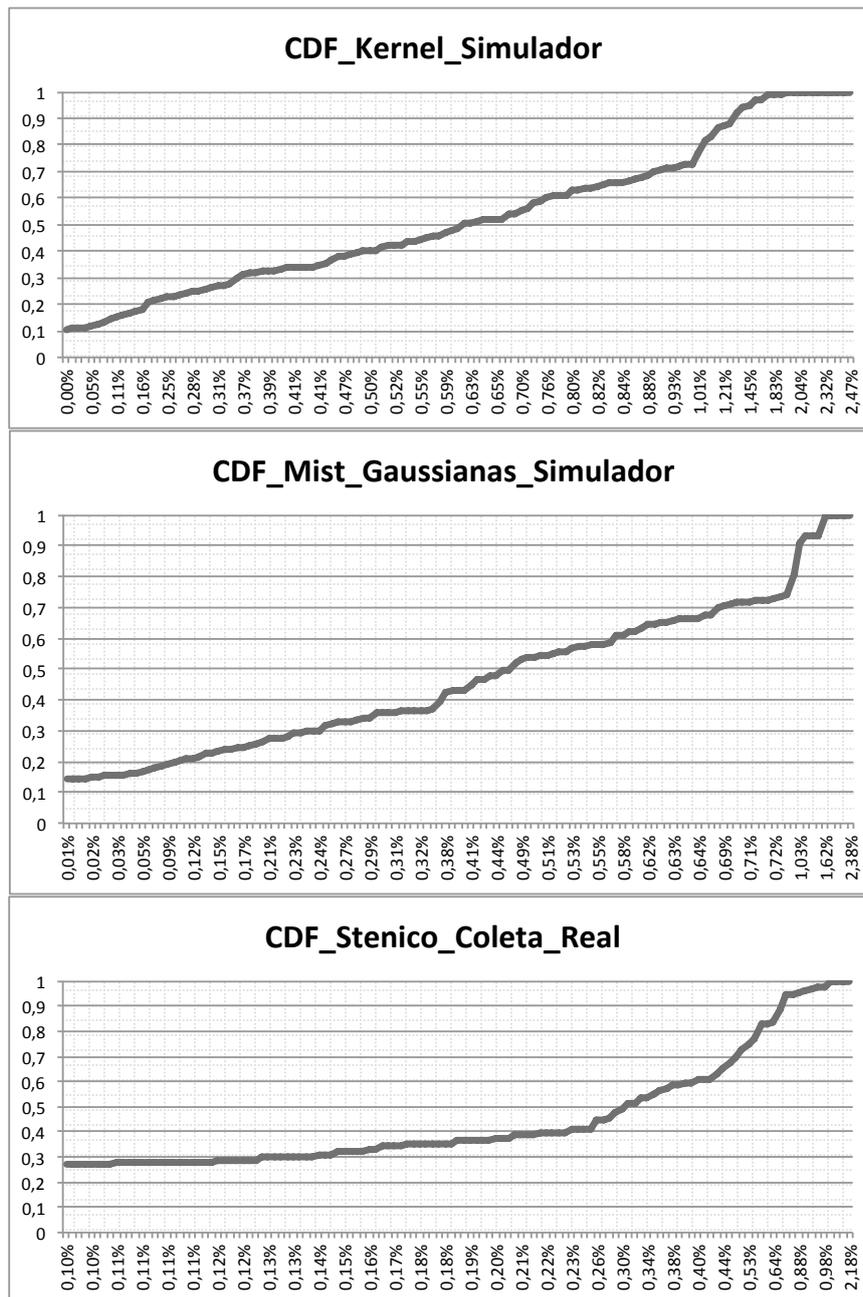


Figura 3.15 – Comparação das CDFs da probabilidade de erro.

A Fig.3.16 mostra uma comparação entre os métodos com relação à economia que poderiam gerar em termos de alocação efetiva de banda. Observa-se que o método das misturas gaussianas tem um desempenho melhor que o método de Kernel.

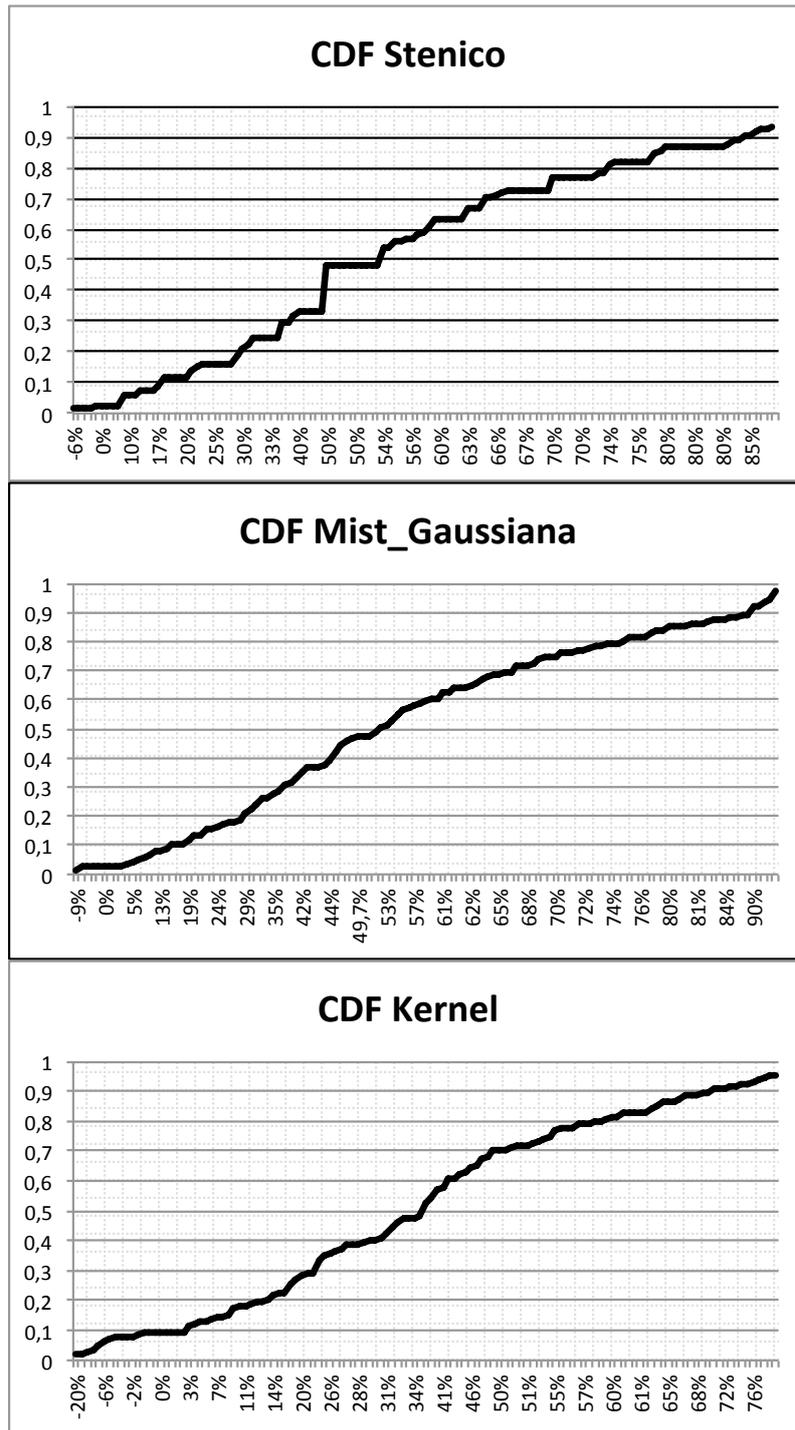


Figura 3.16 – Comparação da economia de banda.

Para este trabalho fui usado o método de Stênico na grande maioria do tempo, porém para efeito comparativo, o método de misturas Gaussianas foi também usado e será apresentado nos capítulos posteriores.

A decisão final deve levar em consideração a facilidade em se caracterizar o tráfego e da extração dos parâmetros que serão usados para o cálculo da banda efetiva. Em uma rede real, se para extrair os dados e se calcular o tempo for superior a 5 minutos para esta ação isolada, dificilmente a área de operações irá tomar a decisão com base nesta informação, pois os roteadores são planejados para esta condição e variações podem comprometer o desempenho em termos de processamento

3.8 ESTIMADORES PARA NOVAS APLICAÇÕES

3.8.1 O WebRTC.

O WebRTC (webrtc, 2015) é uma iniciativa para a construção de bases para a comunicação em tempo real através de APIs (Application Programming Interface) de forma simples.

A sua arquitetura oferece a capacidade de se escrever aplicações multimídia que trabalhem em tempo real, sem a necessidade de plugins, downloads ou instalações. Seu objetivo é ajudar a construir uma plataforma RTC (Real Time Communications) que funcione em qualquer navegador e também que possa ser usado por múltiplas plataformas.

Na Fig. 3.17 é possível ser observado que o framework se baseia em três pilares, o gerador de áudio, o de vídeo e o transporte.

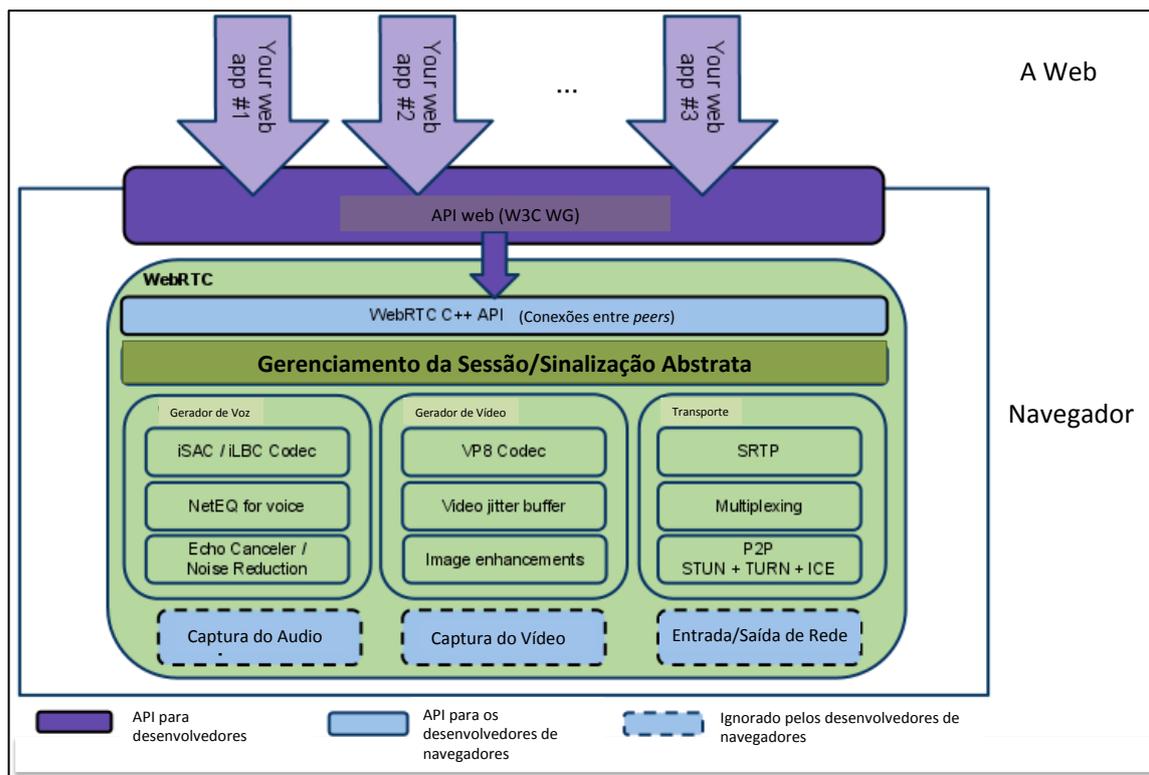


Figura 3.17 – Arquitetura WebRTC, em acordo com (webrtc, 2015)

A estimação de banda referente a cada conexão irá depender do CODEC e protocolos que serão utilizados. Esta comunicação é ponto-a-ponto e peer-to-peer, desta forma a estimação da banda para cada conexão é dada pela definição do próprio CODEC. Este assunto é tratado em (Carvalho et al., 2007), sendo esta condição diferente das estimativas de banda necessárias para o backbone ou núcleo da rede, uma vez que para este último trata-se de tráfego altamente agregado com diversidade de conexões.

3.9 CONCLUSÃO DO CAPÍTULO.

A caracterização é necessária devido à variação do tipo de aplicação que ocorre na Internet, fazendo com que a modelagem que esteja sendo usada possa não mais ser aquela que representa o processo natural. Se isso ocorre o processo real não será corretamente modelado e qualquer estimação será prejudicada. Por outro lado é necessário que o modelo utilizado para representar o tráfego real deve capturar da melhor forma possível, através de poucos e assertivos parâmetros o comportamento real do processo.

Se o comportamento do tráfego não puder ser representado por um processo de forma assertiva, então a banda (ou velocidade) estimada não conseguirá (por si apenas) representar o comportamento de todo o sistema de encaminhamento de pacotes e transmissão. Para uma tomada de decisão, seja em longo ou curto prazo, em uma rede de pacotes de uma operadora de telecomunicações a estimação de banda, portanto, tem um alto grau de relevância e alto impacto para a tomada de decisão, seja para planejar um aumento de capacidade a ser construída, envolvendo novos custos, necessidade de atender a requisitos mínimos de qualidade.

Nesse trabalho o ciclo de curto prazo será o objeto principal de análise, porém sem deixar de considerar a importância do longo prazo.

No próximo capítulo a tomada de decisão será discutida, focando no curto prazo.

4 A INTERFERÊNCIA RACIONAL

De acordo com (Boucadair e Jacquenet, 2014), de uma forma geral a tomada de decisão está presente em todo o ciclo de vida e morte de um processo natural. Por este motivo, de acordo com (Charnes *et al.*, 1978), é preciso caracterizar e fazer com que seja possível a medição da efetividade de uma tomada de decisão. No trabalho (Papadimitriou e Fortz, 2014), a tomada de decisão é estudada com relação à sua interferência no funcionamento de um processo e, dessa forma, faz-se necessário que a tomada de decisão aconteça com o objetivo de melhorar o processo, sem levar o processo para a instabilidade.

Para que a relação entre os sistemas autônomos seja analisada e sejam realizadas, acertadamente, tomadas de decisão que ocorrem em função da necessidade de otimização dos recursos que interconectam estes sistemas, é necessário que parâmetros e medidas sejam estabelecidos de forma a gerar conclusão da efetividade da tomada de decisão. A necessidade de caracterizar, parametrizar e medir os resultados leva a questão para as definições relacionadas ao que é importante ser considerado ao se propor o estudo da tomada de decisão. Em (Charilas *et al.*, 2014), é apresentada uma metodologia para a medição da tomada de decisão em redes. No mesmo trabalho, o *Multi Attribute Decision Making* (MADM) é considerado para o estabelecimento dos parâmetros que serão usados, além dos pesos que cada um deles terá no momento da tomada de decisão. Neste capítulo, serão abordadas algumas técnicas utilizadas para a tomada de decisão de forma a se estabelecer possíveis caminhos para um ciclo de tomada de decisão.

No trabalho de (Griffin e Peroul, 2012), o processo de tomada de decisão do BGP é analisado em relação à sua estabilidade frente às necessidades da tomada de decisão. Ao se tratar do processo da tomada de decisão, faz-se necessário que as consequências da ação sejam possíveis de serem identificadas, de outra forma a análise dos resultados será prejudicada, assim como a análise da estabilidade. Para (Chang *et al.*, 2014), de acordo com a decisão a ser tomada, o conhecimento do processo é absolutamente necessário para que a tomada de decisão possa ocorrer de forma a se efetivar alguma melhoria ou continuidade de um processo. Ainda de acordo com (Chang *et al.*, 2014), a continuidade de

um processo, no caso de serviços, é sem dúvida um bom parâmetro de medida para a efetividade de uma tomada decisão.

No caso das redes de comunicação, (Charnes *et al.*, 1978) e (García-Dorado *et al.*, 2011) apontam para um problema relacionado com os tipos de serviço que não têm como ser caracterizados de forma única. Em (García-Dorado *et al.* 2011), é mostrado que, como as redes IP podem transportar qualquer tipo de tráfego *multimedia*, a caracterização será sempre necessária para que se determine um modelo de tráfego compatível com aqueles serviços que estejam usando a rede no período em que uma decisão deverá ser tomada.

Não é possível se afirmar que determinada rede sempre terá o mesmo tipo de comportamento, pois não se tem garantia que os serviços continuarão a usar os mesmos protocolos e forma de comunicação e adaptabilidade às variações da rede. De acordo com (Aroussi e Mellouk, 2014), as medidas comuns de qualidade relacionadas com QoS (*Quality of Service*) e QoE (*Quality of Experience*) podem continuar a serem usadas como parâmetros de efetividade, porém sempre escolhidas após a caracterização do tipo de tráfego encontrado em determinada rede ou parte desta. Em (Khitmoh *et al.*, 2014), é observado que a qualidade da experiência do usuário, cada vez mais, domina o ambiente das redes IP. No mesmo trabalho, observa-se a necessidade de mais desenvolvimento de metodologias similares ao MOS - *Mean Opinion Score* - para o uso em ambientes da Internet, de forma a se definirem padrões de qualidade além daqueles predefinidos em termos de velocidade em *bps* (bits por segundo).

Para efeito deste trabalho, a definição de tomada de decisão aqui é todo o conjunto de ações ou estratégias que levem a um resultado que modifique a condição da rede através do BGP.

Nas próximas seções, serão discutidos alguns mecanismos de tomada de decisão, uma discussão sobre o conhecimento especialista e mecanismos efetivos para a melhora do processo de tomada de decisão, mas que devem ser usados de forma anterior ao processo de tomada de decisão.

4.1 DESENVOLVIMENTO DE MECANISMOS DE ALGORITMOS DISTRIBUÍDOS

Em (Fiegenbaum, 2007) e (Gattas e Peleg, 2013), é mostrado que os mecanismos de tomada de decisão necessitam ser suportados por algoritmos que possam descrever o processo de forma direta. Destaca-se dentro desta visão o AMD - *Algorithm Mechanism Design* - (Fiegenbaum, 2007), que presume a existência de um ambiente centralizado e confiável para o suporte à tomada de decisão. Porém existem problemas de tomada de decisão que não podem ser resolvidos desta forma, pois não podem depender de centralização, conforme avaliado por (Winter, 2012), em relação à análise da tomada de decisão do BGP. Ainda segundo (Fiegenbaum, 2007), por esse motivo, faz-se necessário que uma abordagem distribuída seja considerada, abrangendo nesse conceito o próprio conceito centralizado. Segundo (Winter, 2012), a DAMD (*Distributed Algorithm Mechanism Design*) é uma tentativa de se explicarem de forma mais abrangente os mecanismos de desenvolvimento de algoritmos. O roteamento EGP (*Exterior Gateway Protocol*), que trata basicamente do BGP (*Border Gateway Protocol*), é um tipo de algoritmo que, por definição, não pode ser tratado de forma centralizada, quando relacionado à troca de tráfego interdomínio. De fato, e por definição (Rekter, 2006), um AS (*Autonomous System*) é autocontido gerencialmente, não aceitando nenhum tipo de interferência externa direta.

Esta definição dificulta o processo de escolha de melhor caminho, melhor custo ou qualquer outra escolha que não esteja dentro da fronteira do AS gerenciado. De forma geral, consegue-se pleno gerenciamento do tráfego que sai, porém nenhum gerenciamento direto do tráfego que entra em um AS vindo da Internet. Dentro das ciências que tratam a engenharia e a computação, tradicionalmente, assume-se a existência de um planejador centralizado que irá definir quais serão os algoritmos que serão usados por cada nó computacional (Fiegenbaum, 2007). No entanto, quando se trata de tráfego Internet, um enlace que liga dois ASes distintos não pode ser visto como um recurso de apenas um dos lados, tampouco apenas dos dois lados em conjunto. Observa-se que os recursos são compartilhados e que a visão sobre eles é a de independência, sob o ponto de vista computacional, não podendo ser considerado, nesse caso, o uso de um plano central. É possível que a visão que melhor se assemelhe a esse caso seja a de agentes egoístas, onde

cada decisão é vista apenas como forma de se maximizar os resultados sob o ponto de vista de apenas um único recurso (ou conjunto), porém sempre dentro de um mesmo domínio. Como as rotas devem ser computadas sempre na perspectiva distribuída, ou seja, por todos os elementos que possuem função de roteamento, ao mesmo tempo todos possuem informações de todos. Cada um dentro da tabela de sua própria tabela de roteamento completa, porém cada decisão a ser tomada é baseada unicamente em critérios autocontidos gerencialmente em determinado AS.

De acordo com o trabalho de (Fiengenbaum, 2007), o processo de computação de rotas deverá ter capacidade de gerenciar a quantidade de interconexões diretamente conectadas ou não (AS-AS), ainda os diferentes modos com que cada AS decide e também as constantes mudanças entre as condições de topologia, utilização e qualidade a que cada conexão está sujeita.

Segundo (Fiengenbaum, 2007), uma forma coerente de se definir o problema de roteamento interdomínio é definir determinada topologia em termos de um grafo.

$$G = (N, L) \tag{4.1}$$

em que cada nó em N , com $N = \{1, \dots, n\}$, corresponde a um AS na Internet e cada enlace em L corresponde a uma conexão direta entre dois AS vizinhos. Pode-se claramente definir AS_d como o destino e P^s como um conjunto de todos os caminhos, sem *loops*, definidos entre origem s e destino d em G . A função do protocolo de roteamento interdomínios é alocar para cada nó $s \in N$ uma rota $R_s \in P^s$.

Em uma abordagem realizada por (Fiengenbaum, 2007), os principais aspectos de construção que deverão ser considerados para a análise da tomada de decisão do protocolo a ser usado são os seguintes.

- i. O protocolo deverá ser distribuído e ter suas informações compartilhadas.

- ii. Para cada pacote, individualmente, o encaminhamento deverá ser baseado em destino. Nesse ponto, cada AS tem o seu próprio salto – *next-hop* – para um destino d que resulta em uma alocação de rotas $T_d = \{R_1, \dots, R_n\}$, formando um par origem-destino para o destino d .
- iii. Ser adaptativo em função das informações de estado e topologia recebidas.
- iv. O protocolo deverá levar em consideração a eficiência em termos de tempo, comunicação entre os nós e armazenamento. Pois deverá ser ágil para repassar informação com eficiência e, devido à quantidade de dados gerados, deverá possuir mecanismos que minimizem a necessidade de armazenamento de informações não úteis ao protocolo.

Observa-se, pelos requisitos no caso de conexões interdomínio (Fiegenbaum, 2007), que apenas o protocolo do tipo *path-vector* terá condições de suprir esses requisitos quando comparados com os mecanismos *distance-vector* e *link-state*.

4.2 SOLUÇÃO POR ANALOGIA, POSSÍVEL USO DE SISTEMAS MULTIAGENTES OU NÃO COOPERATIVOS.

Em acordo com (Shoham, 2009), uma abordagem interessante para o processo de tomada de decisão que leve à mitigação dos problemas de assimetria de tráfego é o uso de sistemas multiagentes que combinam entidades autônomas, cada uma dessas tendo interesses divergentes e ainda informações diversas. Ainda segundo (Shoham, 2009), a arquitetura da Internet é um caso bastante específico para esta abordagem, pois a descrição dos sistemas multiagentes pode ser compatível com esta abordagem.

Um exemplo intuitivo.

No caso do BGP, é possível se fazer uma abordagem intuitiva. O parâmetro do BGP usado na tomada de decisão para influenciar um AS externo é o AS-PATH. Esse parâmetro pode ser usado para que determinado caminho seja preterido em relação a outro. Para que o AS-PATH tenha efeito, o AS de origem encaminha uma nova publicação com toda a informação relativa a um melhor ou pior caminho. Após a publicação, aguarda até que a informação tenha sido propagada pelo BGP na internet, para analisar se a medida obteve o resultado esperado.

Uma estratégia que pode ser usada é a de verificação do congestionamento (perda de pacotes ou atraso) e, a partir dos valores coletados, se tomar a decisão de alteração. Nesse caso, a definição do jogo será relacionada ao número de jogadores que, neste exemplo, são os ASes envolvidos. Ainda para a definição do jogo, é necessária a definição do conjunto de ações que serão realizadas por cada jogador (AS), bem como a de uma função utilidade ou recompensa. Nas próximas seções, algumas analogias serão realizadas com o objetivo de se compararem as diversas teorias que podem ser aplicadas ao caso particular do BGP e de sua função no relacionamento entre sistemas autônomos (ASes).

Uma possível definição de jogo normal ou modo de estratégia.

Para a teoria dos jogos (Nash, 1951) e conforme também apresentado em (Shoham, 2009), o jogo é representado por uma matriz e nesta são mostrados os jogadores, as estratégias e as recompensas. A estratégia é definida como um conjunto de ações que, em função dos dados ou parâmetros, leva a uma recompensa. E a recompensa é a medida final de um conjunto de ações ou estratégias em função da interação entre dois jogadores. Em (Shoham, 2009), é possível se observar que a definição de um jogo na forma normal pode ser usada quando um sistema autônomo atua internamente, isto é, a estratégia não é condicionada ao conhecimento da ação ou da estratégia do outro. No caso do BGP, é interessante notar que, quando a tomada de decisão é focada no relacionamento entre dois ou mais sistemas autônomos na Internet, a estratégia poderia ser chamada de política interna do sistema autônomo, caso a solução passasse pelo uso da teoria dos jogos, em especial, relativa a um jogo na forma normal.

Ainda fazendo uma analogia, dentro dessa abordagem a teoria dos jogos não cooperativos (Nash, 1951) possui ferramental matemático para ser aplicado ao problema da tomada de decisão em termos de encaminhamento de tráfego entre ASes distintos e, ainda, no estabelecimento de topologias criadas pelo protocolo BGP, em função das diversas informações coletadas e do interesse egoísta que cada uma dessas entidades possui.

Em acordo com (Shoham, 2009), é importante notar que a teoria dos jogos não cooperativos é um estudo matemático da tomada de decisão que visa a modelar o indivíduo (*e.g.* um Sistema Autônomo), suas preferências e possíveis ações distintas. Ao final, o objetivo é que seja possível a caracterização dos processos de tomada de decisão em função do comportamento de um grupo, não apenas do indivíduo, mas de suas ações em relação a decisões internas que, por outro lado, geram ações dos demais participantes do grupo. É importante observar que, mesmo para o caso não cooperativo, não se aplicam apenas para situações onde os interesses dos agentes conflitam.

4.3 ANALOGIA ENTRE O PROCESSO DE TOMADA DE DECISÃO DE UM SISTEMA AUTÔNOMO E AGENTES EGOÍSTAS (OU INTERESSADOS APENAS EM SI MESMO - *SELF-INTERESTED* -)

Segundo (Wolsink, 2007), agentes egoístas, ou interessados apenas em si mesmos, são aqueles que necessariamente se preocupam apenas com eles mesmos, porém não necessariamente querem estabelecer uma relação de vantagem constante com relação aos outros agentes. Para esse tipo de agente, cada indivíduo possui sua própria descrição de estados, dentro do universo em que estejam contidos, que lhe seja mais favorável, não importando se o efeito nos outros é positivo ou negativo, pois isso não lhes interessa. Um AS é, sem dúvida, um excelente exemplo a ser estudado desse tipo de agente, pois se encaixa totalmente nessa definição. Além disso, dentro do AS, o protocolo BGP, que tem a responsabilidade de transportar informação para as tomadas de decisão, é controverso quando deve estabelecer possibilidades de caminhos de interconexão, pois isso se constitui em um grau de dependência forte entre os ASes, mas sem gerar nenhuma oposição a tomada de decisão interna ou alterar o comportamento egoísta dos sistemas.

Analogamente, para modelar os interesses de um agente (neste caso um sistema autônomo) pode ser usada a teoria da utilidade, de forma a poder ter uma abordagem teórica para quantificar o grau de preferência de um agente face a um grupo de alternativas disponíveis. Nessa linha, também é buscado entender como essas preferências mudam em função da incerteza sobre as alternativas. A função utilidade deve mapear estados do universo onde os agentes estiverem contidos em números reais, que serão interpretados de forma que, quando um agente está em dúvida com relação a qual estado gerará a melhor decisão, a sua utilidade é definida como o valor esperado da sua função utilidade com respeito da distribuição de probabilidade sobre os estados.

O fato de ser difícil determinar se a tomada de decisão irá gerar a recompensa desejada por um agente faz com que essa recompensa deva ser determinada por algum tipo de parâmetro mensurável. A função utilidade pode ser usada para essa finalidade de forma mais específica. Por outro lado, na análise da tomada de decisão de um Sistema Autônomo, não se tratando apenas de melhor decisão tática ou operacional, de fato qualquer ação não mapeada pela camada de estratégia certamente não tem como ser medida e, nesse caso, não tem como se ter um critério de tomada de decisão definido.

4.3.1 A decisão e a recompensa do BGP

De acordo com (Shoham, 2009), a utilidade está relacionada com a preferência para melhorar o entendimento das recompensas de um processo. Esse conceito foi inicialmente proposto por Von Neumann e Morgenstern e é chamado de função utilidade Neumann-Morgentern. Para entender esse conceito, denota-se O um conjunto finito de saídas e, para cada par $o_1, o_2 \in O$, faz-se:

- a. $o_1 \succcurlyeq o_2$ quando a proposição de agente preferir levemente o_1 a o_2 .
- b. $o_1 \sim o_2$ quando a proposição de um agente for indiferente a o_1 ou o_2 .
- c. $o_1 \succ o_2$ quando a proposição de um agente preferir estritamente o_1 a o_2 .

É importante notar que a primeira proposição acima pode gerar qualquer uma das duas seguintes da seguinte forma:

Para $o_1 \succ o_2$, pode-se declarar uma relação em que: $o_1 \succcurlyeq o_2$ e não $o_2 \succcurlyeq o_1$.

Para $o_1 \sim o_2$, pode-se declarar uma relação em que: $o_1 \succcurlyeq o_2$ e $o_2 \succcurlyeq o_1$.

Dessa forma, conclui-se que, com apenas o símbolo \succcurlyeq , é possível se gerarem as demais possibilidades.

Ainda de acordo com (Shoham, 2009), na tomada de decisão, a incerteza de qual saída terá a maior recompensa em função de como as preferências interagirão é algo que precisa ser minimizada. A teoria da utilidade emprega o conceito de loteria para atingir o menor grau de incerteza. Formalmente, uma loteria é a distribuição de probabilidade de acordo com as saídas, onde p_k relaciona o grau de preferência de uma posição o_k até que todas as possibilidades de interação sejam concluídas. O somatório de todas das probabilidades individuais do par $[p_k; o_k]$ é igual a 1.

$$[p_1: o_1, \dots, p_k: o_k] \Rightarrow o_i \in O; p_i \geq 0 \text{ e } \sum_{i=1}^k p_i = 1 \quad (4.2)$$

Assume-se que \mathcal{L} define um conjunto de todas as loterias. Estendendo a relação \succcurlyeq e aplicando aos elementos de \mathcal{L} assim como a todos os elementos de O , efetivamente deverão ser consideradas as loterias sobre as saídas para se encontrar as saídas.

No caso particular do BGP, devido à definição de um sistema autônomo, a decisão ocorre sempre de forma egoísta: a recompensa dos agentes terá relação direta apenas com o definido pelas políticas (ou políticas internas, por redundância). A relação de preferência pode ser vista por meio do teorema da relação de preferência.

O que interessa ao final, em se tratando da mitigação de problemas de desempenho, é que a decisão que tenha sido tomada seja aquela que produziu a melhor recompensa. No capítulo 5, uma das recompensas medidas é o grau de efetividade que uma estratégia produz. Para isso, é realizado um estudo com engenheiros com experiências distintas com o BGP. Cada um é acompanhado por um período de tempo e ao final do estudo é verificado que o grau de efetividade, que relaciona o número de intervenções necessárias para a solução de um

problema de interconexão, ou seja, a efetividade aumenta no sentido em que o número de intervenções necessárias diminui para a solução de um problema.

4.3.2 Definição das estratégias da tomada de decisão.

De acordo com (Klein, 2008), é interessante observar que, em um jogo, existem diversas estratégias que podem estar disponíveis para cada um dos jogadores e devem ser definidas. De acordo com (Wassim *et al.*, 2014), para o controle de tráfego entre os sistemas autônomos (ASes), a estratégia pode ser considerada de forma distribuída ou centralizada. Quando a estratégia é centralizada, todos os jogadores (ASes) encaminham para um ponto centralizado suas informações e, a partir desse ponto, as decisões são tomadas e depois distribuídas. A estratégia totalmente distribuída é aquela em que não existe ponto de tomada de decisão centralizado.

Em (Griffin e Perouli, 2012), é observado que, em ambos os casos, a tomada de decisão é dependente das informações que são trocadas entre os diversos jogadores, neste caso, os ASes. Em (Teixeira *et al.*, 2007), a interação entre os ASes é analisada por uma abordagem do controle interno, ou seja, a tomada de decisão mais importante não leva em consideração o controle do tráfego que chega (*inbound*), mas o do tráfego que sai (*outbound*) do AS. Ainda em (Teixeira *et al.*, 2007), os diversos nós que compõem o AS tomam, ainda assim, suas próprias decisões, baseados em uma política comum definida pelo administrador da rede.

Em (Shoham, 2009), é definido que o perfil de uma estratégia mista (P.E.M.) é mostrada como um conjunto de perfis estratégias mistas será o produto cartesiano do conjunto de estratégias mistas individuais, onde S é a estratégia e $S_1 \times \dots \times S_n$. $S_i(a_i)$ é definido como a probabilidade que uma ação irá jogar sob a estratégia s_i . Por outro lado, o suporte à estratégia mista é dado pela utilidade esperada.

Em (Teixeira *et al.*, 2007) e (Wang, 2013), observa-se que tanto a tomada de decisão centralizada quando a distribuída usam a estratégia mista. Em função disto, é possível o uso da utilidade esperada de uma estratégia mista - $E(uE.M.)$: Dada uma forma-normal de

um jogo (N, A, u) , a utilidade esperada u_i para um jogador i de um perfil de estratégias mistas $s=(s_1, \dots, s_n)$ é definido por:

$$u_i(s) = \sum_{a \in A} u_i(a) \prod_{j=1}^n s_j(a_j) \quad (4.3)$$

Usando as definições de (Shoham, 2009), tem-se uma tupla (N, A, u) , em que:

N é um conjunto finito de n jogadores indexados por $i = 1, 2, \dots, n$;

$A = A_1 \times \dots \times A_n$, em que A_i é um conjunto finito de ações disponíveis ao jogador i , $i = 1, 2, 3, \dots, n$, em que cada vetor $a = (a_1, \dots, a_n) \in A$ é chamado um perfil de ação.

$u = (u_1, \dots, u_n)$, em que $u_i: A \mapsto \mathbb{R}$ é o valor real da função utilidade do jogador i , $i = 1, 2, 3, \dots, n$.

A utilidade pode ser um dos parâmetros a serem usados para se medir a eficácia da tomada de decisão. No caso do relacionamento entre sistemas autônomos, a analogia que está sendo proposta neste trabalho é o uso das medidas de atraso, perda de pacotes e grau de simetria para determinação das recompensas.

4.3.3 Jogo de Soma Zero

O tipo de relacionamento entre os ASes não é, necessariamente, uma condição em que se um ganha tudo e o outro perde tudo. Não é um jogo de soma zero. Essa condição poderia explicar a motivação de ASes *TIER-1s* também aceitarem o *prepend* como uma possível solução para a decisão interna, sendo essa decisão influenciada externamente, independentemente do tamanho do AS que esteja tentando influenciar o *TIER-1*.

Em (Das *et al*, 2013), é observado que, na teoria da decisão de um único agente, o ponto chave é a definição de uma estratégia ótima que será aquela que maximizar a expectativa de retorno do agente para um dado ambiente em que este agente atua. Para o caso de um agente único, caso o ambiente seja modelado por um processo estocástico ou, até mesmo, caso o ambiente seja apenas parcialmente observável, isso é, caso a incerteza domine os

processos, o agente estará sujeito a situações muito difíceis de serem mapeadas. Em (Papadimitriou *et al.*, 2013), no caso de múltiplos agentes, ou multi-agentes, a situação fica ainda mais crítica, pois, nesse caso, a discussão inclui outros ambientes ou ainda outros agentes que também esperam maximizar as suas expectativas de retorno. Para esse caso, a expectativa de retorno de um agente depende também da escolha dos outros. Em (Shoham, 2009), o conceito de múltiplos agentes é identificado como um subconjunto de saídas *ou* conceito de soluções que interessem em qualquer sentido.

Em (Emrouznejad *et al.*, 2010), a definição de otimização de Pareto leva em consideração o fato de não ser possível, para um observador externo, definir se a saída individual de um é melhor que a do outro. Ainda segundo (Emrouznejad *et al.*, 2010), isto é impossível, pois os interesses de um agente não podem ser ditos mais importantes que os interesses de outro. No entanto, se for usado o Teorema de von Neumann e Morgenstern, é possível se multiplicar todo o retorno de um agente por um número positivo, fazendo com que exista uma mudança na maximização dos resultados da soma das funções utilidade dos diferentes agentes. Para este caso, é possível, também dizer que algumas saídas podem ser mais importantes que outras.

No caso do BGP ter-se-ão recompensas diferentes dependendo o tipo de estratégia que for usada e também retornos diferentes para cada um dos tipos de interação que estiver ocorrendo.

Para o caso do BGP, as políticas de cada um dos ASes, são consideradas as estratégias. Estas são individuais para cada um destes.

Assim como analisado por (Winter, 2012) e (Teixeira *et al.*, 2007), para um AS que esteja recebendo tráfego de outro, é possível afirmar que a sua otimização de recompensa ocorrerá se os enlaces que estiverem suportando esta conexão estiverem sendo usados de forma balanceada e sem possibilidade de perda enquanto existir capacidade agregada disponível. Porém, esta não é uma condição de recompensa simétrica, pois, para o AS que está encaminhando tráfego, não há nenhuma vantagem em se mudar a estratégia. Este é um exemplo interessante onde será necessário encontrar, se possível, uma condição de domínio ou otimização de Pareto, que poderia ser usada para se determinar o perfil de uma

estratégia ou das políticas internas de um sistema autônomo (AS), quando relacionadas à configuração do BGP.

De acordo com (Shoham, 2009), domínio de Pareto pode ser definido como o perfil de estratégia de Pareto domina o perfil de estratégia \mathbf{s}' se para todo $\mathbf{i} \in \mathbb{N}$, $\mathbf{u}_i(\mathbf{s}) \geq \mathbf{u}_i(\mathbf{s}')$ e exista algum $\mathbf{j} \in \mathbb{N}$ para o qual $\mathbf{u}_j(\mathbf{s}) > \mathbf{u}_j(\mathbf{s}')$. De forma mais explicativa, em uma estratégia de domínio de Pareto, o perfil de um jogador pode ser mudado para melhor sem fazer com que o perfil dos demais seja piorado.

Otimização de Pareto: o perfil de estratégia \mathbf{s} é o ótimo de Pareto ou com a melhor eficiência de Pareto se não existir outro perfil estratégico $\mathbf{s}' \in \mathbf{S}$ em que a definição de Pareto domine \mathbf{s} . Para este caso, a melhor estratégia pode levar a mais de uma saída ótima; para cada jogo deverá existir no mínimo uma saída ótima.

De forma interessante, observa-se que atingir o equilíbrio não é um objetivo das grandes corporações quando se trata de definições da estratégia ou da definição das políticas, pois, em muitas situações, o desequilíbrio, ou a instabilidade, na estratégia de um jogador de menor porte interessa ao de maior porte.

Em (Emrouznejad *et al*, 2010) e em (Misyak e Chater, 2014), é observado que a função utilidade que todos vão buscar em seus perfis estratégicos é a de se maximizar o desbalanceamento em seu favor ou, via de regra, a de se buscar o equilíbrio fraco e, por isso, muito instável. Ao se observar a atuação humana apenas, verifica-se um grande esforço operacional para manter as redes em funcionamento, pois, de fato, faz-se necessária a constante intervenção do engenheiro de redes no sentido de melhorar a otimização dos recursos disponíveis.

No caso do uso da teoria dos jogos (Nash, 1951), observa-se que o teorema baseia-se na existência de um número finito de jogadores, que podemos assumir como os ASes na Internet, e nos perfis estratégicos, que são as estratégias que cada um dos ASes possui ao estabelecer suas políticas. Dessa forma, pode-se assumir que existe, ao menos, um equilíbrio de Nash para a relação entre dois ou mais ASes, e este deve ser buscado.

O objetivo é o de se maximizar a recompensa que cada um dos jogadores (ASes) terá. No caso mais específico que está sendo estudado nesse trabalho, o foco será minimizar os efeitos da assimetria de tráfego entre ASes com menor poder de geração de tráfego em relação aos TIER-1s, que segundo (Lodhi *et al*, 2014), também está presente nos Estados Unidos da América e Europa.

4.4 CARACTERIZANDO A TOMADA DE DECISÃO

Conforme discutido, a tomada de decisão do AS tem caráter egoísta e normalmente tem suas ações regidas por um protocolo pelo qual fica claro que a estratégia dominante (Shoham, 2009) é a que pode melhor se adequar às regras de comportamento do mesmo, não sendo, necessariamente, a que trará os melhores resultados. No caso do BGP, pode-se analisar a Fig. 4.1 onde é descrita a estratégia de tomada de decisão, dando a cada um dos parâmetros um peso e precedência com relação aos demais.

	Weight	Local Preference	Rotas locais	AS PATH
Weight	<i>wg,wg</i>	<i>wg,lp</i>	<i>wg,rl</i>	<i>wg,as</i>
Local Preference	<i>lp,wg</i>	<i>lp,lp</i>	<i>lp,rl</i>	<i>lp,as</i>
Rotas locais	<i>rl,wg</i>	<i>rl,lp</i>	<i>rl,rl</i>	<i>rl,as</i>
AS PATH	<i>as,wg</i>	<i>as,lp</i>	<i>as,rl</i>	<i>as,as</i>

wg>lp>rl>as

Parâmetro	Codigo	Peso
WEIGHT	wg	2
LOCAL PREF	lp	1
ROTAS LOCAIS	rl	0
AS PATH	ap	-1

Figura 4.1 - Jogo entre dois ASes baseado em estratégia dominante.

Pode-se observar pela tabela que, em função da precedência entre os parâmetros, existem situações mapeadas que nunca serão usadas caso determinado parâmetro de mais alta precedência esteja configurado para ser escolhido em detrimento dos demais. Uma saída

para este problema é tentar remover a estratégia dominante. Aqui é importante deixar claro que o caso de dominação pode ocorrer em qualquer sentido, mas o será mais importante quando o AS que estiver recebendo tráfego quiser modificar o seu perfil de tráfego de entrada (*inbound*), pois este não é controlado por ele mesmo, sendo este um caso particular para a situação de assimetria de tráfego.

4.5 ANÁLISE DA ESTRATÉGIA USADA PELO BGP

Em (Shoham, 2009), é proposta uma definição de dominação. Fazendo s_i e s'_i duas estratégias para o jogador i e S_{-i} um conjunto de todas os perfis estratégicos do restante dos jogadores. Então:

1. s_i domina estritamente s'_i se, para todo $s_{-i} \in S_{-i}$, é o caso de $u_i(s_i, s_{-i}) > u_i(s'_i, s'_{i-i})$. Dominação Forte
2. s_i domina fracamente s'_i se, para todo $s_{-i} \in S_{-i}$, é o caso de $u_i(s_i, s_{-i}) \geq u_i(s'_i, s'_{i-i})$ e, para pelo menos um $s_{-i} \in S_{-i}$, $s_{-i} \in S_{-i}$, é o caso de $u_i(s'_i, s'_{i-i}) > u_i(s_i, s_{i-i})$. Dominação fraca.
3. s_i domina muito fracamente s'_i se, para todo $s_{-i} \in S_{-i}$, é o caso de $u_i(s'_i, s'_{i-i}) \geq u_i(s_i, s_{-i})$. Dominação muito fraca.

Analogamente à questão do relacionamento entre sistemas autônomos, o problema da dominação é que acaba por levar a disputa (pelo equilíbrio) para um conjunto menor de soluções que possam gerar uma recompensa favorável para os agentes. Uma vez que existe um conjunto de estratégias que sempre irão prevalecer em relação às demais, algumas estratégias acabarão por se tornar sem função no certame. Esse caso é comum em relações entre ASes de tamanhos diferentes (*TIERs*). Esse também é o caso do uso do parâmetro AS-PATH para gerar o *prepend*, estratégia que se trata basicamente de inserir na descrição do caminho o próprio AS de origem, com o objetivo de diminuir a chance de uso de uma rota indesejável, e com isso tentar mudar uma interpretação de estratégia de um AS que esteja lhe encaminhando tráfego.

Como o parâmetro AS-PATH só vem a ser analisado após três outros terem sido analisados, a estratégia local sempre será dominante. Para se equilibrar o jogo, usando-se essa linha de pensamento, é necessário que a dominação dos parâmetros precedentes seja anulada. Por outro lado, isso faz com que o AS perca em termos de auto gerenciamento (por definição), dificultando o seu controle por estar muito susceptível a interferências externas. A possibilidade de tentativa de modificação do *prepend* é um objeto de estudo nesse trabalho, com alguns resultados práticos que serão discutidos.

O protocolo BGP é o protocolo especificado pela RFC 1771 e atualizado pela RFC 4271, sendo o objetivo principal, conforme já explicado, a troca de informação de rotas entre os ASes. O ponto principal para o processo do BGP é manter a individualidade de tomada de decisão dentro do próprio AS. Segundo (Fiegenbaum, 2007), a autonomia do BGP pode ser expressa em função do grau de liberdade que cada AS possui ao escolher localmente a forma de importar ou exportar suas rotas, podendo construir suas políticas sem nenhuma interação com outros sistemas autônomos.

Apesar de já definido, novamente em acordo com (Rekther, 2006), um AS é, por definição, um sistema com gerenciamento autocontido, não sendo possível a interferência externa direta em seus processos de tomada de decisão. A política de decisão do BGP é constituída para suportar as necessidades internas do AS. Este tipo de definição se relaciona muito bem com os processos egoístas ou *selfish* (Wolsink, 2007). Sem dúvida, a abordagem egoísta traz vantagens sob o ponto de vista de gerenciamento de capacidades internas e segurança, porém não em termos de otimização de recursos.

Em acordo com (Woodward, 2013), a assimetria de tráfego, hoje, é constante em muitos dos serviços e, também, nos casos analisados e relacionados com a dependência dos países da America do Sul ao conteúdo presente na America do Norte. Se a principal característica do BGP é a de não permitir, diretamente e prioritariamente, que sua tomada de decisão seja influenciada externamente, como fazer com que o tráfego entrante, nesse caso a maior parcela, seja direcionado de acordo com as capacidades existentes?

Caso nenhuma solução seja possível em relação a modificações propostas, percebe-se que uma solução para o caso é a da negociação entre os administradores de sistemas

autônomos, chegando-se a uma solução de compromisso que interesse a ambos. Nesse caso, pode envolver questões financeiras entre as empresas envolvidas. Por outro lado, mesmo quando se encontra um meio termo, este é normalmente subjetivo, baseado em experiências passadas e normalmente sem um modelo matemático ou computacional que justifique a tomada de decisão, mesmo nesse nível. Não é difícil perceber que a tomada de decisão é afetada, também aqui, pela falta de modelos de predição que possam sustentá-la e gerar a confiança da efetividade com melhoria, definidas as métricas para acompanhamento (Aitken, 2010). Nesse ponto, destaca-se uma abordagem de estratificação da tomada de decisão em camadas conforme Fig. 1.3 1.3. onde deve ser considerada a construção de uma política de troca de tráfego que será definida em função das necessidades e objetivos que a organização ou empresa tiver para o uso do sistema autônomo. Somente após a definição das políticas será possível se definir ou se programar o nível tático, onde as ferramentas disponíveis serão usadas com o objetivo de se chegar à melhor decisão, ou àquela que consiga gerar a melhor eficiência possível de uso de recursos apenas por reprogramação dos recursos existentes ou, ainda, a realimentação do planejamento de longo prazo com o acréscimo de capacidade.

No nível operacional, a tomada de decisão poderá ser baseada na existência de problemas anteriores que possam ser usados como base de conhecimento e comparação para se encontrar uma solução adequada e atual para o problema ou, ainda, através da busca parcial ou cognitiva, quando não existir base de conhecimento com soluções anteriores que possam ser usadas como solução para o problema atual.

No nível estratégico, as políticas podem estar relacionadas com vantagens comerciais, tais como menor preço, necessidade de interconexão física com restrições de atraso e perda de pacote, entre outros mecanismos que podem não estar relacionados com aspectos unicamente técnicos. É importante entender que o nível tático é programado seguindo as definições do nível estratégico e o processo de tomada de decisão do próprio BGP. Na Fig. 1.1, têm-se os mecanismos do BGP para a tomada de decisão e que são levados em consideração. O fluxo apresentado denota que, quanto mais local, mais prioritário é o parâmetro. No caso, o peso das interfaces tem maior prioridade. Em caso de empate, o próximo parâmetro é o LOCAL PREFERENCE. Apenas em terceira opção vem o AS-PATH, que, por outro lado, é um parâmetro altamente utilizado para tentativas de

influenciar a tomada de decisão de um AS externo ao de próprio domínio. O parâmetro ORIGIN tem o objetivo de mais uma vez dar maior prioridade ao que foi aprendido localmente em detrimento do que foi aprendido externamente, ou seja, nesse ponto o IGP (*Interior Gateway Protocol*) tem mais prioridade que o EGP (*Exterior Gateway Protocol*) e, por último, as rotas que estão com informação inconsistente ou incompletas. O parâmetro AS-PATH tem hoje um papel preponderante no funcionamento da Internet. Na Fig. 4.2.a, tem-se uma análise de soluções com o uso do *prepend* de uma rede real no período de 12 meses entre jan/2013 a dez/2013. Nesse caso, fez-se uso do AS-PATH para tentativa de modificação de encaminhamento de tráfego por AS externo.

Observa-se que mais de 69% das soluções ocorrem com o uso do AS-PATH, porém apenas 29,55% na primeira tentativa e 39,59% com mais de uma tentativa. Problemas de roteamento externos ou erros de configuração do BGP foram responsáveis por 10,92% das soluções. Para 10,48% dos problemas, a solução foi dada com o uso de *communities* e, ainda, 9,46% das soluções tiveram problema originado em erros de configuração dos protocolos internos.

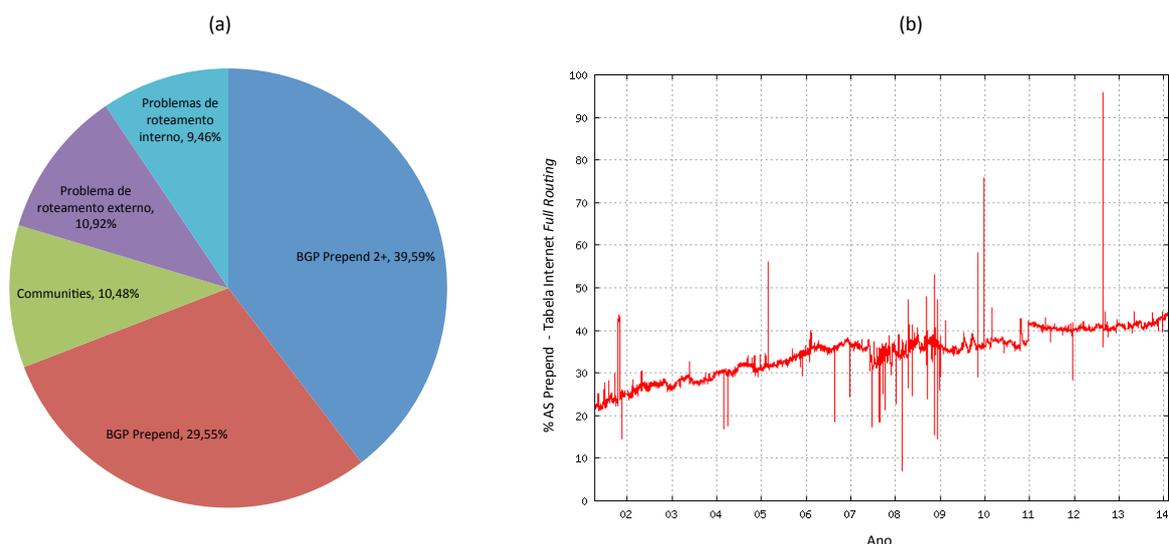


Figura 4.2 - (a) Dados reais extraídos de uma rede real em relação aos tipos de problemas ocorridos entre janeiro e dezembro de 2013. (b) Indicação de probabilidade de uso do *prepend* com base nas medidas das rotas com descrição específica. Dados extraídos de (Geoff, 2014) em <http://bgp.potaroo.net/as6447/>].

Outra característica importante a ser analisada é a topologia da rede. De forma a ser possível uma rápida análise do processo de tomada de decisão da Internet, foi utilizado um algoritmo específico para a coleta de dados relativos ao raio da Internet. Essa informação será útil, também, na definição do tipo de solução a ser aplicada em determinado problema de tráfego de origem. Usando o critério de Bellmand (Brandes, 2001), um vertex $v \in V$ encontra-se em um caminho mais curto entre os vértices $s, t \in V$, se e somente se $d_G(s, t) = d_G(s, v) + d_G(v, t)$.

Apresenta-se o algoritmo:

```

Dada uma tabela de roteamento cheia  $T=d_G(s,t)$ 
Para uma subrede  $S_j$ 
  Para um Caminho $_{S_j}=\{AS_0, AS_1; AS_{j-1}; AS_j\}$ 
    Agregue  $\{Path_{S_j}\}$ 
    Min  $\{Path_{S_j}\}$ 
    Conte até  $j$ 
     $\{S_j\} \in AS_k$ 
     $r_{ASK}=j$ 
  Fim
Fim

```

Observa-se, ainda, que na tabela de rotas analisada (*full table* de março de 2013 extraída de um roteador em operação em uma rede real) tem-se grande parte dos ASes conectados em até 3 saltos de distância. De acordo com (Winter, 2012), o uso do *prepend* é uma possibilidade de solução de interferência na tomada de decisão externa, somente podendo ocorrer quando o caráter egoísta é menos importante na política interna do AS.

O modelo de tomada de decisão que possa levar a uma condição de efetividade na tomada de decisão deve levar em conta o conhecimento dos serviços, do tráfego por eles gerado e das configurações físicas e lógicas, incluindo as topologias e protocolos utilizados. A caracterização do tráfego e da topologia interna e externa ao AS é imprescindível para o processo de predição de utilização dos recursos de rede, seja no ciclo curto ou longo de operação de rede. Com relação ao BGP, é possível se trabalhar com as condições descritas pelas RFCs atuais ou, ainda, se fazer uma proposta de modificação do modelo de decisão que vise a tocar na estratégia e, com isso, a se modificar o tático e o operacional. Uma proposta de modificação do BGP será apresentada na seção seguinte.

Usando o WEKA (Weka, 2013) para a codificação do algoritmo, foi possível chegar aos resultados da Fig. 4.3. Nesse caso o AS_x é a representação do número de saltos de um AS a outro, sendo x o valor do raio.

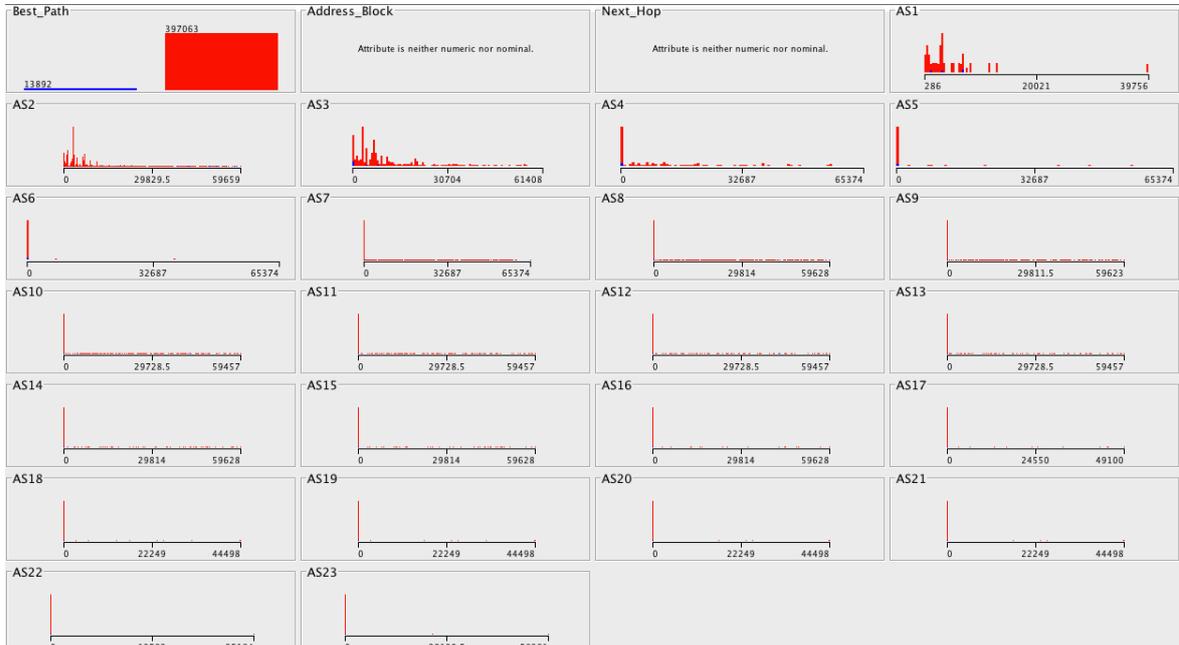


Figura 4.3 - Cálculo do raio da Internet com um algoritmo proposto com o uso da ferramenta WEKA.

4.6 MODIFICAÇÃO NA TOMADA DE DECISÃO DO BGP (BÔNUS TrB) OU SOLUÇÃO SEMI-INTRUSIVA

Uma outra possibilidade de modificação da forma com que a decisão ocorre entre dois sistemas autônomos é a modificação do protocolo. Nesta seção é proposta uma solução, minimamente invasiva, do protocolo BGP. Atualmente, um dos conceitos correntes na Internet é que as redes que iniciaram a Internet e possuem abrangência geográfica são denominadas TIER-1. Por esse motivo, esses operadores normalmente não trocam tráfego por meio de *peering* – sem pagamento da interconexão – com outras redes que não possuam condições semelhantes. Pelo lado econômico, é importante entender que existe a necessidade da proteção do investimento e que as redes não se constroem sem viabilidade e retorno provável do investimento. Mas por outro lado, em alguns países, o Brasil como exemplo, o interesse no conteúdo gerou condições de interconexão para que provedores de conteúdo, que não possuem rede ou abrangência geográfica até o usuário final, conseguissem fechar acordos de *peering* com base no interesse mútuo. É inegável que

apenas a rede não é o suficiente, e o provedor de conteúdo é também importante. Por outro lado, existem os novos serviços baseados em distribuição de conteúdo *multimedia*, como exemplo interessante o serviço NETFLIX (NetFlix, 2014), onde o operador de serviço de distribuição de vídeo não possui rede. Existe, ainda, o serviço do Google (Google, 2014), com a parte econômica bem estruturada e em um dos exemplos de serviço calcado em propaganda direcionada pelo conhecimento do perfil de uso do usuário. Esses exemplos denotam a complexidade de se chegar a um modelo que possa satisfazer a todos os interesses envolvidos no nível estratégico da tomada de decisão de controle e uso de capacidade de tráfego.

Uma possibilidade interessante poderia estar relacionada com um modelo de bônus de tráfego – TrB – onde cada *AS*, em função de suas características básicas de função ou quantidade de tráfego gerado ou consumido, poderia ter créditos a serem usados para a interferência inteligente nas tomadas de decisão relacionadas ao encaminhamento do tráfego. Os créditos de tráfego não têm a função de alteração na estratégia ou modelo econômico-financeiro de cada *AS*. Ao contrário, serviriam apenas para facilitar ou aumentar a probabilidade de uso do *prepend* como uma forma de dar a um *AS* externo mais condições de alterar o perfil de tráfego recebido. A modificação proposta está descrita no fluxograma da Fig. 4.4. O TrB_{int} é o valor de interesse a partir do qual o *AS* de interesse externo possibilitará que seu processo de tomada de decisão seja alterado. O processo descrito na Fig. 4.4 é basicamente o mesmo processo descrito no BGP com a inserção de uma tomada de decisão baseada no parâmetro TrB. O algoritmo é iniciado com o $TrB=0$ e o $TrB_{int}=100$. O administrador da rede pode variar o TrB_{int} fazendo com que este seja sensível a valores de TrB provenientes do *AS* considerado. Caso o $TrB > TrB_{int}$ o *AS* PATH (*prepend*) passa a ser considerado logo após do parâmetro *weight* (pesos) aumentando-se a probabilidade de sucesso na interferência direta do roteamento reverso.

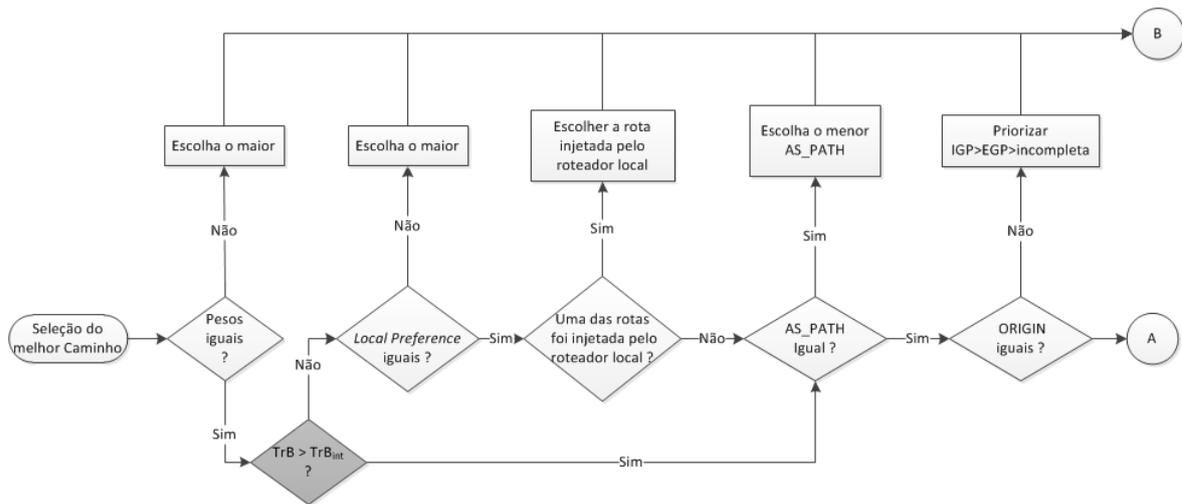


Figura 4.4 - Processo parcial de tomada de decisão do BGP com a introdução do crédito de tráfego.

Na proposta de construção do sistema de bônus, apenas dois grupos são propostos. O primeiro está relacionado a entidades de ensino e pesquisa, mantendo esse grupo em um patamar inicial elevado de bônus. O segundo engloba todos os demais que não se enquadram no primeiro quadro. Outro ponto a ser levado em consideração é que, quanto mais tráfego entregue, mais bônus; quanto mais endereços ativos, mais bônus. A nova tabela de interesse é apresentada em conformidade com a Fig. 4.5. Observa-se que o TrB, se aceito pelo AS externo, altera a sensibilidade do AS externo de forma que o mesmo possa acatar modificações que sejam encaminhadas por fontes externas.

	Weight	TrB	Local Preference	Rotas locais	AS PATH
Weight	3,3	3,2	3,1	3,0	3,-1
TrB	2,3	2,2	2,1	2,0	2,-1
Local Preference	1,3	1,2	1,1	1,0	1,-1
Rotas locais	0,3	0,2	0,1	0,0	0,-1
AS PATH	-1,3	-1,2	-1,1	-1,0	-1,-1

wg>TrB>lp>rl>as

Figura 4.5 – Sensibilidade a alterações parametrizadas via BGP.

A arquitetura de interconexão da proposta de modificação de tomada de decisão do protocolo está definida na Fig. 4.6, onde o próprio BGP é usado para transportar todos os dados relativos ao parâmetro *TrB*, sem modificações, usando o campo opcional. No caso apresentado, o principal objetivo da *Clearinghouse* é manter o valor acumulado de *TrB* para cada AS participante e distribuir essa informação aos participantes. O *TrB* é uma variável composta do ASN (número de identificação do AS) e o valor acumulado variando entre 0 e 65.534, sendo o valor mais alto o mais prioritário.

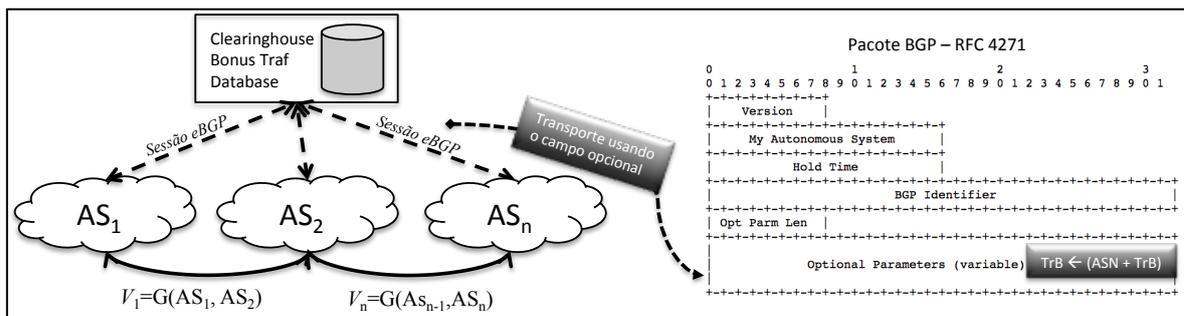


Figura 4.6 - Arquitetura do protocolo.

Por se tratar de uma política, a mesma será tratada aqui como proposta para o parâmetro *TrB*, sendo apresentada na Tab. 4.1 a distribuição de capacidade de acordo com os parâmetros e tipos de instituição. A sugestão é que a validação do tráfego será realizada pela *clearinghouse* para os participantes com base nas informações fornecidas.

Tabela 4.1 - Proposta de cálculo do *TrB*

Tipo de Instituição	TrB_{typ}	TrB_{ipa}	TrB_{trf}
Instituições de Ensino e Pesquisa	100	5 para cada bloco /18 IPv4	$TrB_{trf} = \frac{Trafego_{out} + Trafego_{in}(Gbps)}{10Gbps}$ <p>Soma de todo o tráfego do AS</p>
Outros	1	10 para cada bloco /64 IPv6	
Efetivamente publicados na Internet			
$TrB_{tot} = TrB_{typ} + TrB_{ipa} + TrB_{trf}$			

A TrB_{typ} está ligada ao tipo de instituição, priorizando aquelas que têm condições de beneficiar a rede com informações que auxiliem no desenvolvimento da rede. A TrB_{ipa} está

relacionada com *ASes* que possuem número elevado de clientes, caracterizando-se como provedores de acesso, não necessariamente de conteúdo, e, por último, a TrB_{trf} está relacionada com o tráfego total gerado. O objetivo da TrB_{tot} é o de parametrizar informações que possam passar informações relativas ao perfil das diversas redes, trazendo a camada de decisão estratégica para o nível tático.

Na secção de ensaios e análise de casos, uma simulação será realizada para comparar essa modificação com o uso atual. O aumento da sensibilização a fatores externos é uma possibilidade para se alterar a estratégia do jogo. Desta forma, mesmo que apenas alguns *ASes* modificassem a sua estratégia, os benefícios já poderiam ser vistos, conforme simulação na Fig. 4.2.(a), onde é mostrado que 69,14% das soluções de roteamento ocorrem por intermédio do parâmetro *ASPATH* (*prepend*), que por sua vez tem prioridade inferior ao peso, preferência local e rotas aprendidas por protocolos internos.

A principal característica que suporta a proposta do TrB é a não necessidade de modificação do BGP. Ou seja, o campo de parâmetros opcionais é utilizado para o transporte das informações adicionais. O objetivo é gerar compatibilidade entre o utilizador da metodologia e aquele que não queira. Ao final, o TrB será uma aplicação que estará ativa no sistema operacional do roteador, podendo ser ativado assim como ocorre quando se escolhe o OSPF ou o IS-IS.

Na Fig. 4.7a e Fig. 4.7b temos uma análise realizada através do OMNET⁺⁺ em relação ao uso do TrB. Na Fig. 4.7a a simulação ocorre sem uso do TrB, observa-se um processo de comunicação mais longo, porém com 34 μ s de tempo de uso de máquina.

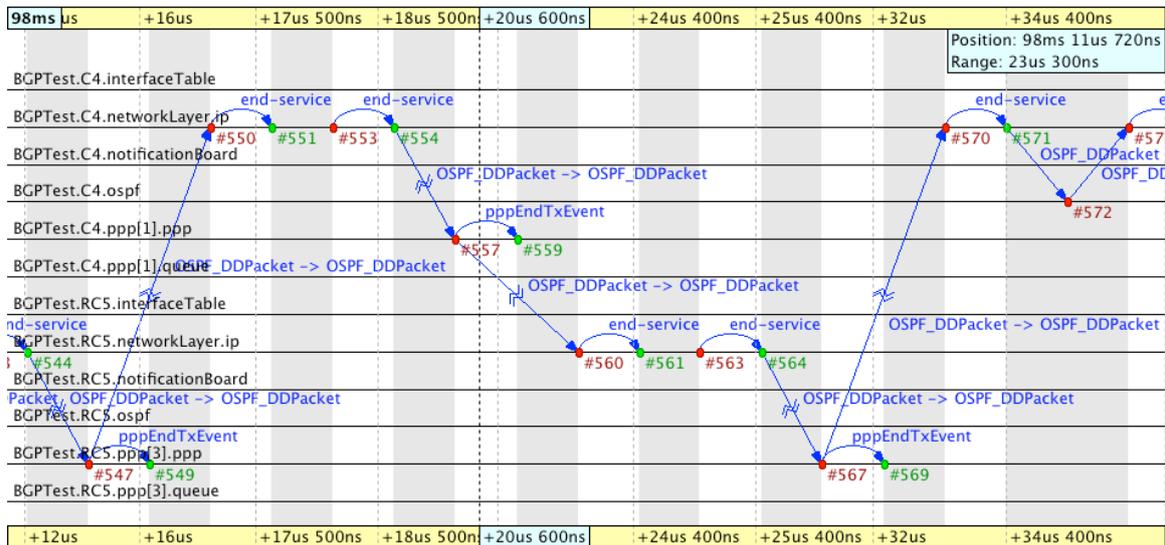


Figura 4.7a – Processo simulado do BGP sem o TrB.

No caso da Fig. 4.7b temos um processo de comunicação com apenas dois acessos a camada de rede, porém com 45 μ s de tempo de máquina.

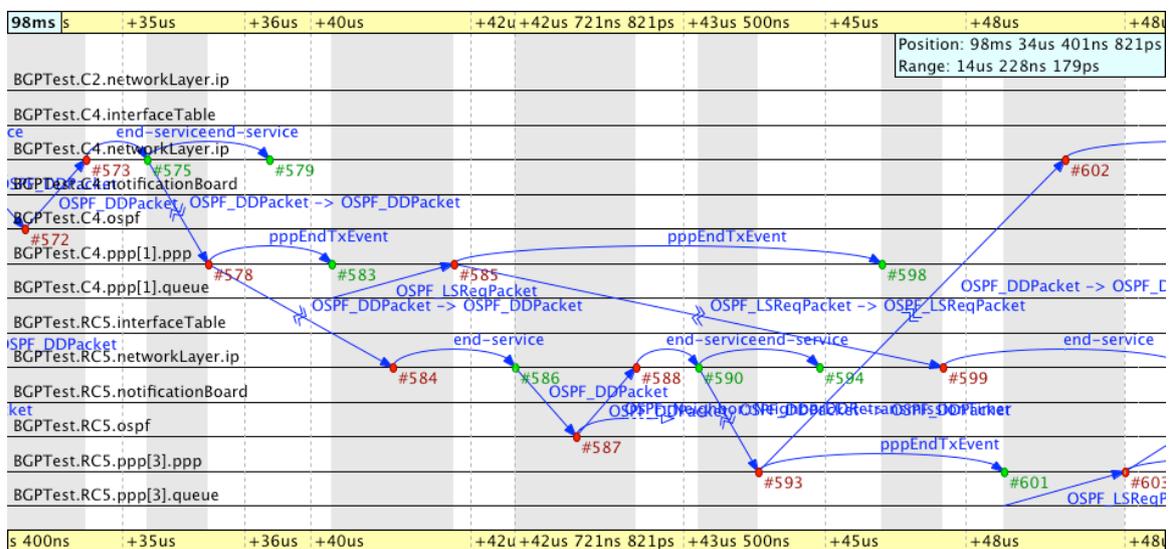


Figura 4.7b – Processo simulado do BGP com o TrB.

A Fig. 4.8 mostra que os tempos de convergência da tabela de roteamento, ou seja, após uma intervenção, quanto tempo leva-se para estabilização. Para as 85 simulações, os tempos não tiveram variações abaixo de 50ms ou acima de 90ms.

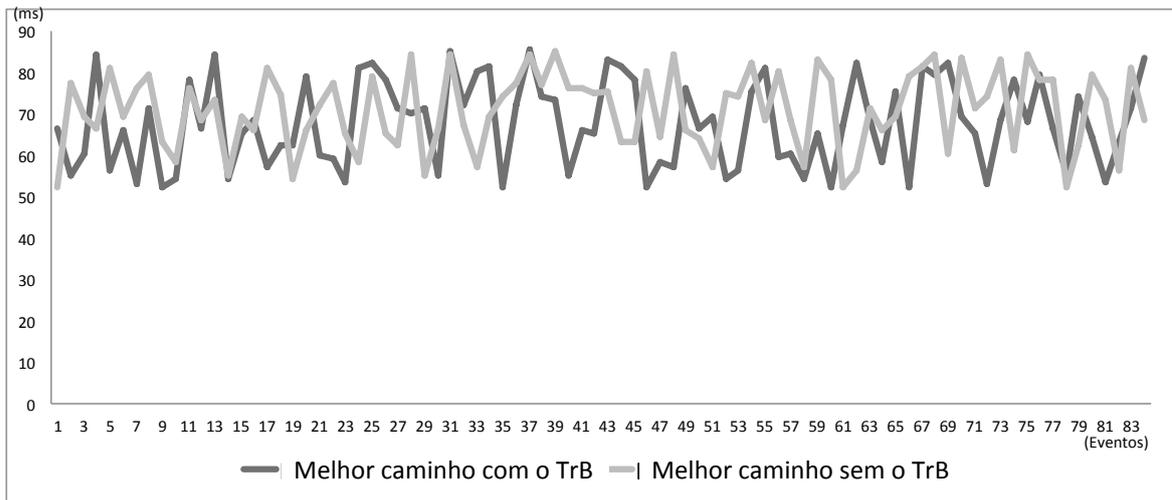


Figura 4.8 – Tempo de convergência com e sem o uso do TrB.

Estas simulações contribuem para o entendimento da melhor estratégia a ser empregada na solução.

4.7 TOMADA DE DECISÃO BASEADA EM CONHECIMENTO ESPECIALISTA

A tomada de decisão especialista sofre influência direta dos valores pessoais que cada especialista possui em relação à sua tomada de decisão. O conhecimento especialista é relativizado em função dos seus acúmulos de conhecimento ao longo do tempo. Na Fig.4.9, tem-se um mecanismo de tomada de decisão especialista analisado, onde o especialista é informado sobre o problema por uma reclamação do cliente ou ainda por um sistema de gerência que detecta o problema e o informa automaticamente.

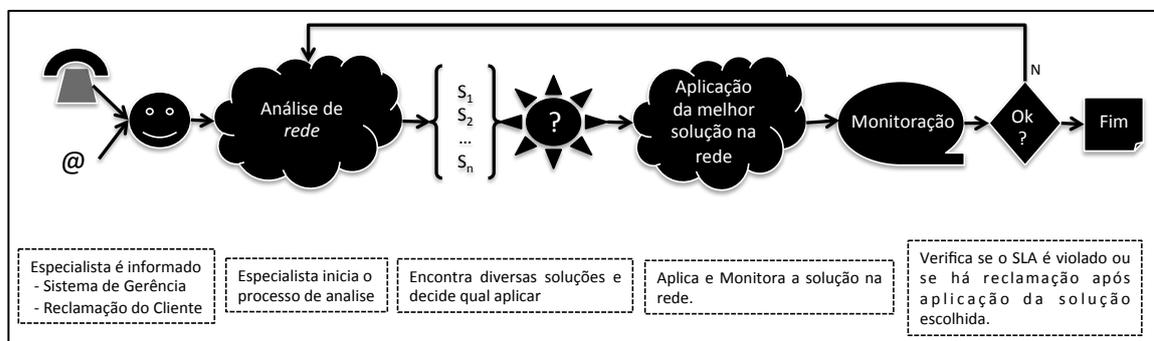


Figura 4.9 - Mecanismo de tomada de decisão especialista.

Após isso, inicia-se a análise da rede e se chega a um conjunto de soluções $C_s = \{S_j\}$. Caso a melhor solução $S_{ms} \in \{S_j\}$, então o sistema terá a melhor solução, porém não existe esta

garantia caso toda a tomada de decisão esteja baseada apenas no conhecimento de único especialista.

A tomada de decisão do especialista pode ser influenciada, também, pela experiência técnica e tempo de aprendizado do especialista em determinada rede. No capítulo relativo a ensaios, são mostrados resultados relativos a esse caso e, ainda, o grau de efetividade das soluções propostas e aplicadas em uma rede real em função do grau de experiência pessoal de cada engenheiro de rede.

4.8 REAGINDO À ESTRATÉGIA DOMINANTE DE FORMA INTUITIVA

A descrição da estratégia dominante traz consigo uma carga de valor interessante para que seja possível que os agentes (nesse caso os ASes) tenham como melhorar suas recompensas e buscar o equilíbrio de forma mais rápida. O uso do conhecimento especialista é atualmente o melhor método para se buscar o melhor retorno em termos de balanceamento de tráfego, mesmo tendo todos os recursos sido construídos para dificultar esta busca, haja vista o fato de as interfaces e os enlaces padronizados, exceto no acesso, serem simétricos ao passo que a Internet de fato não é completamente simétrica (Woodward *et al.*, 2013).

O próprio conceito do BGP RFC 1771 (Rekter, 1995) e 4271 (Rekter, 2006) deixa claro que o AS é uma unidade autônoma e por este motivo completamente egoísta. A sua tomada de decisão preconiza o uso de estratégias dominantes, pois, de fato, foram assim concebidas e nada há de errado nisso, haja vista o fato de se ter uma Internet com o sucesso alcançado, e de forma irrefutável. Porém, quando se trata de questões operacionais, é importante mostrar que as soluções já apresentadas não se mostram totalmente compatíveis com as necessidades de todos os usuários.

A Fig.4.10 mostra uma estratégia de se tentar modificar o perfil de tráfego com o uso de informações extraídas da própria rede e com isso se aumentar o grau de confiança para que o tomador de decisão possa optar por usar ou não aquela solução proposta, maximizando a efetividade do uso dos recursos e minimizando a instabilidade, isso sem que seja necessária alteração no protocolo ou na forma com que os agentes trabalham atualmente. O

processo se inicia com a caracterização com base na tabela de roteamento. O *routeviews* é usado como fonte para a coleta da tabela completa de roteamento. O processo de caracterização do *prepend* é usado para se definir a viabilidade da aplicação do processo.

Para cada linha da tabela de roteamento é analisado o *AS PATH* de forma a se caracterizar a utilização do *prepend*. Caso não seja possível se utilizar o *prepend* o administrador da rede deve tentar negociar diretamente com aquele que deseja modificar externamente. Caso seja possível, deve ser calculado, por um modelo de cálculo de capacidade quais serão os recursos necessários.

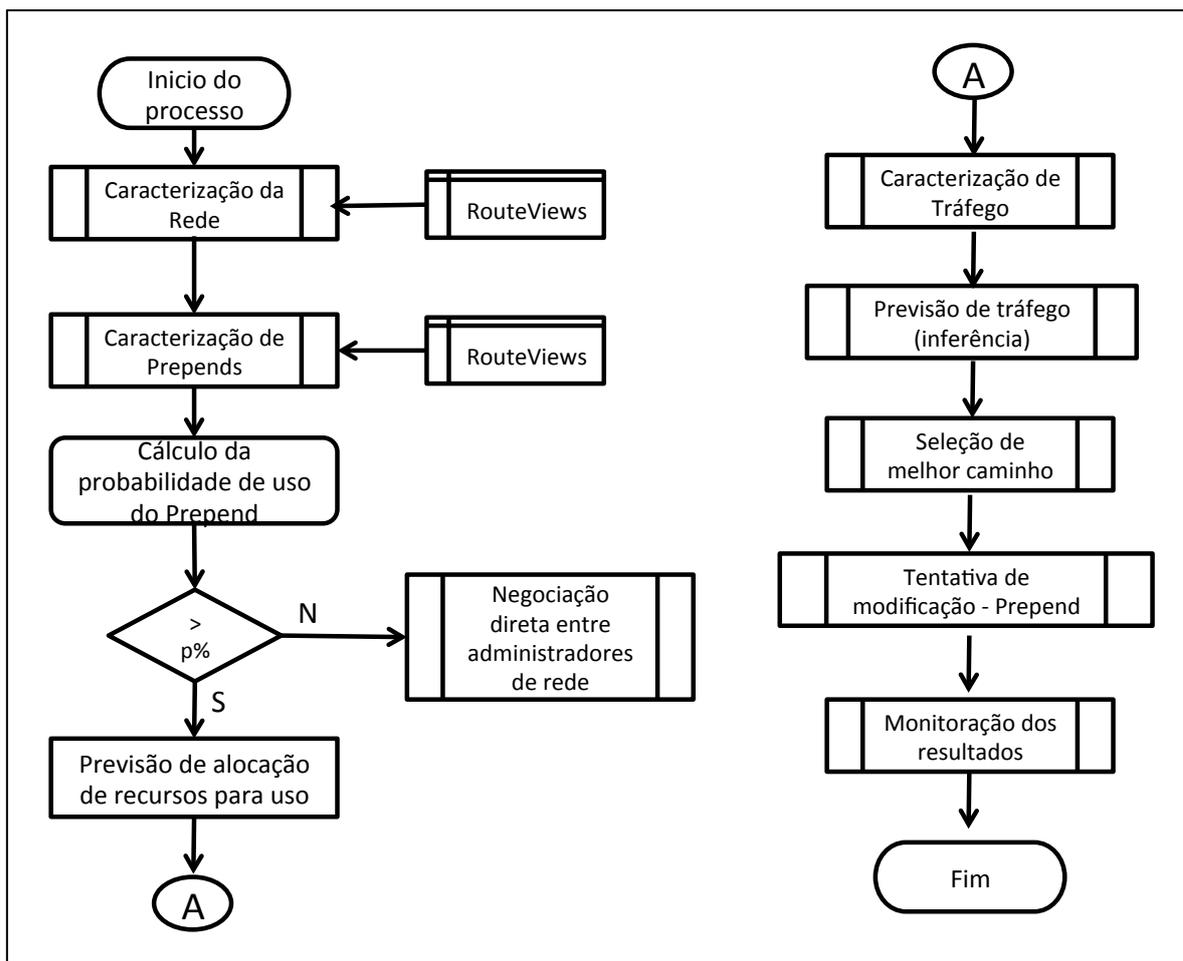


Figura 4.10 – Tentativa de alteração do tráfego com o uso do *Prepend*

Para o caso do banda, o tráfego é caracterizado e um modelo escolhido. O melhor caminho é determinado após a análise dos recursos disponíveis, logo após aplicando-se o preprend de forma a tentar influenciar o AS externo.

Por outro lado, a proposta de alteração do BGP não pode ser descartada, pois se não é possível alterar a estratégia então será necessário pensar em uma proposta onde o jogo possa ter ao menos um equilíbrio. Para isso, as ações seriam revistas (caso particular da alteração no protocolo).

4.9 ESTABILIDADE DO BGP

Pode-se afirmar que, se o relacionamento entre dois sistemas autônomos é análogo a uma dominação fraca, esse relacionamento pode gerar instabilidades nos parâmetros que definem as recompensas. Por outro lado, em (Papadimitriou *et al.*, 2013), a autonomia do BGP tem um significado importante para a análise da estabilidade do protocolo, observando-se que, para que o processo de convergência do BGP ocorra, faz-se necessário que um estado de encaminhamento de pacotes seja escolhido, sem levar em conta, inicialmente, nenhum critério de eficiência.

No mesmo trabalho (Papadimitriou *et al.*, 2013), são apresentadas métricas específicas para a análise da estabilidade. No trabalho de (Fiegenbaum, 2007), por outro lado, a independência do AS faz com que seja impossível que se evitem *loops* quando se utilizam algoritmos do tipo *path-vector*, pois, nesse caso, não existem trocas de informação de descrição completa do caminho, apenas parcial, haja vista que no BGP a informação se limita ao número do AS.

De forma interessante, quando um protocolo que usa o *path-vector* tenta prever um *loop*, o critério da convergência não pode ser garantido. Para se melhorar a garantia de convergência, o BGP utiliza os critérios de tomada de decisão em que todas as rotas atuais são consideradas como preferenciais em detrimento daquelas novas aprendidas. No trabalho (Oti e Hayfron-Acquah, 2014), outros aspectos importantes relacionados à segurança de rede também são inseridos. No caso da segurança, segundo (Oti e Hayfron-Acquah, 2014), um ataque do tipo *hijacking* pode influenciar diretamente a estabilidade,

pois as políticas internas estarão vulneráveis a mudanças não programadas. Portanto, ao se combater um ataque, também está sendo dada à rede mais robustez. Por outro lado, segundo (Fiegenbaum, 2007), o aumento da garantia da estabilidade leva o protocolo para uma condição de robustez, porém não garante flexibilidade quando da mudança do estado de um enlace ou nó, não resolvendo, dessa forma, totalmente o problema. A melhor solução ficará sempre entre ser robusto (estável) mas não deixando de se adaptar às modificações de estado da rede.

Um problema de estabilidade conhecido do BGP, ou de qualquer outro protocolo que use o *path-vector*, está descrito em (Fiegenbaum, 2007). Para entender esse problema, considere a situação ilustrada na Fig. 4.10. Na situação ilustrada, considere que o AS AS_1 prefere o caminho $AS_1AS_2AS_d$ para a rota AS_1AS_d e, ao mesmo tempo, que o AS AS_2 prefere o caminho $AS_2AS_1AS_d$ para a rota AS_2AS_d .

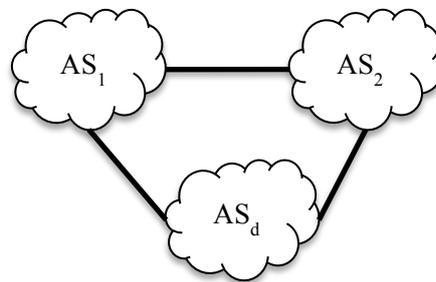


Figura 4.11 - Conexão entre três *ASes* com análise de estabilidade.

Essa condição faz com que o algoritmo *path-vector* não convirja, pois nesse caso ambos os *ASes* AS_1 e AS_2 preferem uma rota indireta a uma diretamente conectada. Considerando o pior caso, observa-se, com a simulação, que o AS_d , no momento inicial, anuncia-se, ao mesmo tempo, para o AS_1 e para o AS_2 . Quando isso ocorre esses são os únicos caminhos disponíveis para os AS_1 e AS_2 chegarem ao AS_d . Por esse motivo, tanto o AS_1 quanto o AS_2 se anunciarão como rotas diretamente conectadas ao AS_d .

Logo em seguida, cada um dos *ASes*, respectivamente, irá alterar sua tabela para os caminhos $AS_1AS_2AS_d$ e $AS_2AS_1AS_d$. No entanto, como as rotas diretas AS_1AS_d e AS_2AS_d deixam de ser usadas, a condição inicial deixa de ser verdadeira e um novo anúncio leva à destruição dos caminhos $AS_1AS_2AS_d$ e $AS_2AS_1AS_d$, forçando o uso dos caminhos AS_1AS_d e

AS_2AS_d inicialmente anunciados, realimentando o processo em uma oscilação infinita, o que levará o protocolo a nunca convergir. A solução atual para esse problema é tratada na camada estratégica, com o estabelecimento de políticas de roteamento que não deixem o protocolo tomar uma decisão que o leve à instabilidade.

4.10 ESTABILIDADE DA REDE

Para a análise da estabilidade da rede quando da necessidade da tomada de decisão, alguns testes em uma rede real foram realizados. Para um teste de estabilidade, uma rede real, esquematizada na Fig. 4.12, foi analisada com relação ao uso do *prepend*. O teste focou na comparação entre as ações dos engenheiros de rede que fizeram uso da metodologia apresentada na Fig. 4.10.

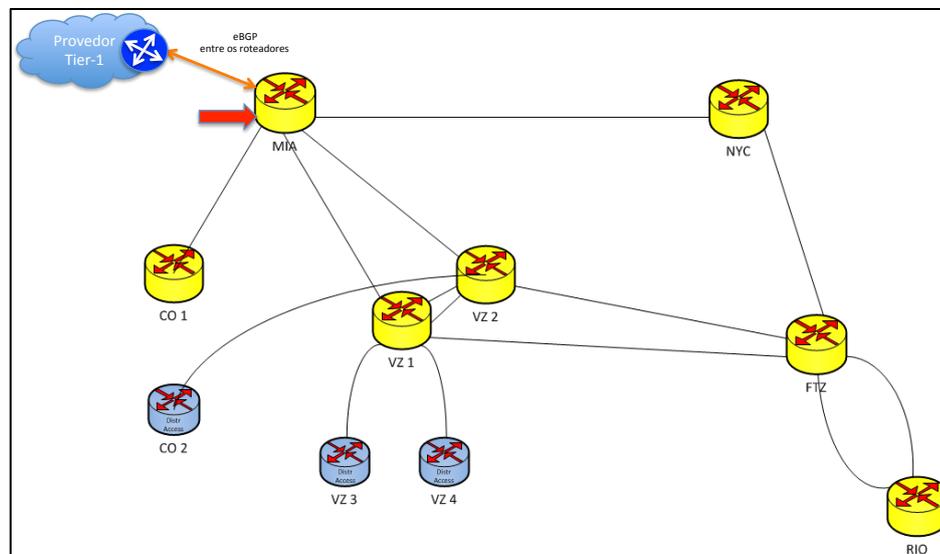


Figura 4.12 – Exemplo de rede real, com conexão entre o roteador MIA e a Internet via TIER-1, usada para teste de estabilidade.

Ainda para a análise da estabilidade, foi gerado um processo de coleta diferente das coletas realizadas pelo SNMP (*Simple Network Management Protocol*), pois, uma vez que o padrão de coletas é realizado em intervalos de 5 minutos, esse padrão não seria adequado para a análise de convergência ou estabilidade das rotas após modificação na tabela RIB (*Routing Information Base*), conforme Tabela 4.2. As informações coletadas foram todas disponibilizadas na tabela para conexões externas (EBGP).

Tabela resumo da RIB (<i>Routing Information Base</i>)	
RIB Name	Nome do grupo da RIB
Total de Prefixos	Numero total de prefixos do <i>peer</i> , ambos ativos e inativos, que estão na mesma tabela de roteamento.
Prefixos ativos	Numero de prefixos recebidos dos <i>peers</i> EBGP que estão ativos na tabela de roteamento.
Prefixos suprimidos	Numero de rotas recebidas dos <i>peers</i> EBGP correntes que estão inativos devido a um <i>damping</i> ou outros motivos.
Histórico de prefixos	Histórico de rotas recebidas ou suprimidas.
Prefixos descartados	Número de rotas atualmente inativos devido a um <i>damping</i> ou outros motivos. Estas rotas não aparecem na tabela de encaminhamento e não são exportadas.
Prefixos pendentes	Número de rotas pendentes.
Estado	Estado do processo <i>graceful restart</i> para esta tabela de roteamento. Possíveis estados: <i>BGP restart is complete</i> , <i>BGP restart in progress</i> , <i>VPN restart in progress</i> , <i>VPN restart is complete</i> .

Tabela 4.2 – Tabela RIB

No roteador MIA, foi inserido um *script* para tornar possível a coleta de informações, conforme código abaixo.

```

my %miami_router = (

    access => $access,
    login => $marcio,
    password => $xs$5&&%$,
    hostname => $mial_1,
    junos_key => $junos_key,

);
JUNOS::Trace::init(1) if $opt{d};
my $outputfile = $opt{o} || "bgp_stability.txt" ;

## Conta entradas il
get_system_FIB_RIB_information method: => $_ARGS,il

```

```

get__bgp__ASPATH__information__method:

##Metodo : <get-system-ASPATH-information>
## inicializa contador
get__uptime__information => $_ARGS,t1

## Conta entradas i2
get__system__FIB__RIB__information__method => $_ARGS,i2
if ($i1<>$i2) {
get__system__FIB__RIB__information__method:=> $_ARGS,i2
then
get__system__FIB__RIB__information__method:=> $_ARGS,i3
if ($i2<>$i3) {
get__system__FIB__RIB__information__method:=> $_ARGS,i3
then
get__uptime__information => $_ARGS,t2

```

Na Fig.4.13 que cerca de 25% das modificações ocorridas na RIB tiveram origem no parâmetro AS_PATH ou ação de *prepend* (000x1F3).

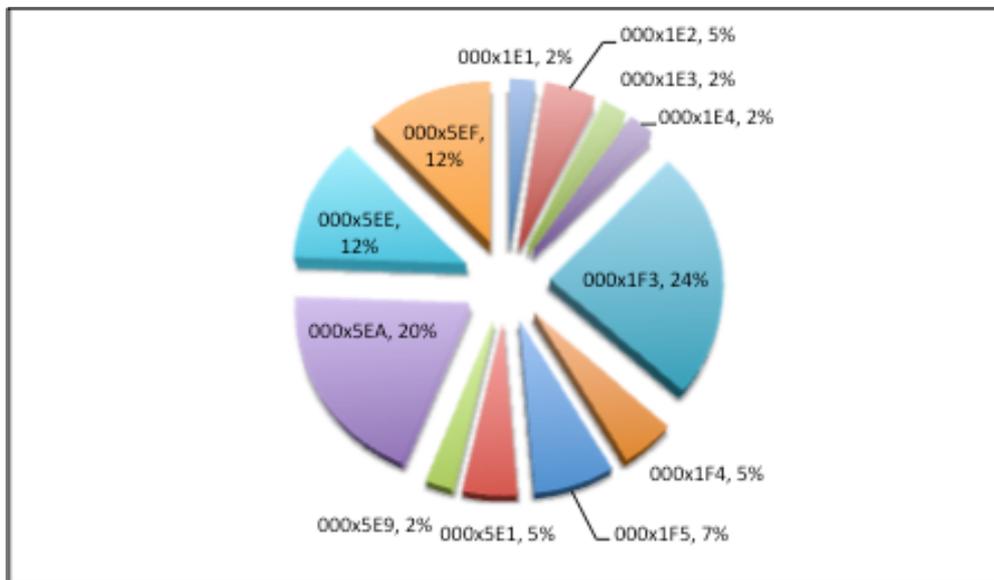


Figura 4.13 – Código 000x1F3 é relacionado a modificações na RIB provocadas pelo uso do AS_PATH.

Na Fig. 4.14. é mostrada a coleta realizada para todos os eventos e de acordo com a distribuição da Fig. 4.15.



Figura 4.14 – Todos os eventos coletados.

Na Fig. 4.15, são mostrados eventos analisados de agosto de 2013 a fevereiro de 2014 sem a aplicação da metodologia, tendo como resultado uma média de 336 segundos para a estabilização da RIB quando uma modificação ocorreu exclusivamente devido ao parâmetro AS_PATH. Na mesma figura, é informado o valor médio, tendo o Potaroo (Geoff, 2014) apenas como referência.

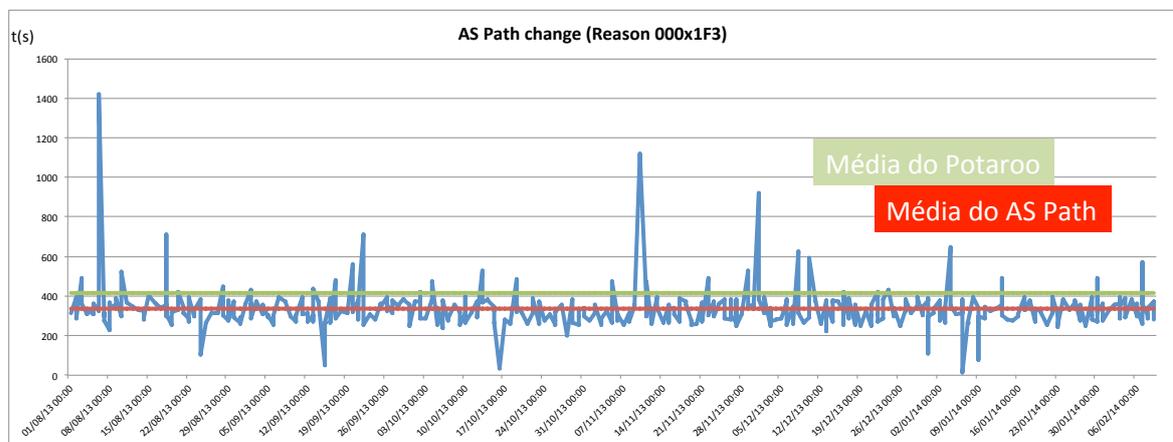


Figura 4.15 – Eventos coletados por modificação do AS_PATH sem aplicação da metodologia.

Na Fig. 4.16, é apresentada uma análise do mês de março, quando eventos relacionados ao AS_PATH foram coletados com o uso da metodologia, porém com determinação de banda com o uso do modelo DLD. Ainda assim, observa-se que a metodologia faz com que a média diminua para 208 segundos.

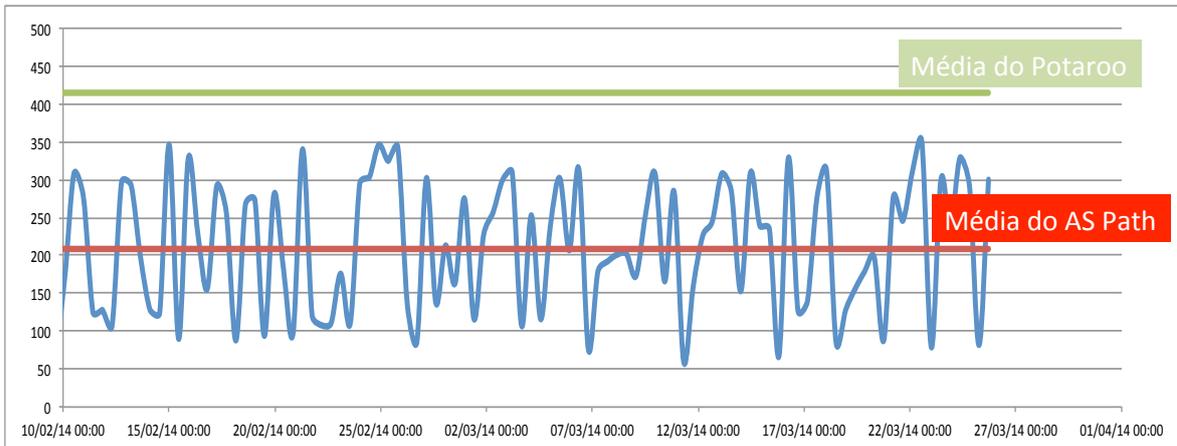


Figura 4.16 - Eventos coletados por modificação do AS_PATH com aplicação da metodologia.

4.11 CONCLUSÃO DO CAPÍTULO.

A estratégia de interferência em uma rede deve ser sustentada por conhecimento que contenha alto grau de assertividade. A motivação para a tomada de decisão também deve levar em consideração o conhecimento de todos os agentes envolvidos no processo de tomada de decisão e seus interesses. Diversos parâmetros devem ser definidos para que o tomador de decisão consiga interpretar a leitura dos dados de forma a entender qual será a decisão que levará a rede para a condição esperada. Os aspectos operacionais e de estabilidade de rede são importantes para o estabelecimento dos critérios de tomada de decisão. Se determinada mudança leva a rede para uma condição não estável, esta provavelmente não deve ser realizada.

5 APLICAÇÕES DA INTERFERÊNCIA RACIONAL

5.1 A ANÁLISE DA TOMADA DE DECISÃO

O processo de tomada de decisão deve possuir parâmetros que possam determinar se as recompensas (Shoham, 2007) do sistema foram melhoradas ou levadas para o grau de serviço previamente planejado, ou seja, para os parâmetros previamente definidos como mínimos ou máximos para a operação da rede. Para isso, faz-se necessário que os parâmetros a serem medidos possam trazer informação relevante e, principalmente, possível de ser coletada, bem como de ser caracterizada antes de poder ser efetivamente usada. Na Fig. 5.1, é apresentado um modelo que sugere a verificação da eficácia da decisão - ϵ_d - antes e depois da tomada de decisão.

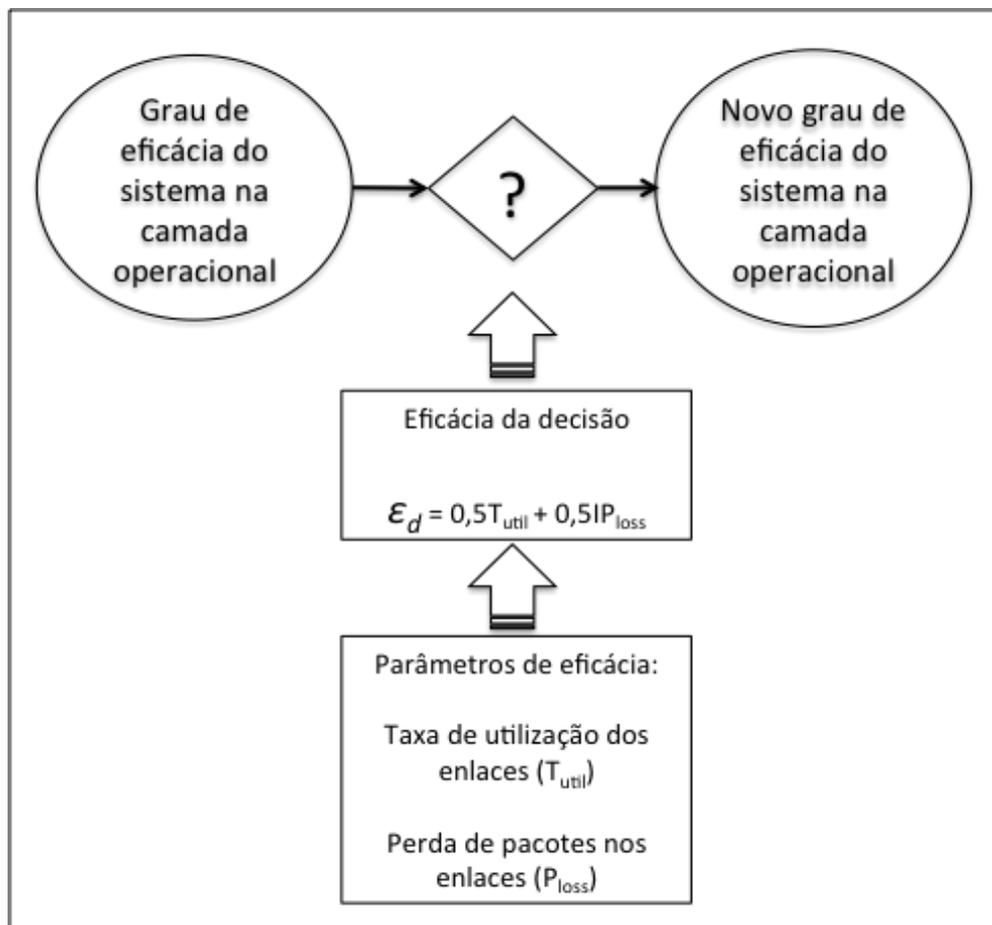


Figura 5.1 – Definição de parâmetros de grau de eficácia para a tomada de decisão.

O ε_d , para o exemplo adotado, leva em consideração a possibilidade do uso de informações de função de utilização de um enlace (τ_{util}) e da taxa de perda de pacotes (IP_{loss}), criando-se uma relação em que $\varepsilon_d(\tau_{util}, IP_{loss})$ está definido entre $[0,1]$ e, portanto, τ_{util} e IP_{loss} também. No caso do IP_{loss} , faz-se necessária a normalização da perda de pacotes máxima aceitável na construção dos acordos de nível de serviço com a perda real encontrada na monitoração da rede, devendo a escala estar no intervalo $[0,1]$.

Uma decisão que consiga melhorar, no modelo proposto, o grau de eficácia no uso dos recursos da rede pode também ser pensada no sentido de se propor uma medida do grau de felicidade do utilizador do recurso de rede ou agente com base nas estratégias utilizadas. Nesse caso os parâmetros modificados serão observados antes e depois da tomada de decisão. Para este caso a medida poderia ser usada como uma possibilidade de comparação referenciada em dados coletados da rede. Esta medida poderia complementar o conceito de qualidade da experiência de forma referenciada.

Nesse ponto, já se pode afirmar que os mecanismos utilizados para a tomada de decisão em situações reais muitas vezes cruzam informações de camadas diferentes como se fosse possível um único roteador modificar toda a estratégia de uma empresa. Se nos cálculos de planejamento, acurados, chegou-se a conclusão que seriam necessários roteadores com capacidade de processar 500 mil pacotes por segundo, porém, por questões orçamentárias, equipamentos com apenas 100 mil pacotes por segundo de capacidade foram adquiridos, não há o que se falar em tomada de decisão operacional que possa levar a um grau de felicidade aceitável pelo agente. De fato, o problema aqui relatado está na camada estratégica, e, por esse motivo, sua solução também. Não está em discussão aqui a análise *crossover* da tomada de decisão, sem dúvida nesse exemplo, apenas uma camada irá ter atuação para a solução do problema de capacidade.

Por outro lado, quando se trata de decisões no nível operacional, em curto prazo, é necessário que mais de uma camada seja analisada quando um problema ocorre e é necessária uma decisão. No caso de redes Internet, mais especificamente o caso das redes presentes na América do Sul, é inegável a necessidade constante de interações entre camadas para se resolver problemas relacionados a tráfego. O primeiro problema surge quando se caracteriza o tráfego e observam-se os problemas relacionados à assimetria, esta

gerada pela concentração dos serviços ou interesse de tráfego nos Estados Unidos da América, Europa e Ásia.

Para o operador da rede que está tentando gerar um ambiente controlado surge uma condição extremamente desfavorável ao seu trabalho: o nível estratégico não consegue resolver o problema apenas adicionando ou adquirindo mais capacidade, pois os princípios de funcionamento da Internet não levam em consideração a possibilidade de se dividir o controle gerencial de um AS.

Esse mesmo operador, ainda tentando encontrar uma saída para o problema apresentado, busca, normalmente, formas de solução para o problema, que, nesse caso, está relacionado a desbalanceamento entre enlaces de tráfego, e não consegue uma solução usando o mecanismo do *prepend* (adicionar o seu próprio ASN - *AS number* - à descrição do *PATH* ou caminho). Última alternativa é tentar um contato direto com o operador da rede que está encaminhando o tráfego de forma diferente daquela que provocaria uma experiência melhorada observada pelo agente. Porém, nesse caso, a solução volta para a camada de estratégia, pois a análise volta a ser puramente de negócios ou vantagens no relacionamento entre os pares.

De qualquer forma, após analisar o grau de incerteza que existe hoje nas tomadas de decisão, mesmo quando apenas vinculadas ao uso do *prepend* como solução, é evidente que esta solução também pode ser melhorada. Na seção a seguir, serão analisados alguns ensaios realizados com simulações ou aplicações reais em uma rede existente. Quando uma conexão entre dois ASes passa por situações de assimetria e desbalanceamento, o uso do *prepend* pode ser uma solução até um limite máximo de aplicabilidade que depende de como o AS que esteja encaminhando tráfego aceite interferência no seu gerenciamento interno.

É ainda possível se observar que a solução dada pelo uso do *prepend* tem um grau de incerteza que pode ser dividido em dois níveis. O primeiro está relacionado à própria incerteza de sua efetividade em função da não possibilidade do controle do gerenciamento externo e o segundo, relacionado com a assertividade da decisão, ou melhor, definição da causa-efeito da decisão e questões relacionadas ao efeito que a decisão irá gerar no

comportamento do tráfego, por exemplo, ao longo de todos os intervalos de tempo analisados. Para o segundo caso, é ainda importante observar que, quando se detectam problemas que estejam levando a rede a ter aumento na variação do tempo de propagação (*jitter*), aumento do tempo de propagação (*delay*), aumento da perda de pacotes (*packet loss*), esses problemas devem ser analisados no tempo completo de operação.

Uma perda de pacotes detectada apenas entre 10 h e 12 h das segundas-feiras da semana pode não ser o bastante para se tentar modificar a configuração da rede por meio do *prepend*, considerando o período de instabilidade que uma tentativa de alteração poderá acarretar.

Nesse caso, outras soluções podem ser necessárias para se complementar uma possível tentativa de se modificar ou, a depender dos acordos de nível de serviço, pode até não ser necessária alteração alguma. Observa-se que em redes de telecomunicações, em alguns casos, a decisão mais difícil pode ser aquela em que nenhuma ação será tomada em termos de modificação.

Para efeito deste trabalho, a definição de tomada de decisão aqui é todo o conjunto de ações ou estratégias que levem a um resultado que modifique a condição da rede através do BGP.

5.2 ENSAIO 1

Na Fig. 5.2., será analisado o caso de uma rede real em um período de implantação quando foram possíveis testes de tomada de decisão com base na modificação do *prepend*. A empresa analisada não pode ser identificada, pois está protegida por um N. D. A. (*Non Disclosure Agreement*). A sua rede utiliza o protocolo IS-IS como iGP e o BGPv4 para a função de conexão. Todos os roteadores em Miami, Tuckerton, Maiquetia e Rio de Janeiro possuem interconexão com outros ASes.

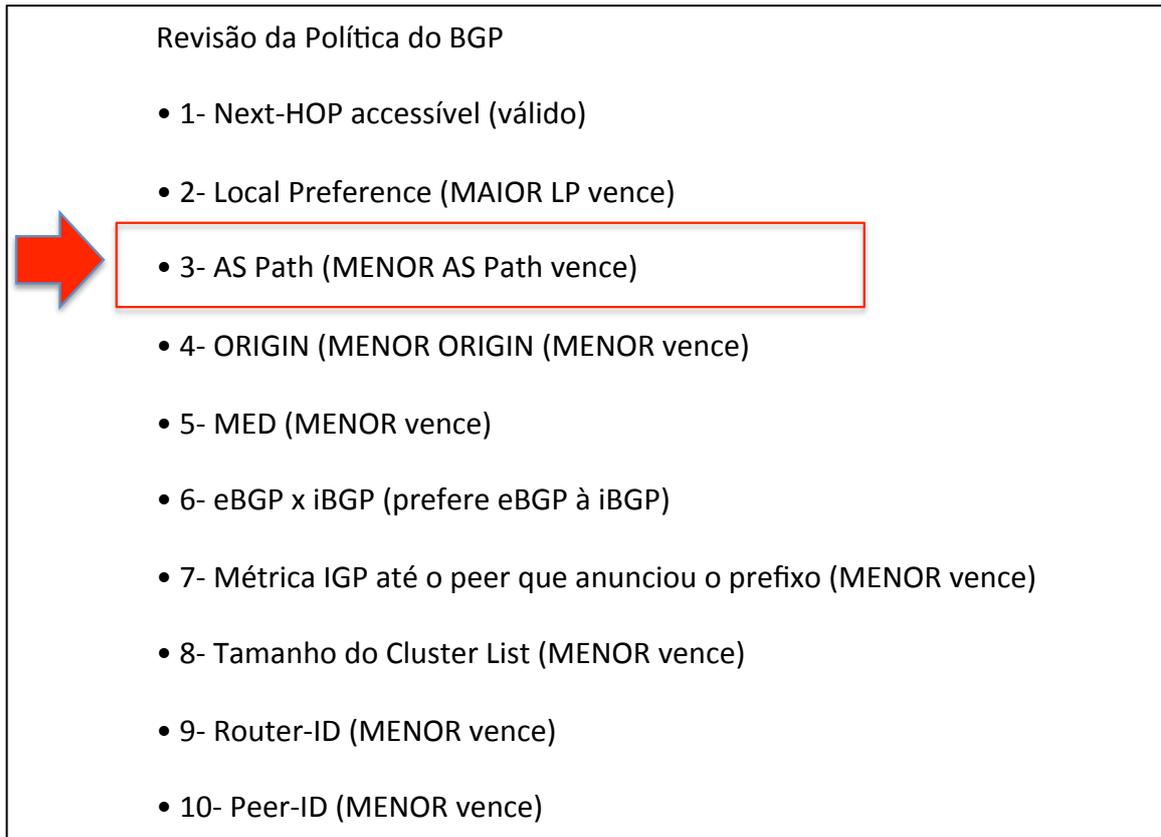


Figura 5.3 – Política de decisão do BGP

A proposta de alteração tem o seu início mostrado na Fig. 5.4, com a caracterização da rede, observando-se que esse conhecimento é necessário para que o diagrama da Fig. 5.2 seja efetivamente conhecido, principalmente com relação às conexões externas. Dessa forma, será possível o conhecimento da topologia da rede.

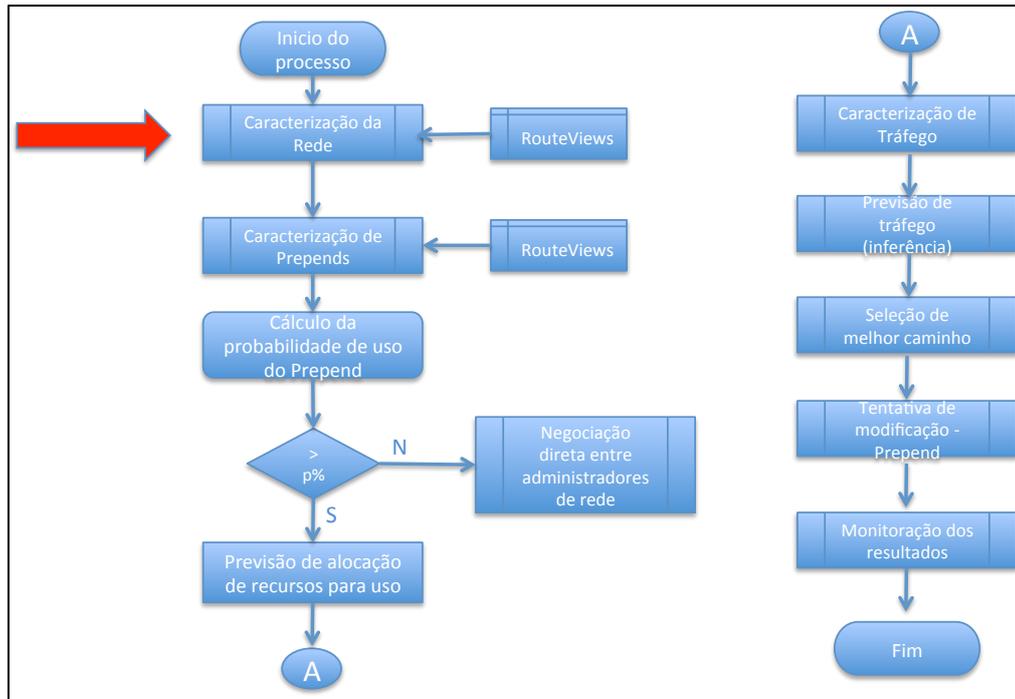


Figura 5.4 – Processo de tomada de decisão para interferência inteligente com base no *prepend*

Na Fig. 5.5, é mostrado, após análise vetorial da tabela de rotas da Internet, todos os possíveis caminhos entre os ASes que estão sendo analisados. Na figura mostrada, as informações foram extraídas da tabela do roteador de MIA, confrontado com a base de dados do projeto Routeviews (Meyer, 2014).

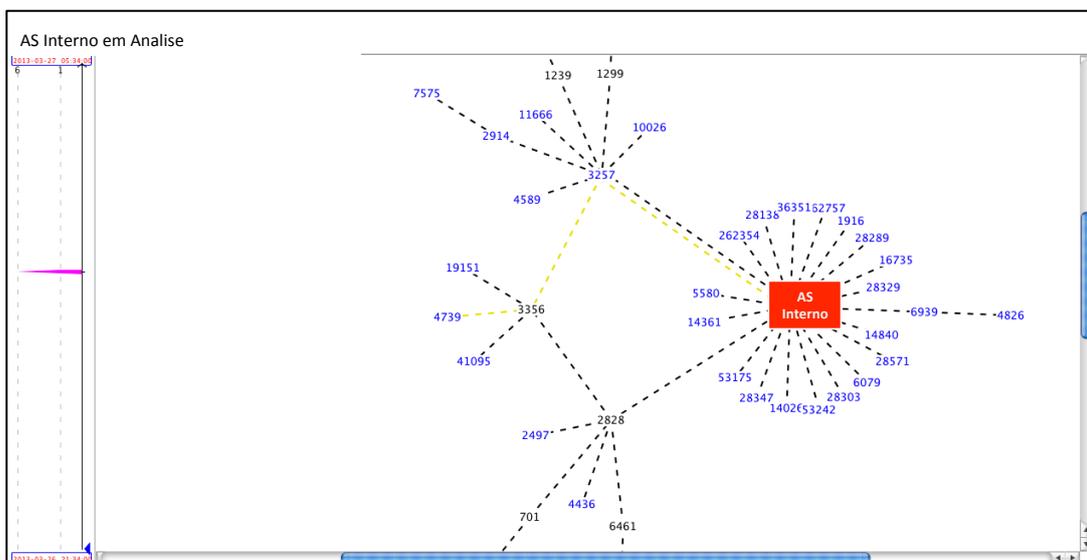


Figura 5.5 - Topologia da rede a partir da informação do BGP via tabela de roteamento da Internet (Identificação do AS real suprimida devido ao N. D. A.)

Observa-se que, na Internet, a maior parte dos ASes está distante em 2 AS de comprimento, fazendo com que o uso do *prepend* tenha um grau de efetividade relacionado mais diretamente apenas com as políticas internas de cada roteador. Tal observação pode ser vista na Fig. 5.6, onde a análise foi feita com base na tabela de roteamento do projeto routeviews (Meyer, 2014).

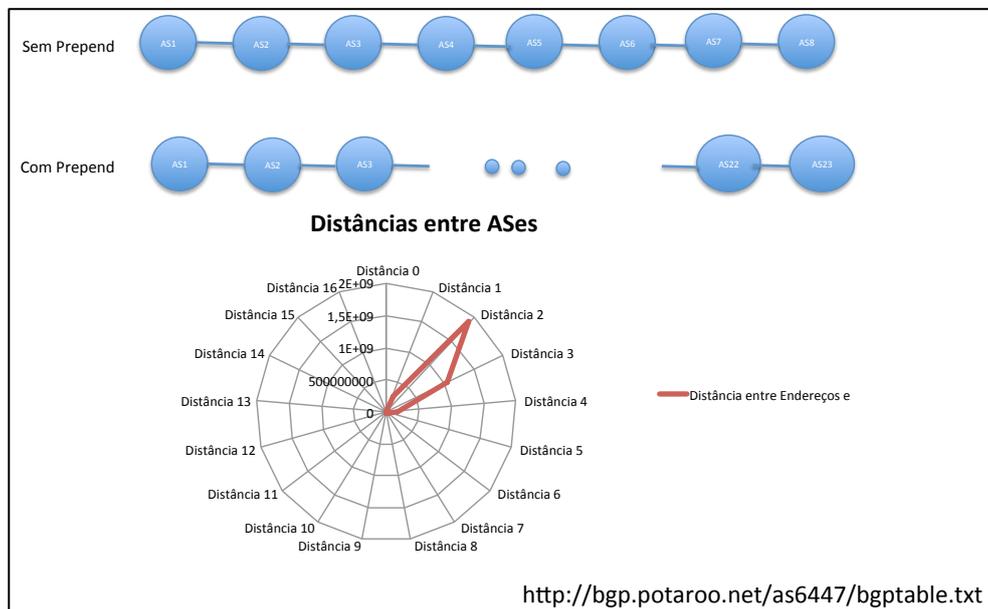


Figura 5.6 – Caracterização do raio entre ASes (número de saltos por ASes)

Na Fig. 5.7., usando apenas a tabela de rotas do roteador de MIA e aplicando na ferramenta Weka, foi possível se fazer uma separação e mostrar que, de fato, a maior parte dos ASes está interconectada em até 2 ASes de distância, porém nesse caso não muito incomum também ASes com distâncias de até 3 ASes. Nesse caso, observa-se que o AS de origem carrega dentro de si informações em que o mesmo é a origem do grafo. Pode-se entender essa condição de forma mais simples observando que, na América do Sul, as distâncias de até 3 ASes são importantes. Na Fig. 5.6, a origem dos grafos é um AS na Universidade de Oregon nos EUA.

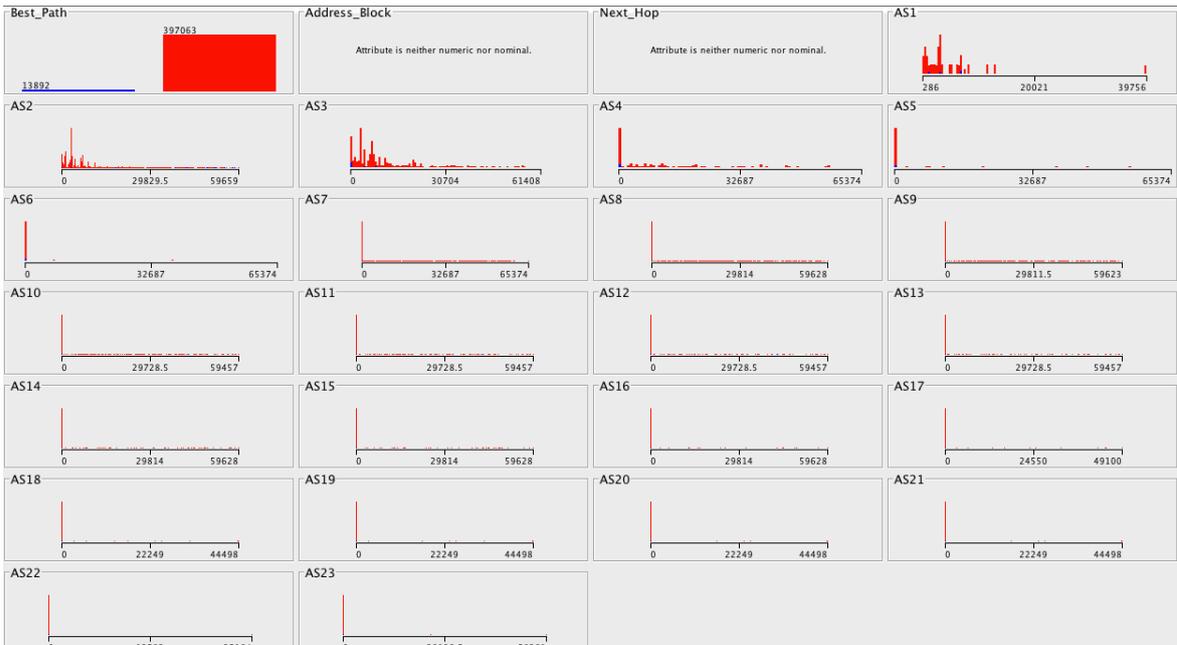


Figura 5.7 – Caracterização do *prepend* AS n , em que n é igual à distância entre ASES.

Da Fig. 5.4., observa-se a necessidade de se caracterizar o tráfego, pois será necessário para o entendimento da quantidade de recursos que será necessária para a nova configuração da rede.

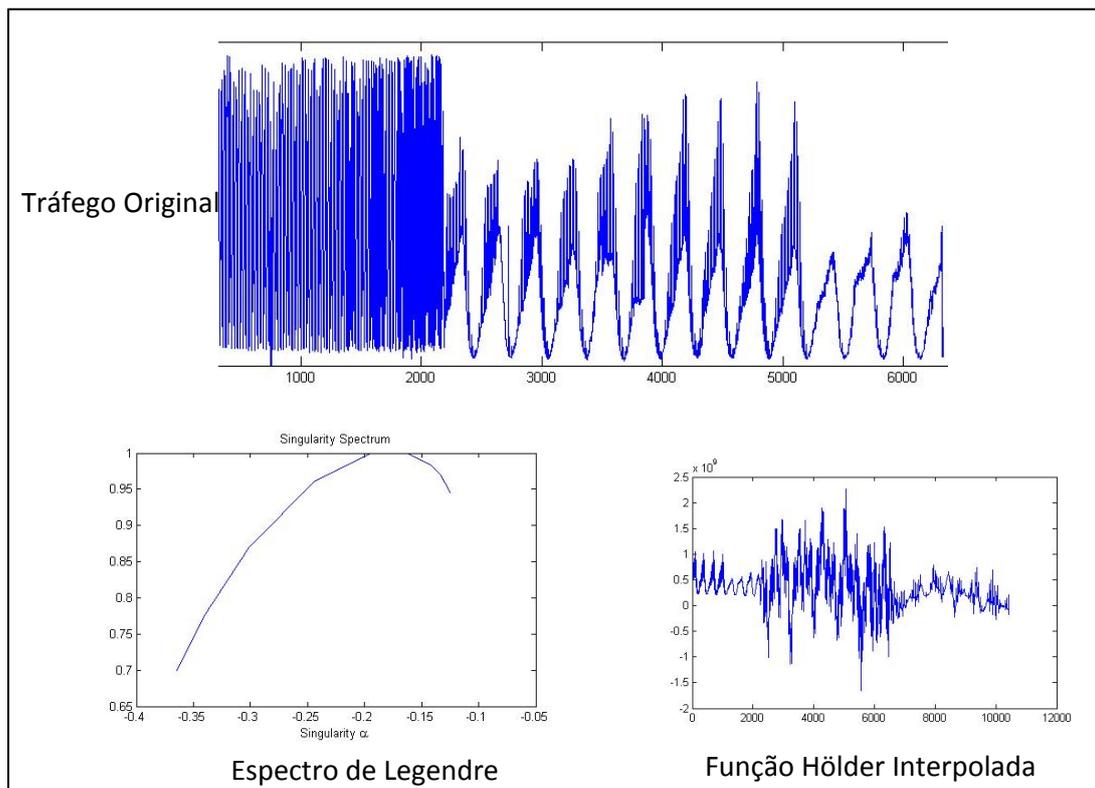


Figura 5.8 – Caracterização do tráfego → DLD.

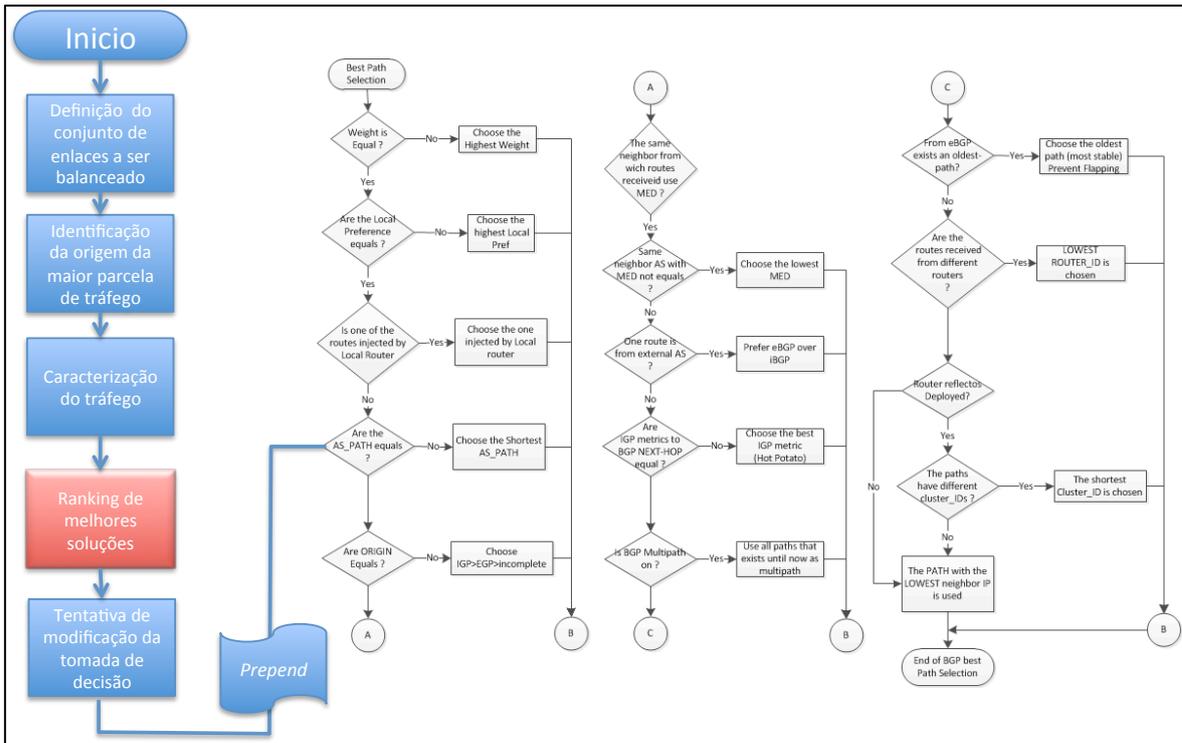


Figura 5.10 – Processo de alteração do *prepend*

Na Fig. 5.11, é mostrado, no *routeviews*, o momento de instabilidade, observando via *routeviews* a partir do AS origem que as conexões não são mais as mesmas durante a instabilidade, ou seja, o grafo foi modificado.

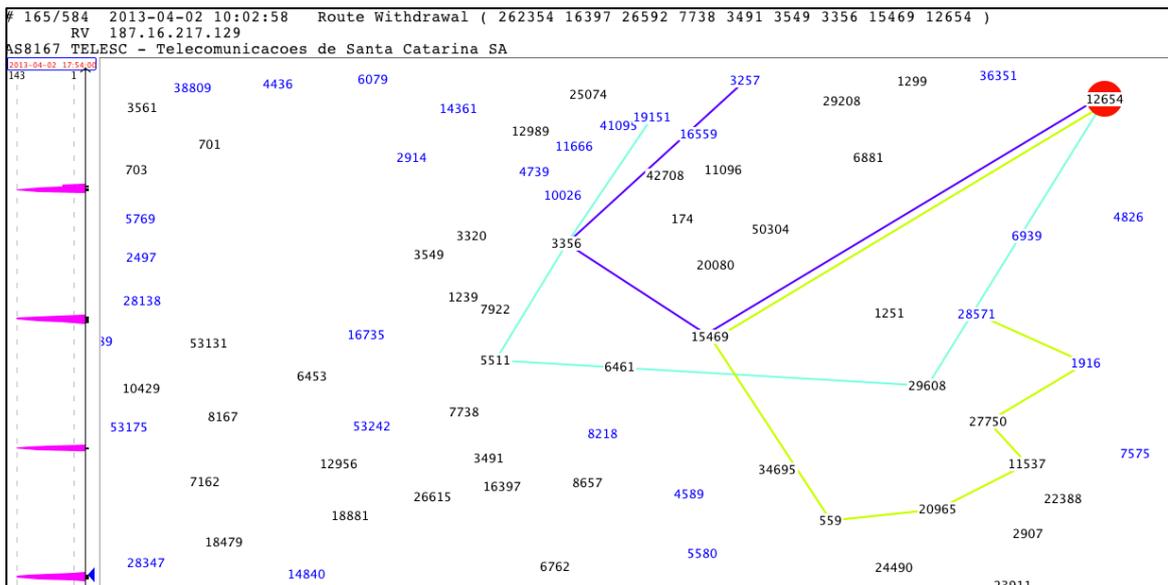


Figura 5.11 –Ruptura do encaminhamento de tráfego *prepend* - Extraído da tabela de rotas de um roteador real e analisado pelo *BGPplay* (Meyer, 2014).

Conforme a Fig. 5.12, para que o grafo retorne à mesma condição inicial, são necessários cerca de 300 s, e, somente após esse retorno, o tráfego é então roteado pelo novo caminho.

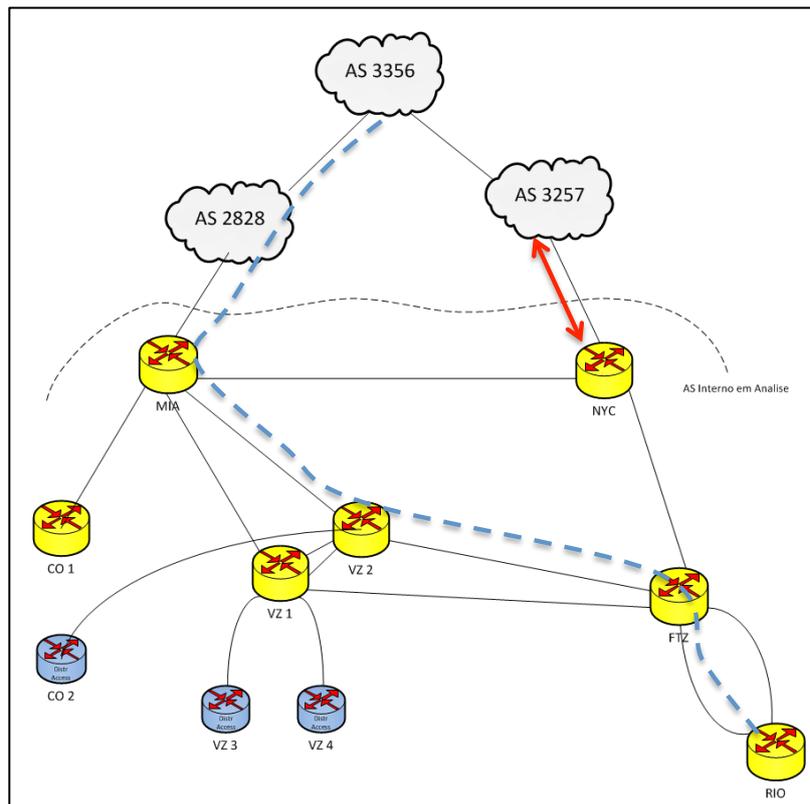


Figura 5.12 – Tráfego modificado.

Observa-se que o uso do *prepend* é amplamente utilizado como solução para engenharia de tráfego na Internet. Aqui é importante se definir engenharia de tráfego como qualquer alteração na rede que não tenha ocorrido por decorrência de um protocolo eGP (*Exterior Gateway Protocol*) ou iGP (*Interior Gateway Protocol*).

Na Fig. 5.13, pode-se verificar que o uso do *prepend* tem grau de eficiência interessante, porém sua eficácia pode ser questionada, principalmente quando se trata de situação que pode levar a rede a um período de instabilidade onde é possível que o encaminhamento de pacotes seja paralisado até que os protocolos de roteamento convirjam novamente. Observa-se da Fig. 5.13 que, quanto maior o raio, menor a probabilidade de efetividade.

De outro lado, é também necessário que o grau de eficácia seja verificado, pois, quando se trata de decisão que certamente levará a rede à instabilidade, essa decisão deve ocorrer

com o máximo de garantias que levarão o agente a um grau de eficácia maior que aquele anterior própria eficácia.

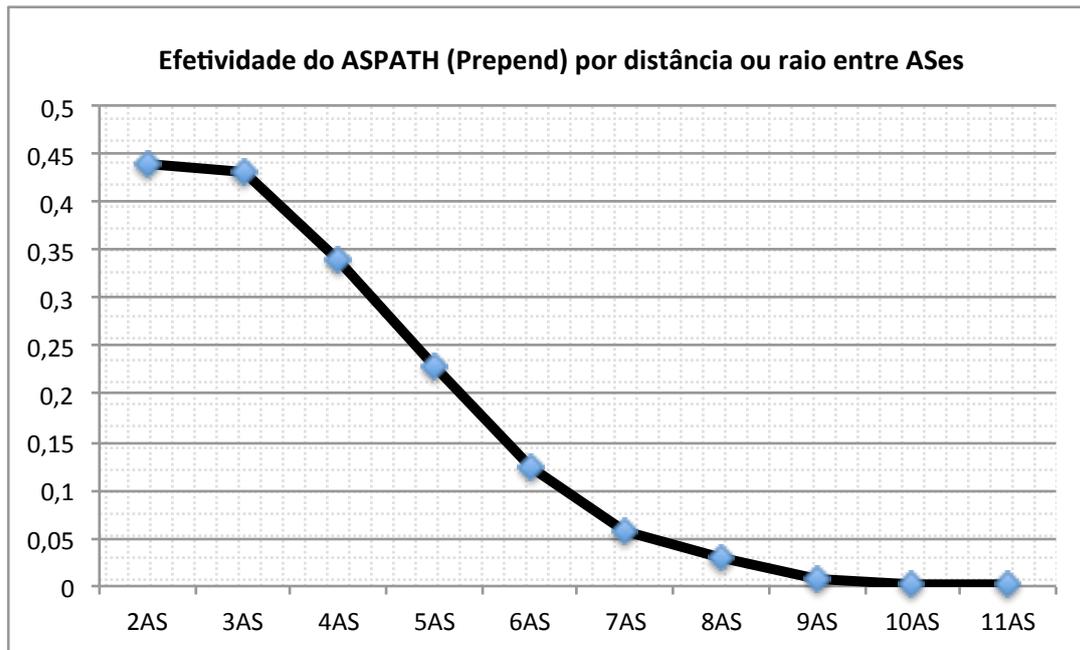


Figura 5.13 – Efetividade do uso do *prepend*.

Na mesma rede real analisada, também o grau de eficácia foi analisado e, para decisões tomadas por agentes humanos, sem metodologia específica, os resultados estão descritos na Fig. 4.2., em que se observa que os resultados são inferiores a 30% na primeira tentativa. Na segunda tentativa ou em tentativas de maior ordem, seguramente diferente da primeira configuração, observa-se que a eficácia é superior a 30%, portanto o uso da solução de *prepend* atende a mais de 60% das ações que ocorrem em uma rede quando da necessidade de modificação do perfil de encaminhamento ou recebimento de pacotes por um AS.

O método para o aumento da eficácia na primeira tentativa é interessante e certamente poderá melhorar o desempenho da interconexão entre as redes, pois irá diminuir os períodos de instabilidade da rede em função da modificação da tabela de roteamento Internet, para os casos aqui analisados extraída de roteador real ou através do projeto *routeviews*.

5.3 ENSAIO 2 – TENTATIVA DE CONTROLE DO TRÁFEGO USANDO O CONHECIMENTO ESPECIALISTA PARA O ENTENDIMENTO DO PROCESSO DE DECISÃO NA AMÉRICA DO SUL

O fato de sistemas autônomos (AS), por definição, não aceitarem prioritariamente qualquer controle externo faz com que qualquer tentativa de controle de tráfego assimétrico seja um desafio quando o sentido da maior parte do tráfego é o entrante, ou *ingress*. O problema da assimetria é visto, com frequência, em redes hospedadas em países da América do Sul. Essas redes, comparadas com as redes hospedadas na América do Norte, são muito pequenas em número de nós e, também, em geração de conteúdo. Dessa forma, observa-se um desequilíbrio de quantidade de tráfego de entrada e saída à taxa superior a , conforme observado na Fig. 3.1., em algumas situações. Neste trabalho, algumas redes reais da América do Sul serão analisadas, caracterizadas e o comportamento especialista (por exemplo, *network engineer*) será estudado com relação à efetividade da sua tomada de decisão.

Parte dos resultados relacionados à caracterização foi publicada no SBrT 2013 (Deus *et al.*, 2013). Outra parte integrante dos resultados relacionados a processo de decisão com uso do conhecimento especialista foi apresentada no AINA 2014 (Deus *et al.*, 2014).

5.3.1 - Analisando a assimetria do tráfego

De acordo com (He *et al.*, 2005), a assimetria de tráfego na Internet pode ser encontrada em mais de 90% de todas as conexões e enlaces, ou seja, o problema não ocorre apenas nas redes da América do Sul. Por outro lado, a maior parte das soluções e padrões usados nessas mesmas interconexões, excetuando-se os padrões no acesso (ADSL ou redes móveis, onde o *downlink* assume banda diferente da do *uplink*). Na Fig. 5.14, na mesma perspectiva, é possível se observar nas amostras coletadas na Colômbia, na Venezuela e no Brasil que o tráfego possui alto grau de assimetria.

A falta de infraestrutura de *datacenters* e, portanto, a geração de conteúdo com armazenamento local, características presentes nesses países, são fatores que podem explicar o desbalanceamento. Independentemente disso, pode ser observado que, devido à baixa importância dessas redes para o cenário de tráfego observado nos Estados Unidos,

existem condições desfavoráveis para o controle de tráfego.

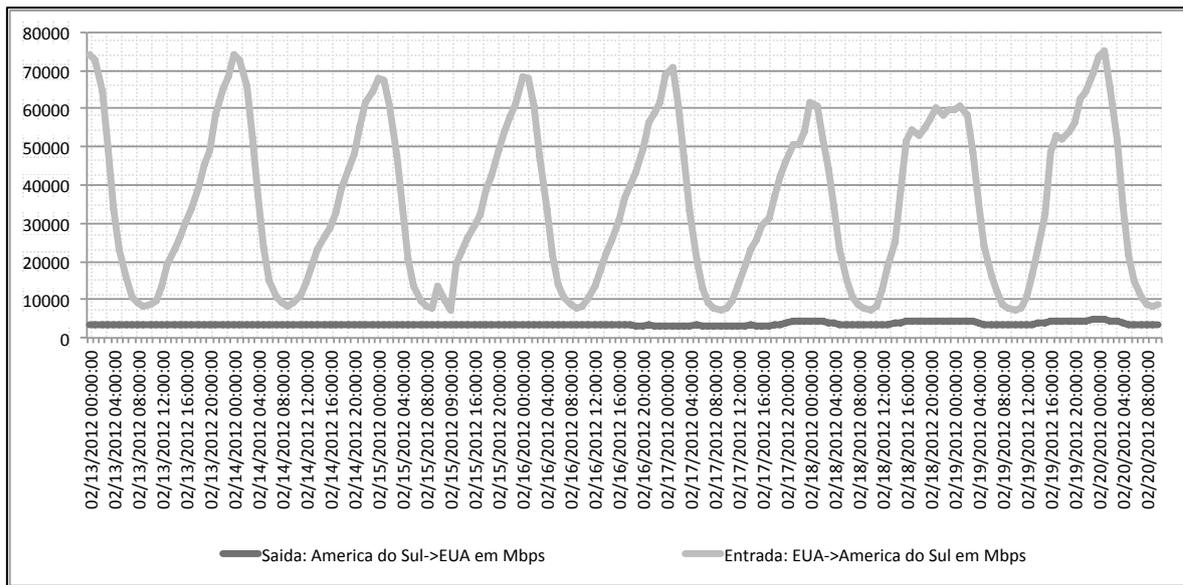


Figura 5.14a – Tráfego, por horário, dos Estados Unidos da América para Venezuela e Colômbia, em Mbps (devido a acordo de confidencialidade, considerar os valores apenas para cálculo da razão, que nesse caso é superior a 20:1, sendo que todos os valores reais foram divididos por n , $n \geq 1$). Coleta de tráfego em maio de 2012. SNMP/MIB: 5 min. entre coletas.

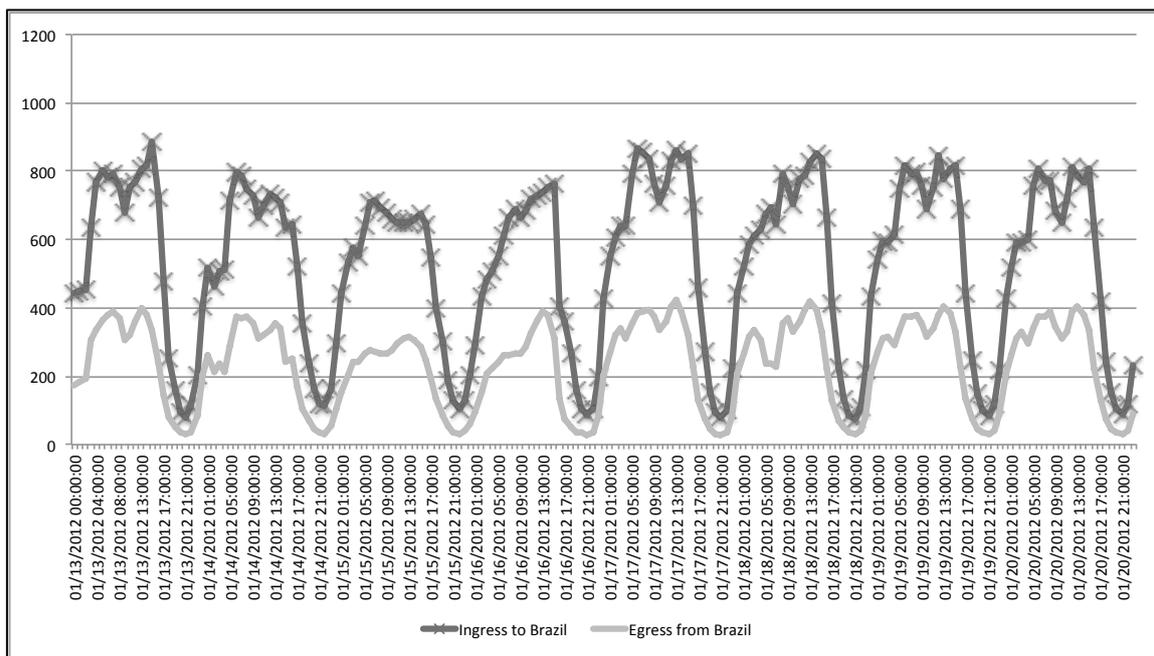


Figura 5.14b - Tráfego horário dos Estados Unidos para o Brasil em Mbps (Devido a um acordo de confidencialidade considerar os valores apenas para um cálculo da razão, que neste caso é superior a 5:1, todos os valores reais foram divididos por n , $n \geq 1$) coletados em Maio, 2012. SNMP/MIB: 5 min. entre coletas

5.3.1 – Caracterizando o tráfego

Na Fig. 5.15, as coletas relativas à Fig. 5.14 são analisadas para a caracterização do tráfego. Em (Véhel e Tricot, 2004), é apresentado o espectro de Legendre e mostrada a função de interpolação do expoente de Hölder. Devido à irregularidade do expoente de Hölder, é possível caracterizar o tráfego ilustrado na Fig. 5.14 dentro dos padrões multifractais.

Já o espectro de Legendre assume uma forma côncava, também característica dos processos multifractais. No caso do espectro de Legendre, o expoente de Hölder é representado pelo (α) , e o eixo das ordenadas representa a probabilidade de ocorrência de um dado valor do expoente de Hölder ocorrer. Dessa forma, o processo Multifractal ou DLD é satisfeito se:

$$E(|X(t)|)^q = c(q)t^{\tau(q)+1} \quad (5.1)$$

em que $t \in T$ e $q \in Q$, sendo T e Q os intervalos reais; $\tau(q)$ e $c(q)$ são funções no domínio Q . Em (5.1), T e Q assumem valores positivos e $0 \in T$ e $[0,1] \subseteq Q$. Tem-se, ainda, que $c(q)$ é o fator de tempo do processo. De acordo com (Véhel e Tricot, 2006), se q é linear, então o processo é dito monofractal ou autosimilar, de outra forma, o processo é Multifractal. O espectro de Legendre é definido por (5.2). Essas definições e outros resultados mais detalhados podem ser encontrados em (Véhel e Tricot, 2006).

$$f_L(\alpha) = \tau^*(\alpha) \quad (5.2)$$

em que, segundo (Véhel e Tricot, 2006), $\tau(q)$ é o espectro de Legendre.

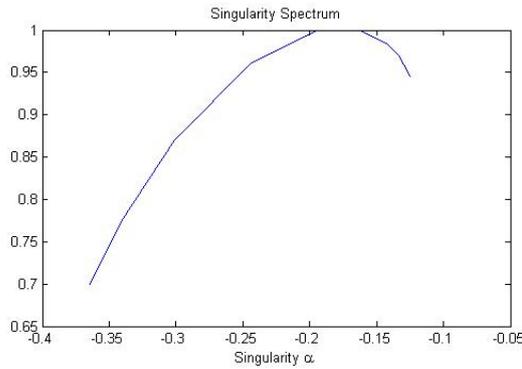


Figura 5.14a - Análise Multifractal – DLD - espectro de Legendre para o tráfego *ingress*.

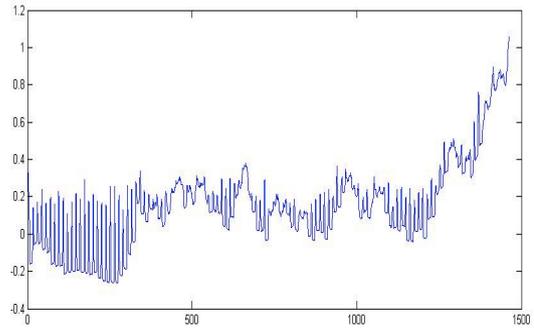


Figura 5.14b - Função de interpolação do expoente de Hölder.

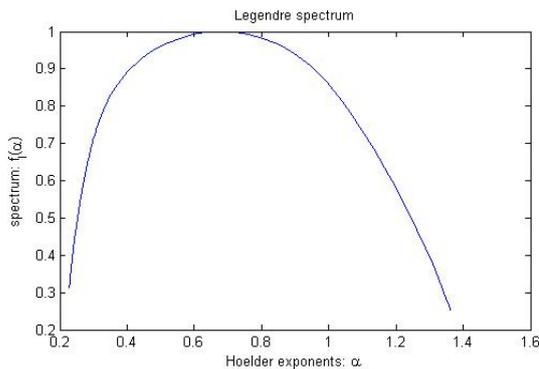


Figura 5.14 c - Análise Multifractal ou DLD do espectro de Legendre para o tráfego *egress*.

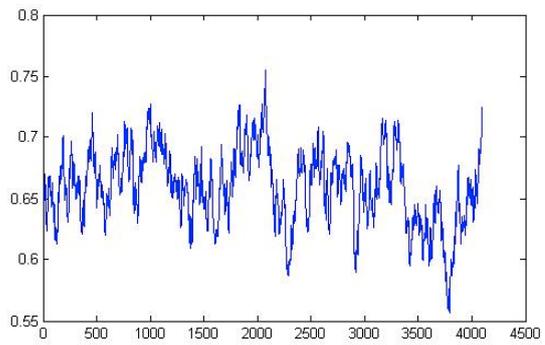


Figura 5.14d - Função de interpolação Hölder.

Ao final, observa-se de maneira mais importante o fato da existência ou não de processos com memória, o que irá gerar a Dependência de Longa Duração ou DLD.

A estrutura da rede que está sendo analisada é apresentada na Fig. 5.15. Essa é uma rede de longa distância que usa cabos submarinos entre o Brasil, Venezuela, Colômbia e Estados Unidos da América. Devido a acordo de confidencialidade, a empresa e o seu ASN não podem ser identificados. Observa-se que o *prepend* (uso do AS-PATH) é realizado com base na priorização que o BGP leva em consideração para o estabelecimento da estratégia ou política interna, o que é mostrado na Fig. 5.16.

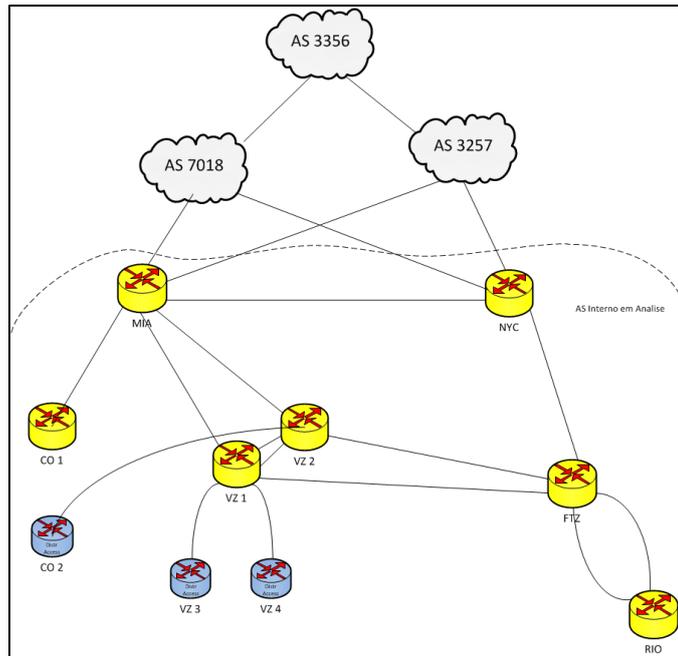


Figura 5.15 - Estrutura da rede em análise (N. U. T. – *network under the test*).

Política ou conjunto de ações (Estratégias) do BGP (Prioridade 1 é a maior)

- 1- Next-HOP acessível (válido)
- 2- Local Preference (MAIOR LP vence)
- 3- AS Path (MENOR AS Path vence)
- 4- ORIGIN (MENOR ORIGIN (MENOR vence)
- 5- MED (MENOR vence)
- 6- eBGP x iBGP (prefere eBGP à iBGP)
- 7- Métrica IGP até o peer que anunciou o prefixo (MENOR vence)
- 8- Tamanho do Cluster List (MENOR vence)
- 9- Router-ID (MENOR vence)
- 10- Peer-ID (MENOR vence)



Figura 5.16 - Política de tratamento dos parâmetros do BGP com prioridades.

O *prepend* é caracterizado pela tentativa de alteração de caminho por iniciativa do AS de destino (AS_D), que tenta influenciar o AS fonte (AS_S). Conforme Fig. 5.17, para esse caso, se o caminho do tráfego entrante ou *egressé* $path_{egress_1} = \{AS_{S1}, AS_{p11}, AS_{p21}, AS_D\}$. Por outro lado, se um caminho alternativo produz recompensas que interessam mais ao AS_D , sendo $path_{egress_2} = \{AS_{S1}, AS_{p1n}, AS_{pnn}, AS_D\}$ um conjunto dessas possibilidades, então o *prepend* é a ação iniciada pelo AS_D que visa à alteração do caminho, porém sem garantia de 100% de sucesso nessa modificação.

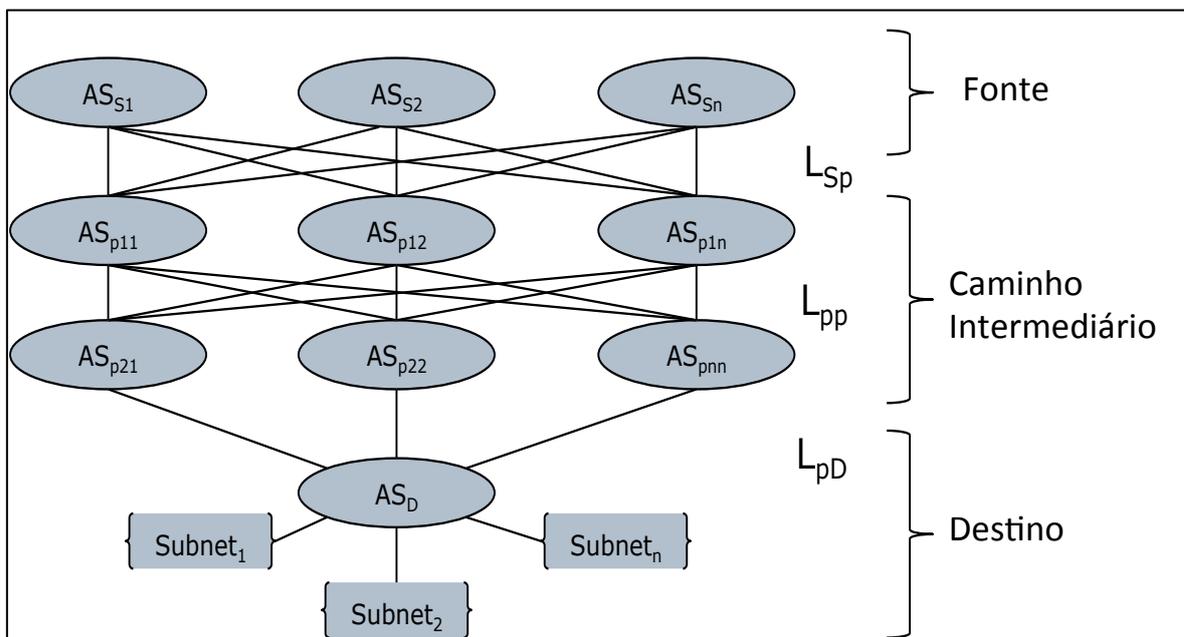


Figura 5.17 - Política de tratamento dos parâmetros do BGP com prioridades.

A decisão final se baseia no fluxo da figura 5.18, onde o ciclo é iniciado com a coleta de informação de todas as rotas presentes na Internet (*full routing table*). Com base na tabela de rotas, que pode ser observada na Fig. 5.19, a probabilidade de sucesso do *prepend* é calculada e, se essa probabilidade for maior que 0,5, então o processo é iniciado. Caso contrário, a probabilidade de sucesso do *prepend* sendo menor que 0,5, então a negociação deverá ocorrer por via direta entre os engenheiros de rede do AS_S e AS_D .

A partir de então, a necessidade de banda é calculada pelo período mínimo de uma janela de estabilidade. A janela de estabilidade deve ser o mínimo necessário para evitar que ocorram violações no SLA (*Service Level Agreement*), normalmente nunca inferior a 24 h para os casos de modificações no BGP. Após o cálculo da capacidade prevista necessária, um caminho deverá ser escolhido e por este ocorrerão as mudanças propostas com o uso do

AS-PATH ou *prepend* de rotas. Após essa aplicação, a **efetividade** ocorrerá se a modificação ocorrer conforme planejada na primeira tentativa. A monitoração dos resultados ocorre durante todo o processo de mudança e também após a mudança.

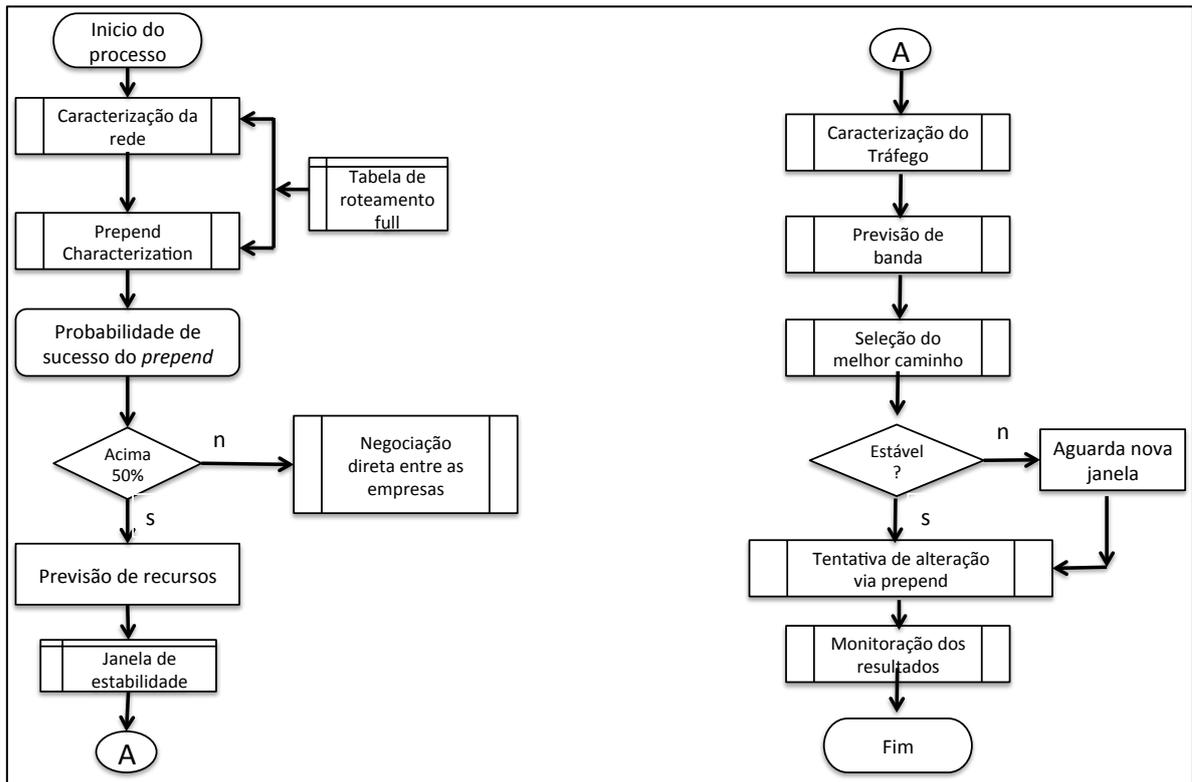


Figura 5.18 – Ciclo completo de tomada de decisão para aplicação em rede real.

A Fig. 5.19 mostra o processo de decisão não automatizado, levando-se em consideração o processo realizado conforme descrito na Fig.5.18, mas inserindo um novo parâmetro relacionado com a experiência do especialista (Engenheiro de Redes). Este ensaio ocorreu durante 5 meses em uma rede real.

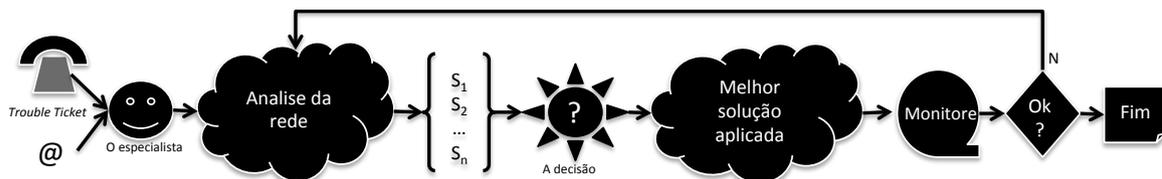


Figura 5.19 – Ciclo completo de tomada de decisão do especialista.

A Fig. 5.20 ilustra o resultado do acompanhamento de três grupos de engenheiros. Nesse caso, o *high skilled* possui experiência maior que 5 anos de atividades profissionais na área; o *medium skilled*, entre 2 e 5 anos; e o *low skilled*, menor que 2 anos. A pesquisa foi

realizada entre dezembro de 2012 e maio de 2013. A melhor efetividade é observada no grupo mais experiente, seguido pelo grupo intermediário e, por último, o grupo menos experiente com o controle do BGP. A figura mostra a efetividade, uma das medidas de recompensa usadas neste trabalho para a tomada de decisão.

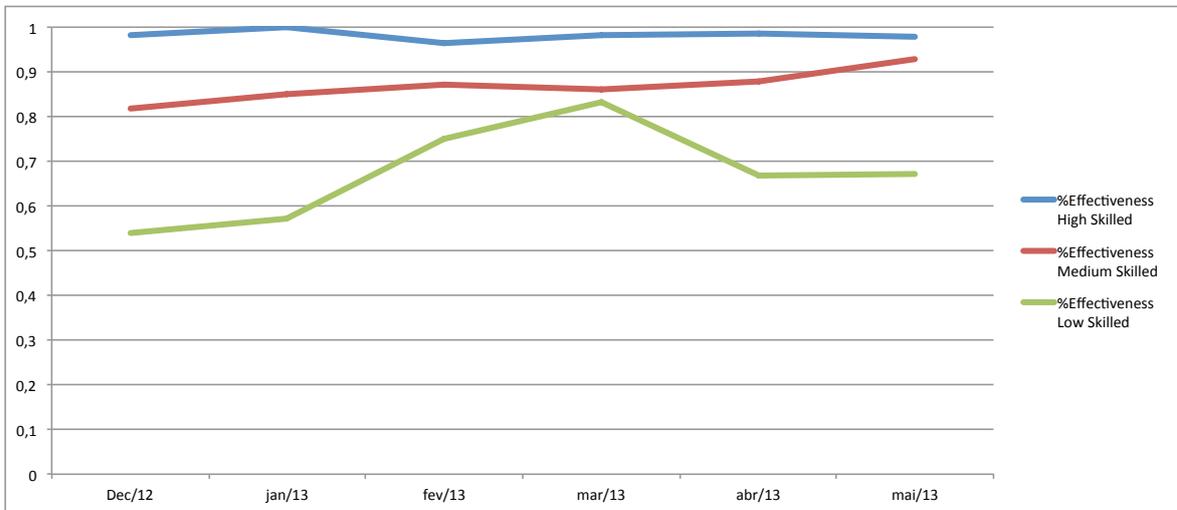


Figura 5.20 – Percentual de **efetividade** por grau de experiência do especialista.

Na mesma linha da efetividade, o tempo de solução também foi analisado. Na Fig. 5.21, é observado que a experiência do especialista é um fator interessante a ser considerado na tomada de decisão.

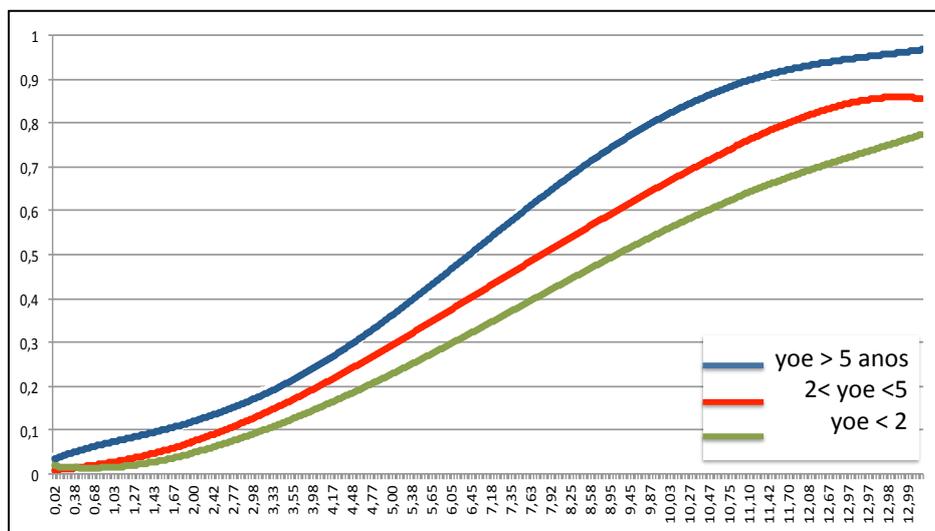


Figura 5.21 – CDF do tempo de solução em função da experiência do especialista (yoe).

Para esse ensaio, uma conclusão importante é que a decisão de modificar a rede deve ser acompanhada do gerenciamento do risco ou da estabilidade da rede. Caso uma modificação na rede tiver baixa probabilidade de ser efetiva na primeira tentativa é necessário que os riscos de se inserir uma alteração sejam bem conhecidos. Para um provedor de serviços, a pior condição a ser dominada é uma transgressão ou violação do SLA (*Service Level Agreement*) de um produto ou serviço.

5.4 ENSAIO 3 – TENTATIVA DE CONTROLE DO TRÁFEGO POR MEIO DO CICLO COMPLETO COM AUTOMATIZAÇÃO DE RESULTADOS.

Na Fig. 5.21, é mostrado o processo inicial do ciclo de tomada de decisão completo com automatização parcial relativa a coleta e caracterização. Todo o processo é automático, porém, como a rede sob análise está em produção, nenhuma intervenção ocorre sem a supervisão do engenheiro de redes.

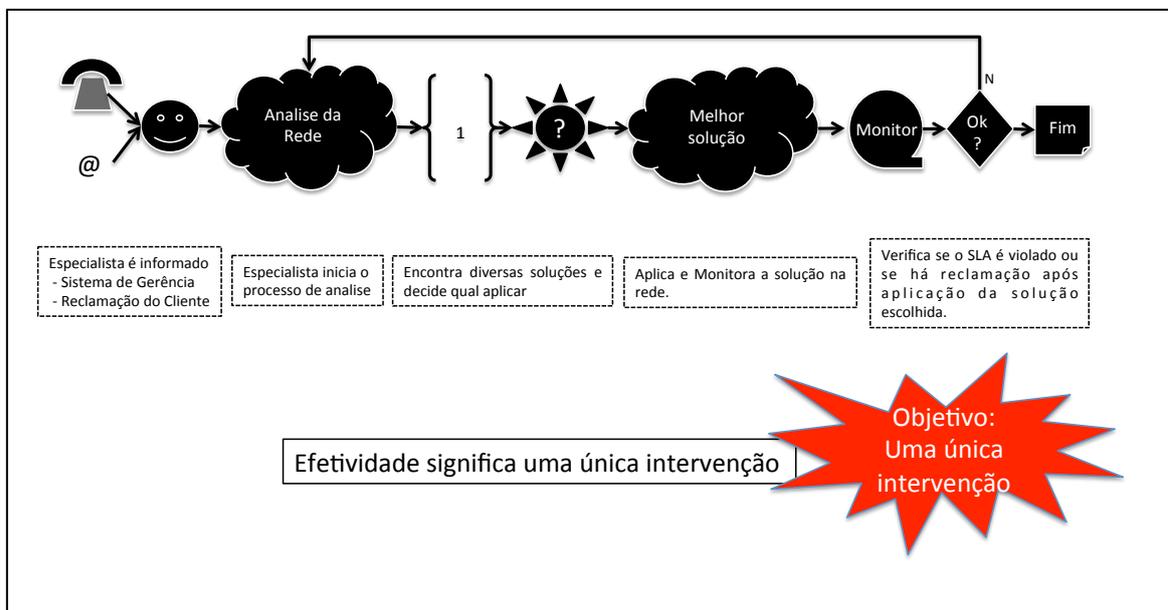


Figura 5.20 – Ciclo completo..

Para os casos analisados, foram considerados eventos gerados por reclamação do cliente final, que neste caso é também um sistema autônomo. De todos os eventos recebidos, 125 foram submetidos à análise e, destes, 100% tiveram solução com base no processo sugerido. Usando a mesma estratégia disposta na Fig. 5.18, o ciclo foi iniciado com a coleta

dos dados e caracterização do *prepend*. Logo após, foram analisadas as possibilidades de caminhos distintos em condições de se melhorar as recompensas.

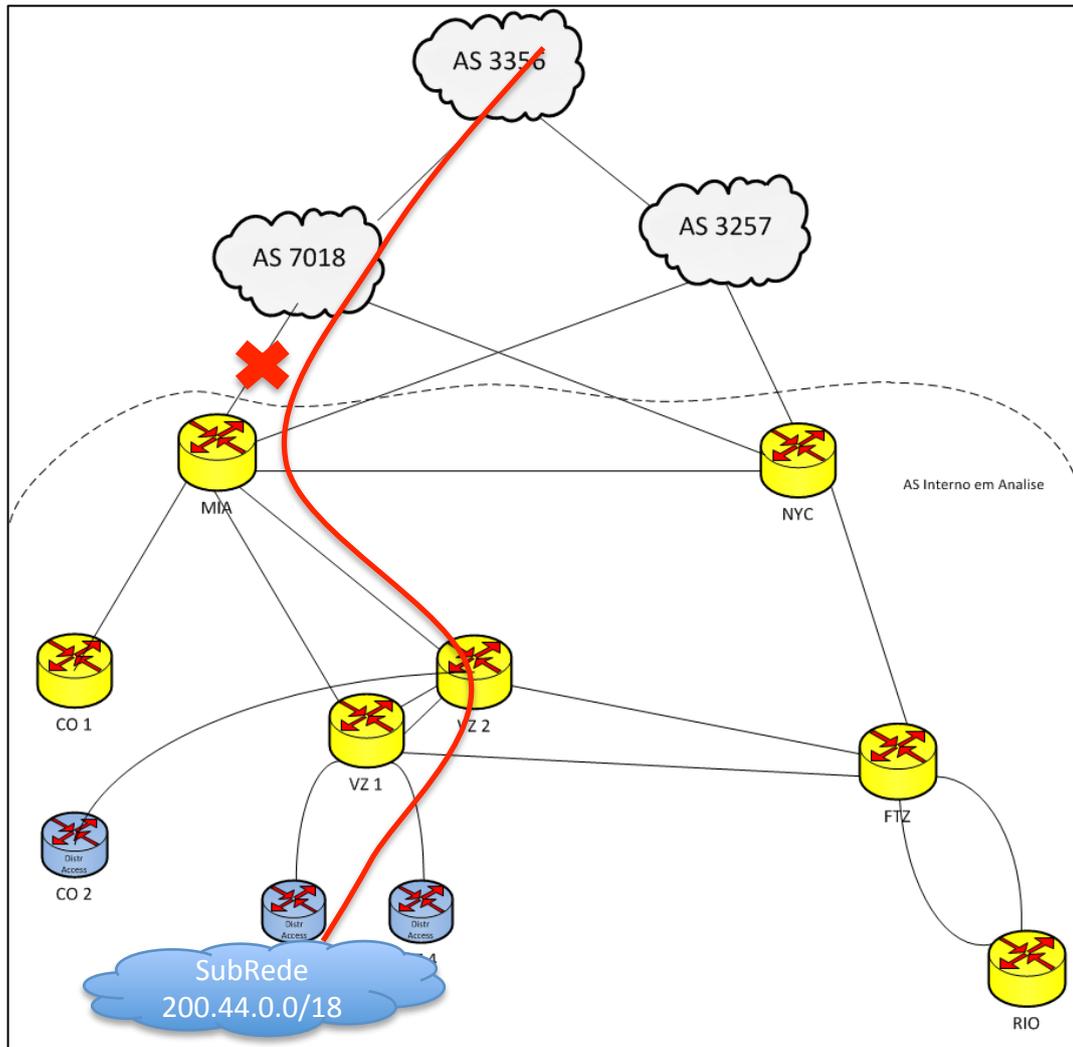


Figura 5.22 – Rede sob análise e subrede destino.

Na Fig. 5.23, é observado um congestionamento no caminho (*path*) relativo à rede da Fig. 5.22.

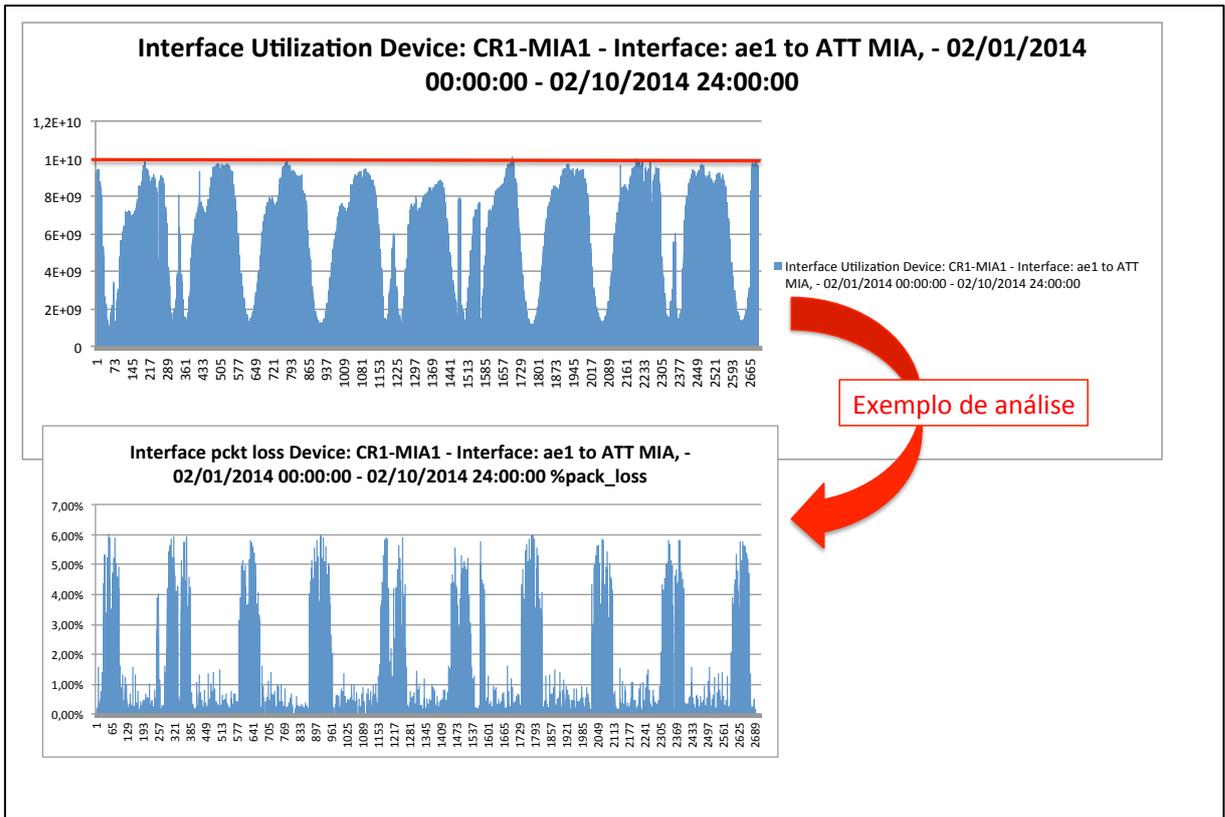


Figura 5.23 – Enlace congestionado.

Na Fig. 5.24, o tráfego é caracterizado por meio do coeficiente ou expoente de Hölder.

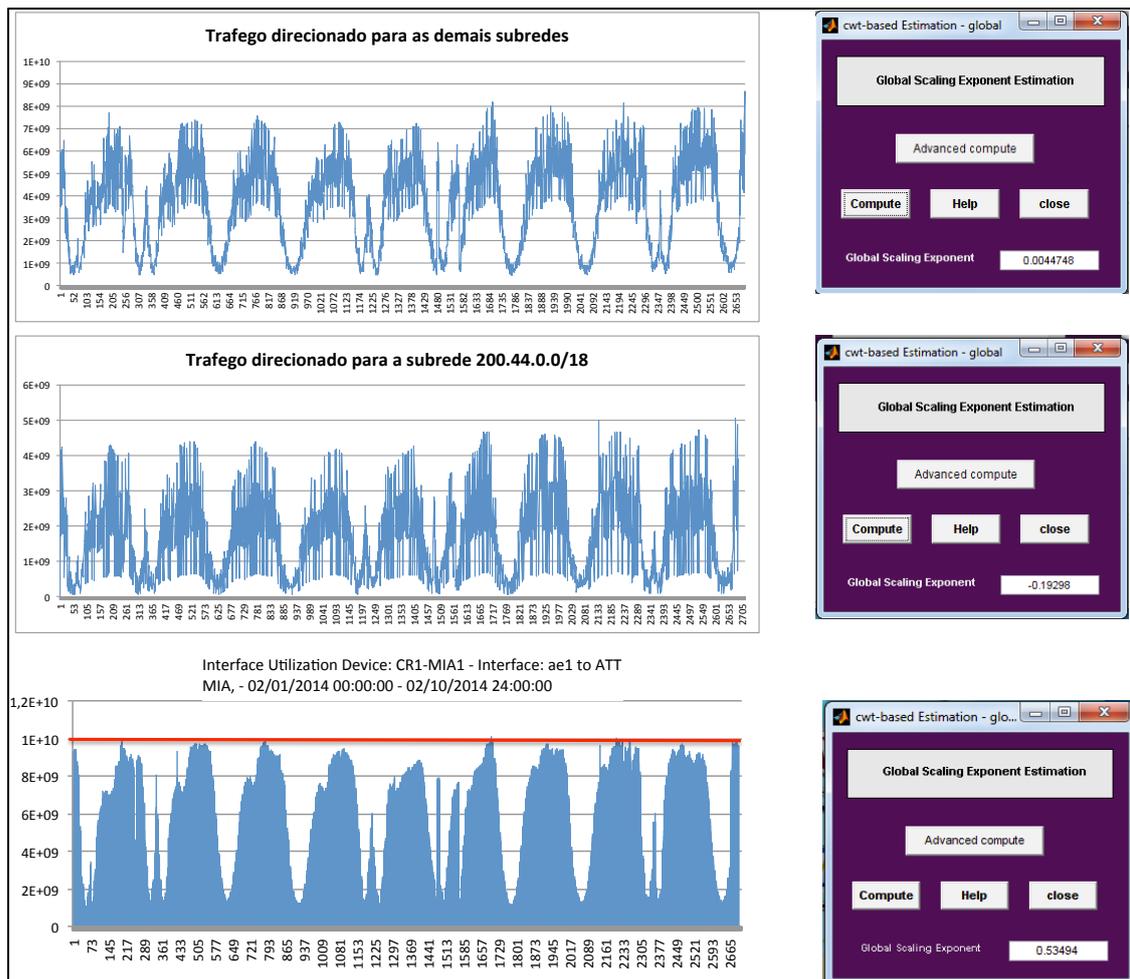


Figura 5.23 – Caracterização do Tráfego para algumas das 125 amostras. Uso da ferramenta Fraclab (Véhel, 2014).

Na Fig. 5.24, são calculados os diversos espectros de Legendre para as amostras de tráfego. Na Fig. 5.25, pelo fato de as amostras possuírem características multifractais, é usada a abordagem de (Stênico e Ling, 2013) para o cálculo da banda efetiva.

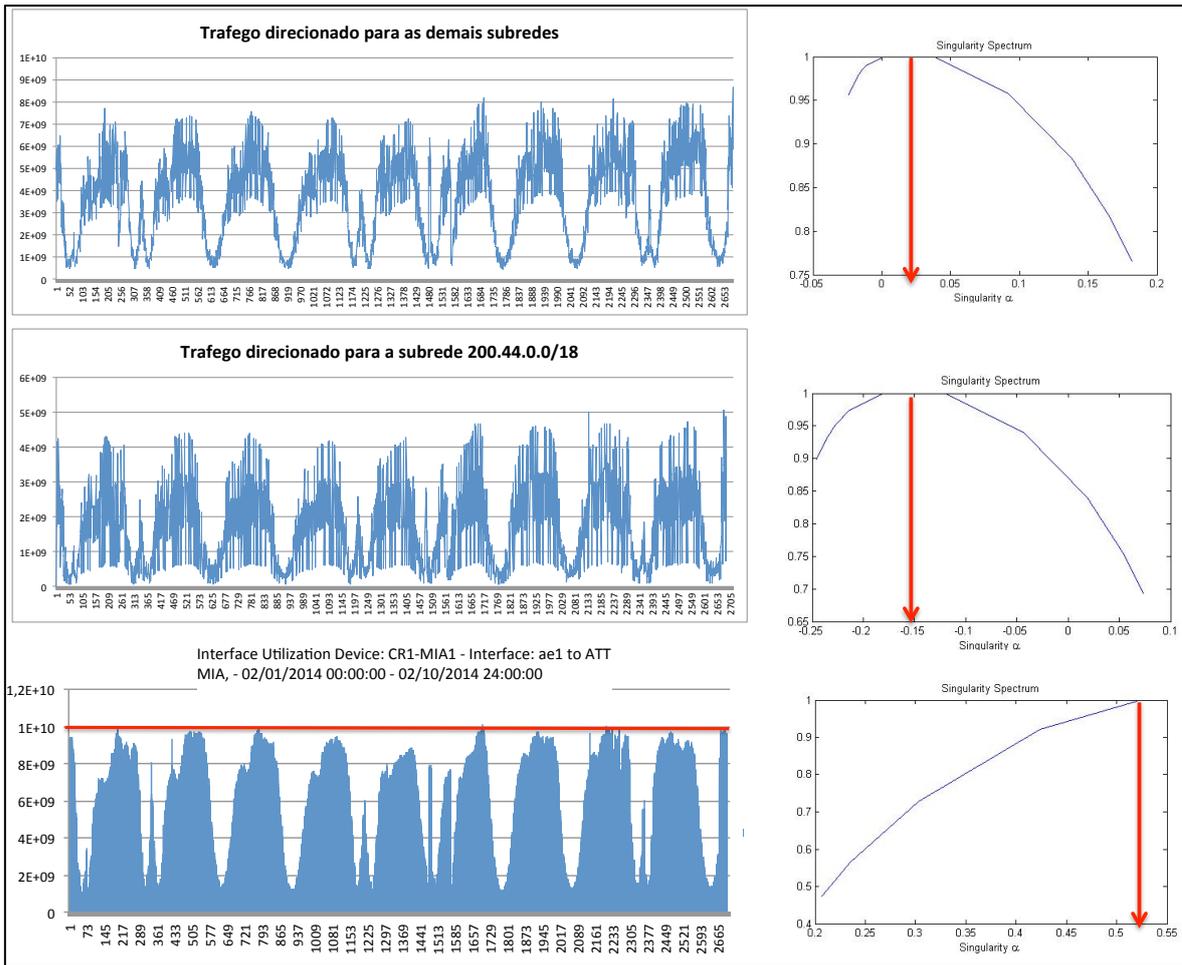


Figura 5.24 – Caracterização do Tráfego – Espectro de Legendre para algumas amostras.

Na Fig. 5.25, é mostrada a sequência das equações que compõem o cálculo da banda efetiva em acordo com (Stênico e Ling, 2013).

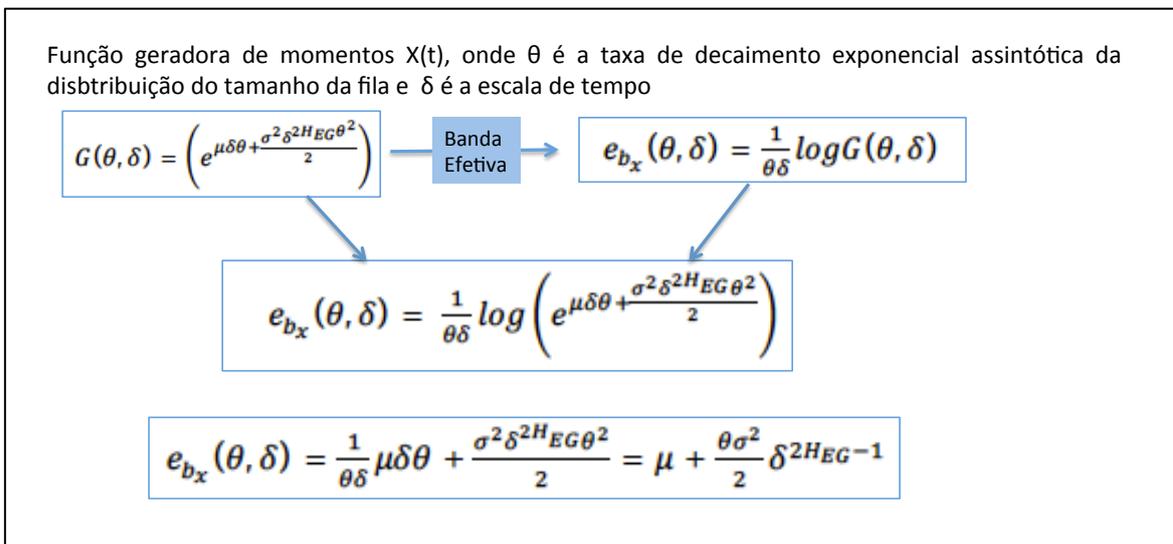


Figura 5.25 – Cálculo da Banda Efetiva (e_{bx} = Banda efetiva).

Na Tabela 5.1, são mostrados os resultados dos cálculos para o estabelecimento do processo de previsão de recursos, conforme 5.18.

OS	Date	Customer	Requested Bw	μ	θ	σ^2	δ (5 min)	H_{EG}	$e_{b_x}(\theta, \delta) = \mu + \frac{\theta \sigma^2}{2} \delta^{2H_{EG}-1}$	Effective inserted Bw	MAX % Packet Loss	% Saved Bw
1520001470	12/06/14 08:15	MQT.1.3.21	700	275,0	0,1	4291925,16	0,00333333	1,24	319	325	0,22%	54%
1520001489	12/06/14 09:52	BAR.2.3.12	300	150,0	0,1	4291925,16	0,00333333	1,23	203	210	0,10%	30%
1520001503	12/06/14 10:09	FTZ.2.22.3	700	230,0	0,1	4291925,16	0,00333333	1,12	406	420	0,46%	40%
1520001522	12/06/14 13:24	RIO.4.4.2	500	150,0	0,1	4291925,16	0,00333333	1,06	493	500	0,34%	0%
1520001536	12/06/14 14:34	MIA.3.4.5	1000	320,0	0,1	4291925,16	0,00333333	1,04	796	800	0,63%	20%
1520001542	12/06/14 15:27	MQT.1.3.3	1000	2400,0	0,1	4291925,16	0,00333333	0,93	3.997	4.000	12,32%	-300%
1520001550	12/06/14 20:19	FTZ.2.22.5	400	342,0	0,1	4291925,16	0,00333333	1,07	667	670	0,29%	-68%
1520001557	13/06/14 00:17	MQT.1.3.22	700	1850,0	0,1	4291925,16	0,00333333	0,90	4.193	4.200	9,23%	-500%
1520001560	13/06/14 03:41	BAR.2.3.13	1000	500,0	0,1	4321531,6	0,00333333	1,05	887	900	0,30%	10%
1520001576	13/06/14 06:46	FTZ.2.22.4	100	25,0	0,1	4344862,06	0,00333333	1,25	65	80	0,15%	20%
1520001578	13/06/14 07:57	RIO.4.4.3	1000	239,0	0,1	4375174,1	0,00333333	1,18	333	340	0,66%	66%
1520001588	13/06/14 10:18	MIA.3.4.6	600	450,0	0,1	4402785,12	0,00333333	1,26	489	500	0,14%	17%
1520001598	13/06/14 10:27	MQT.1.3.4	1000	333,3	0,1	4437360,64	0,00333333	1,05	737	750	0,21%	25%
1520001600	13/06/14 12:48	FTZ.2.22.6	200	50,0	0,1	4472481,13	0,00333333	1,30	73	80	0,18%	60%
1520001605	13/06/14 12:57	MQT.1.3.23	1000	250,0	0,1	4499432,86	0,00333333	1,15	385	400	0,39%	60%
1520001607	13/06/14 17:40	BAR.2.3.14	900	225,0	0,1	4511889,18	0,00333333	1,13	397	400	0,18%	56%
1520001618	13/06/14 22:31	FTZ.2.22.5	400	100,0	0,1	4568539,73	0,00333333	1,19	186	200	0,22%	50%
1520001626	14/06/14 00:09	RIO.4.4.4	200	50,0	0,1	4589610,98	0,00333333	1,15	192	200	0,11%	0%
1520001637	14/06/14 00:35	MIA.3.4.7	300	75,0	0,1	4627241,89	0,00333333	1,36	87	100	0,35%	67%
1520001644	14/06/14 03:58	MQT.1.3.5	900	300,0	0,1	4659846,71	0,00333333	1,15	447	450	0,17%	50%
1520001648	14/06/14 06:20	MQT.1.2.21	300	75,0	0,1	4698641,41	0,00333333	1,31	99	100	0,11%	67%
1520001660	14/06/14 06:37	BAR.2.3.2	100	3,0	0,1	4723446,36	0,00333333	1,44	8	20	0,18%	80%
1520001663	14/06/14 07:13	FTZ.2.21.3	800	266,7	0,1	4763336,95	0,00333333	1,09	547	550	0,15%	31%
1520001677	14/06/14 07:39	RIO.4.1.2	200	100,0	0,1	4800656,85	0,00333333	1,27	135	150	0,10%	25%
1520001691	14/06/14 10:27	MIA.3.4.5	900	300,0	0,1	4833457,94	0,00333333	1,03	889	900	0,17%	0%
1520001706	14/06/14 14:08	MQT.1.2.3	800	266,7	0,1	4859493,92	0,00333333	0,96	1.594	1.600	8,33%	-100%
1520001725	14/06/14 18:51	BAR.2.3.15	700	233,3	0,1	4888338,72	0,00333333	1,18	336	350	0,11%	50%
1520001742	14/06/14 19:26	FTZ.2.22.6	500	166,7	0,1	4929743,59	0,00333333	1,10	427	430	0,85%	14%
1520001745	14/06/14 21:21	RIO.4.4.5	200	22,0	0,1	4959297,05	0,00333333	1,53	24	35	0,11%	83%
1520001763	15/06/14 00:44	MIA.3.4.8	100	50,0	0,1	4983211,5	0,00333333	1,30	78	90	0,13%	10%
1520001780	15/06/14 01:28	MQT.1.3.6	500	166,7	0,1	5014538,92	0,00333333	1,21	244	250	0,11%	50%
1520001798	15/06/14 05:27	MQT.1.2.22	300	100,0	0,1	5051942,57	0,00333333	1,19	195	200	0,21%	33%

Figura 5.26 – Cálculo da banda efetiva para cada um dos casos analisados.

Na Tabela 5.1, são mostrados os resultados dos cálculos para o estabelecimento do processo de previsão de recursos, iniciando com o cálculo do expoente de Hölder, conforme 5.18. Na Fig. 5.27, é mostrado como uma das fontes de tráfego foi identificada. Somente após a identificação da fonte de tráfego é possível se determinar por qual novo caminho o tráfego deverá ser encaminhado.

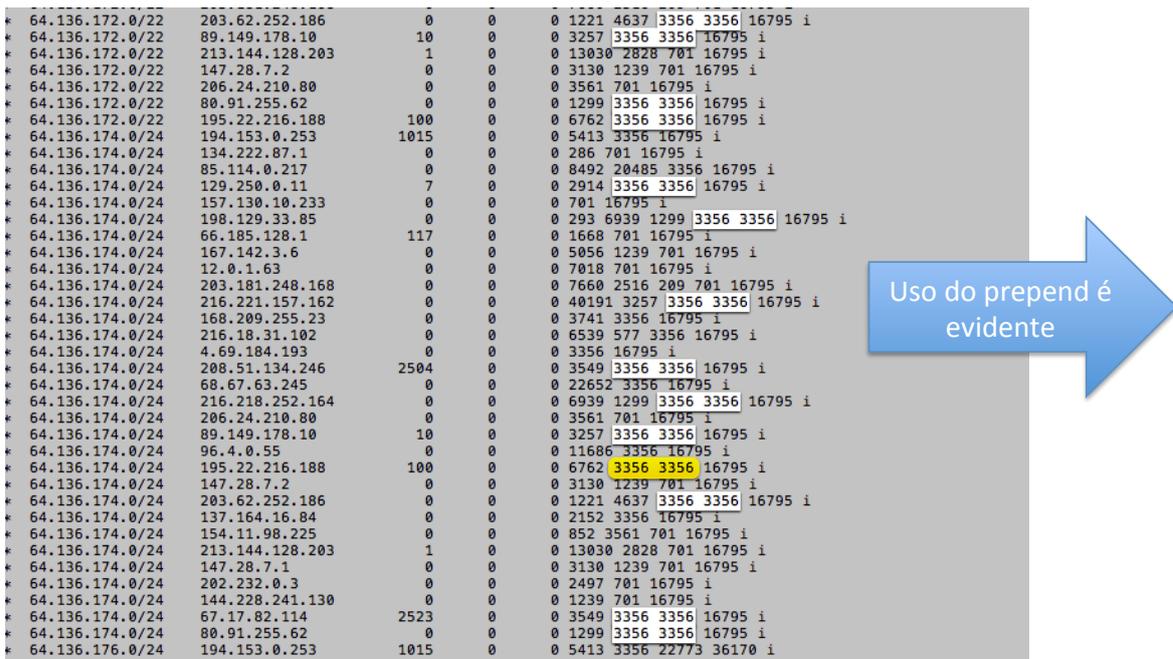
Whois ? Endereço IPv4, IPv6 - ASN

Autonomous System Number
Number 3356
Name LEVEL3
Handle AS3356
Organization Level 3 Communications, Inc. (LVLT)
Registration Date 2000-03-10
Last Updated 2012-02-24
Comments
RESTful Link <http://whois.arin.net/rest/asn/AS3356>
Function Point of Contact
Tech LC-ORG-ARIN (LC-ORG-ARIN)
See Also Organization's POC records.

LVLT-ORG-205-180 (NET-205-180-0-0-1) 205.180.0.0 - 205.183.255.255
LVLT-ORG-216-202 (NET-216-202-0-0-1) 216.202.0.0 - 216.202.255.255
LVLT-209-241 (NET-209-241-0-0-1) 209.241.0.0 - 209.241.255.255
LVLT-ORG-64-8 (NET-64-8-0-0-1) 64.8.0.0 - 64.8.95.255
LVLT-ORG-64-9 (NET-64-9-0-0-1) 64.9.0.0 - 64.9.127.255
LVLT-ORG-8-8 (NET-8-0-0-0-1) 8.0.0.0 - 8.255.255.255

Figura 5.27 – Identificação da fonte do tráfego.

Na Fig. 5.28, é mostrado como a probabilidade do uso do *prepend* é determinada.



Uso do prepend é evidente

Figura 5.28a– Uso do *prepend*.

Na Fig. 5.29, é mostrado o cálculo que foi realizado individualmente para cada um dos casos analisados.

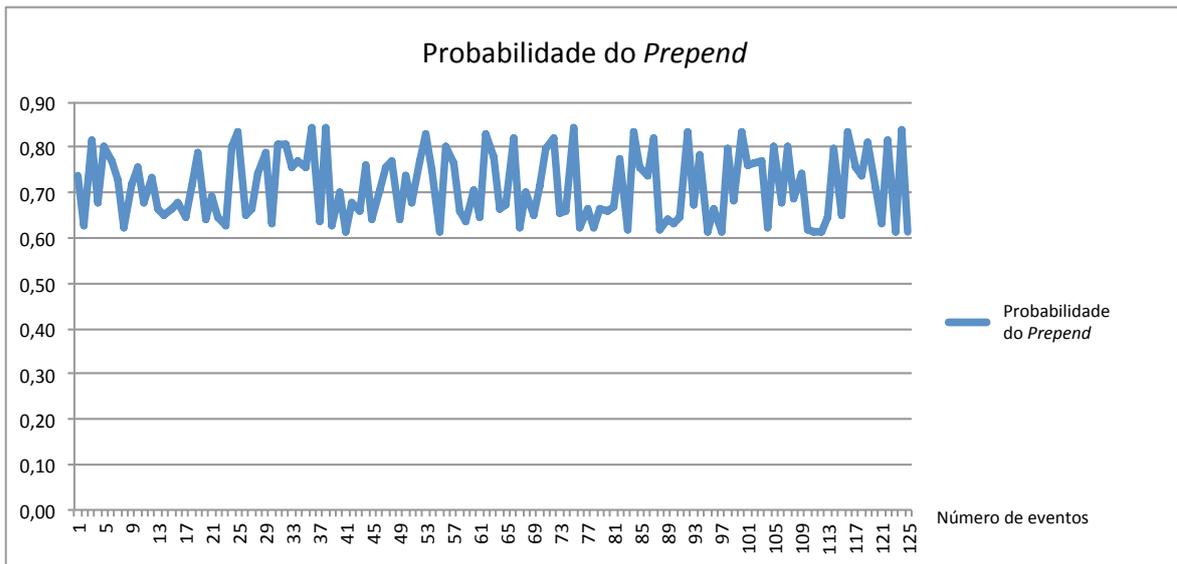


Figura 5.28b– Uso do *prepend*.

A predição da banda é realizada conforme processo definido na Fig. 3.11 e os resultados estão mostrados na Fig. 5.29.

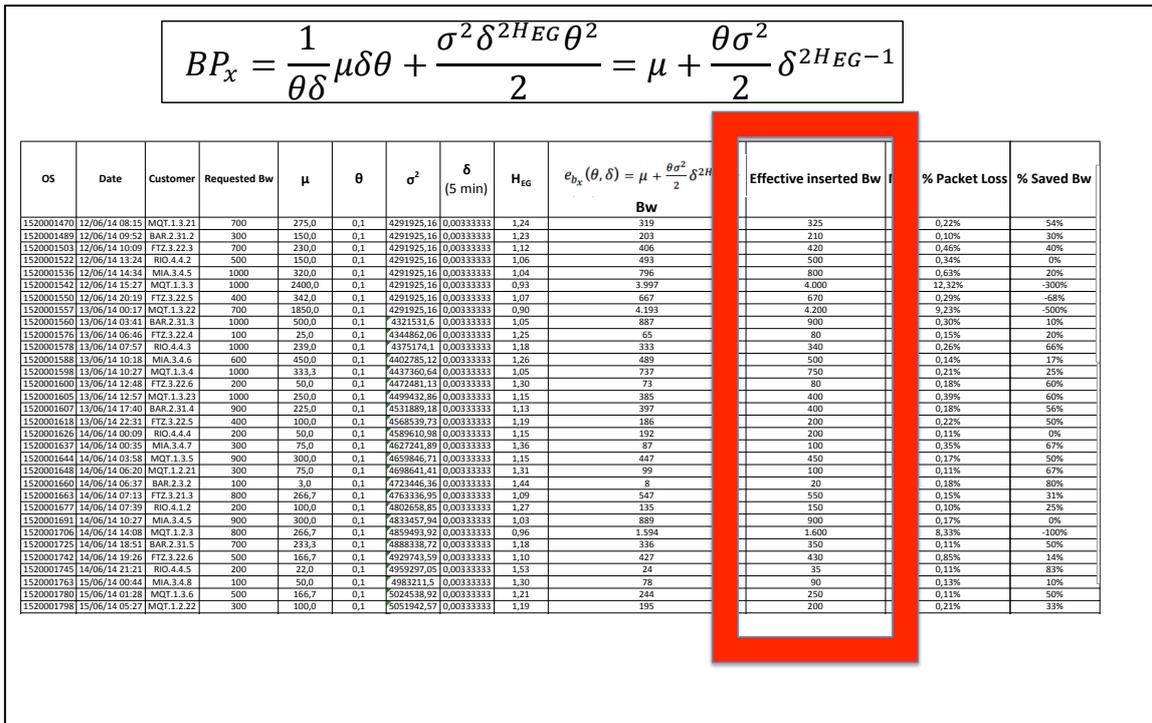


Figura 5.29– Cálculo da Banda Efetiva.

Para os 125 casos coletados, foram executadas análises de economia de recursos. Um exemplo de análise é mostrado na Fig. 5.30.

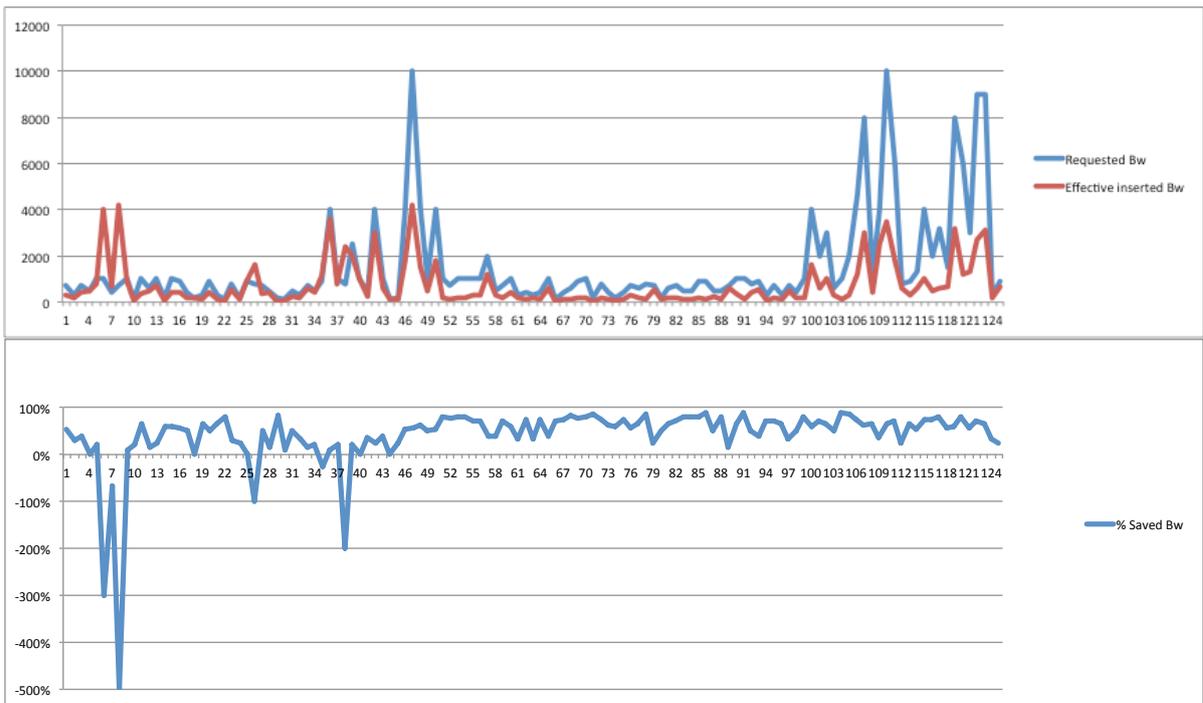


Figura 5.30 – Banda efetiva requisitada (azul) e inserida. A diferença é a economia e o acerto proporcionado pela metodologia.

Na Fig. 5.30, os valores negativos, todos sem excessão, são provenientes de erros do operador (engenheiro de rede, que não aplicou a metodologia, conforme mostrado na Fig. 5.31).

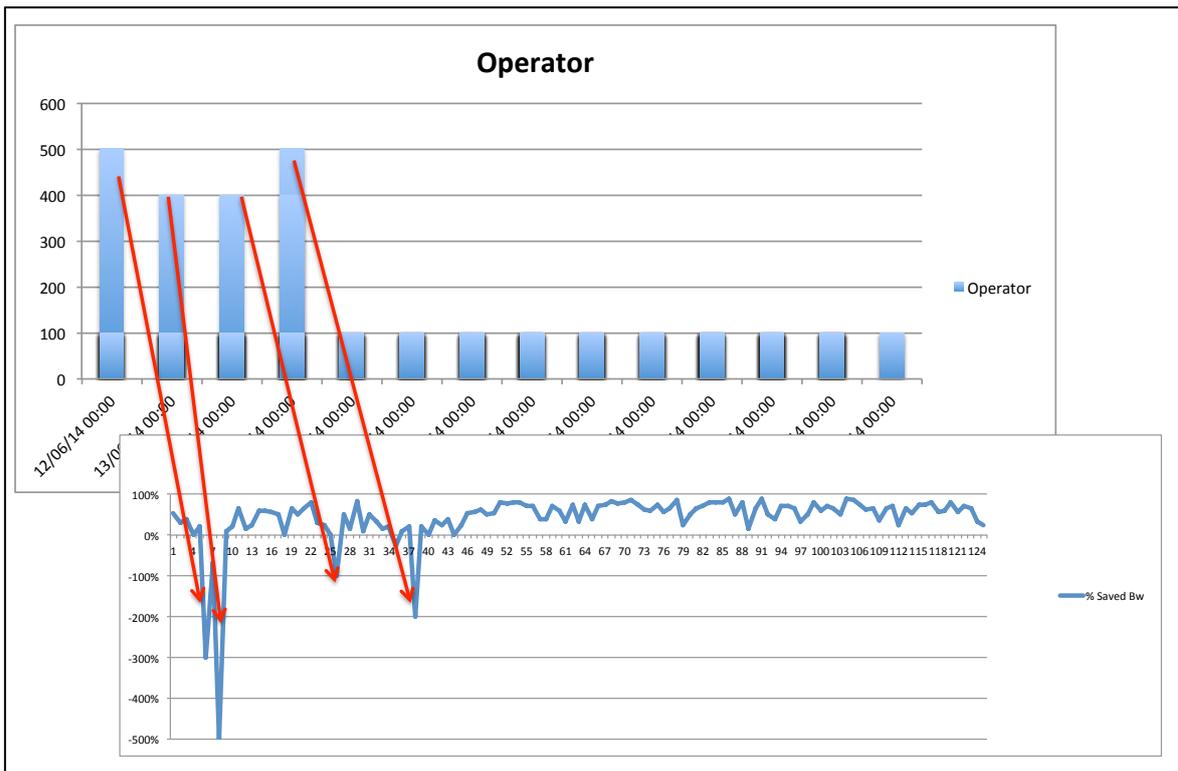


Figura 5.31 – Os casos mostrados com economia de banda negativa são exatamente aqueles em que o operador não aplicou a metodologia ou a aplicou com erro.

Comparando a Fig. 5.32 é possível ver um exemplo em que o *prepend* teve sucesso em modificar o caminho do tráfego por uma solicitação externa, de baixa prioridade.

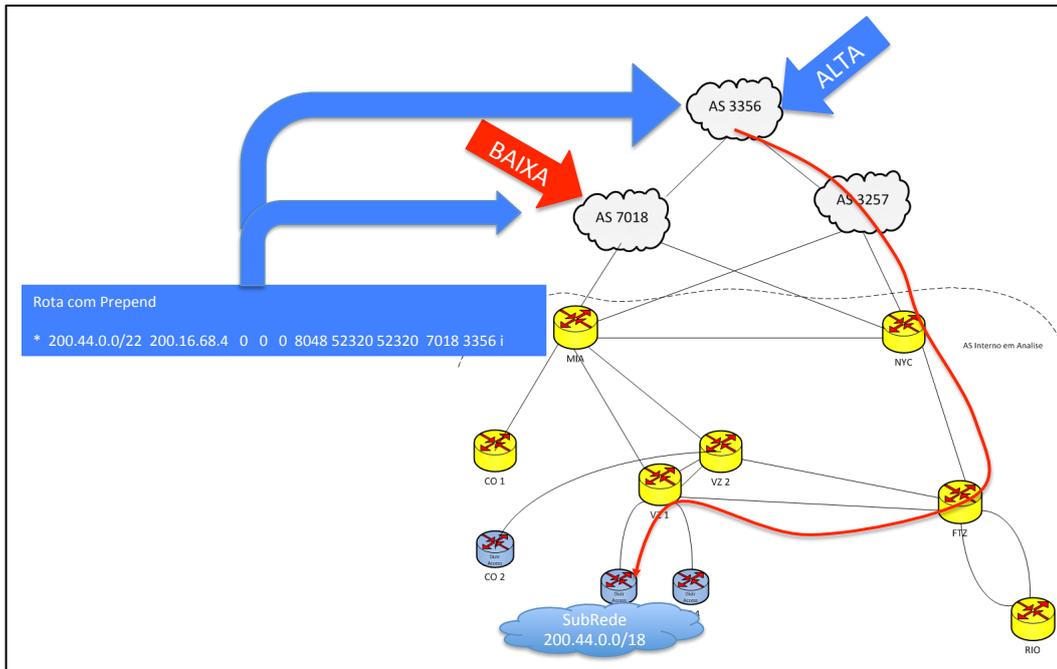


Figura 5.32 – Rede após a alteração com o uso do *prepend*.

Na Fig. 5.33, é mostrado o estado de um dos 125 enlaces, como exemplo, após a modificação da proposta.

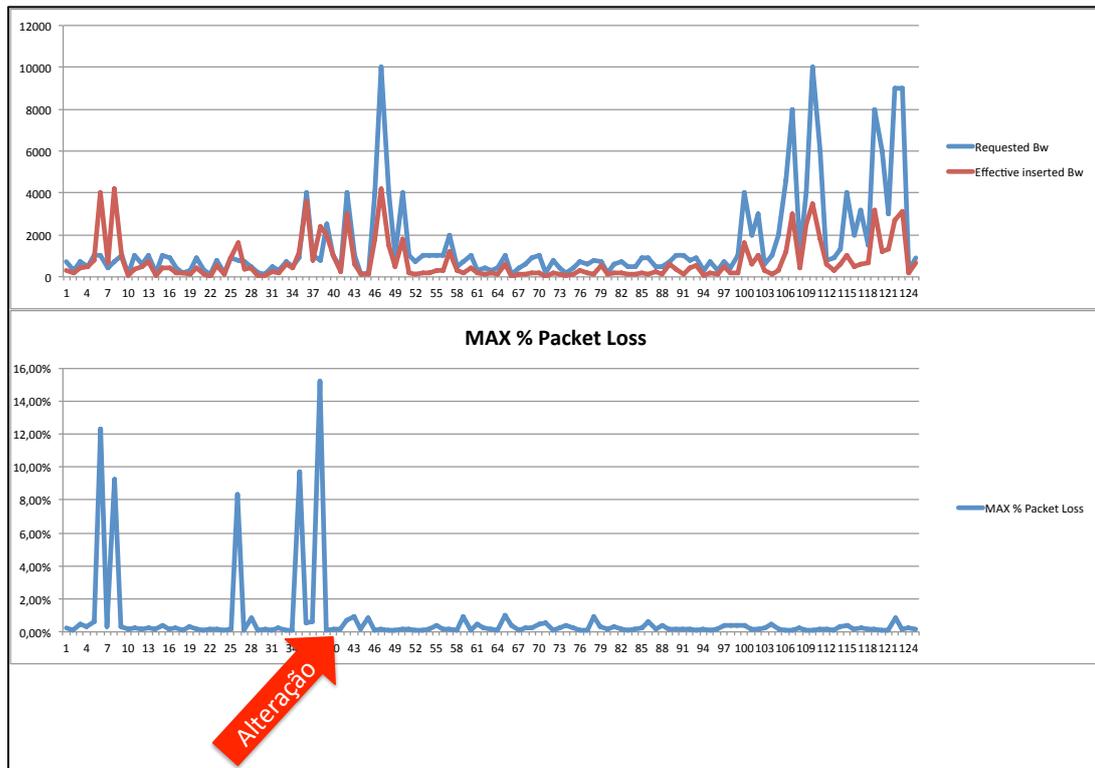


Figura 5.33 – Perda de pacotes após a alteração.

Finalmente, na Fig. 5.34, é mostrado a CDF com os dados comparativos de tempo de solução, tendo como base os processos atualmente em uso e o proposto neste trabalho.

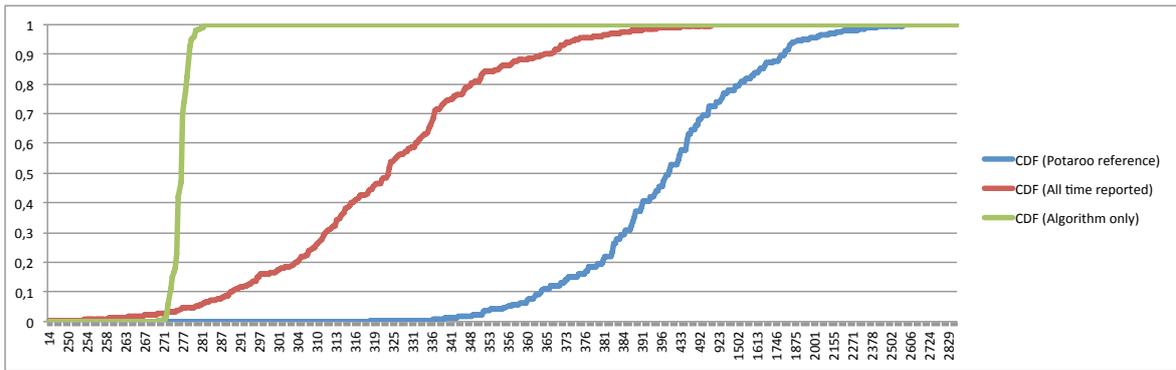


Figura 5.34 – CDF comparativa dos tempos de solução para os algoritmos analisados.

O Potaroo (Geoff, 2014) é usado e sugerido por todos os grandes fabricantes de equipamentos com função de roteamento na Internet. Ou seja, vale apenas a experiência do usuário, normalmente sem cálculo de necessidades futuras e sem garantia de efetividade de solução na primeira tentativa. Os casos *all time reported* relacionam todos os casos coletados, incluindo mais 392 casos que não usaram a metodologia aqui descrita. Os casos *Algorithm Only* são os 125 casos completos analisados neste ensaio.

Os resultados aqui apresentados indicam que a metodologia pode ser usada para a mitigação de problemas de desempenho entre sistemas autônomos com situações de assimetria de tráfego.

5.5 ENSAIO 4 – COMPARAÇÃO DOS ESTIMADORES DE BANDA RELATIVA A MEDIDAS GAUSSIANAS E STÊNICO COM APLICAÇÃO EM PROCESSOS SEMI-AUTOMATIZADOS DE TENTATIVA DE CONTROLE

O processo de comparação dessa seção é baseado em coletas realizadas em uma rede real que transporta aplicações e serviço de trânsito IP entre a América do Sul e os Estados Unidos da América. O principal objetivo foi analisar o comportamento dos estimadores de banda já testados em simulador computacional, passando para uma rede real em produção.

Na Fig. 5.35a e 5.35b, é apresentada a análise da banda solicitada *versus* a banda aplicada na rede após o processamento com o uso do estimador de Stênico. Observa-se que, dos 125 casos analisados, ocorreram poucos casos em que a banda inserida não gerou economia de recursos.

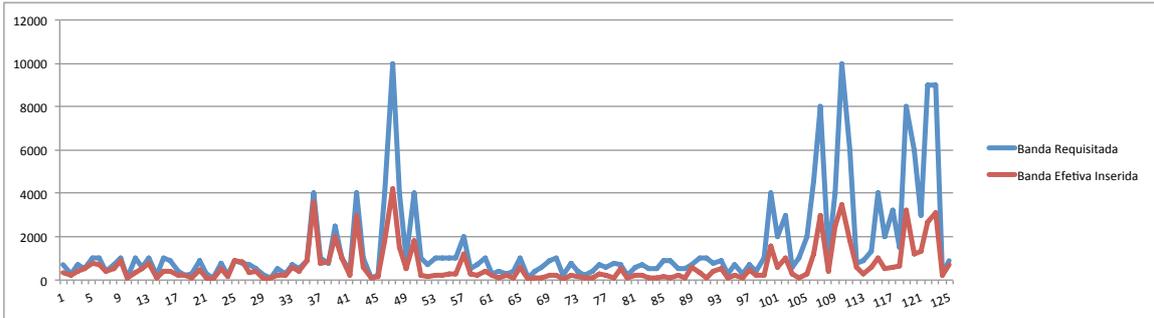


Figura 5.35a – Comparação da banda solicitada pelo cliente *versus* a banda inserida após a estimação da banda efetiva pelo método de Stênico. Medidas de uma rede real extraídas entre 12/4/2015 e 19/6/2015.

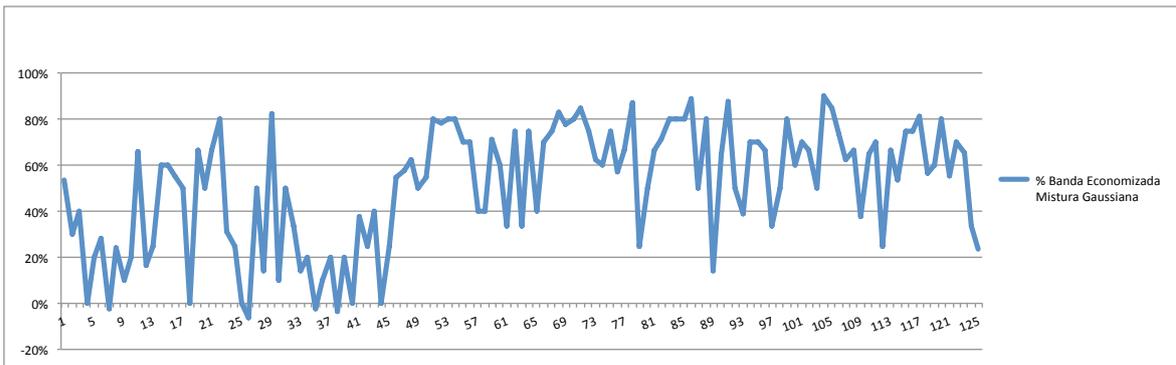


Figura 5.35b – Percentual de economia de banda após a estimação da banda efetiva pelo método da Stênico. Medidas de uma rede real extraídas entre 12/4/2015 e 19/6/2015.

Na Fig. 5.36a e 5.36b, é apresentada a análise da banda solicitada *versus* banda aplicada na rede após o processamento com o uso do estimador de Mistura Gaussiana. Observa-se que, em todos os 53 casos analisados, houve economia de recursos.



Figura 5.36a – Comparação da banda solicitada pelo cliente *versus* a banda inserida após a estimação da banda efetiva pelo método da Mistura Gaussiana. Medidas de uma rede real extraídas entre 15/6/2015 e 10/7/2015.

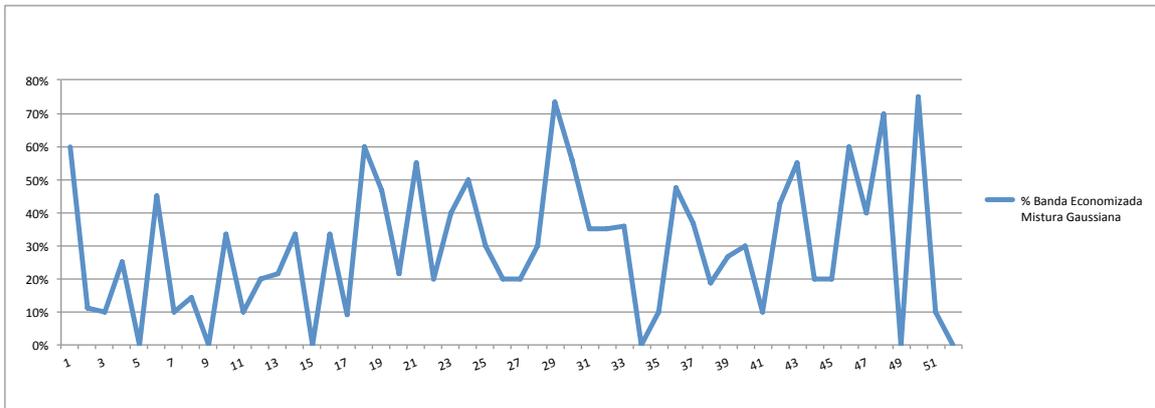


Figura 5.36b – Percentual de economia de banda após a estimação da banda efetiva pelo método da Mistura Gaussiana. Medidas de uma rede real extraídas entre 15/6/2015 a 10/7/2015.

Nas Fig. 5.37a e 5.37b, apresenta-se a análise da máxima taxa de pacotes observada em cada caso específico de resultado de banda efetiva para o método de Stênico *versus* o de Misturas Gaussianas. Nas mesmas figuras é possível também se observar os valores médio e mínimo de cada conjunto de amostras. O método das Misturas Gaussianas, em todos os casos, nunca ultrapassou 1% de perda de pacotes. Esse valor é o mesmo observado em condições normais de uso da rede. Para o caso do método de Estênico, observam-se valores de pico próximos a 2% quando os valores de banda inseridos geraram problemas relativos a perda de pacote, mas ainda dentro de uma condição aceitável em condições normais de operação uma vez que a média e valores mínimos são baixos.

O valor máximo foi usado para efeito de tomada de decisão e ainda por estar, em muitos casos, especificado como parâmetro de acordo de nível de serviço. Ainda assim, o seu comportamento é interessante à operadora, uma vez que se trata ainda de valores aceitáveis para serviço IP.

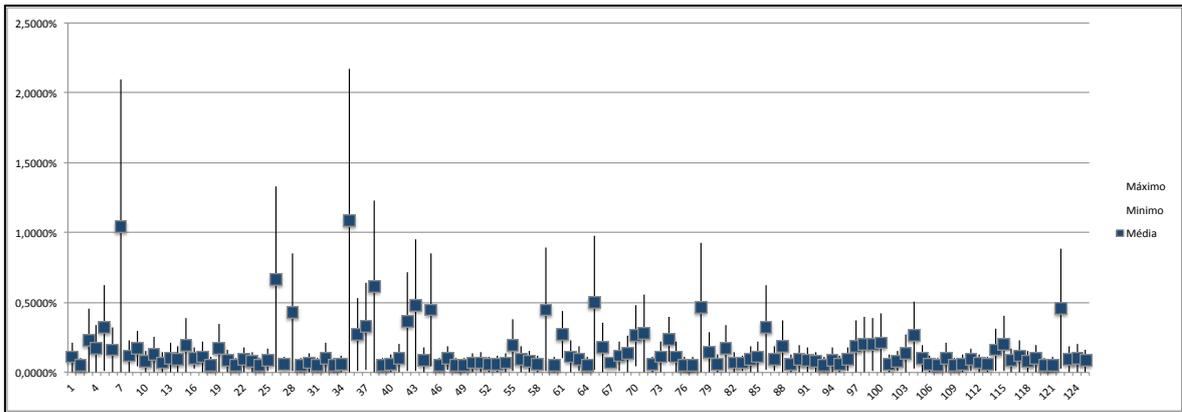


Figura 5.37a – Taxa de perda mínima, máxima e média por intervalo de coleta de pacotes após a estimação da banda efetiva pelo método de Stênico. Medidas de uma rede real extraídas entre 12/4/2015 e 19/6/2015.

Esta mesma conclusão pode ser observada na CDF apresentada para cada um dos métodos nas Figs. 5.38a e 5.38b, respectivamente, para os métodos de Stênico e de Misturas Gaussianas. Ao final, a conclusão é o que método das Misturas Gaussianas foi bem sucedida em quando obsevados os quesitos de economia de banda e perda de pacotes para o processo. Porém, não há uma degradação significativa de resultados quando comparado com o método com o suporte da banda efetiva de Stênico.

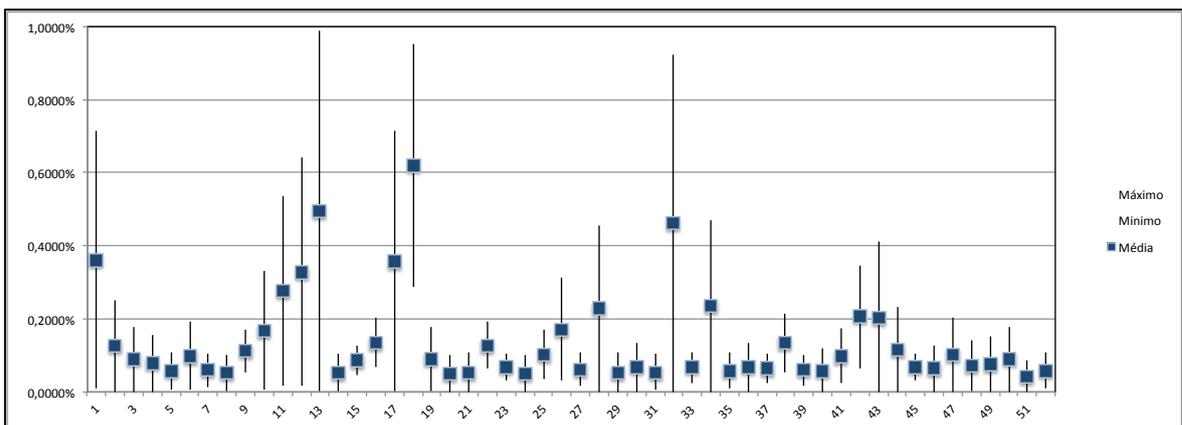


Figura 5.37b – Taxa de perda mínima, máxima e média por intervalo de coleta de pacotes após a estimação da banda efetiva pelo método da Mistura Gaussiana. Medidas de uma rede real extraídas entre 15/6/2015 e 10/7/2015

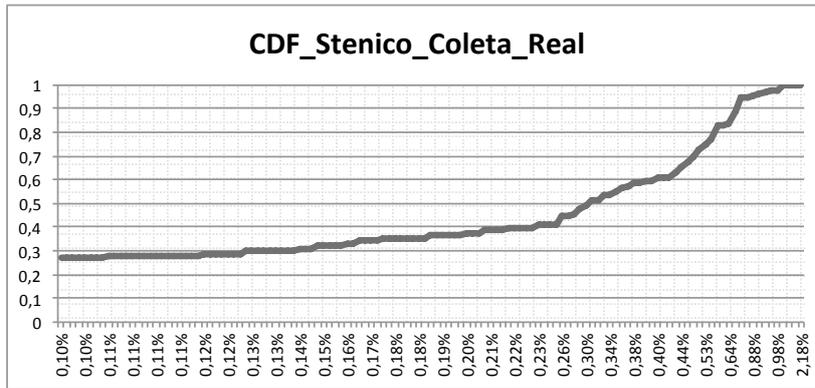


Figura 5.38 – CDF da taxa de perda máxima de pacotes após a estimação da banda efetiva pelo método de Stênico. Medidas de uma rede real extraídas entre 12/4/2105 e 19/6/2015.

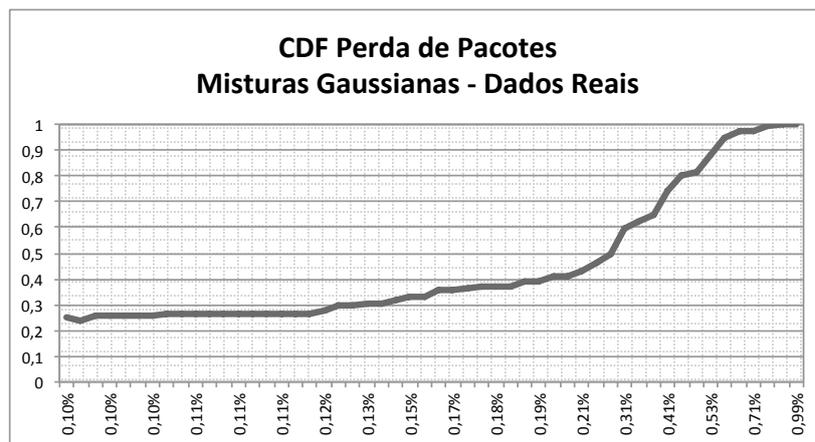


Figura 5.39 – CDF da taxa de perda máxima de pacotes após a estimação da banda efetiva pelo método da Mistura Gaussiana. Medidas de uma rede real extraídas entre 15/06 a 10/07/2015.

6 CONCLUSÃO E TRABALHOS FUTUROS

Os resultados apresentados apontam para aplicações que podem ser utilizadas em questões práticas. Nos cenários testados, o uso da interferência racional gerou benefícios em termos da estabilidade das conexões entre ASes na Internet. Ainda com base nos cenários testados os recursos puderam ser otimizados, considerando-se os limites impostos pelos acordos de nível de serviço. A redução da necessidade de novos investimentos em redes ou a sua postergação também é um efeito do processo de tomada de decisão. A economia de banda, para todos os casos, foi em média de aproximadamente 50%. Tanto o método de Stênico ou de Misturas Gaussianas funcionou, no entanto devido a facilidade de extração de parâmetros de caracterização, o segundo foi o escolhido. O método de Stênico, devido ao fato de ser baseado em processos fBm necessita de maior esforço computacional no cálculo de seus parâmetros. Neste trabalho, o método Stênico foi usado por mais de 6 meses em uma rede real e o método das Misturas Gaussianas usado por mais de 2 meses continuamente. O método de Kernel foi descartado, devido ao mesmo ter tido pior desempenho em termos de perdas de pacotes.

A análise de continuidade, relacionadas com a melhor maneira de se trocar informação entre os ASes, foi realizada com base em um ciclo de simulações para a verificação da aplicabilidade do Bônus de Tráfego (TrB). Ao final esta solução também mostrou-se compatível com as necessidades apontadas.

A estabilidade relacionada ao processo de decisão para o roteamento foi analisada. Partindo de sugestões para a análise da continuidade e ainda dos resultados já encontrados, o estudo da estabilidade foi aprofundado com a apresentação de melhorias da ordem de 21% em média. As simulações e coletas de dados reais foram usadas para o desenvolvimento dos ensaios com a conclusão de usabilidade.

O IPv6 foi analisado. Este protocolo ainda não tem o seu uso totalmente difundido, principalmente nos acessos, mas ao mesmo tempo possui poucos prefixos sendo encaminhados na Internet. Devido a esta condição, as simulações foram importantes para demonstrar que não existirão acréscimos de carga de processamento. Já o núcleo da

Internet, atualmente, trabalha com *dual stacking* ou seja, convive naturalmente com IPv6 e com IPv4, não necessitando de provas de conceito para demonstrar aplicabilidade.

A conclusão final é que o uso do conhecimento especialista em conjunto com a estratégia da interferência racional possibilita uma solução aplicável diretamente em redes reais.

Para trabalhos futuros a integração deste método em processos SDN (*Software Defined Networks*) e automatização são sugestões de continuidade. A investigação e novas propostas de interfaces que tenham controle autônomo de simetria entre a banda reservada para a transmissão versus recepção é um assunto já analisado pela arquitetura OBS (*Optical Burst Switching*). No entanto, ainda faltam análises que permitam o uso da proposta de otimização de recursos com a possibilidade de controle dinâmico da banda na interface de um determinado enlace. De forma mais direta, faltam análises de controle dinâmico que permitam a alteração da quantidade de recursos em função de uma necessidade momentânea. Para esta análise são necessárias investigações entre camadas (*cross-layers*) suportadas por modelos de cálculo de banda efetiva e tomada de decisão.

6.1 PUBLICAÇÃO EM PERIÓDICOS

Deus, M.A.; Carvalho, P.H.P.; Leite, J.P..(2015). “Internet Capacity: Optimizing the AS inbound traffic using specialist knowledge as support for decision-making”. *Annals of Telecommunications*. ISSN: 1958-9395. Volume 70, Issue 7-8, pp 331-343. Accept for publication in Nov 25th 2014. Published Aug 2015.

6.2 ARTIGOS PUBLICADOS, APRESENTADOS EM CONGRESSOS OU ACEITOS PARA PUBLICAÇÃO

Deus, M.A.; Carvalho, P.H.P; Leite, J.P. (2015). “Ensaio sobre a Neutralidade de Rede no Brasil”. XXXIII SIMPÓSIO BRASILEIRO DE TELECOMUNICAÇÕES (SBrT-2015) Juiz de Fora, MG, 1 a 4 de Setembro 2015 .

Deus, M.A.; Carvalho, P.H.P; Leite, J.P. (2014). “Internet Traffic Engineering: Understanding the specialist decision-making process for traffic management in South America”. 28th IEEE International Conference on Advanced Information Networking and Applications (AINA-2014) Victoria, Canada, May 13 - 16, 2014.

- Deus, M.A.; Carvalho, P.H.P.; Leite, J.P. (2013). “Internet Traffic Engineering: Understanding the decision-making process for traffic management in South America”. In: PTT Forum 7 - Comitê Gestor da Internet no Brasil, 2013, São Paulo. Internet Traffic Engineering: Understanding the decision-making process for traffic management in South America, 2013.
- Deus, M.A.; Carvalho, P.H.P.; Leite, J.P. (2013). “BGP Traffic Engineering: Understanding South America Traffic Patterns to Improve Decision-Making”. SBrT 2013. ISBN 978-85-89748-09-4. 9788589748094
- Deus, M.A.; Carvalho, P.H.P.; Solis, P.B. (2012). “IP and 3G Bandwidth Management Strategies applied to Capacity Planning”. In: Ortiz, Jesus H.. (Org.). Telecommunications Networks - Current Status and Future Trends. 1ed.Croatia: In Tech Open Access, 2012, v. 01, p. 1-16.
- Deus, M.A. ; Carvalho, P.H.P. ; Barreto, P.S. (2009). “Alocação de Banda Efetiva para Tráfego Multimídia em Redes IP/MPLS”. In: I2TS 2009, 2009, FLORIANOPOLIS. 8th International Information and Telecommunication Technologies Symposium, 2009, 2009.
- Deus, M.A.; Carvalho, P.H.P.; Barreto, P.S.; Fraga, T.; Paiva, V. (2008). “Identificação de Características Multifractais para Tráfego de Redes”. In: XXVI Simpósio Brasileiro de Telecomunicações (SBrT'08), 2008, Rio de Janeiro, RJ. Anais do XXVI Simpósio Brasileiro de Telecomunicações, 2008.

6.3 ARTIGOS SUBMETIDOS OU AGUARDANDO RESPOSTA

- Deus, M.A.; Carvalho, P.H.P.; Leite, J.P. (2015). “IPv4 & IPv6 BGP stability analysis on a decision-making perspective”. Submetido ao periódico IEEE Communication Letters. (ISSN 1089-7798) em 10/07/2015.
- Deus, M.A.; Carvalho, P.H.P.; Leite, J.P. (2015). “TrB Traffic Bonus Proposal for BGP Non-Centralized Decision-Making Interference”. Em revisão para submissão ao IEEE Communication Letters. (ISSN 1089-7798) até 30/10/2015.

7 REFERÊNCIAS BIBLIOGRÁFICAS

- Abry, P.; Baraniuk, R.; Flandrin, P.; Riedi, R.; Veitch D. (2002). "The Multiscale nature of network traffic discovery, analysis and modeling". *IEEE Signal Processing Magazine*, 19(3):28-46.
- Adibi, S.; Mobasher, A. e Tofigh, T.. (2014). "LTE Networking: Extending the Reach for Sensors in mHealth Applications." *Transactions on Emerging Telecommunications Technologies* 25 (7): 692–706. doi:10.1002/ett.2598.
- Aitken, Jonathan M.; Alexander, Rob; Kelly, Tim. (2010). "A Case for Dynamic Risk Assessment in NEC Systems of Systems". 2010 5th International Conference on System of Systems Engineering.
- Akyildiz, I.; Lee, A., Wang, P.; Luo, M., Chou, W. (2014). "A roadmap for traffic engineering in software defined networks". *Computer Networks Journal*, Elsevier DOI: 10.1016/j.comnet.2014.06.0021389-1286/2014. B.V.
- Albanese, I.; Yazır, Y.; Neville, S.; Ganti, S. e Darcie, T. (2015). "Big File Protocol for OTN and Ethernet Transport Systems," *J. Opt. Commun. Netw.* 7, 96-108 (2015).
- Anderson, L., Doolan, P., Feldman, N., Fredette, A., Thomas, B. (2001). "RFC 3036, LDP Specification". January 2001. (Format: TXT=274855 bytes)(Status: PROPOSED STANDARD).
- Aroussi, S. e Mellouk, A.. (2014) "Survey on Machine Learning-Based QoE-QoS Correlation Models." 2014. In , pp 200–204. IEEE. doi:10.1109/ComManTel.2014.6825604.
- AT&T (2014). www.att.com acessado em 02/01/2014.
- Bang, D.; Fusaroli, R.; Tylén, K.; Olsen, K.; Latham, P. E.; Lau, J. Y. F., Roepstorff, A.; Rees, G.; Frith C. D. and Bahrami, B. (2014). "Does Interaction Matter? Testing Whether a Confidence Heuristic Can Replace Interaction in Collective Decision-Making." *Consciousness and Cognition* 26: pp. 13--23. doi:10.1016/j.concog.2014.02.002.
- Barreto, Priscila S. B. (2007). "Otimização de Roteamento Adaptativo em Redes Convergentes com tráfego autosimilar". Tese de Doutorado, UnB.
- Beran, J. (1994). "Statistics For Long-Memory Processes". Chapman and Hall. Pg. 100-230. ISBN 9780412049019.

- Behdin, Shahrooz (2013). "Traffic Estimation, Prediction and Provisioning in IP Networks". McMaster University. Open Access Dissertations and Theses. Paper 7648.
- Bekkers, R.; Bongard, René; and Nuvolari, Alessandro. (2011). "An Empirical Study on the Determinants of Essential Patent Claims in Compatibility Standards." *Research Policy*, Issue dedicated to Chris Freeman, Founding Editor, 40 (7): 1001–15. doi:10.1016/j.respol.2011.05.004.
- Bitar, N.; Daikoku, M.; Fang, L.; Pan, P. e Zhang, R.. (2014). "MPLS Transport Profile (MPLS-TP) Applicability: Use Cases and Design." Accessed July 29th 2014. <http://tools.ietf.org/html/rfc6965>.
- Boucadair, M. and Jacquenet, C.. (2014). "Software-Defined Networking: A Perspective from within a Service Provider Environment." Accessed September 15. <http://tools.ietf.org/html/rfc7149>.
- Bowman, A. W.; Azzalini, A.. "Applied Smoothing Techniques for Data Analysis". New York: Oxford University Press, 1997.
- Braden E., Zhang, L., Berson, S., Herzog, S., Jamin, S.. (1997). "RFC 2205 Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification". R. September 1997. (Format: TXT=223974 bytes) (Updated by RFC2750, RFC3936, RFC4495) (Status: PROPOSED STANDARD)
- Braden, R., Clark, D., Shenker, S.. (1994). "RFC 1633 Integrated Services in the Internet Architecture: an Overview". June 1994. (Format: TXT=89691,PS=207016, PDF=201858 bytes) (Status: INFORMATIONAL)
- Brandes, U.. (2001). "A Faster Algorithm for Betweenness Centrality". *Journal of Sociology Mathematics*. 25(2001) 2,pp.163-177.
- Brewka, L., V.B. Iversen, and G. Kardaras.. (2014). "Integrated Service Resource Reservation Using Queueing Networks Theory." *IET Networks* 3 (1): 16–21. doi:10.1049/iet-net.2013.0121.
- Carvalho, P. H. P., Solis P. A. B, Deus, M., Queiroz, B., Carneiro, B. (2007). "A per Application Traffic Analysis in a Real IP/MPLS Service Provider Network". The 2nd IEEE IFIP/ International Workshop on Broadband Convergence Networks(IM2007/BCN2007), IEEE Communications Society , Munique, Alemanha, 21 a 25 de maio de 2007 ISBN: 1-4244-1297-8. Digital Object Identifier: 10.1109/BCN.2007.372751.

- Carvalho, P.H.P., Barreto, P. S., Queiroz, B., Carneiro, B.N. (2006). Modelagem, Geração e Análise de Tráfego em Redes Multiserviços, GTAR, LEMOM, UnB.
- Castro E Silva, J. L. (2004). “ProCon - Prognóstico de Congestionamento de Redes de Computadores usando Wavelets”. Tese de Doutorado – Universidade Federal de Pernambuco. Programa de Pós-Graduação em Ciência da Computação, Recife, PE, Brasil.
- Charilas, D. E., Panagopoulos, A. D., & Markaki, O. I. (2014). A unified network selection framework using principal component analysis and multi attribute decision making. *Wireless Personal Communications*, 74(1), 147-165.
- Chamania, M., and Jukan, A.. (2014). “A Comparative Analysis of the Effects of Dynamic Optical Circuit Provisioning on IP Routing.” *IEEE/ACM Transactions on Networking* 22 (2): 429–42. doi:10.1109/TNET.2013.2251897.
- Chang, I-Cheng; Liu, Chuang-Chun, and Chen, K.. (2014). “The Push, Pull and Mooring Effects in Virtual Migration for Social Networking Sites.” *Information Systems Journal* 24 (4): 323–46. doi:10.1111/isj.12030.
- Charnes, A.; Cooper, W. W.; and Rhodes, E. (1978). “Measuring the Efficiency of Decision Making Units.” *European Journal of Operational Research* 2 (6): pp 429–44. doi:10.1016/0377-2217(78)90138-8.
- Chen, Y.; Savage, S.J.. (2011). The effects of competition on the price forcable modem internet access. *The Review of Economics and Statistics* 93, 201–217.
- Cheng T., Ee.; Breslau, Lee M., and Ramakrishnan, K. K.. (2014). “Methods and Apparatus to Distribute Network IP Traffic.” US8687638 B2, 01-Apr-2014.
- Choi, J.P., Kim, B.C., 2010. Net neutrality and investment incentives. *RAND. Journal of Economics* 41, 446–471.
- Chwif, L., Medina, A. (2006). “Modelagem e Simulação de eventos discretos: teoria e prática”. São Paulo, Ed. dos autores, 2006, ISBN 85-905978-1-4
- CISCO. (2014). Roteadores GSR 12000 series, documentação disponível eletronicamente na página <http://www.cisco.com/en/US/products/hw/routers/ps167/>, acessada em 10/01/2014.
- Claise, B. (2004). RFC 3954. “Cisco Systems NetFlow Services Export Version 9”. disponível <http://www.ietf.org/rfc/rfc3954.txt> . Ed. Cisco
- Clegg, R.(2006). “A Practical Guide to Measuring the Hurst Parameter”. *International Journal of Simulation: Systems, Science & Technology* 7(2) pp 3-14.

- Condord, CA Computer, E-Helth, <http://www.ca.com>, acessado em 20/01/2007.
- Courcoubetis, C.; Sdrolas, K. and Weber, R. 2014. "Revenue Models, Price Differentiation and Network Neutrality Implications in the Internet". *SIGMETRICS Perform. Eval. Rev.* 41, no 4 (abril de 2014): pp 20–23. doi:10.1145/2627534.2627540.
- Cucchiara, J., Sjostrand, H., Luciani, J. (2004) RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP). June 2004. (Format: TXT=215916 bytes) (Status: PROPOSED STANDARD)
- Das, T.; Drogon, M.; Jukan, A. e Hoffmann, M.. (2013). "An Agent-Based Modeling Approach of Network Migration to New Technologies." In *2013 IEEE International Conference on Communications (ICC)*, 2583–88. doi:10.1109/ICC.2013.6654924.
- De Cola, T.; Marchese, M.; Cello, M. and Mongelli, M.. (2014). "QoS and QoE Evaluation of Web-Browsing over an SI-SAP-Enabled DVB-S2/RCS System." In *2014 European Conference on Networks and Communications (EuCNC)*, 1–5. doi:10.1109/EuCNC.2014.6882680.
- Davie, B. S., Rekther, Y. (2000) "MPLS: Technology and applications". Morgan Kofmann Ed. 19, may 2000, ISBN: 1-558-60656-4. Digital Object Identifier 10.1109/PACRIM.1997.620401.
- Droms, R. E., Sudan, M.; Desai, S. H.; Chapman, J. T.; and Krishnan, R. S.. (2014). "Use of IPv6 in Access Networks." <http://www.google.com/patents/US8635314>.
- Economides, N. e Tåg, J.. "Network Neutrality on the Internet: A Two-Sided Market Analysis." *Information Economics and Policy* 24, no. 2 (June 2012): 91–104. doi:10.1016/j.infoecopol.2012.01.001.
- Eittenberger, P.M.; Schneider, K.M.; Krieger, U.R., (2013). "Performance Evaluation of Next Generation Content Delivery Proposals," Next Generation Mobile Apps, Services and Technologies (NGMAST), 2013 Seventh International Conference on , vol., no., pp.136,141, 25-27 Sept. 2013 doi: 10.1109/NGMAST.2013.32
- Emrouznejad, A.; Latef Anouze, A. e Thanassoulis E.. (2010). "A Semi-Oriented Radial Measure for Measuring the Efficiency of Decision Making Units with Negative Data, Using DEA." *European Journal of Operational Research* 200 (1): 297–304. doi:10.1016/j.ejor.2009.01.001.

- Epstein, M. J. ; Buhovac, A. R. (2014). “Making Sustainability Work: Best Practices in Managing and Measuring Corporate Social, Environmental, and Economic Impacts.” pp. 121—162. Berrett-Koehler Publishers. ISBN 9781609949945.
- Erramilli, A., Narayan, O., Neidhart, A., Saniee, I. (2001). “Multi-scaling models of TCP/IP and sub-frame VBR video traffic”. *Journal of Communications and Networks*, 3(4):383-395.
- Erramilli, A., Narayan, O., Neidhart, A., Saniee, (2000). “Performance impacts of multi-scaling in area TCP/IP traffic”. In *IEEE INFOCOM*, pages 352-359.
- ETHERREAL, acessado em <http://www.ethereal.com/download.html> em 15/06/2006.
- EVA (2007), Economic Value Added, <http://www.sternstewart.com/evaabout/whatis>. acessado em 25 de maio 2007.
- Evans, J., Filsfils, C. (2007). “Deploying IP and MPLS QoS for multiservice networks”. Morgan Kaufmann, ISBN-13: 978-0-12-370549-5.
- Fallon, L; and O’Sullivan, D.. 2014. “Semantic-Based Service Analysis and Optimization.” In , 1–7. IEEE. doi:10.1109/NOMS.2014.6838283.
- Faucheur , F. L., Lai, W. (2005). “RFC 3564, Requirements for support of Differentiated Services-aware MPLS Traffic Engineering”. (Format TXT=50808 bytes) (Status: INFORMATIONAL)
- Ferreira, P. J. S. (2005) “Modelação de tráfego em redes de telecomunicações: modelos Markovianos e baseados em sistemas de Lindenmayer”. Tese de Doutorado. Universidade de Aveiro, Departamento de Electrónica e Telecomunicações, 2005.
- Fiegenbaum, Joan.(2007). “Distributed Algorithm Design”. *Algorithmic Game Theory*. ISBN 978-0-521-87282-9. Cambridge University Press.
- Fisher,S. (2014). “Challenges of the Internet of Services”. Chapter of book: *Towards the Internet of Services: The THESEUS Research Program Cognitive Technologies*. 2014, pp 15-27. Cognitive Technologies. Cham: Springer International Publishing. <http://link.springer.com/10.1007/978-3-319-06755-1>.
- Fonseca N. L. S., Drummond, A. C., Devetsikiotis, M. (2005). “Uma Avaliação de Estimadores de Banda Passante Baseados em Medições”. Instituto de Computação– Universidade Estadual de Campinas. Department of Electrical and Computer Engineering – North Carolina State University Raleigh, USA
- García-Dorado, J. L., Hernández, J. A.; Aracil, J.; de Vergara, J. E. L. e Lopez-Buedo, S.. (2011). “Characterization of the Busy-Hour Traffic of IP Networks Based on

- Their Intrinsic Features.” *Computer Networks* 55 (9): 2111–25. doi:10.1016/j.comnet.2011.02.015.
- Ghattas, J., Soffer, P. and Peleg, M. (2013). “Improving Business Process Decision Making Based on Past Experience.” *Decision Support Systems* 59 (March): 93–107. doi:10.1016/j.dss.2013.10.009.
- Ghezzi, A.; Dramitinos, M.; Agiatzidou, E.; Johanes, F. T.; Losethagen, H.; Rangone, A. e Balocco, R. (2014). “Internet Interconnection Techno-Economics: A Proposal for Assured Quality Services and Business Models.” In , 708–17. IEEE. doi:10.1109/HICSS.2014.95.
- Giang Ngo, Hoang; Liquori, Luigi; Ciancaglini, Vincenzo; Maksimovic, Petar And Nguyen Chan, Hung. (2013). “A Backward-Compatible Protocol for Inter-Routing over Heterogeneous Overlay Networks.” In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, 649–51. SAC ’13. New York, NY, USA: ACM. doi:10.1145/2480362.2480485.
- Go, Y.; Won, J.; Kune, D. F.; Jeong, E.; Kim, Y. and Park, K.. (2014). “Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission.” In . Internet Society. doi:10.14722/ndss.2014.23118
- Gómez, G.; Pérez, Q.; Lorca, J. e García, R.. 2014. “Quality of Service Drivers in LTE and LTE-A Networks.” *Wireless Personal Communications* 75 (2): 1079–97. doi:10.1007/s11277-013-1409-0.
- Gonçalves, B. H. P.; Vieira, F. H. T. . “Estimação de Banda Efetiva para Tráfego de Redes Utilizando Função de Escala e Fator de Momento”. In: *CNMAC - 34o Congresso Nacional de Matemática Aplicada e Computacional*, Águas de Lindóia-SP, 2012.
- Gonçalves, B. H. P.; Vieira, F. H. T.; Costa, V. H. T. . “Alocação Dinâmica de Slots de Tempo Multiusuário para Redes OFDM/TDMA baseada em Banda Efetiva”. In: *XXXI Simpósio Brasileiro de Telecomunicações*, Fortaleza-CE, 2013.
- Guivarc’h, Y. (1987), “Remarques sur les Solutions d’ une Equation Fonctionnelle Non Linéaire de Benoît Mandelbrot”. *Comptes Rendus (Paris)* 305I,139, 1987.
- Gubner, J. A. (2005). “Theorems and Fallacies in the Theory of Long-Range-Dependent Processes”, *IEEE Trans. Inf. Theory*, vol 51, no 3, pp. 1234-1239.
- Gunter, B., Greiner S., De Meer G., Trivedi K. S. (1998). “Queueing networks and Markov Chains”. John Wiley & Sons, Inc.

- Griffin, Timothy G.; Perouli, Debbie (2012). “Reducing the Complexity of BGP Stability Analysis with Hybrid Combinatorial-Algebraic Models”. The 2nd International Workshop on Rigorous Protocol Engineering (WRiPE), October 2012.
- Halbach,T.; Wien, M.. (2007) “CONCEPTS AND PERFORMANCE OF NEXT-GENERATION VIDEO COMPRESSION STANDARDIZATION”. acessado em http://www.ncesd.org/vc/docs/H264_explained.pdf dia 15/08/2007.
- Hall, C.; Yu, D.; Zhang,Z.L.; Stout, J.; Odlyzko, A.; Moore, A. W.; Camp, J.; Benton, K. and Anderson, R. (2014). “Collaborating with the enemy on network management” in: Security Protocols Workshop 2014, Lecture Notes in Computer Science, Springer, 2014. ISBN 978-3-319-12399-8.
- Hall, Mark; Frank, Eibe; Holmes, Geoffrey; Bernhard, Pfafringer; Reutmann, Peter; Witten, Ian. (2009); “The WEKA Data Mining Software: An Update; SIGKDD Explorations”. Volume 11, Issue 1.
- Haucap, J. e Heimeshoff, U.. (2014). “Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?” *International Economics and Economic Policy* 11 (1-2): 49–61. doi:10.1007/s10368-013-0247-6.
- Hawkinson, J.,Bates, T. (1996). “RFC 1930 Guidelines for creation, selection, and registration of an Autonomous System (AS)”. (Format: TXT=22073 bytes) (Also BCP0006) (Status: BEST CURRENT PRACTICE).
- He, Y.; Faloutsos, M. S.; Krishnamurthy; Huffaker, B.. (2005). On Routing Asymmetry in the Internet. Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE.
- Hurst, H.E. (1951). “Long-term storage capacity of reservoirs”. *Trans. Am. Soc. Civ. Eng.* Vol. 116 (1951), pp. 770-808 Key: citeulike:7655765
- ILBC codec. http://www.globalipsound.com/pdf/gips_iLBC.pdf, acessado em 11 de junho de 2007.
- iSAC codec. http://www.globalipsound.com/pdf/gips_iSAC.pdf, acessado em 11 de junho de 2007.
- ITU-T, P.800, (International Telecommunication Union – T)
- Jeffconnor-Linton. (2006). Chi Square Tutorial accessed 10/18/2006 and available at: http://www.georgetown.edu/faculty/ballc/webtools/web_chi_tut.html
- Kelly, F.P., Zachary, S., Ziedins, I., editors (1996). “Notes on Effective Bandwidth”. pages 141–168. Oxford University Press.

- Kettani, H., Gubner, J.A. A. (2002). "Novel Approach the Estimation of the Hurst Parameter in Self-similar Traffic". Proceedings of IEEE Conference on Local Computer Networks, Tampa, Flórida, November 2002.
- Khitmoh, N.; Wuttidittachotti, P. e Daengsi, T.. (2014). "A Subjective VoIP Quality Estimation Model for G.729 Based on Native Thai Users." In ,pp 48--53. Global IT Research Institute (GIRI). doi:10.1109/ICACT.2014.6778920.
- Klein, G.. (2008). Naturalistic Decision Making. HUMAN FACTORS, Vol.50, No. 3, June 2008, pp. 456–460. DOI 10.1518/001872008X288385. Copyright © 2008, Human Factors and Ergonomics Society.
- Kleinrock, L. (1962). "Message Delay in Communication Nets with Storage" (PhD thesis) (Cambridge, MA: Massachusetts Institute of Technology). Dec. 1962
- Kleinrock, L. (1964). "Communication Nets: Stochastic Message Flow and Design". McGraw-Hill. p. 220. 1964. ISBN 978-0486611051.
- Kleinrock, L. (1975). "Queueing Systems: Volume I – Theory". New York: Wiley Interscience. p. 417. January, 1975. ISBN 978-0471491101.
- Kotler, P. (1998). "Administração de Marketing: análise, planejamento, implementação e controle". 5.ed. São Paulo: Atlas.
- Lodhi, A., Dhamdhere, A., & Dovrolis, C. (2014). Open peering by Internet transit providers: Peer preference or peer pressure?. In *Proceedings of IEEE INFOCOM*.
- Leland W. (1994). "On the self-similar nature of ethernet traffic (extended version)". IEEE/ACM Trans. on Networking, vol. 2, no. 1, pp. 1--15.
- Masuyama, H., Takine, T., Okazaki, K., (2004). "IP Traffic Modeling: Most Relevant Time-Scale and Local Poisson Property". Proceedings of the 12th International Conference on Informatics Research for Development of Knowledge Society Infrastructure (ICKS'04), 2004.
- Melo, C. A.V. (2004). "Modelagem e Computação de Banda Passante Equivalente de Fluxos Multifractais". Tese de Doutorado. Unicamp.
- Meyer, D..(2014) Routeviews. <http://www.routeviews.org>.
- Mishra, Ajay R. (2004). "Fundamentals of Cellular Network Planning and Optimisation: 2G/2.5G/3G". Evolution to 4G, by, 2004, ISBN 047086267X
- Misyak, J. B. e Chater, N.. (2014). "Virtual Bargaining: A Theory of Social Decision-Making." *Philosophical Transactions of the Royal Society B: Biological Sciences* 369 (1655): 20130487. doi:10.1098/rstb.2013.0487.

- Nadeau, T., Srinivasan, C., Viswanathan, A. (2004). “RFC 3814 Multiprotocol Label Switching (MPLS) Forwarding Equivalence Class To Next Hop Label Forwarding Entry (FEC-To-NHLFE) Management Information Base (MIB)”. (Format: TXT=87518 bytes) (Status: PROPOSED STANDARD), June 2004.
- Nash, J. (1951). Non-cooperative games. *Annals of Mathematics*, 54, 286-295.
- Netflow Cisco Systems, <http://www.cisco.com> acessado em 10/02/2007.
- NIC.BR (2014). <http://simet.nic.br/>. Acessado em 20/01/2014.
- Nichols, K.,Blake, S.,Baker, F.,Black,D. (1998). “RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers”. December 1998. (Format: TXT=50576 bytes) (Obsoletes RFC1455, RFC1349) (Updated by RFC3168, RFC3260) (Status: PROPOSED STANDARD).
- Ning, Hu; Wang, BaoSheng; and Liu, Xin. 2014. “Cooperative Monitoring BGP among Autonomous Systems: Increasing the Security of BGP by Cooperative Monitoring.” *Security and Communication Networks*, May, n/a–n/a. doi:10.1002/sec.1024.
- Norros, Ilkka. (1995). “On the use of factional Brownian motion in the theory of connectionless networks”. *IEEE Journal of Selected Areas in Communications*, 13(6):953-962.
- Oetiker, T.. (1998). “MRTG: The Multi Router Traffic Grapher”. Large Installation System Administrator’s Conference, USENIX Association, ed. 1998. Proceedings of the Twelfth Systems Administration Conference, LISA XII: December 6-11, 1998, Boston, MA, USA. Berkeley, CA: USENIX Association.
- OI (2014). www.oi.com.br acessado em 02/01/2014.
- OPNET (2014). Modeler, SP Guru, IT Guru Academic Edition. Documentação disponível eletronicamente em www.opnet.com.
- Osborne, E., Simha, A. (2003). *Traffic Engineering with MPLS*. Cisco Press, 2003.
- Oti, S. B.; e Hayfron-Acquah, J. B.. (2014). “Practical Security Approaches against Border Gateway Protocol (BGP) Session Hijacking Attacks between Autonomous Systems.” *Journal of Computer and Communications* 02 (08): 10–21. doi:10.4236/jcc.2014.28002.
- Papadimitriou, D., Cabellos-Aparicio, A., e Coras, F.. (2013). “Stability Metrics and Criteria for Path-Vector Routing.” In 2013 International Conference on

- Computing, Networking and Communications (ICNC), 1036–42. doi:10.1109/ICCNC.2013.6504234.
- Papadimitriou, D., e Fortz, B.. (2014). “Time-Dependent Combined Network Design and Routing Optimization.” In *2014 IEEE International Conference on Communications (ICC)*, 1124–30. doi:10.1109/ICC.2014.6883472.
- Perlingeiro, F. R., E Ling, L. L.. (2005). “Estudo de Estimação de Banda Efetiva para Tráfego auto-similar com variância infinita.” SBrT’05, 04-08 de setembro de 2005, Campinas, SP
- PMBOK 5. PMI (2012), A Guide to the Project Management Body of Knowledge, 5th Ed. PMI Institute. ISBN PMI Product - 00101388701/ISBN13 – 9781935589679.
- Postel, J. (1981). IETF RFC 0791. “RFC IP Protocol”. Disponível na página do IETF localizada eletronicamente em <http://www.ietf.org/rfc/rfc0791.txt?number=791>, September 1981, acessada em 01/09/2006.
- Geoff, H.. (2014). *www.potaroo.net* mantido por Geoff Huston. Accessed on Feb, 2012. Mar, 2013. Apr, 2014.
- Petkov, V., Rajagopal, R., And Obraczka, K. (2013). “Characterizing per-application network traffic using entropy.” *ACM Trans. Model. Comput. Simul.* 23, 2, Article 14 (May 2013), 25 pages. DOI: <http://dx.doi.org/10.1145/2457459.2457463>
- Presuhn, R. (2002). “Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)”. Disponível em <http://tools.ietf.org/html/rfc3418>.
- Ratnam, G.; Rangarajan, K.; Agarwal, S.; Bismpiagiannis, A.; Srinivasan, N.; Raman, R.; Agrawal, L.; Bennet, A.; and Yeleshwarapu, C.. (2014). “Method and System for Providing Decision Making Based on Sense and Respond.” <http://www.google.com/patents/US8719207>.
- Ravindranath, L.; Agarwal, S.; Padhye, J.; and Riederer, C.. (2014). “Procrastinator: Pacing Mobile Apps’ Usage of the Network.” In , 232–44. ACM Press. doi:10.1145/2594368.2594387.
- Rekther, Y.; Li, T. e Hares, S..(2006). RFC 4271 - A Border Gateway Protocol 4 (BGP-4). Internet Engineering Task Force. Obsoletes RFC 1771. dx.doi.org/10.17487/RFC4271
- Resch, B.. (2010). “Mixtures of Gaussians, A Tutorial for the Course Computational Intelligence”. Signal Processing and Speech Communication Laboratory.

- <http://www.igi.tugraz.at/lehre/CI/tutorials/MixtGaussian/MixtGaussian.html>, Inffeldgasse 16c, last updated: 24. Jun 2010.
- Riedi, R. H., Crouse, M. S., Ribeiro, V. J., Baraiuk, R. G. (1999). “A multifractal wavelet model with application to network traffic.” *IEEE Transactions on Information Theory*, 45(4):992-1018,1999.
- Secci, S., J. Rougier, A Pattavina, F. Patrone, And G. Maier. (2011). “Peering Equilibrium Multipath Routing: A Game Theory Framework for Internet Peering Settlements.” *IEEE/ACM Transactions on Networking* 19, no. 2 (April 2011): 419–32. doi:10.1109/TNET.2010.2062535.
- Seuret S., VeheL, L. J. (1995). “The local Hölder function of a continuous function.” *Projet Fractales*, INRIA Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex, France E-mail address: {Stephane.Seuret, Jacques.LevyVeheL}@inria.fr.
- Seuret, S., Gilbert, A. (2000). “Pointwise Hölder exponent estimation in data network traffic.” AT&T Labs-Research, ERNST, In ITC Specialist Seminar, Monterey, CA.
- Shenker (1995). “Fundamental design issues for the future Internet. *IEEE Journal on Selected Areas in Communications*.” (Volume:13 , Issue: 7). DOI 10.1109/49.414637.
- Shoham, Yoav; Leyton-Brown, Kevin. (2009). *Multiagents Systems*. Cambridge Press. ISBN 978-0-521-89943-7
- Silva, P. R. T.(2005) Silva. *Estudo do Tráfego Auto-similar em Redes Multiserviço*, Departamento de Engenharia Elétrica, UnB.
- Skype FAQ. http://www.skype.com/help_faq.html, acessado em 11 de junho de 2007.
- Soochang, Park; Crespi, N.; Park, Hosung and Kim, Sang-ha. (2014). “IoT Routing Architecture with Autonomous Systems of Things.” In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 442–45. doi:10.1109/WF-IoT.2014.6803207.
- Song, S.,Kee-Yin, J.,Tang B. (2004). “Some Results on the Self-Similarity Property in Communication Networks”, *IEEE Trans. Communications*, vol 52, no 10, pp. 1636-1642.
- Submarine Cable Industry Report (2013). “Submarine Telecoms Forum, Inc.” Downloaded on 02/01/2013. www.subtelforum.com

- Stênico, J. W. De G.; Ling, L. (2013) Estimativa de Banda Efetiva para Tráfego de Rede Multifractal. SBrT 2013. Fortaleza CE. ISBN 978-85-89748-09-4.
- Stevens, W. R. (1994). TCP/IP Illustrated, Volume 1. Addison Wesley Professional Computing Series, 1994, October, 2000. ISBN: 0-201-63346-9
- Swift, D. K., and Dagli, C. H.. (2013). “Methods and System for Modeling Network Traffic.” <http://www.google.com/patents/US8352392>.
- T-Mobile (2014). www.t-mobile.com acessado em 03/01/2014.
- Takine, T., Okazaki, K., Masuyama, H. (2004). IP Traffic Modeling: Most Relevant Time-Scale and Local Poisson Property. Department of Applied Mathematics and Physics Kyoto University. (ICKS'04) Informatics Research for Development of Knowledge Society Infrastructure
- Tanenbaum, A.S. (2010). Computer Networks 5th Edition. Prentice Hall; 5th edition (October 7, 2010). ISBN-10: 0132126958.
- Taqq, M. S.; Willinger, W.; Sherman, B. (1997). Proof of a fundamental result in selfsimilar traffic modeling, Computer Communication Review, vol. 27, p. 5-23.
- Teixeira, R.; Griffin, T. G.; Resende, M. G.; Rexford J. (2007). “Tie Breaking: Tunable Interdomain Egress Selection”. Transactions on Networking/ACM. IETF, January 2007. ISSN :1063-6692. INSPEC Accession Number: 9607174. DOI:10.1109/TNET.2007.893877.
- Varadhan, S. R. (2007). página pessoal disponível na New York University website, Mathematics Dept., <http://math.nyu.edu/faculty/varadhan/processes.html> acessada em 07 de junho de 2007.
- Vargas, A. (2014). Omnet framework. Available at <http://www.omnetpp.org>
- Véhel, J. L. (2006). FRACLAB tool. Inria. Disponível em <http://www.irccyn.ec-nantes.fr/hebergement/FracLab/about.html> , acessado em 18/06/2006.
- Véhel, J. L. e Tricot, C.. (2004). On various multifractal spectra, in: Fractal Geometry and Stochastics III, Progress in Probability, Birkhäuser, ISBN 376437070X, 9783764370701, 2004, vol. 57, p. 23-42, C. Bandt, U. Mosco and M. Zähle (Eds), Birkhäuser Verlag. (FracLab Tool).
- Veitch, D. (2011) <http://www.cubinlab.ee.mu.oz.au/~darryl/> , acessado em 08 de juho de 2011.
- Vieira, F. H. T. (2006). “Contribuições ao calculo de banda e de probabilidade de perda para trafego multifractal de redes”. Tese de doutorado, Unicamp.

- Vieira, F.H.T. (2006). Queuing performance estimation for general multifractal traffic. *Int. J. Commun. Syst.*, 2006., 16(2), 117–136
- Verdi, F.L. ; Duarte, R. ; De Lacerda, F.C. ; Cardozo, E. (2006). “Provisioning and Management of Interdomain Connections in Optical Networks: A Service Oriented Architecture-based Approach.” *NOMS IEEE 2006*. ISBN: 1-4244-0142-9. DOI 10.1109/NOMS.2006.1687624.
- Viswanathan, A., Srinivasan, C., Nadeau, T. (2004). “RFC 3812, Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)”. C. June 2004. (Format: TXT=136475 bytes) (Status: PROPOSED STANDARD)
- Viswanathan, A., Srinivasan, C., Nadeau, T. (2004). “RFC 3813, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)”. June 2004. (Format: TXT=116120 bytes) (Status: PROPOSED)
- Wang, Zhenxing, Yu Wang, Yi Guo, Liancheng Zhang, and Jizhong Li. (2013). “Situation Assessment Model for Inter-Domain Routing System.” *IET Software*, September. doi:10.1049/iet-sen.2012.0197.
- Wang, Jessie, Dah Chiu, John Lui, And Rocky Chang. (2007). “Inter-AS Inbound Traffic Engineering via ASPP.” *IEEE Transactions on Network and Service Management* 4 (1): 62–70. doi:10.1109/TNSM.2007.030106.
- Wassim, Itani; Ghali, Cesar; Bassil, Ramzi; Kayssi, Ayman and Chehab, Ali. (2014). “ServBGP: BGP-Inspired Autonomic Service Routing for Multi-Provider Collaborative Architectures in the Cloud.” *Future Generation Computer Systems* 32 (March): 99–117. doi:10.1016/j.future.2012.05.013.
- WebRTC, 2015. www.webrtc.org. Acessado em 02/03/2015.
- Winter, Rolf. (2012). “Explicitly Accommodating Origin Preference for Inter Domain Traffic Engineering”. *ACM Symposium on Applied Computing*, 2012
- Woodward, S.L.; Zhang, W.; Bathula, B.G.; Choudhury; Sinha, G. R.K.; Feuer, M.D.; Strand; J. and Chiu, AL.. (2013). “Asymmetric Optical Connections for Improved Network Efficiency.” *IEEE/OSA Journal of Optical Communications and Networking* 5 (11): 1195–1201. doi:10.1364/JOCN.5.001195.
- Wolfgang, John. Dusi, Maurizio And Claffy, K. C. (2010). “Estimating Routing Symmetry on Single Links by Passive Flow Measurements.” In , 473. ACM Press. doi:10.1145/1815396.1815506.

- Wolsink, Maarten. (2007). Planning of renewables schemes: Deliberative and fair decision-making on landscape issues instead of reproachful accusations of non-cooperation. <http://dx.doi.org/10.1016/j.enpol.2006.12.002>.
- Xu, L.; He,W. and Li, S. (2014). “Internet of Things in Industries: A Survey.” IEEE Transactions on Industrial Informatics, 1–1. doi:10.1109/TII.2014.2300753.
- Zhang, H.F.; Shu, Y.T.;Yang, O. (1997). Estimation of Hurst parameter by variance-time plots. Communications, Computers and Signal Processing, 1997. apos;10 Years PACRIM 1987-1997 - Networking the Pacific Rimapos;. 1997 IEEE Pacific Rim Conference on Volume 2, Issue , 20-22 Aug 1997 Page(s):883 - 886 vol.2.
- Zhang, Ying. (2013). “Method and System for Effective BGP AS-Path Pre-pending”. US20130132542 A1 US Patent.

8 ANEXO I

8.1 FERRAMENTA: OMNET⁺⁺

Trata-se de ferramenta desenvolvida por (Vargas, 2014), o OMNeT⁺⁺ é um ambiente de simulação discreta. Sua aplicação primária é para comunicação de redes, teoria das filas e simulação mais específica de eventos discretos. O ambiente é totalmente aberto e pode ser totalmente modificado, pois os arquivos com o código fonte são incorporados e regidos por licença GNU.

O *framework* do OMNeT⁺⁺ provê uma arquitetura onde cada objeto pode ser estruturado para prover uma função ou conjunto dessas para a geração de um modelo. Um modelo pode ser um elemento de rede (roteador, comutador, enlace). Cada módulo é programado usando C⁺⁺ e por este motivo a ferramenta funciona sobre a plataforma Eclipse. Foi criada uma linguagem de alto nível chamada de NED para a montagem dos componentes no ambiente de trabalho para se formar uma rede.

Componentes principais:

1. *Simulation kernel library*
2. *NED topology description language*
3. *OMNeT⁺⁺ IDE based on the Eclipse platform*
4. *GUI for simulation execution, links into simulation executable (Tkenv)*
5. *Command-line user interface for simulation execution (Cmdenv)*
6. *Utilities (makefile creation tool, etc.)*
7. *Documentation, sample simulations, etc.*
8. *Platforms*

A versão utilizada nesse trabalho é a OMNET⁺⁺ 4.4.1 e o pacote INET 2.2.0 que encontravam-se estáveis em fevereiro de 2014. Na Fig. 10.1 é possível ter uma visão da interface gráfica do OMNET.

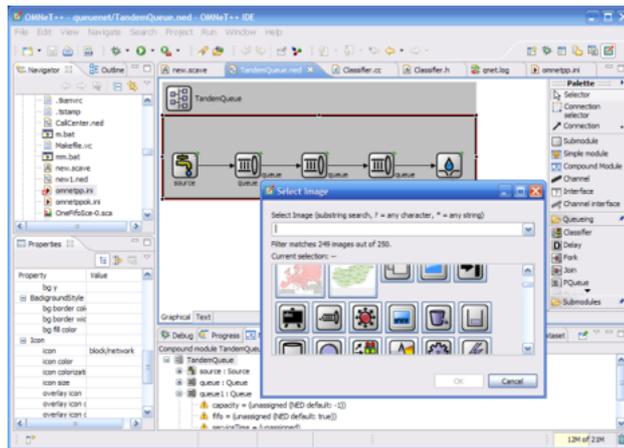


Figura 10.1 – Interface gráfica Eclipse (OMNET)

Nas simulações executadas com o OMNET foram utilizadas topologias iguais àquelas encontradas no ambiente real. Na Fig. 10.2 é mostrada a topologia criada para os testes relativos ao ciclo completo com o uso dos modelos de Kernel, Stênico e Misturas Gaussianas. Estes testes serviram de base para que o processo pudesse ser testado em ambiente real.

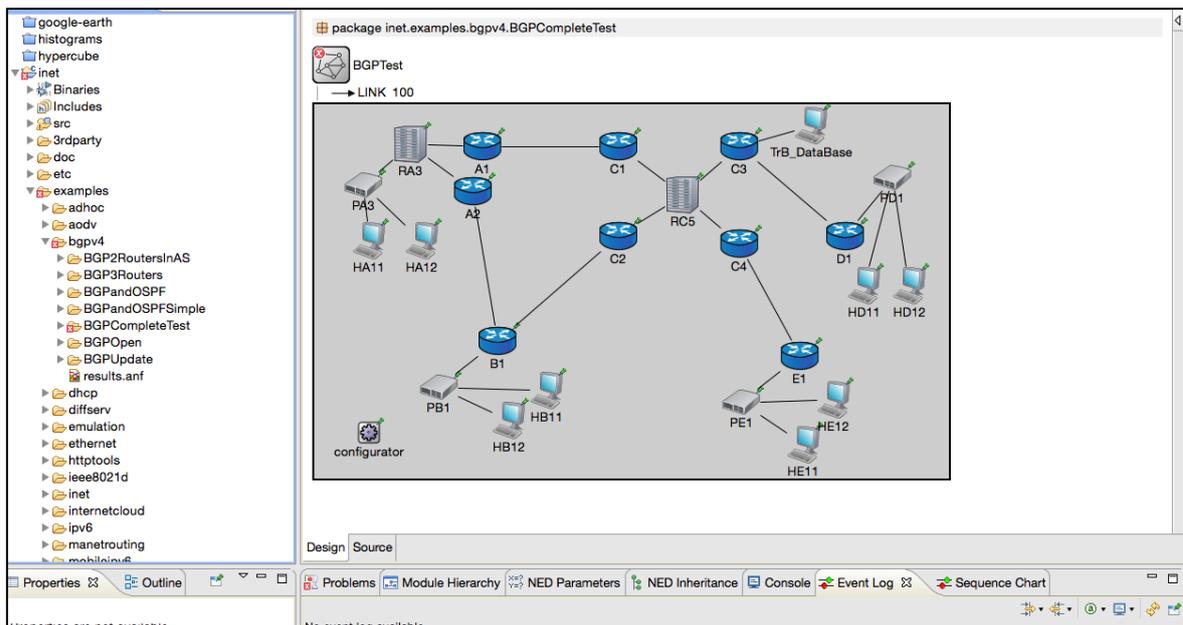


Figura 10.2 – *Network Under the Test* usando o OMNET.

Com o uso desta mesma topologia o TrB foi também testado, indicando que não oferece complexidade computacional ao processo.

Na Fig. 10.3 é detalhado um diagrama em blocos de um roteador que dispõe de protocolo BGP e OSPF extraído diretamente do ambiente do OMNET⁺⁺.

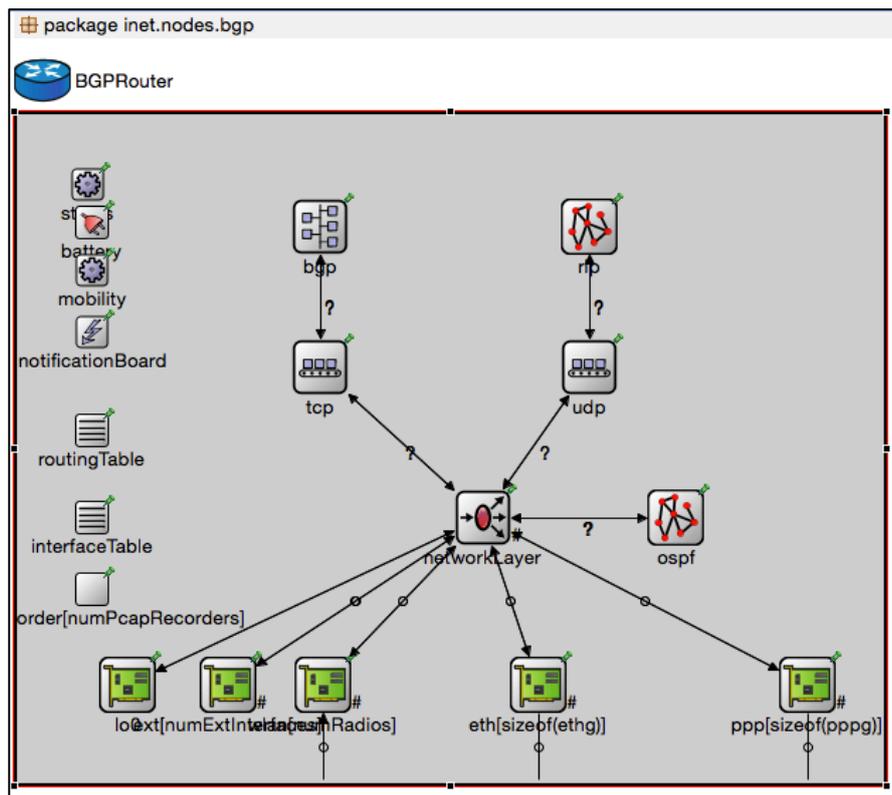


Figura 10.3 – Diagrama de blocos de um roteador com BGP OMNET.

Na Fig. 10.4 é detalhado um diagrama de estados de teste realizado para se determinar a complexidade computacional da inserção do TrB na rede com o uso do OMNET⁺⁺.

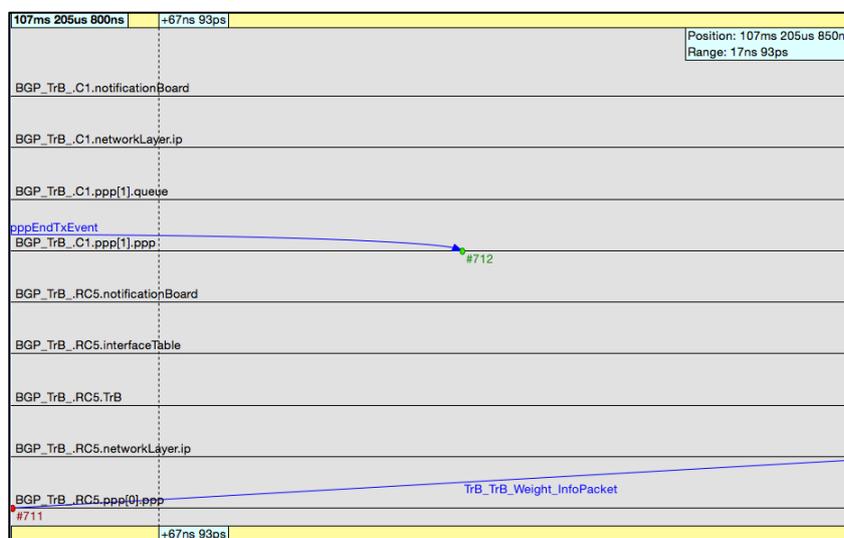


Figura 10.4 – Diagrama de estado do parâmetro TrB

A Tab. 10.1 corresponde a um exemplo de configuração usando a linguagem de programação descritiva NED. Na Tab. 10.2 é mostrado um exemplo de configuração de estado com o uso dos modelos de trafego sendo acionados dentro do ambiente de programação. A Tab. 10.3 é um exemplo de configuração padrão do IPv6 dentro do ambiente OMNET/INET.

Tabela 10.1 – Configuração do ambiente NUT para testes com BGP

```

package inet.examples.bgpv4.BGPCompleteTest;

import
inet.networklayer.autorouting.ipv4.IPv4NetworkConfigurator;
import inet.nodes.bgp.BGPRouter;
import inet.nodes.ethernet.EtherSwitch;
import inet.nodes.inet.StandardHost;
import inet.nodes.ospfv2.OSPFRouter;
import inet.util.ThruputMeteringChannel;

network BGPTest
{
    types:
        channel LINK_100 extends ThruputMeteringChannel
        {
            parameters:
                delay = 0;
                datarate = 100Mbps;
                thruputDisplayFormat = "#N";
        }
    submodules:
        A1: BGPRouter {
            parameters:
                @display("p=178,45");
            gates:
                pppg[2];
        }
        A2: BGPRouter {
            parameters:
                @display("p=168,93");
            gates:
                pppg[2];
        }
        B1: BGPRouter {

```

```

        parameters:
            @display("p=194,253");
        gates:
            pppg[2];
            ethg[1];
    }
    C1: BGPRouter {
        parameters:
            @display("p=322,45");
        gates:
            pppg[2];
    }
    C2: BGPRouter {
        parameters:
            @display("p=322,141");
        gates:
            pppg[2];
    }
    C3: BGPRouter {
        parameters:
            @display("p=450,45");
        gates:
            pppg[2];
    }
    C4: BGPRouter {
        parameters:
            @display("p=450,149");
        gates:
            pppg[2];
    }
    D1: BGPRouter {
        parameters:
            @display("p=562,141");
        gates:
            pppg[1];
            ethg[1];
    }
    E1: BGPRouter {
        parameters:
            @display("p=514,269");
        gates:
            pppg[1];
            ethg[1];
    }
    RA3: OSPFRouter {
        parameters:

```

```

        @display("p=102,43;i=device/router");
    gates:
        pppg[2];
        ethg[1];
}
RC5: OSPFRouter {
    parameters:
        @display("p=390,97;i=device/router");
    gates:
        pppg[4];
}
PA3: EtherSwitch {
    parameters:
        @display("p=52,86;i=device/switch");
    gates:
        ethg[3];
}
PB1: EtherSwitch {
    parameters:
        @display("p=132,302;i=device/switch");
    gates:
        ethg[3];
}
PD1: EtherSwitch {
    parameters:
        @display("p=612,78;i=device/switch");
    gates:
        ethg[3];
}
PE1: EtherSwitch {
    parameters:
        @display("p=452,318;i=device/switch");
    gates:
        ethg[3];
}
HA11: StandardHost {
    parameters:
        @display("p=58,146;i=device/pc");
    gates:
        ethg[1];
}
HA12: StandardHost {
    parameters:
        @display("p=114,146;i=device/pc");
    gates:
        ethg[1];
}

```

```

}
HB11: StandardHost {
    parameters:
        @display("p=246,306;i=device/pc");
    gates:
        ethg[1];
}
HB12: StandardHost {
    parameters:
        @display("p=206,338;i=device/pc");
    gates:
        ethg[1];
}
HD11: StandardHost {
    parameters:
        @display("p=582,194;i=device/pc");
    gates:
        ethg[1];
}
HD12: StandardHost {
    parameters:
        @display("p=630,194;i=device/pc");
    gates:
        ethg[1];
}
HE11: StandardHost {
    parameters:
        @display("p=518,364;i=device/pc");
    gates:
        ethg[1];
}
HE12: StandardHost {
    parameters:
        @display("p=550,316;i=device/pc");
    gates:
        ethg[1];
}
configurator: IPv4NetworkConfigurator {
    @display("p=58,351");
    config = xmldoc("IPv4Config.xml");
    //assignAddresses = false;
    //assignDisjunctSubnetAddresses = false;
    addStaticRoutes = false;
    addDefaultRoutes = false;
    addSubnetRoutes = false;
}

```

```

TrB_DataBase: StandardHost {
    parameters:
        @display("p=526,23;i=device/pc");
    gates:
        ethg[1];
}
connections:
//LAN RA3
HA11.ethg[0] <--> LINK_100 <--> PA3.ethg[0];
HA12.ethg[0] <--> LINK_100 <--> PA3.ethg[1];
PA3.ethg[2] <--> LINK_100 <--> RA3.ethg[0];

//LAN B1
HB11.ethg[0] <--> LINK_100 <--> PB1.ethg[0];
HB12.ethg[0] <--> LINK_100 <--> PB1.ethg[1];
PB1.ethg[2] <--> LINK_100 <--> B1.ethg[0];

//LAN D1
HD11.ethg[0] <--> LINK_100 <--> PD1.ethg[0];
HD12.ethg[0] <--> LINK_100 <--> PD1.ethg[1];
PD1.ethg[2] <--> LINK_100 <--> D1.ethg[0];

//LAN E1
HE11.ethg[0] <--> LINK_100 <--> PE1.ethg[0];
HE12.ethg[0] <--> LINK_100 <--> PE1.ethg[1];
PE1.ethg[2] <--> LINK_100 <--> E1.ethg[0];

//OSPF A
RA3.pppg[0] <--> LINK_100 <--> A1.pppg[1];
RA3.pppg[1] <--> LINK_100 <--> A2.pppg[1];

//OSPF C
RC5.pppg[0] <--> LINK_100 <--> C1.pppg[1];
RC5.pppg[1] <--> LINK_100 <--> C2.pppg[1];
RC5.pppg[2] <--> LINK_100 <--> C3.pppg[1];
RC5.pppg[3] <--> LINK_100 <--> C4.pppg[1];

//BGP
A1.pppg[0] <--> LINK_100 <--> C1.pppg[0];
A2.pppg[0] <--> LINK_100 <--> B1.pppg[0];
B1.pppg[1] <--> LINK_100 <--> C2.pppg[0];
C3.pppg[0] <--> LINK_100 <--> D1.pppg[0];
C4.pppg[0] <--> LINK_100 <--> E1.pppg[0];
TrB_DataBase.ethg[0] <--> C3.ethg++;
}

```

Tabela 10.2 – Testes com banda efetiva Kernel, Stênico e Misturas Gaussianas

```
//  
// Copyright (C) 2004 Andras Varga  
// Copyright (C) 2014 OpenSim Ltd.  
//  
//Copyright (C) 2014 INET  
//  
// This program is free software; you can redistribute it and/or  
// modify it under the terms of the GNU Lesser General Public License  
// as published by the Free Software Foundation; either version 2  
// of the License, or (at your option) any later version.  
//  
// This program is distributed in the hope that it will be useful,  
// but WITHOUT ANY WARRANTY; without even the implied warranty of  
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the  
// GNU Lesser General Public License for more details.  
//  
// You should have received a copy of the GNU Lesser General Public License  
// along with this program; if not, see <http://www.gnu.org/licenses/>.  
//  
//Modificado nos termos da licença GNU para uso com o IPv4 e IPv6  
  
#ifndef __INET_IPv4_H  
#define __INET_IPv4_H  
  
#ifndef __INET_IPv6_H  
#define __INET_IPv6_H  
  
  
#include "INETDefs.h"  
  
#include "IARPCache.h"  
#include "ICMPAccess.h"  
#include "ILifecycle.h"  
#include "INetfilter.h"  
#include "IPv4Datagram.h"  
#include "IPv4FragBuf.h"  
#include "IPv6Datagram.h"  
#include "IPv6FragBuf.h"  
#include "ProtocolMap.h"  
#include "QueueBase.h"  
#include "bufferKernel.h"  
#include "bufferStenico.h"  
#include "bufferMistGauss.h"
```

```

class ARPPacket;
class ICMPMessage;
class IInterfaceTable;
class IRoutingTable;
class NotificationBoard;
class buffer_todos;

/**
 * Calculo da Banda de Kernel.
 *
 * class INET_API IPv4 : public QueueBase, public INetfilter, public ILifecycle, public
cListener
{
public:
/**
 * Represents an IPv4Datagram, queued by a Hook
 */
class buffer_todos {
public:
    QueuedDatagramForHook(IPv4Datagram* datagram, const InterfaceEntry* inIE,
const InterfaceEntry* outIE, const IPv4Address& nextHopAddr, IHook::Type hookType) :
        datagram(datagram), inIE(inIE), outIE(outIE), nextHopAddr(nextHopAddr),
hookType(hookType) {}
    virtual ~QueuedDatagramForHook() {}

    IPv4Datagram* datagram;
    const InterfaceEntry* inIE;
    const InterfaceEntry* outIE;
    IPv4Address nextHopAddr;
    const IHook::Type hookType;
};
typedef std::map<IPv4Address, cPacketQueue> PendingPackets;

protected:
    static simsignal_t completedARPResolutionSignal;
    static simsignal_t failedARPResolutionSignal;
*/
class INET_API IPv4 : public QueueBase, public INetfilter, public ILifecycle, public
cListener
{
public:
/**
 * Represents an IPv4Datagram, queued by a Hook
 */
class QueuedDatagramForHook {

```

```

public:
    QueuedDatagramForHook(IPv4Datagram* datagram, const InterfaceEntry* inIE,
const InterfaceEntry* outIE, const IPv4Address& nextHopAddr, IHook::Type hookType) :
        datagram(datagram), inIE(inIE), outIE(outIE), nextHopAddr(nextHopAddr),
hookType(hookType) {}
    virtual ~QueuedDatagramForHook() {}

    IPv4Datagram* datagram;
    const InterfaceEntry* inIE;
    const InterfaceEntry* outIE;
    IPv4Address nextHopAddr;
    const IHook::Type hookType;
};
typedef std::map<IPv4Address, cPacketQueue> PendingPackets;
/**
 * Represents an IPv6Datagram, queued by a Hook
 */
class QueuedDatagramForHook {
public:
    QueuedDatagramForHook(IPv6Datagram* datagram, const InterfaceEntry* inIE,
const InterfaceEntry* outIE, const IPv6Address& nextHopAddr, IHook::Type hookType) :
        datagram(datagram), inIE(inIE), outIE(outIE), nextHopAddr(nextHopAddr),
hookType(hookType) {}
    virtual ~QueuedDatagramForHook() {}

    IPv6Datagram* datagram;
    const InterfaceEntry* inIE;
    const InterfaceEntry* outIE;
    IPv6Address nextHopAddr;
    const IHook::Type hookType;
};
typedef std::map<IPv6Address, cPacketQueue> PendingPackets;

protected:
    static simsignal_t completedARPResolutionSignal;
    static simsignal_t failedARPResolutionSignal;

    IRoutingTable *rt;
    IInterfaceTable *ift;
    NotificationBoard *nb;
    IARPCache *arp;
    ICMPAccess icmpAccess;
    cGate *arpInGate;
    cGate *arpOutGate;
    int transportInGateBaseId;
    int queueOutGateBaseId;

    // config
    int defaultTimeToLive;

```

```

int defaultMCTimeToLive;
simtime_t fragmentTimeoutTime;
bool forceBroadcast;
bool useProxyARP;

// working vars
bool isUp;
long curFragmentId; // counter, used to assign unique fragmentIds to datagrams
IPv4FragBuf buffer_Kernel; // fragmentation reassembly buffer
simtime_t lastCheckTime; // when fragbuf was last checked for state fragments
ProtocolMapping mapping; // where to send packets after decapsulation

// working vars
bool isUp;
long curFragmentId; // counter, used to assign unique fragmentIds to datagrams
IPv4FragBuf buffer_Stenico; // fragmentation reassembly buffer
simtime_t lastCheckTime; // when fragbuf was last checked for state fragments
ProtocolMapping mapping; // where to send packets after decapsulation

// working vars
bool isUp;
long curFragmentId; // counter, used to assign unique fragmentIds to datagrams
IPv4FragBuf buffer_Mist_Gauss; // fragmentation reassembly buffer
simtime_t lastCheckTime; // when fragbuf was last checked for state fragments
ProtocolMapping mapping; // where to send packets after decapsulation

// ARP related
PendingPackets pendingPackets; // map indexed with IPv4Address for outbound
packets waiting for ARP resolution

// statistics
int numMulticast;
int numLocalDeliver;
int numDropped; // forwarding off, no outgoing interface, too large but "don't fragment"
is set, TTL exceeded, etc
int numUnroutable;
int numForwarded;

// hooks
typedef std::multimap<int, IHook*> HookList;
HookList hooks;
typedef std::list<QueuedDatagramForHook> DatagramQueueForHooks;
DatagramQueueForHooks queuedDatagramsForHooks;

protected:
// utility: look up interface from getArrivalGate()
virtual const InterfaceEntry *getSourceInterfaceFrom(cPacket *packet);

```

```

// utility: look up route to the source of the datagram and return its interface
virtual const InterfaceEntry *getShortestPathInterfaceToSource(IPv4Datagram
*datagram);

// utility: show current statistics above the icon
virtual void updateDisplayString();

// utility: processing requested ARP resolution completed
void arpResolutionCompleted(IARPCache::Notification *entry);

// utility: processing requested ARP resolution timed out
void arpResolutionTimedOut(IARPCache::Notification *entry);

/**
 * Encapsulate packet coming from higher layers into IPv4Datagram, using
 * the given control info. Override if you subclassed controlInfo and/or
 * want to add options etc to the datagram.
 */
virtual IPv4Datagram *encapsulate(cPacket *transportPacket, IPv4ControlInfo
*controlInfo);

/**
 * Creates a blank IPv4 datagram. Override when subclassing IPv4Datagram is needed
 */
virtual IPv4Datagram *createIPv4Datagram(const char *name);

/**
 * Handle IPv4Datagram messages arriving from lower layer.
 * Decrements TTL, then invokes routePacket().
 */
virtual void handleIncomingDatagram(IPv4Datagram *datagram, const InterfaceEntry
*fromIE);

// called after PREROUTING Hook (used for reinject, too)
virtual void preroutingFinish(IPv4Datagram *datagram, const InterfaceEntry *fromIE,
const InterfaceEntry *destIE, IPv4Address nextHopAddr);

/**
 */
virtual void handleIncomingDatagram(IPv6Datagram *datagram, const InterfaceEntry
*fromIE);

// called after PREROUTING Hook (used for reinject, too)
virtual void preroutingFinish(IPv6Datagram *datagram, const InterfaceEntry *fromIE,
const InterfaceEntry *destIE, IPv6Address nextHopAddr);

/**

```

```

* Handle messages (typically packets to be send in IPv4) from transport or ICMP.
* Invokes encapsulate(), then routePacket().
*/
virtual void handlePacketFromHL(cPacket *packet);
/**

* Handle messages (typically packets to be send in IPv6) from transport or ICMP.
* Invokes encapsulate(), then routePacket().
*/
virtual void handlePacketFromHL(cPacket *packet);

/**
* TODO
*/
virtual void handlePacketFromARP(cPacket *packet);

/**
* Routes and sends datagram received from higher layers.
* Invokes datagramLocalOutHook(), then routePacket().
*/
virtual void datagramLocalOut(IPv4Datagram* datagram, const InterfaceEntry* destIE,
IPv4Address nextHopAddr);

/**
*/
virtual void datagramLocalOut(IPv6Datagram* datagram, const InterfaceEntry* destIE,
IPv4Address nextHopAddr);

/**

* Handle incoming ARP packets by sending them over to ARP.
*/
virtual void handleIncomingARPPacket(ARPPacket *packet, const InterfaceEntry
*fromIE);

/**
* Handle incoming ICMP messages.
*/
virtual void handleIncomingICMP(ICMPMessage *packet);

/**
* Performs unicast routing. Based on the routing decision, it sends the
* datagram through the outgoing interface.
*/
virtual void routeUnicastPacket(IPv4Datagram *datagram, const InterfaceEntry
*fromIE, const InterfaceEntry *destIE, IPv4Address requestedNextHopAddress);
*/
virtual void routeUnicastPacket(IPv6Datagram *datagram, const InterfaceEntry
*fromIE, const InterfaceEntry *destIE, IPv4Address requestedNextHopAddress);

```

```

// called after FORWARD Hook (used for reinject, too)
void routeUnicastPacketFinish(IPv4Datagram *datagram, const InterfaceEntry *fromIE,
const InterfaceEntry *destIE, IPv4Address nextHopAddr);

/**
*fromIE, const InterfaceEntry *destIE, IPv6Address requestedNextHopAddress);

// called after FORWARD Hook (used for reinject, too)
void routeUnicastPacketFinish(IPv6Datagram *datagram, const InterfaceEntry *fromIE,
const InterfaceEntry *destIE, IPv6Address nextHopAddr);

/**

* Broadcasts the datagram on the specified interface.
* When destIE is NULL, the datagram is broadcasted on each interface.
*/
virtual void routeLocalBroadcastPacket(IPv4Datagram *datagram, const InterfaceEntry
*destIE);

/**
* Broadcasts the datagram on the specified interface.
* When destIE is NULL, the datagram is broadcasted on each interface.
*/
virtual void routeLocalBroadcastPacket(IPv6Datagram *datagram, const InterfaceEntry
*destIE);

/**

* Determines the output interface for the given multicast datagram.
*/
virtual const InterfaceEntry
*determineOutgoingInterfaceForMulticastDatagram(IPv4Datagram *datagram, const
InterfaceEntry *multicastIFOption);

/**
* Forwards packets to all multicast destinations, using fragmentAndSend().
*/
virtual void forwardMulticastPacket(IPv4Datagram *datagram, const InterfaceEntry
*fromIE);

/**
/**
* Forwards packets to all multicast destinations, using fragmentAndSend().
*/
virtual void forwardMulticastPacket(IPv6Datagram *datagram, const InterfaceEntry
*fromIE);

/**

```

```

* Perform reassembly of fragmented datagrams, then send them up to the
* higher layers using sendToHL().
*/
virtual void reassembleAndDeliver(IPv4Datagram *datagram);

// called after LOCAL_IN Hook (used for reinject, too)
virtual void reassembleAndDeliverFinish(IPv4Datagram *datagram);

/**
 * Decapsulate and return encapsulated packet after attaching IPv4ControlInfo.
 */
virtual cPacket *decapsulate(IPv4Datagram *datagram);

/**
/**
 * Decapsulate and return encapsulated packet after attaching IPv4ControlInfo.
 */
virtual cPacket *decapsulate(IPv6Datagram *datagram);

/**

 * Call PostRouting Hook and continue with fragmentAndSend() if accepted
 */
virtual void fragmentPostRouting(IPv4Datagram *datagram, const InterfaceEntry *ie,
IPv4Address nextHopAddr);

/**
 * Fragment packet if needed, then send it to the selected interface using
 * sendDatagramToOutput().
 */
virtual void fragmentAndSend(IPv4Datagram *datagram, const InterfaceEntry *ie,
IPv4Address nextHopAddr);

/**
 * Send datagram on the given interface.
 */
virtual void sendDatagramToOutput(IPv4Datagram *datagram, const InterfaceEntry *ie,
IPv4Address nextHopAddr);

virtual MACAddress resolveNextHopMacAddress(cPacket *packet, IPv4Address
nextHopAddr, const InterfaceEntry *destIE);

virtual void sendPacketToIeee802NIC(cPacket *packet, const InterfaceEntry *ie, const
MACAddress& macAddress, int etherType);
 * Send datagram on the given interface.
 */
virtual void sendDatagramToOutput(IPv6Datagram *datagram, const InterfaceEntry *ie,
IPv4Address nextHopAddr);

```

```

    virtual MACAddress resolveNextHopMacAddress(cPacket *packet, IPv6Address
nextHopAddr, const InterfaceEntry *destIE);

    virtual void sendPacketToNIC(cPacket *packet, const InterfaceEntry *ie);

public:
    IPv4() { rt = NULL; ift = NULL; arp = NULL; arpOutGate = NULL; }

public:
    IPv6() { rt = NULL; ift = NULL; arp = NULL; arpOutGate = NULL; }

protected:
    virtual int numInitStages() const { return 2; }
    virtual void initialize(int stage);
    virtual void handleMessage(cMessage *msg);

    /**
     * Processing of IP datagrams. Called when a datagram reaches the front
     * of the queue.
     */
    virtual void endService(cPacket *packet);
    /**

    // NetFilter functions:
protected:
    /**
     * called before a packet arriving from the network is routed
     */
    IHook::Result datagramPreRoutingHook(IPv4Datagram* datagram, const
InterfaceEntry* inIE, const InterfaceEntry*& outIE, IPv4Address& nextHopAddr);

    /**
     */
    IHook::Result datagramPreRoutingHook(IPv6Datagram* datagram, const
InterfaceEntry* inIE, const InterfaceEntry*& outIE, IPv6Address& nextHopAddr);

    /**

     * called before a packet arriving from the network is delivered via the network
     */
    IHook::Result datagramForwardHook(IPv4Datagram* datagram, const InterfaceEntry*
inIE, const InterfaceEntry*& outIE, IPv4Address& nextHopAddr);

    IHook::Result datagramForwardHook(IPv6Datagram* datagram, const InterfaceEntry*
inIE, const InterfaceEntry*& outIE, IPv6Address& nextHopAddr);

```

```

/**
 * called before a packet is delivered via the network
 */
IHook::Result datagramPostRoutingHook(IPv4Datagram* datagram, const
InterfaceEntry* inIE, const InterfaceEntry*& outIE, IPv4Address& nextHopAddr);

IHook::Result datagramPostRoutingHook(IPv4Datagram* datagram, const
InterfaceEntry* inIE, const InterfaceEntry*& outIE, IPv6Address& nextHopAddr);

/**
 * called before a packet arriving from the network is delivered locally
 */
IHook::Result datagramLocalInHook(IPv4Datagram* datagram, const InterfaceEntry*
inIE);

/**
 * called before a packet arriving locally is delivered
 */
IHook::Result datagramLocalOutHook(IPv4Datagram* datagram, const
InterfaceEntry*& outIE, IPv4Address& nextHopAddr);

IHook::Result datagramLocalOutHook(IPv4Datagram* datagram, const
InterfaceEntry*& outIE, IPv6Address& nextHopAddr);

public:
/**
 * registers a Hook to be executed during datagram processing
 */
virtual void registerHook(int priority, IHook* hook);

/**
 * unregisters a Hook to be executed during datagram processing
 */
virtual void unregisterHook(int priority, IHook* hook);

/**
 * drop a previously queued datagram
 */
void dropQueuedDatagram(const IPv4Datagram * datagram);
void dropQueuedDatagram(const IPv6Datagram * datagram);

/**
 * re-injects a previously queued datagram
 */
void reinjectQueuedDatagram(const IPv4Datagram * datagram);

/**

```

```

* send packet on transportOut gate specified by protocolId
*/
void sendOnTransportOutGateByProtocolId(cPacket *packet, int protocolId);

/**
* ILifecycle method
*/

virtual bool handleOperationStage(LifecycleOperation *operation, int stage,
IDoneCallback *doneCallback);

/// cListener method
virtual void receiveSignal(cComponent *source, simsignal_t signalID, cObject *obj);

protected:
virtual bool isNodeUp();
virtual void stop();
virtual void start();
virtual void flush();
};

#endif

```

Tabela 10.3 – Modelo INET OMNET IPv6

```

\chapter{IPv6 and Mobile IPv6}
\label{cha:ipv6}

\section{Overview}

IPv6 support is implemented by several cooperating modules. The IPv6 module
implements IPv6 datagram handling (sending, forwarding etc). It relies on
\nedtype{IPv6RoutingTable} to get access to the routes. \nedtype{IPv6RoutingTable} also
contains the neighbour discovery data structures (destination cache, neighbour cache,
prefix list -- the latter effectively merged into the route table). Interface
configuration (address, state, timeouts etc) is held in the \nedtype{InterfaceTable},
in \cppclass{IPv6InterfaceData} objects attached to \cppclass{InterfaceEntry}
as its \ttt{ipv6()} member.

The module \nedtype{IPv6NeighbourDiscovery} implements all tasks associated with
neighbour discovery and stateless address autoconfiguration. The data
structures themselves (destination cache, neighbour cache, prefix list)
are kept in \nedtype{IPv6RoutingTable}, and are accessed via public C++ methods.
Neighbour discovery packets are only sent and processed by this module --
when IPv6 receives one, it forwards the packet to \nedtype{IPv6NeighbourDiscovery}.

```

The rest of ICMPv6 (ICMP errors, echo request/reply etc) is implemented in the module `\nedtype{ICMPv6}`, just like with IPv4. ICMP errors are sent into `\nedtype{IPv6ErrorHandling}`, which the user can extend or replace to get errors handled in any way they like.

```
%%% Local Variables:
%%% mode: latex
%%% TeX-master: "usman"
%%% End:
```

A Fig. 10.4 é um dos diagramas de estado do `corresponde` a configuração usando a linguagem de programação descritiva NED. Na Tab. 10.2 é mostrado um exemplo de configuração de estado com o uso dos modelos de tráfego sendo acionados dentro do ambiente de programação. A Tab. 10.3 é um exemplo de configuração do IPv6 dentro do ambiente OMNET/INET.

A Tab. 10.4 é mostrado um exemplo de coleta de dados simulados no ambiente OMNET/INET.

Tabela 10.4 – Exemplo de extração de dados OMNET⁺⁺

```
results.sca

version 2
run config1-0-20150302-02:28:49-8799
attr configname config1
attr datetime 20140709-02:28:49
attr experiment config1
attr inifile omnetpp.ini
attr iterationvars ""
attr iterationvars2 $repetition=0
attr measurement ""
attr network BGPTest
attr processid 8799
attr repetition 0
attr replication #0
attr resultdir results
attr runnumber 0
attr seedset 0

scalar BGPTest.HA11.udpApp[0] "packets sent" 41
```

```

scalar BGPTest.HA11.udpApp[0]    "packets received"    0
scalar BGPTest.HA11.udpApp[0]    rcvdPk:count    0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HA11.udpApp[0]    rcvdPk:sum(packetBytes)    0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HA11.udpApp[0]    rcvdPkLifetime:stats
field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "received packet lifetime, stats"
attr unit s
scalar BGPTest.HA11.udpApp[0]    sentPk:count    41
attr interpolationmode none
attr source sentPk
attr title "packets sent, count"
scalar BGPTest.HA11.udpApp[0]    sentPk:sum(packetBytes)    1312
attr interpolationmode none
attr source sentPk
attr title "packets sent, sum(packetBytes)"
scalar BGPTest.HA12.udpApp[0]    rcvdPk:count    36
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HA12.udpApp[0]    rcvdPk:sum(packetBytes)    1152
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HA12.udpApp[0]    endToEndDelay:histogram
field count 36
field mean 6.5952e-05
field stddev 1.1429e-05
field sum 0.0023743
field sqrsum 1.6116e-07
field min 6.232e-05
field max 0.0001124
attr interpolationmode none

```

```

attr source messageAge(rcvdPk)
attr title "end-to-end delay, histogram"
attr unit s
bin -INF 0
bin 3.728e-05 0
bin 4.0619e-05 0
bin 4.3957e-05 0
bin 4.7296e-05 0
bin 5.0635e-05 0
bin 5.3973e-05 0
bin 5.7312e-05 0
bin 6.0651e-05 34
bin 6.3989e-05 0
bin 6.7328e-05 0
bin 7.0667e-05 0
bin 7.4005e-05 0
bin 7.7344e-05 0
bin 8.0683e-05 0
bin 8.4021e-05 0
bin 8.736e-05 0
bin 9.0699e-05 0
bin 9.4037e-05 0
bin 9.7376e-05 0
bin 0.00010071 0
bin 0.00010405 0
bin 0.00010739 0
bin 0.00011073 2
bin 0.00011407 0
bin 0.00011741 0
bin 0.00012075 0
bin 0.00012409 0
bin 0.00012742 0
bin 0.00013076 0
bin 0.0001341 0
bin 0.00013744 0
scalar BGPTest.HB11.udpApp[0] "packets sent" 40
scalar BGPTest.HB11.udpApp[0] "packets received" 0
scalar BGPTest.HB11.udpApp[0] rcvdPk:count 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HB11.udpApp[0] rcvdPk:sum(packetBytes) 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HB11.udpApp[0] rcvdPklifetime:stats

```

```

field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "received packet lifetime, stats"
attr unit s
scalar BGPTest.HB11.udpApp[0] sentPk:count 40
attr interpolationmode none
attr source sentPk
attr title "packets sent, count"
scalar BGPTest.HB11.udpApp[0] sentPk:sum(packetBytes) 1280
attr interpolationmode none
attr source sentPk
attr title "packets sent, sum(packetBytes)"
scalar BGPTest.HB12.udpApp[0] rcvdPk:count 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HB12.udpApp[0] rcvdPk:sum(packetBytes) 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HB12.udpApp[0] endToEndDelay:histogram
field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "end-to-end delay, histogram"
attr unit s
bin -INF 0
bin -0.5 0
bin -0.46667 0
bin -0.43333 0
bin -0.4 0
bin -0.36667 0
bin -0.33333 0

```

```

bin -0.3 0
bin -0.26667 0
bin -0.23333 0
bin -0.2 0
bin -0.16667 0
bin -0.13333 0
bin -0.1 0
bin -0.066667 0
bin -0.033333 0
bin 0 0
bin 0.033333 0
bin 0.066667 0
bin 0.1 0
bin 0.13333 0
bin 0.16667 0
bin 0.2 0
bin 0.23333 0
bin 0.26667 0
bin 0.3 0
bin 0.33333 0
bin 0.36667 0
bin 0.4 0
bin 0.43333 0
bin 0.46667 0
bin 0.5 0
scalar BGPTest.HD11.udpApp[0] "packets sent" 40
scalar BGPTest.HD11.udpApp[0] "packets received" 0
scalar BGPTest.HD11.udpApp[0] rcvdPk:count 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HD11.udpApp[0] rcvdPk:sum(packetBytes) 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HD11.udpApp[0] rcvdPkLifetime:stats
field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "received packet lifetime, stats"

```

```

attr unit s
scalar BGPTest.HD11.udpApp[0] sentPk:count 40
attr interpolationmode none
attr source sentPk
attr title "packets sent, count"
scalar BGPTest.HD11.udpApp[0] sentPk:sum(packetBytes) 1280
attr interpolationmode none
attr source sentPk
attr title "packets sent, sum(packetBytes)"
scalar BGPTest.HD12.udpApp[0] rcvdPk:count 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HD12.udpApp[0] rcvdPk:sum(packetBytes) 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HD12.udpApp[0] endToEndDelay:histogram
field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "end-to-end delay, histogram"
attr unit s
bin -INF 0
bin -0.5 0
bin -0.46667 0
bin -0.43333 0
bin -0.4 0
bin -0.36667 0
bin -0.33333 0
bin -0.3 0
bin -0.26667 0
bin -0.23333 0
bin -0.2 0
bin -0.16667 0
bin -0.13333 0
bin -0.1 0
bin -0.066667 0
bin -0.033333 0
bin 0 0

```

```

bin 0.033333 0
bin 0.066667 0
bin 0.1 0
bin 0.13333 0
bin 0.16667 0
bin 0.2 0
bin 0.23333 0
bin 0.26667 0
bin 0.3 0
bin 0.33333 0
bin 0.36667 0
bin 0.4 0
bin 0.43333 0
bin 0.46667 0
bin 0.5 0
scalar BGPTest.HE11.udpApp[0] "packets sent" 40
scalar BGPTest.HE11.udpApp[0] "packets received" 0
scalar BGPTest.HE11.udpApp[0] rcvdPk:count 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HE11.udpApp[0] rcvdPk:sum(packetBytes) 0
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HE11.udpApp[0] rcvdPkLifetime:stats
field count 0
field mean 0
field stddev nan
field sum 0
field sqrsum 0
field min 0
field max 0
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "received packet lifetime, stats"
attr unit s
scalar BGPTest.HE11.udpApp[0] sentPk:count 40
attr interpolationmode none
attr source sentPk
attr title "packets sent, count"
scalar BGPTest.HE11.udpApp[0] sentPk:sum(packetBytes) 1280
attr interpolationmode none
attr source sentPk
attr title "packets sent, sum(packetBytes)"
scalar BGPTest.HE12.udpApp[0] rcvdPk:count 34

```

```

attr interpolationmode none
attr source rcvdPk
attr title "packets received, count"
scalar BGPTest.HE12.udpApp[0] rcvdPk:sum(packetBytes) 1088
attr interpolationmode none
attr source rcvdPk
attr title "packets received, sum(packetBytes)"
statistic BGPTest.HE12.udpApp[0] endToEndDelay:histogram
field count 34
field mean 0.058884
field stddev 0.34301
field sum 2.002
field sqrsum 4.0005
field min 5.596e-05
field max 2.0001
attr interpolationmode none
attr source messageAge(rcvdPk)
attr title "end-to-end delay, histogram"
attr unit s
bin -INF 0
bin -0.99998 0
bin -0.86664 0
bin -0.7333 0
bin -0.59996 0
bin -0.46663 0
bin -0.33329 0
bin -0.19995 0
bin -0.066613 33
bin 0.066725 0
bin 0.20006 0
bin 0.3334 0
bin 0.46674 0
bin 0.60008 0
bin 0.73341 0
bin 0.86675 0
bin 1.0001 0
bin 1.1334 0
bin 1.2668 0
bin 1.4001 0
bin 1.5334 0
bin 1.6668 0
bin 1.8001 0
bin 1.9335 1
bin 2.0668 0
bin 2.2001 0
bin 2.3335 0

```

bin	2.4668	0		
bin	2.6001	0		
bin	2.7335	0		
bin	2.8668	0		
			bin	3.0002 0

8.2 FERRAMENTA: Weka

O Weka é um pacote voltado para a mineração de dados. O **Waikato Environment for Knowledge Analysis** foi uma iniciativa do corpo acadêmico da Universidade de Waikato, Nova Zelândia e teve início em 1993, usando Java. O texto da licença LGPL está disponível aqui e mais informações podem ser obtidas da *Free Software Foundation*.

O objetivo principal é agregar algoritmos oriundos de diferentes abordagens de Inteligência Computacional dedicada ao estudo da aprendizagem por parte de máquinas. O objetivo principal é o desenvolvimento de ambiente com algoritmos e técnicas que permitam a um computador adquirir e analisar dados de forma indutiva ou dedutiva.

O Weka realiza análise computacional e estatística dos dados fornecidos com a ajuda de técnicas de data-mining tentando, indutivamente, a partir dos padrões encontrados gerar hipóteses para soluções e no extremos inclusive teorias sobre os dados em questão. O weka está disponível para *download* em: <http://www.cs.waikato.ac.nz/ml/weka/>

8.3 FERRAMENTA: C-BGP

O C-BGP é uma ferramenta para auxílio no desenvolvimento e entendimento do protocolo BGP. A versão original de C-BGP foi escrita por Bruno Quoitin, no laboratório de redes IP, Departamento de Ciências da Computação e Engenharia da Universidade Católica de Louvain (UCLouvain), na Bélgica. Continua sendo mantido pelo laboratório de redes da Universidade de Mons (UMONS). O C-BGP é escrito em linguagem C. É principalmente usado e testado em Linux e Mac OS X. Também tem sido usado em outras plataformas, tais como FreeBSD, Solaris e mesmo sob Windows, usando o API do Cygwin. C-BGP é Open-Source e fornecido sob a licença LGPL. O texto da licença LGPL está disponível aqui e mais informações podem ser obtidas da *Free Software Foundation*.

O C-BGP está disponível para download em:<http://c-bgp.sourceforge.net/>

8.4 FERRAMENTA: FRACLAB

FracLab é uma ferramenta para processamento de sinais. Disponibiliza um módulo para análise com base em métodos e multifractais fractal. O FracLab pode ser abordado a partir de duas perspectivas diferentes: Análise Fractal. Um grande número de procedimentos permitem calcular diversas quantidades fractal associados com sinais de 1D ou 2D, tais como dimensões, expoentes titular ou espectros multifractal ou de Dependência de Longa Duração. Ou através do Processamento de sinais: Como alternativa, pode-se usar FracLab diretamente para executar muitas tarefas básicas no processamento de sinais, incluindo uma estimativa, detecção, denoising, modelagem, segmentação, classificação e síntese.

Uma interface gráfica faz FracLab auxiliar na interface. Além disso, várias ferramentas wavelet-relacionadas estão disponíveis em FracLab.

Sistema

FracLab é um software livre desenvolvido na equipe Regularidade no INRIA Saclay / Ecole Centrale de Paris.

Ela consiste principalmente de rotinas desenvolvidas em Matlab versão 7.7 (R2008a) e algumas rotinas desenvolvidas em C-código. Ele é executado em ambientes Windows, Mac OSX e Linux.

Desde FracLab 2,02 existe uma versão autônoma que ele seja executado em Windows, Mac OSX e ambientes Linux.

Condições de utilização

Este Software é (INRIA de Copyright. 1998 2010 1)

INRIA detém todos os direitos de propriedade sobre o Software. A comunidade científica é convidada a usar o software, a fim de testar e avaliar.

INRIA concede livremente o direito de usar modificar o Software, integrá-lo em outro Software. Qualquer uso ou reprodução deste Software para obter lucro ou para fins comerciais está sujeita à obtenção da autorização prévia e expressa do INRIA.

INRIA autoriza qualquer reprodução deste Software.

8.5 FERRAMENTA: LABORATÓRIO DE UMA OPERADORA DE TELECOMUNICAÇÕES.

Este laboratório é composto por equipamentos roteadores Juniper MX960, T640 e T320. Diversas simulações reais foram possíveis devido ao acesso a esta plataforma de testes. Todos os testes, não possíveis de serem realizados. Na Fig. 7.5 é apresentada a topologia física do Laboratório.

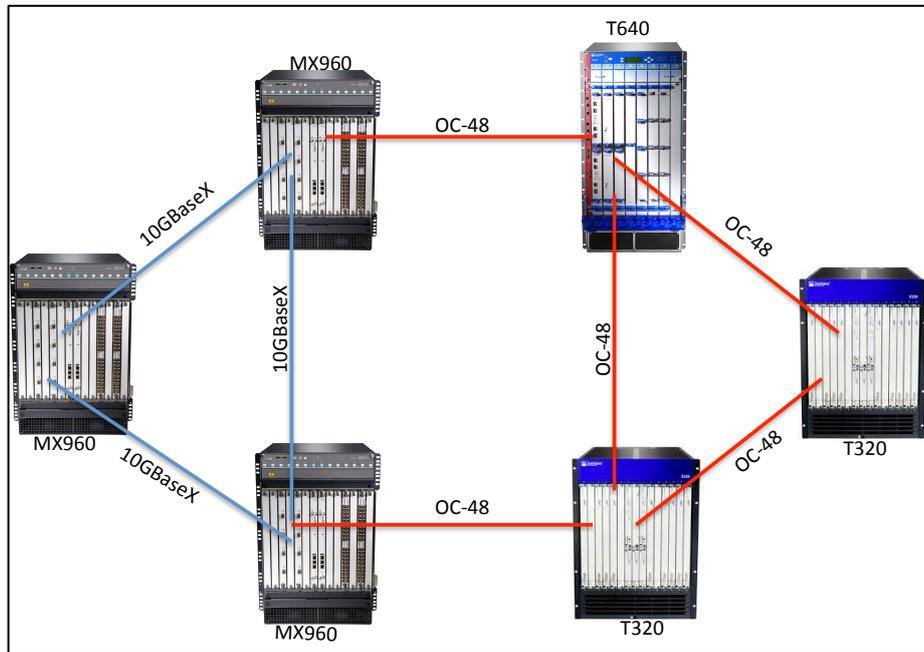


Figura 7.5 – Topologia física do Laboratório com uso de equipamentos reais Juniper.