

UNIVERSIDADE SANTA CECÍLIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA MECÂNICA
MESTRADO EM ENGENHARIA MECÂNICA

ALESSANDRO DE LIMA MARREIRO

APLICAÇÃO DA LÓGICA PARACONSISTENTE ANOTADA EVIDENCIAL ET COM
ALGORITMO ADAPTATIVO DE ROTEAMENTO PARA DISTRIBUIÇÃO DE
CARGA EM REDES DE TELECOMUNICAÇÕES

SANTOS/SP

2017

ALESSANDRO DE LIMA MARREIRO

**APLICAÇÃO DA LÓGICA PARACONSISTENTE ANOTADA EVIDENCIAL E COM
ALGORITMO ADAPTATIVO DE ROTEAMENTO PARA DISTRIBUIÇÃO DE
CARGA EM REDES DE TELECOMUNICAÇÕES**

Dissertação apresentada a Universidade Santa Cecília como parte dos requisitos para obtenção de título de mestre no Programa de Pós-Graduação em Engenharia Mecânica, sob a orientação do Prof. Dr. Cláudio Rodrigo Torres.

SANTOS/SP

2017

Autorizo a reprodução parcial ou total deste trabalho, por qualquer que seja o processo, exclusivamente para fins acadêmicos e científicos.

511.31

M324a Marreiro, Alessandro de Lima.

Aplicação da lógica paraconsistente anotada evidencial Et com algoritmo adaptativo de roteamento para distribuição de carga em redes de telecomunicações.

Alessandro de Lima Marreiro - 2017.
138 p.

Orientador: Prof. Dr. Cláudio Rodrigo Torres

Dissertação (Mestrado) - Universidade Santa Cecília, Programa de Pós-Graduação em Engenharia Mecânica, Santos, SP, 2017.

1. Lógica Paraconsistente Anotada. 2. Sistema de Controle. 3. Sistema Inteligente. 4. Algoritmos Adaptativos. 5. Rede Neural Artificial Paraconsistente.

I. Torres, Cláudio Rodrigo.

II Aplicação da lógica paraconsistente anotada evidencial Et com algoritmo adaptativo de roteamento para distribuição de carga em redes de telecomunicações.

Elaborada pelo SIBi – Sistema Integrado de Bibliotecas – Unisanta

DEDICATÓRIA

Dedico este trabalho a todos aqueles que acreditam em seus sonhos e naqueles que estão ao seu lado para ajudar a realizá-los.

AGRADECIMENTOS

A meu orientador Sr. Cláudio Rodrigo Torres, por seus direcionamentos, recomendações e retorno às dúvidas, sempre com cordialidade e companheirismo em nossas discussões sobre o desenvolvimento do trabalho.

A Universidade Santa Cecília, UNISANTA, representada pelo Sr. Marcos Tadeu Tavares Pacheco Coordenador Geral da Pós-Graduação - Stricto Sensu.

Ao Sr. João Inácio da Silva Filho, com o ensino da Lógica Paraconsistente que permitiu a compreensão de sua aplicabilidade em várias áreas de conhecimento.

A minha família pelo amor, apoio e força, acreditando em meu potencial para continuar seguindo em frente na incessante busca pelo conhecimento.

Ao saudoso amigo Nilson Magalhães Bueno, por seu incentivo e apoio para o ingresso no programa de Mestrado.

Aos colegas mestrandos da UNISANTA, pelos momentos de convívio e de colaboração mútua na busca dos objetivos acadêmicos.

A todo corpo docente do programa de Mestrado, que sabiamente contribuíram para minha formação e a equipe da secretaria, especialmente a Sra. Sandra e Sra. Imaculada, pelo respeito, profissionalismo e atenção durante todo o Mestrado.

RESUMO

Neste trabalho emprega-se a Lógica Paraconsistente Anotada Evidencial E_{τ} na construção e no estudo de um sistema inteligente utilizando sensores de desempenho existentes em equipamentos de interconexão. Esse sistema possui a função de identificar um ambiente com degradação de desempenho na transmissão entre dispositivos que se comunicam em uma rede de dados. As informações coletadas desses sensores são processadas de acordo com um algoritmo Para analisador distribuído em uma rede de análise paraconsistente, que possui sua estrutura baseada na Lógica Paraconsistente Anotada Evidencial E_{τ} , que permite reconhecer e interpretar dados contraditórios, incertos, e paracompletos sem trivialização. Os temas desenvolvidos neste trabalho sugerem sua aplicabilidade em ambientes de rede que fazem uso ou não de protocolos de roteamento com algoritmos adaptativos, por exemplo, em redes metropolitanas onde o fator desempenho e confiabilidade são fundamentais.

Palavras Chave: Lógica Paraconsistente Anotada. Sistema de Controle. Sistema Inteligente. Algoritmos adaptativos. Rede Neural Artificial Paraconsistente.

ABSTRACT

In this work we use the Paraconsistent Annotated Evidential Logic E_{τ} in the construction and study of an intelligent system using existing performance sensors in interconnection equipment. This system has the function of identifying an environment with degraded performance in the transmission between devices that communicate in a data network. The information collected from these sensors is processed according to an analyzer algorithm distributed in a paraconsistent analysis network, which has its structure based on the Paraconsistent Annotated Evidential Logic E_{τ} , which allows to recognize and interpret contradictory, uncertain, and paracomplete data without trivialization. The themes developed in this work suggest its applicability in network environments that make use of routing protocols with adaptive algorithms, for example, in metropolitan networks where the performance and reliability factor are fundamental.

Keywords: Paraconsistent Annotated Logic. Control System. Intelligent System. Adaptive Algorithms. Paraconsistent Analysis Neural Artificial Network.

LISTA DE ILUSTRAÇÕES

Figura 1 - Classificação de algumas lógicas.	24
Figura 2 - Reticulado finito de “quatro estados”	26
Figura 3 - O extremo estado da lógica.	28
Figura 4 - O não extremo dos estados lógicos.	29
Figura 5 - Reticulado finito de Hasse com anotações da LPA2v.....	31
Figura 6 - Representação dos Graus de Certeza e de Contradição.....	32
Figura 7 - Representação do grau de certeza.	33
Figura 8 - Representação do grau de contradição.	34
Figura 9 - Ponto de interpolação (G_c , G_{ct}) e distância D	35
Figura 10 - Grau de Certeza de valor resultante real - G_{cr} no reticulado.	36
Figura 11 - Grau de Certeza de valor real G_{cr} no reticulado da LPA2v quando G_c é negativo e G_{ct} positivo.	37
Figura 12 - Símbolo de um Nó de Análise Paraconsistente típico.....	38
Figura 13 - Conversão de Grau de Certeza real G_{cr} em Grau de Evidência resultante real μ_{ER}	39
Figura 14 - Conversão de Grau de Contradição G_{ct} em Grau de Contradição normalizado μ_{ctr}	40
Figura 15 - Símbolo do Algoritmo Paraconsistente Extrator de efeitos da Contradição.....	43
Figura 16 - Rede de Análise Paraconsistente em Configuração Simples.	46
Figura 17 - Mapa da área de atuação das entidades RIRs.	48
Figura 18 - Classificação dos Protocolos de Roteamento dinâmico.....	50
Figura 19 - Decisão de encaminhamento do datagrama no equipamento de interconexão.....	51
Figura 20 - Exemplo de tabelas de roteamento em equipamentos de interconexão.	52
Figura 21 - Protocolos de roteamento IGP em relação à EGP.....	53
Figura 22 - Ramificação SMLv1.	58
Figura 23 - Ramificação SMLv2.	60
Figura 24: <i>Round Trip Time</i>	64
Figura 25 - Variação no atraso (<i>Jitter</i>) e compensação no receptor.....	66
Figura 26 - Componentes do IP SLA.....	67

Figura 27 - Funcionamento Cisco IP SLA.	68
Figura 28 - Diagrama em blocos do Sistema especialista de gerenciamento usando Lógica Paraconsistente Evidencial $E\tau$	72
Figura 29 - Controlador Paraconsistente.....	73
Figura 30 - <i>Interface</i> do Sistema Especialista SharpNet ParaControl.	75
Figura 31 - Fonte de pesquisa da estrutura de conexões: nó inicial de rede.	75
Figura 32 - Módulo Registrador - Painel de rotas e <i>interfaces</i> dos equipamentos. ...	76
Figura 33 - Módulo Registrador - Painel gráfico com as conexões existentes entre os equipamentos.....	76
Figura 34 - Seleção da rota para a rede destino a ser analisada pelo sistema especialista.....	77
Figura 35 - Indicação da rota selecionada no Painel gráfico.....	77
Figura 36 - Módulo Monitor efetuando coleta em tempo real e ativando a análise paraconsistente.	78
Figura 37 - Função de exportação dos dados em formato de planilha e sua exibição.	78
Figura 38 - Ambiente avaliado com roteamento de rede por rotas distintas.	81
Figura 39 - Roteadores instalados na rede piloto.....	82
Figura 40 - Comutadores de rede instalados na rede piloto.....	82
Figura 41 - Confirmação da rota entre a rede de origem e destino (ensaio 01).	92
Figura 42 - Confirmação da rota entre a rede de origem e destino (ensaio 02).	98
Figura 43 - Confirmação da nova rota entre a rede de origem e destino (ensaio 02).	108

LISTA DE GRÁFICOS

Gráfico 1: Valoração do Grau de Evidência com variação linear e diretamente proporcional a grandeza medida.	85
Gráfico 2 - Grandeza da fonte de informação – Variação no atraso de transmissão origem/destino (JSD) - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.....	87
Gráfico 3 - Grandeza da fonte de informação – Variação no atraso de transmissão destino/origem (JDS) - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.....	87
Gráfico 4 - Grandeza da fonte de informação – Latência Total/RTT - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.	88
Gráfico 5 - Grandeza da fonte de informação – Consumo de Processamento/CPU - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.	88
Gráfico 6 - Grandeza da fonte de informação – Perda de Pacotes – variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado	89

LISTA DE QUADROS

Quadro 1 - Tipo de dados SMIv1	59
Quadro 2 - Requerimentos e métricas para monitorar operações IP SLA	69
Quadro 3 - Comandos de configuração e ativação da operação IP SLA	81
Quadro 4 – Configuração dos equipamentos: ERS SITE 1 e 2.....	116
Quadro 5 – Configuração dos equipamentos: PC-1 / 2 / 3 / 4.....	117
Quadro 6 - Configuração dos equipamentos: CE-1A e CE - 1B.....	118
Quadro 7 - Configuração dos equipamentos: PE-1A e PE-1B	119
Quadro 8 - Configuração dos equipamentos: CEA-2A e CE-2B	119
Quadro 9 - Configuração dos equipamentos: PE-2A e PE-2B	120

LISTA DE TABELAS

Tabela 1 - Vazão máxima para diferentes tipos de pacotes.....	61
Tabela 2 - Vazão máxima para diferentes tipos de pacotes.....	62
Tabela 3 - Vazão máxima para diferentes tipos de pacotes.....	62
Tabela 4 - Limite de desempenho recomendado.	70
Tabela 5 - Valores para definições de métricas	80
Tabela 6 - Endereçamento da localidade 01 da rede piloto.	83
Tabela 7 - Endereçamento da localidade 01 da rede piloto.	83
Tabela 8 - Endereçamento da rota A da rede piloto.....	83
Tabela 9 - Endereçamento da rota B da rede piloto.....	84
Tabela 10 - Característica da análise do grau de evidência resultante obtido na saída do algoritmo.....	90
Tabela 11 – 1ª Leitura da rota selecionada no ensaio 01.....	93
Tabela 12 – 2ª Leitura da rota selecionada no ensaio 01.....	93
Tabela 13 – 3ª Leitura da rota selecionada no ensaio 01.....	94
Tabela 14 – 4ª Leitura da rota selecionada no ensaio 01.....	94
Tabela 15 – 5ª Leitura da rota selecionada no ensaio 01.....	94
Tabela 16 – 6ª Leitura da rota selecionada no ensaio 01.....	95
Tabela 17 – 7ª Leitura da rota selecionada no ensaio 01.....	95
Tabela 18 – 8ª Leitura da rota selecionada no ensaio 01.....	95
Tabela 19 – 9ª Leitura da rota selecionada no ensaio 01.....	96
Tabela 20 – 10ª Leitura da rota selecionada no ensaio 01.....	96
Tabela 21 – Algoritmo ParaExtractor aplicado às evidências da rota selecionada no ensaio 01.....	96
Tabela 22 – 1ª Leitura da rota selecionada no ensaio 02.....	99
Tabela 23 – 2ª Leitura da rota selecionada no ensaio 02.....	99
Tabela 24 – 3ª Leitura da rota selecionada no ensaio 02.....	100
Tabela 25 – 4ª Leitura da rota selecionada no ensaio 02.....	100
Tabela 26 – 5ª Leitura da rota selecionada no ensaio 02.....	100
Tabela 27 – 6ª Leitura da rota selecionada no ensaio 02.....	101
Tabela 28 – 7ª Leitura da rota selecionada no ensaio 02.....	101
Tabela 29 – 8ª Leitura da rota selecionada no ensaio 02.....	101

Tabela 30 – 9ª Leitura da rota selecionada no ensaio 02.....	102
Tabela 31 – 10ª Leitura da rota selecionada no ensaio 02.....	102
Tabela 32 – Algoritmo ParaExtrator aplicado às evidências da rota selecionada no ensaio 02.....	102
Tabela 33 – 1ª Leitura da rota alternativa selecionada no ensaio 02.	103
Tabela 34 – 2ª Leitura da rota alternativa selecionada no ensaio 02.	104
Tabela 35 – 3ª Leitura da rota alternativa selecionada no ensaio 02.	104
Tabela 36 – 4ª Leitura da rota alternativa selecionada no ensaio 02.	104
Tabela 37 – 5ª Leitura da rota alternativa selecionada no ensaio 02.	105
Tabela 38 – 6ª Leitura da rota alternativa selecionada no ensaio 02.	105
Tabela 39 – 7ª Leitura da rota alternativa selecionada no ensaio 02.	105
Tabela 40 – 8ª Leitura da rota alternativa selecionada no ensaio 02.	106
Tabela 41 – 9ª Leitura da rota alternativa selecionada no ensaio 02.	106
Tabela 42 – 10ª Leitura da rota alternativa selecionada no ensaio 02.	106
Tabela 43 – Algoritmo ParaExtrator aplicado às evidências da rota alternativa selecionada no ensaio 02.....	107

LISTA DE ABREVIATURAS E SIGLAS

ANS	Acordo de Nível de Serviço
BGP	<i>Border Gateway Protocol</i>
EGP	<i>Exterior Gateway Protocol</i>
EIGRP	<i>Enhanced Interior Gateway Routing Protocol</i>
ICMP	<i>Internet Control Message Protocol</i>
IGP	<i>Interior Gateway Protocol</i>
IP	<i>Internet Protocol</i>
IS-IS	<i>Intermediate System-to-Intermediate System</i>
LP	Lógica Paraconsistente
LPA	Lógica Paraconsistente Anotada
LPA2v	Lógica Paraconsistente Anotada com anotação de 2 valores
LSC	Limite Superior de Controle
LSE	Limite Superior de Especificação
MAN	<i>Metropolitan Area Network</i>
OSPF	<i>Open Shortest Path First</i>
PDU	<i>Protocol Data Unit</i>
QOS	<i>Quality of Service</i>
RAP	Redes de Análise Paraconsistente
RIP	<i>Routing Information Protocol</i>
RNA	Rede Neural Artificial
RNAP	Rede Neural Artificial Paraconsistente
RTP	<i>Real Time Protocol</i>
SLA	<i>Service Level Agreement</i>
SNMP	<i>Simple Network Management Protocol</i>
TCP	<i>Transmission Control Protocol</i>
UDP	<i>User Datagram Protocol</i>
VoIP	<i>Voice over Internet Protocol</i>
WAN	<i>Wide Area Network</i>

LISTA DE SÍMBOLOS

τ	Reticulado finito
$\sim$	Operador de negação
μ	Grau de crença (ou de evidência favorável)
λ	Grau de descrença (ou evidência desfavorável)
$\mathbb{R}$	Conjunto dos números reais
F	Falso
T	Inconsistente
V	Verdadeiro
$\perp$	Paracompleto ou Indeterminado
p_T	Conotação de Inconsistente à proposição p
p_1	Conotação de Verdade à proposição p
p_0	Conotação de Falsidade à proposição p
$p_\perp$	Conotação de Paracompleteza à proposição p
P_μ	Sentença proposicional
QUPC	Quadrado Unitário no Plano Cartesiano
G_C	Grau de Certeza
G_{CR}	Grau de Certeza real
G_{CT}	Grau de Contradição
p	Proposição Inicial
q	Proposição q
V_{icc}	Valor limite inferior de Controle de certeza
V_{ici}	Valor limite inferior de Controle de incerteza
S1	Saída discreta
$G_{cmáxV}$	Valor máximo para um estado lógico de Verdade
$G_{cmáxF}$	Valor máximo para um estado lógico de Falsidade
φ	Intervalo de certeza
$(\pm)$	Intervalo de Certeza sinalizado
φ_E	Intervalo De Evidência Resultante
$(\oplus)$	Intervalo De Evidência Resultante Sinalizado

SUMÁRIO

1.	INTRODUÇÃO.....	18
1.1	OBJETIVO.....	19
1.2	OBJETIVOS ESPECÍFICOS.....	19
1.3	JUSTIFICATIVA E RELEVÂNCIA DO TEMA.....	19
1.4	ORGANIZAÇÃO DA DISSERTAÇÃO.....	20
2.	FUNDAMENTAÇÃO TEÓRICA.....	22
2.1	APLICAÇÃO DA LÓGICA.....	22
2.1.1	A LÓGICA CLÁSSICA.....	22
2.1.2	A LÓGICA PARACONSISTENTE.....	25
2.1.3	LÓGICA PARACONSISTENTE ANOTADA.....	26
2.1.4	LÓGICA PARACONSISTENTE EVIDENCIAL E_{τ}	27
2.1.5	LÓGICA PARACONSISTENTE ANOTADA DE DOIS VALORES.....	30
2.1.6	GRAU DE CERTEZA E DE CONTRADIÇÃO.....	32
2.1.7	GRAU DE CERTEZA DE VALOR REAL.....	34
2.1.8	NÓ DE ANÁLISE PARACONSISTENTE (NAP).....	38
2.1.9	GRAU DE EVIDÊNCIA RESULTANTE REAL.....	39
2.1.10	GRAU DE CONTRADIÇÃO NORMALIZADO.....	40
2.2.11	NÓ DE ANÁLISE PARACONSISTENTE DA LPA2V COM SAÍDA DE GRAU DE EVIDÊNCIA RESULTANTE REAL.....	41
2.2.12	ALGORITMO PARACONSISTENTE EXTRATOR DE EFEITOS DA CONTRADIÇÃO.....	43
2.1.13	REDES DE ANÁLISE PARACONSISTENTE – RAP.....	45
2.2	INTERCONEXÃO DE REDES DE COMPUTADORES.....	47
2.2.1	A REDE DO PROTOCOLO DE <i>INTERNET</i> – REDE IP.....	48
2.2.2	SISTEMAS AUTÔNOMOS.....	48
2.2.3	CARACTERIZAÇÃO E CLASSIFICAÇÃO DOS PROTOCOLOS DE ROTEAMENTO.....	49
2.2.4	ROTEAMENTO INTERNO.....	52
2.2.5	ROTEAMENTO EXTERNO.....	53
2.2.6	PROTOCOLO BGP – <i>BORDER GATEWAY PROTOCOL</i>	53

2.2.7 PROTOCOLO SNMP – <i>SIMPLE NETWORK MANAGEMENT PROTOCOL</i>	54
2.2.8 SNMPV1	55
2.2.9 SNMPV2	56
2.2.10 MIB – <i>MANAGEMENT INFORMATION BASE</i>	57
2.3 TELECOMUNICAÇÕES: MÉTRICAS DE DESEMPENHO E QUALIDADE	60
2.3.1 LARGURA DE BANDA DE VAZÃO	61
2.3.2 PERDA DE PACOTES	63
2.3.3 LATÊNCIA	64
2.3.4 VARIAÇÃO DE ATRASO (<i>JITTER</i>)	65
2.3.5 CISCO IP SLA® - <i>IP SERVICE LEVEL AGREEMENT</i>	66
2.3.6 COMPONENTES DO IP SLA	67
2.3.7 OPERAÇÕES SUPOSTAS PELO IP SLA	69
3. MATERIAIS E MÉTODOS	71
3.1 DESENVOLVIMENTO DO SISTEMA ESPECIALISTA PARA CONSISTENTE “SHARPNET PARA CONTROL”	71
3.1.1 FUNDAMENTO BÁSICO DO CONTROLADOR PARA CONSISTENTE	72
3.1.2 <i>INTERFACE</i> DO SISTEMA E SUAS FUNCIONALIDADES	74
3.2 VALORES PARA DEFINIÇÃO DE MÉTRICAS	79
4. RESULTADOS E DISCUSSÃO	92
5. CONCLUSÃO	110
5.1 TRABALHOS FUTUROS	110
REFERÊNCIAS	112
APÊNDICE A – COMANDOS DE CONFIGURAÇÃO DOS EQUIPAMENTOS DE REDE	116
APÊNDICE B – ALGORITMO DE EXTRAÇÃO DAS ROTAS DOS EQUIPAMENTOS DE INTERCONEXÃO	121
APÊNDICE D – ALGORITMO EXTRATOR DE EFEITOS DA CONTRADIÇÃO	128
APÊNDICE E – ALGORITMO NÓ DE ANÁLISE PARA CONSISTENTE – NAP	130
APÊNDICE F – ALGORITMO DE NORMALIZAÇÃO DA FONTE DE INFORMAÇÃO	133
APÊNDICE G – ALGORITMO DE EXPORTAÇÃO DOS DADOS EM FORMATO DE PLANILHA	134

1. INTRODUÇÃO

As formas e alternativas que envolvem a monitoração e o controle de máquinas, válvulas, grupos de instrumentos e sensores eletromecânicos à longa distância passam por processos que nos remetem diretamente às redes de telecomunicações. Suas condições de operação como padrão de tráfego, topologia, nível de carga e capacidade de vazão, sofrem diversas alterações ao longo do tempo, muitas não previstas, elevando a complexidade e dinamismo do ambiente.

Diante desse contexto, o uso de algoritmos adaptativos proporciona características fundamentais para a transmissão entre elementos comunicadores: resiliência dos enlaces de comunicação bem como a não necessidade de intervenção direta do administrador da rede para reestabelecimento da comunicação como acontece em ocorrências de falha usando algoritmos não adaptativos.

O grande obstáculo encontrado por estes algoritmos adaptativos aplicados em roteamento consiste na adaptação veloz e eficaz a mudanças nas condições de operações da rede em cenários de intermitência da indisponibilidade simultânea de um percentual grande de enlaces ou de sua degradação/saturação.

No mundo real, as contradições e inconsistências proporcionadas por degradações ou saturações de meios físicos são comuns, entretanto a maioria dos sistemas especialistas de roteamento baseia-se em lógica clássica binária para tomada de decisão (DA SILVA FILHO, 1997). Nesse mesmo contexto percebe-se que a qualidade de serviço para aplicações em rede, favorece o uso de sistemas de gerenciamento baseados em políticas capazes de interpretar o grau de exigência da aplicação e traduzi-las para uma distribuição inteligente de tráfego entre os diversos caminhos disponíveis. É desenvolvido nesse estudo, um sistema controlador que analisará o desempenho dos enlaces que compõem uma rota de comunicação, empregando a Lógica evidencial E_{τ} fazendo-se uso do algoritmo para-extrator para alcance dos resultados esperados, permitindo o aproveitamento da disponibilidade dos enlaces de comunicação entre as redes de origem e destino considerando políticas de tráfego e degradações dos meios de comunicação. Assim, este se apresenta como o principal aspecto a ser considerado nesse trabalho.

1.1 OBJETIVO

Esta pesquisa apresenta, como objetivo principal, encontrar novas formas de distribuir de maneira eficiente o tráfego de aplicações entre redes de computadores, em especial a comunicação entre estações de operação e grupos de controladores e acionadores de válvulas e instrumentos, localizados em domínios administrativos diferentes interligados por enlaces redundantes de telecomunicações que se utilizam do protocolo BGP (*Border Gateway Protocol*), aplicando algoritmos estruturados em Lógica Paraconsistente Anotada Evidencial E_{τ} .

1.2 OBJETIVOS ESPECÍFICOS

Extrair as informações do ambiente para popular a base de dados de informações.

Criar nós de análise paraconsistente para formatar o algoritmo de melhor forma para direcionar o tráfego.

Gerar entrada do algoritmo com as informações relevantes que justificam a contradição necessária para a análise paraconsistente.

1.3 JUSTIFICATIVA E RELEVÂNCIA DO TEMA

Os provedores de interconexão de redes estão cada vez mais preocupados em analisar, de forma crítica, qualquer aspecto que possa estar relacionado ao ambiente operacional do seu *backbone*. Sua procura por oportunidades de crescimento e otimização de recursos com custo minimizado para atender os níveis minimamente desejáveis dos serviços solicitados com relação a: atrasos máximos, *jitter*, capacidade da conexão (banda), disponibilidade e perda de pacotes. Assim, busca-se garantir a eficiência no caminho entre origem e destino do tráfego de pacotes na rede.

A eficiência do roteamento é uma componente chave do sucesso ou da falha final de uma rede de telecomunicações. Muitos pedidos de conexões podem ser aceitos, mesmo sendo a rede incapaz de suportar o atendimento desses pedidos. Isto pode resultar em uma significativa degradação do desempenho. Entretanto, se utilizado uma proposta parametrizada em qualidade de serviço pode-se providenciar um algoritmo capaz de identificar tais caminhos que possam ou não atender ao direcionamento do tráfego para os quais a rede suporte.

O Roteamento com foco em restrições tem sido tema de diversas pesquisas (YANG et al., 2003), (MASIP-BRUIN et al., 2003). O estado da arte de roteamento em telecomunicações tem seu apontamento na busca do melhor caminho de uma rede e do tempo necessário para percorrê-lo (KUIPERS et al., 2002).

O roteamento baseado na qualidade de serviço (QoS - *Quality of Service*) pode ser classificado em três principais classes: otimização do enlace, restrição no enlace e otimização do caminho (CHEN e NAHRSTEDT, 1998) (MASIP-BRUIN et al., 2003). Os roteamentos, com foco no enlace, usam funções custo que estimam a ocupação da banda ou do buffer (FORTZ e THORUP, 2002). As técnicas de roteamento que consideram o caminho usam métricas aditivas, tais como o tempo de transferência.

1.4 ORGANIZAÇÃO DA DISSERTAÇÃO

Esta dissertação está organizada da seguinte forma:

Na apresentação é introduzido um breve histórico e destacada a importância do melhor aproveitamento do uso de enlaces redundantes. No capítulo 1 são apresentados os objetivos do trabalho, a justificativa e relevância do tema. No capítulo 2 é feita a fundamentação teórica dos principais conceitos aplicados no desenvolvimento desse projeto. No capítulo 3 desenvolve-se a estrutura da aplicação objeto do projeto bem como seus detalhes por funções.

O capítulo 4 apresenta os resultados e discussões iniciando-se pelos

procedimentos para obtenção dos valores estudados. Estes resultados são os valores obtidos através de um procedimento de coleta de informações dos equipamentos bem como os valores calculados após a aplicação do algoritmo desenvolvido. São discutidos os resultados finais para a tomada de decisão. Por fim, são apresentadas as conclusões e algumas sugestões para novas pesquisas.

2. FUNDAMENTAÇÃO TEÓRICA

Retrataremos neste capítulo, algumas observações sobre interconexão entre localidades através de roteamento em redes de computadores e as justificativas relevantes da Lógica Paraconsistente. Estas observações são precisas para uma total percepção sobre o estudo elaborado utilizando definições da LPA (Lógica Paraconsistente Anotada) para distribuição de carga entre enlaces de comunicação de dados.

2.1 APLICAÇÃO DA LÓGICA

2.1.1 A LÓGICA CLÁSSICA

A Lógica Clássica é considerada a base das teorias científicas o que torna, na grande maioria dos equipamentos como computadores, suas definições uma fundação em seu funcionamento. A lógica Clássica ou Lógica Aristotélica, foi desenvolvida, ao que tudo indica, pelo grego e filósofo Aristóteles (384-322 a.C) e colaboradores, como uma ferramenta para averiguar a veracidade ou não dos raciocínios (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

A Lógica Clássica compreende apenas dois estados: o “verdadeiro” que equivale ao valor 1 ou “falso” que equivale ao valor 0 e dentre seus princípios mais conhecidos estão:

1. **Princípio da Identidade:** $x = x$, ou seja, todo objeto é idêntico a si mesmo;
2. **Princípio do Terceiro Excluído:** $p \vee \neg p$, ou seja, de duas proposições contraditórias (tais que uma é a negação da outra), uma é verdadeira;
3. **Princípio da Não-Contradição:** $\neg(p \wedge \neg p)$, ou seja, entre duas proposições contraditórias, uma é falsa.
4. **Princípio da Identidade Proposicional:** $p \rightarrow p$

O nível de importância da Lógica Aristotélica é considerado elevado, pois as

áreas da tecnologia se amparam nesse princípio. No entanto, os avanços que foram mostrados pelas novas tecnologias, apresentaram uma criação distinta das condições limitadas para a caracterização do conteúdo de onde é viável obter as informações de alto valor em seu ambiente.

Ter o conhecimento dessas informações é fundamental para o momento de agir e controlar os reais cenários. Mesmo observando-se que a lógica Clássica possui grande eficiência, a tecnologia juntamente com seus avanços fez com que faixas de irresoluções ficassem menores através da exigência cada vez mais precisas (DA SILVA FILHO, ABE E LAMBERT-TORRES, 2008).

Para Aristóteles, a Lógica deveria fornecer os instrumentos mentais necessários para enfatizar qualquer tipo de investigação. Mais ainda, deveria explicar o método pelo qual, partindo de uma determinada conclusão, resolve-se precisamente nos elementos dos quais deriva, ou seja, nas premissas e nos elementos de que brota, e assim fica fundamentada e justificada. Tanto que, ele foi o primeiro sábio a notar que certos raciocínios são corretos em virtude unicamente da sua forma (FIGUEIREDO CHAGAS, 2004).

Ao longo do tempo, esses fatores foram apresentando possibilidades que não se encaixam nas regras da Lógica Aristotélica, requerendo técnicas relevantes para a abordagem das informações nessas situações sobre o ambiente.

Em busca de novas formas de tratamento da informação nas situações limites referendadas, criaram-se as lógicas não clássicas. Dessa forma as lógicas não clássicas possuem de certa forma em seus fundamentos, conceitos que desconsideram alguns inflexíveis princípios contidos nas leis binárias da lógica clássica.

As Lógicas não Clássicas violam justamente as suposições binárias que não admitem indefinições, ambiguidades e contradições nos seus fundamentos. Estabelece que o conceito de dualidade é algo que pode coexistir com seu oposto para se obter melhor precisão nas conclusões para a tomada de decisão. As Lógicas não Clássicas podem complementar o escopo da lógica clássica ou podem rivalizar com ela (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Devido a Lógica Clássica ser do tipo binária onde são permitidos somente dois estados do tipo falso ou verdadeiro (valores 1 ou 0), em alguns momentos não corresponde um resultado aceitável da realidade o que se torna inconcluso e

de difícil utilização. Por conta desse fator, houve o surgimento de outras lógicas nas quais são ditas como lógicas não clássicas que são apropriadas para aplicações com uma ampla área de conhecimento.

Diversas lógicas foram desenvolvidas (figura 1), visando complementar a Lógica Clássica tradicional e, até mesmo, derrogar alguns de seus princípios fundamentais.

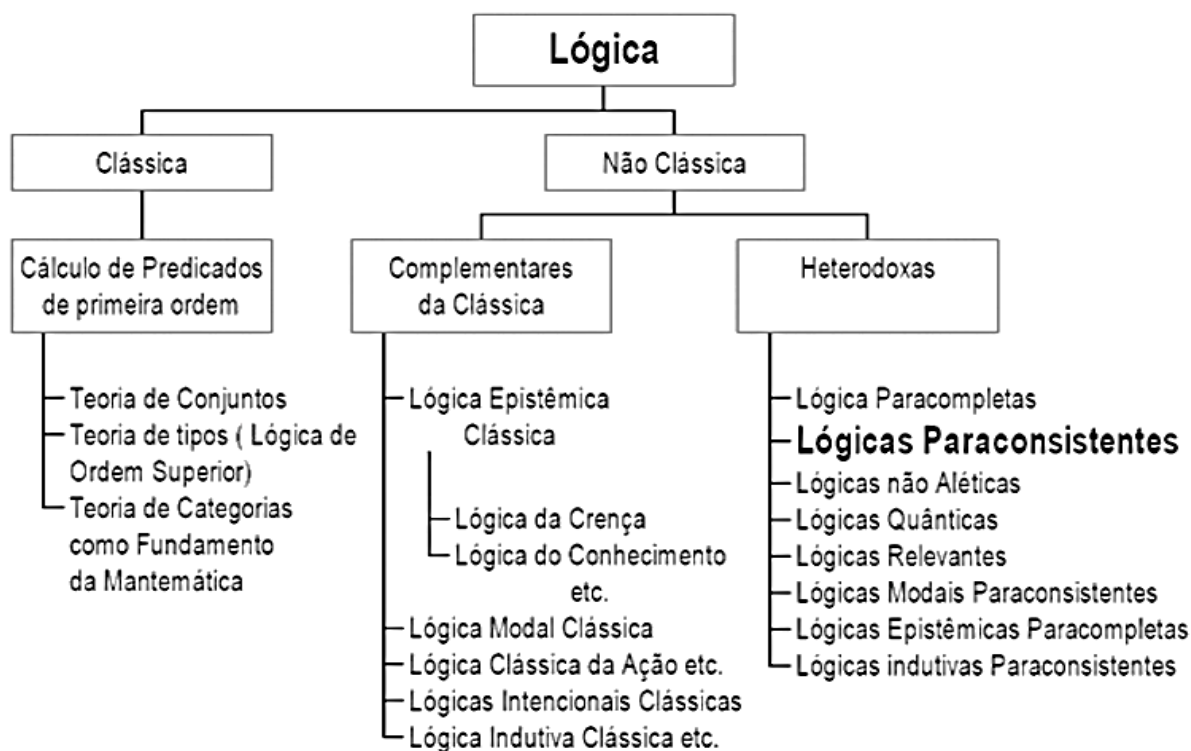


Figura 1 - Classificação de algumas lógicas.

Fonte: (CUNHA et al., 2017).

Entre essas lógicas encontra-se a Lógica Paraconsistente, que visa, entre outras coisas, oferecer alternativas aos princípios clássicos do Terceiro Excluído e da Não Contradição, insuficientes para tratar proposições cuja conclusão seja de valores diferentes de Verdadeiro e Falso.

Algumas áreas de conhecimento, como filosofia, inteligência artificial, robótica e sistemas especialistas estudam Lógica Paraconsistente, pois em suas aplicações são constantes as incertezas e as inconsistências.

2.1.2 A LÓGICA PARACONSISTENTE

Dentro das Lógicas Não-Clássicas, foram criadas suas ramificações que tem como principal fundamento a revogação do princípio do terceiro excluído, portanto, a Lógica Paraconsistente é uma Lógica Não-Clássica que anula o princípio da não contradição e assume o tratamento de sinais contraditórios em sua teoria.

A Lógica Paraconsistente teve seu início através do polonês Jean Lukasiewicz (1876-1956) e no russo Nicolai. A. Vasilév (1880-1940) por volta de 1910 onde sugeriram uma lógica que delimitaria o princípio da contradição. O primeiro a estruturar um cálculo proposicional paraconsistente foi o polonês S. Jaskowski (1906-1965), discípulo de Lukasiewicz, que em 1948 publicou suas ideias sobre lógica e contradição, mostrando como se poderia construir um cálculo sentencial paraconsistente, possuindo motivação conveniente.

O sistema de Jaskowski, nomeado por ele de lógica discursiva, desenvolveu-se posteriormente (a partir de 1968) em virtude das obras de autores como J. Kotas, L. Furmanowski, L. Dubikajtis, Newton Carneiro Affonso da Costa (1929-) e C. Pinter. Assim, chegou-se a edificar uma verdadeira lógica discursiva, englobando um cálculo de predicados de primeira ordem e uma lógica de ordem superior (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

A expressão “Paraconsistente” foi criada em 1976 pelo filósofo peruano Francisco Miró Quesada em uma correspondência com Newton C.A. da Costa e significa “ao lado da consistência” (COSTA e KRAUSE, 2004).

Os princípios que dão sustentação a Lógica Paraconsistente apresentam-se da seguinte maneira:

Diz que a linguagem é trivial quando as sentenças feitas em sua linguagem forem teoremas e por sua vez mostrados em teoria como verdadeiro. Uma teoria é considerada consistente quando não existe entre os teoremas algo que afirme que seja a negação de outros teoremas que fazem parte da teoria. Uma vez ocorrido, a teoria passa a se chamar de inconsistente.

Uma teoria T e uma lógica L são ditas como inconsistentes se entre os teoremas não houver um que anule o outro. A teoria T é denominada trivial se todas as fórmulas que forem fechadas forem teoremas e caso não ocorra T é não trivial.

Caso L seja uma lógica comum, a teoria T é trivial apenas se for inconsistente. Em lógicas desse tipo permanecem o conceito de inconsistência e trivialidade porque, segundo a Lógica Clássica, uma teoria inconsistente é trivial, pois se forem válidas então qualquer conclusão é viável (ABE, 2014). Como esse resultado não é bom, a lógica clássica não aceita contradição sem tornar trivial.

A lógica L é dita como Paraconsistente se trabalhar como causa de teoria inconsistente e não triviais. O significado é que é possível manejar sistemas inconsistentes sem correr o risco de trivialização (DA SILVA FILHO, ABE E LAMBERT-TORRES, 2008).

A Lógica Paraconsistente é considerada como uma lógica não clássica que mostra em seus fundamentos a particularidade de admitir a contradição sem trivialização, logo, sem que o conflito ocorrido pela inconsistência invalide as conclusões (SOUZA, ABE e DA SILVA, 2005).

2.1.3 LÓGICA PARACONSISTENTE ANOTADA

As fórmulas proposicionais na Lógica Paraconsistente Anotada (LPA) vem seguida de anotações onde cada uma delas faz parte de um reticulado finito τ , onde se atribui valores que condizem à sua formula proposicional.

Uma LPA pode ter um reticulado finito de “quatro estados”, de acordo com a figura 2.

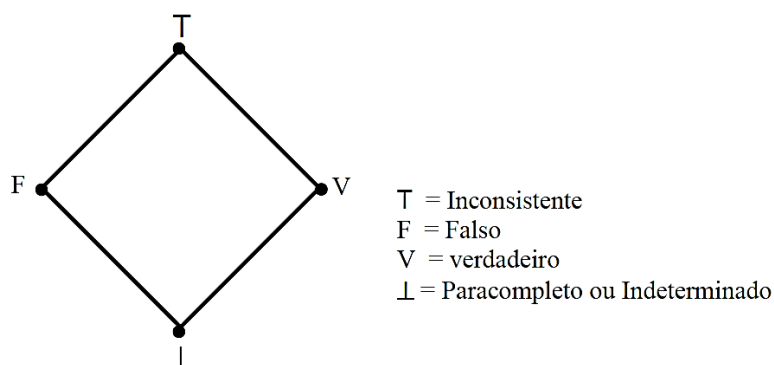


Figura 2 - Reticulado finito de “quatro estados”.

Fonte: (DA SILVA FILHO, 2006).

Na Lógica Paraconsistente Anotada leva-se em consideração um operador $\sim$: $|\tau| \rightarrow |\tau|$ que se diz a negação da LPA e nessa situação determina-se como (DA SILVA FILHO, 2006): $\sim(1) = 0$, $\sim(0) = 1$, $\sim(T) = T$ e $\sim(\perp) = \perp$

Denominamos cada sentença proposicional como proposição.

A fórmula atômica $P\mu$ pode ser lida como: “*creio na proposição p com grau de crença (ou de evidência) de no máximo μ , ou até μ ($\leq \mu$)*” (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008). O grau de evidência é considerado como uma constante anotacional do reticulado. Dessa forma, podemos afirmar que cada grau evidência atribuído à proposição é um valor que está no conjunto de valores composto pelas constantes anotacionais do reticulado $\{T, V, F, \perp\}$ (DA SILVA FILHO, 2006).

A proposição acompanha-se de anotações ou graus de evidência que atribuem conotação lógica a proposição, isto determina uma leitura que segue abaixo e correspondente a cada variável proposicional (DA SILVA FILHO, 2006).

pT = A anotação ou grau de evidência atribui uma conotação de Inconsistente à proposição p .

$p1$ = A anotação ou grau de evidência atribui uma conotação de Verdade à proposição p .

$p0$ = A anotação ou grau de evidência atribui uma conotação de Falsidade à proposição p .

$p\perp$ = A anotação ou grau de evidência atribui uma conotação de Indefinição à proposição p .

2.1.4 LÓGICA PARACONSISTENTE EVIDENCIAL E_τ

A Lógica Paraconsistente Evidencial E_τ é uma área da Lógica Paraconsistente que lida com o conceito de contradição sem trivialização. A Evidencial E_τ é composta por proposições no sentido p ligados à constantes de anotação: (μ, λ) onde $\mu, \lambda \in [0,1]$ (intervalo unitário real) (TORRES et al., 2011). Dessa maneira, uma fórmula atômica Evidencial é da forma $p(\mu, \lambda)$ que pode ser

visto como: a evidência a favor, expressada por p é μ e a prova oposta expressa por p é λ .

O grau de Evidência Favorável (μ) é um valor que representa a evidência favorável onde a sentença é verdadeira e está entre 0 e 1.

O grau de Evidência Desfavorável (λ) é um valor que representa a evidência desfavorável onde a sentença é verdadeira e está entre 0 e 1 (TORRES et al., 2011).

Com o grau de Evidência Favorável μ e o grau de Evidência Desfavorável λ , é possível representar os quatro extremos estados lógicos mostrados na figura 3.

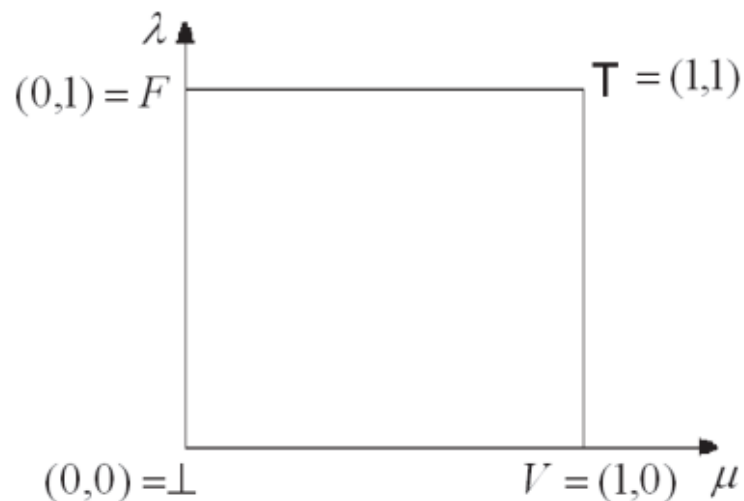


Figura 3 - O extremo estado da lógica.

Fonte: (TORRES et al., 2011).

Os quatro estados lógicos extremos são: Verdadeiro (V), Falso (F), Paracompleto ($\perp$) e Inconsistente (T). No trabalho (ABE et al., 2006) demonstra o algoritmo para-analisador e através do mesmo, pode-se representar o estado lógico não extremo, como se pode ver na figura 4.

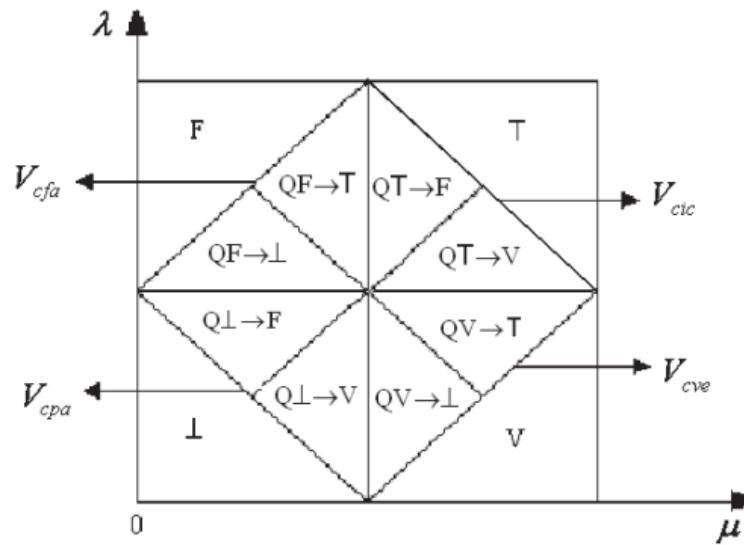


Figura 4 - O não extremo dos estados lógicos.

Fonte: (TORRES et al., 2011).

Podemos identificar suas siglas da seguinte maneira (ABE et al., 2006):

1. – *Quase-verdadeiro* tendendo para Inconsistente – $QV \rightarrow T$
2. – *Quase-verdadeiro* tendendo para Paracompleto – $QV \rightarrow \perp$
3. – *Quase-falso* tendendo para Inconsistente – $QF \rightarrow T$
4. – *Quase-falso* tendendo para Paracompleto – $QF \rightarrow \perp$
5. – *Quase inconsistente* tendendo para Verdadeiro – $QT \rightarrow V$
6. – *Quase-inconsistente* tendendo para Falso – $QT \rightarrow F$
7. – *Quase-paracompleto* tendendo para Verdadeiro – $Q\perp \rightarrow V$
8. – *Quase-paracompleto* tendendo para Falso – $Q\perp \rightarrow F$

Também se pode definir o Grau de Incerteza: $G_{in}(\mu, \lambda) = \mu + \lambda - 1$ e o grau de certeza $G_{ce}(\mu, \lambda) = \mu - \lambda$ ($0 \leq \mu, \lambda \leq 1$) (TORRES et al., 2011).

Alguns valores de controles adicionais são:

- V_{cic} = Valor máximo de controle incerteza;
- V_{cve} = Valor máximo de controle certeza;
- V_{cpa} = Valor mínimo de controle de incerteza;
- V_{cfa} = Valor mínimo de controle de certeza.

A lógica Evidencial E_τ tem seu uso destacado entre as chamadas lógicas paraconsistentes. Sua aplicabilidade e usabilidade em automação e robótica foram apontadas em: (TORRES, 2004), (TORRES, 2009), (DA SILVA FILHO et al., 2006) e (TORRES, ABE e LAMBERT-TORRES, 2005).

2.1.5 LÓGICA PARACONSISTENTE ANOTADA DE DOIS VALORES

A Lógica Paraconsistente Anotada de anotação com dois valores (LPA2v) apresenta-se de forma apropriada quando se aplica o entendimento de evidência para auxiliar na solução de divergências, quando diversas inferências inconsistentes decorrem (DA SILVA FILHO, 2006).

A anotação pode ser feita por 1 ou n valores. Dessa forma, pode-se adquirir um grande comando de representações a respeito de quanto às anotações expõem o conhecimento sobre a proposição P se a representação da evidência (anotação), ao invés de ser formada por somente um símbolo, for feita por dois valores de símbolos.

Dessa maneira, podemos ter um reticulado de pares ordenados, tal que $\tau = \{(\mu, \lambda) | \mu, \lambda \in [0, 1] \subset \mathfrak{R}\}$. Também é inserido um operador $\sim: |\tau| \rightarrow |\tau|$. O operador $\sim$ tem o “significado” dos símbolos de negação que será considerado, e os demais valores do reticulado são (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008):

- $\perp$ indica o mínimo de $\tau = (0, 0)$
- T Indica o máximo de $\tau = (1, 1)$
- *sup* significa operação de supremo
- *Inf* é a operação de ínfimo supremo

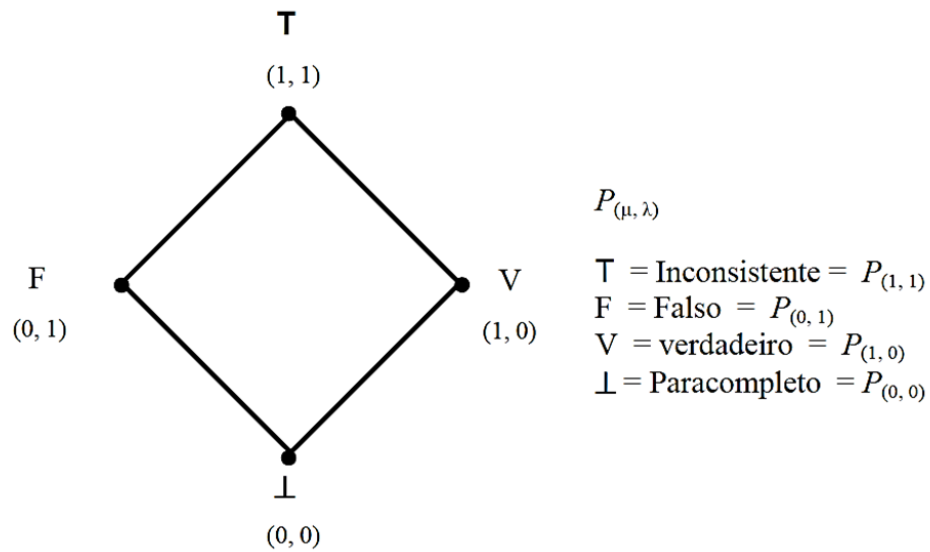


Figura 5 - Reticulado finito de Hasse com anotações da LPA2v.

Fonte: (DA SILVA FILHO, 2006).

Desse modo o estudo do postulado relacionado a associação de uma anotação (μ, λ) à uma proposição P significa que o Grau de Evidência favorável em P é μ , enquanto que o Grau de Evidência desfavorável ou contrária é λ . Por conseguintes, em tal reticulado temos as anotações:

(1, 0) indicando ‘existência de evidência favorável total e evidência desfavorável nula’;

(0, 1) indicando ‘existência de evidência favorável nula e evidência desfavorável total’;

(1, 1) indicando ‘existência de evidência favorável total e evidência desfavorável total’;

(0, 0) indicando ‘existência de evidência favorável nula e evidência desfavorável nula’.

Uma vez que p seja uma fórmula básica, o operador $\sim: |\tau| \rightarrow |\tau|$ é representado como: $\sim [(\mu, \lambda)] = (\mu, \lambda)$ onde: $\{(\mu, \lambda) \in \{x \in \mathfrak{R} \mid 0 \leq x \leq 1\}, \text{ considerando que } (\mu, \lambda) \text{ seja uma anotação de } p \text{ (DA SILVA FILHO, 2006).}$

As coordenadas μ, λ podem ser vistas como: “o grau de evidência favorável atribuído à proposição ‘ p ’ e o grau de evidência desfavorável atribuído à proposição ‘ p ’” (DA SILVA FILHO, 2006).

Os valores dos graus de evidência favorável (μ) e desfavorável (λ) são independentes. Em termos realistas, os valores dos graus de evidência favorável e desfavorável têm como finalidade resolver o problema de sinais contraditórios reunindo confirmações ou afirmativas contrárias e, através de análises, inferir sobre o comportamento do sistema para que as contradições diminuam.

2.1.6 GRAU DE CERTEZA E DE CONTRADIÇÃO

Na LPA2v os valores do grau de certeza (G_C) são expressos em um eixo horizontal compondo o eixo dos graus de certeza. Da mesma forma, os valores do grau de contradição (G_{CT}) são expressos em um eixo vertical, compondo o eixo dos graus de contradição.

Um estado lógico paraconsistente verdadeiro (1,0) está representado na figura 6, pelo ponto D, assim como um estado lógico paraconsistente falso (0,1) está representado pelo ponto B.

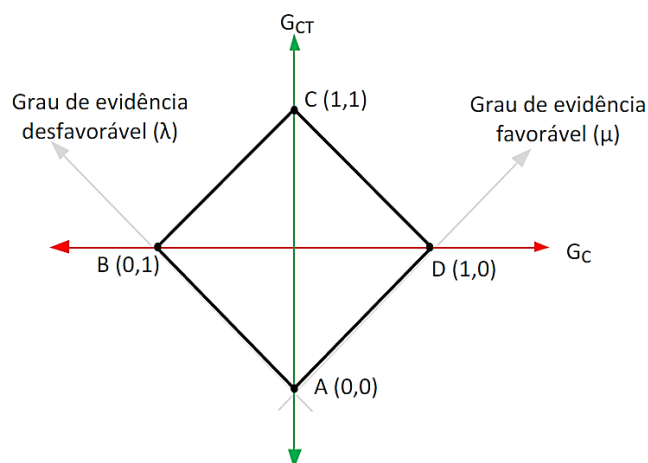


Figura 6 - Representação dos Graus de Certeza e de Contradição.

Fonte: (DA SILVA FILHO, 1999).

Considerando-se que o ponto de intersecção dos eixos dos graus de certeza e contradição é a origem desses valores, ou seja, nesse ponto, $G_C = 0$ e $G_{CT} = 0$, pode-se dizer que quando uma proposição apresentar estado lógico

paraconsistente verdadeiro, o valor do grau de certeza será $G_C = +1$. De forma análoga, quando uma proposição apresentar estado lógico paraconsistente falso, o valor do grau de certeza será $G_C = -1$.

Portanto, pode-se equacionar o Grau de certeza como:

$$G_C = \mu - \lambda$$

Os valores do Grau de Certeza (G_C) pertencem ao conjunto $\Re$, que variam no intervalo fechado $+1$ e -1 e estão no eixo horizontal do reticulado, conforme apresentado na figura 7. Definido por da Costa et al. (1999), o G_C é considerado como o valor que representa no reticulado a distância entre os dois estados extremos denominados de Totalmente Falso e Totalmente Verdadeiro.

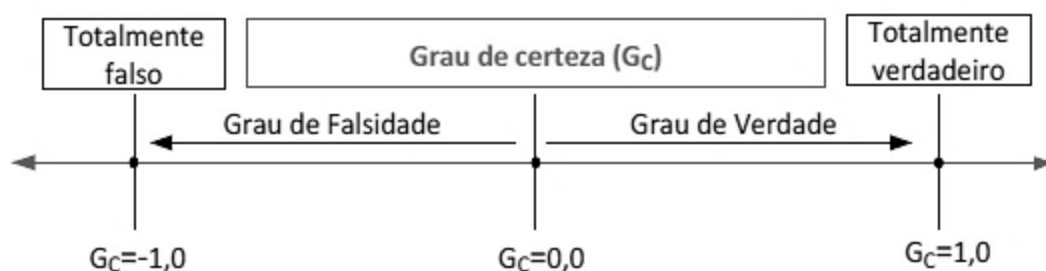


Figura 7 - Representação do grau de certeza.

Fonte: (DA SILVA FILHO, 2006).

Podemos verificar que, na figura 6 acima, que o ponto C é representando pelo estado lógico inconsistente e o ponto A está representado pelo estado indeterminado.

Tratando-se de um sistema de verificação paraconsistente, quando o estado lógico de uma proposição permanecer próximo da seção de reta constituída pelos pontos BD da figura 6, significa que o grau de contradição das procedências de evidência é pequeno e tende a sua não existência. Mas, uma vez que o estado da lógica permanecer uma distância considerável da reta, o grau de contradição será $G_{ct} = +1$ para uma circunstância inconsistente e $G_{ct} = -1$ para indeterminada,

demonstrando um valor grande para a contradição. Em vista disso, a equação do Grau de contradição é: $G_{ct} = \mu + \lambda - 1$.

A figura 8 exibe o eixo dos níveis de contradição juntamente com seus valores de -1 a +1 e faz parte do conjunto $\Re$. Segundo da Costa et al.(1999), o G_{ct} é determinado como o número que retrata entre os dois estado chamados de Totalmente Paracompleto.

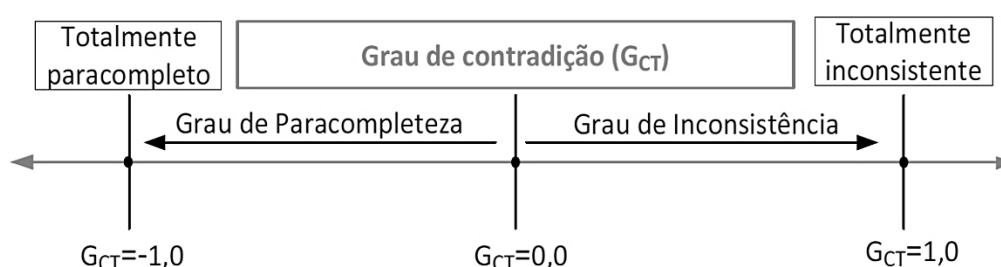


Figura 8 - Representação do grau de contradição.

Fonte: (DA SILVA FILHO, 2006).

2.1.7 GRAU DE CERTEZA DE VALOR REAL

Buscando aprimorar o sistema de tratamento de incerteza as procedências de evidência propício e não propício junto com os níveis de certeza e contradição, uma nova variável passa a ser calculada, Grau de Certeza de valor real (G_{cr}).

Um Sistema de decisão capaz de analisar dados originados do Conhecimento Incerto terá maior robustez quando, ao final da análise, apresentar um resultado que represente o valor de certeza puro, isto é, não contaminado pelos efeitos das incertezas. Portanto, o valor final deve vir subtraído do valor atribuído ao efeito da influência das inconsistências originadas pelas informações conflitantes (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Iniciando da suposição em que uma análise paraconsistente, os cálculos do G_{cr} por meio de (2.1) e G_{ct} (Grau de Contradição) através de (2.2), atinge valores positivos que estão intercalados no reticulado conforme figura 9.

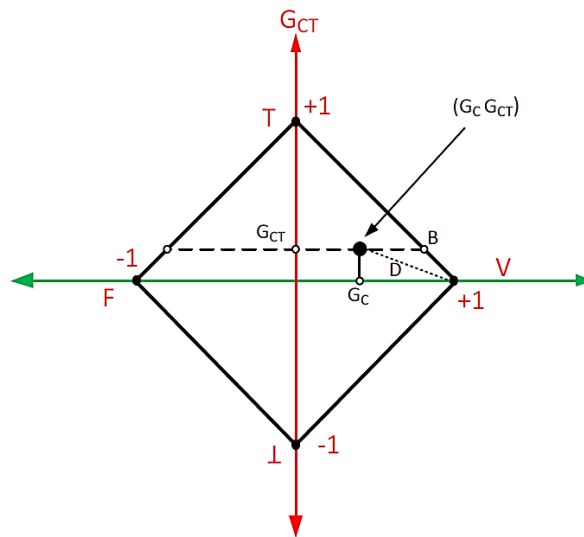


Figura 9 - Ponto de interpolação (G_c , G_{ct}) e distância D .

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

A distância D da reta da figura 9, que vai do ponto de máximo Grau de Certeza V , representada no vértice direito do reticulado, até ao ponto de interpolação (G_c , G_{ct}), é calculada por:

$$D = \sqrt{(1 - |G_c|)^2 + G_{ct}^2}$$

Sendo assim, o Grau de Certeza de valor real G_{cr} será a projeção da distância D no eixo de valores de certeza, conforme se demonstra na figura 10.

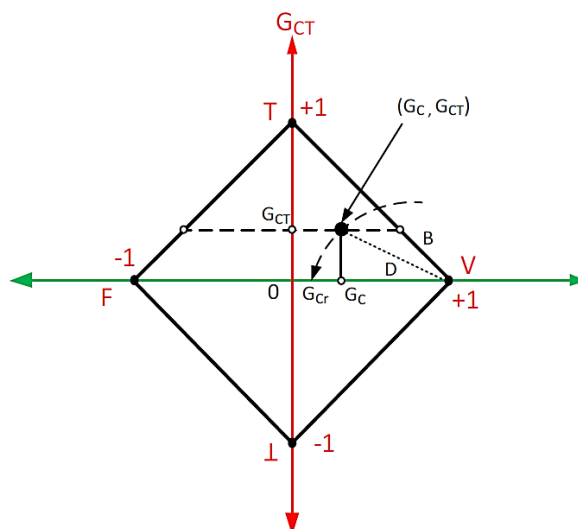


Figura 10 - Grau de Certeza de valor resultante real - G_{cr} no reticulado.

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Se o Grau de Certeza Calculado G_c resultar em valor negativo, a distância D será obtida a partir do ponto de certeza F, representado no vértice esquerdo do reticulado, até ao ponto de interpolação $(-G_c, G_{CT})$. O ponto de interpolação nessas condições está representado na figura 11.

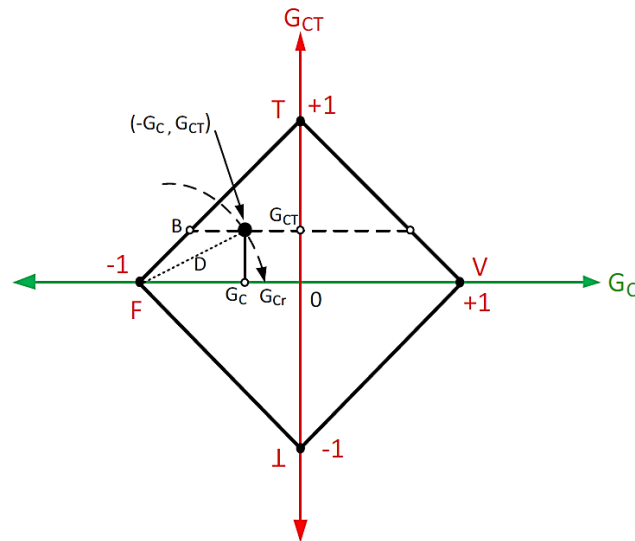


Figura 11 - Grau de Certeza de valor real Gcr no reticulado da LPA2v quando Gc é negativo e Gct positivo.

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Então, o valor do Grau de Certeza real G_{CR} é obtido a partir da determinação da distância D , conforme as condições mostradas abaixo:

Se $G_c > 0$: $G_{CR} = (1 - D)$

ou

$$G_{CR} = 1 - \sqrt{(1 - |G_c|)^2 + G_{ct}^2} \quad (2.4)$$

Se $G_c < 0$: $G_{CR} = (D - 1)$

ou

$$G_{CR} = \sqrt{(1 - |G_c|)^2 + G_{ct}^2} - 1 \quad (2.5)$$

As equações que foram adquiridas a partir da metodologia em estudo na LPA2v irão compor os algoritmos para tomada de decisão e tratamento de incertezas.

2.1.8 NÓ DE ANÁLISE PARACONSISTENTE (NAP)

Conforme observado em Baptista, Da Silva Filho e Morilla (2013), o Nó de Análise Paraconsistente – NAP, trata-se de um algoritmo para tratamento de incertezas, fundamentado em Lógica Paraconsistente Anotada LPA2v. Portanto, o NAP envolve a aplicação das equações apresentadas no item anterior.

Nas redes de análise paraconsistente, os NAPs fazem tratamento de sinais de informação conforme os fundamentos da Lógica Paraconsistente. Com as suas entradas sendo alimentadas pelos Graus de Evidências retirados de base de dados de Conhecimento Incerto os NAPs utilizam as equações obtidas da metodologia da LPA2v e vão obtendo os Graus de Certeza real G_{Cr} acompanhados de seus respectivos Intervalos de Certeza ϕ . Este processo possibilita a obtenção de conclusões à respeito de determinadas proposições (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Na representação de um NAP têm-se duas entradas de Graus de Evidência favorável μ e desfavorável λ a respeito da proposição analisada, e duas saídas de resultados: o Grau de Certeza real (G_{Cr}) e o Intervalo de Certeza (ϕ), conforme se demonstra na figura 12.

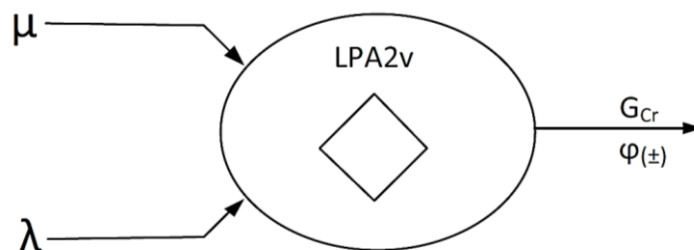


Figura 12 - Símbolo de um Nó de Análise Paraconsistente típico.

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

2.1.9 GRAU DE EVIDÊNCIA RESULTANTE REAL (μ_{ER})

Como uma análise Paraconsistente produz valores de Grau de Certeza real no intervalo fechado entre -1 e +1, para transformar o Grau de Certeza real resultante da análise de uma proposição em Grau de Evidência resultante real (μ_{ER}), que servirá como entrada para outra proposição é feita uma normalização nos seus valores, para que fique no intervalo entre 0 e 1.

Como referência, a figura 13 mostra a equivalência entre os valores dos Graus de Certeza real G_{CR} e os Graus de Evidência resultante (μ_E).

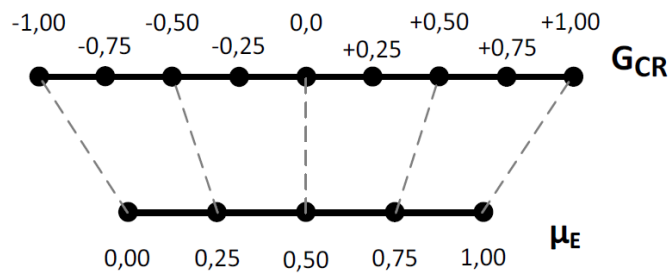


Figura 13 - Conversão de Grau de Certeza real G_{CR} em Grau de Evidência resultante μ_E .

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

O Grau de Evidência resultante real (μ_{ER}) é calculado a partir das equações (2.4) e (2.5) e equacionado por:

$$\mu_{ER} = \frac{G_{CR} + 1}{2}$$

2.1.10 GRAU DE CONTRADIÇÃO NORMALIZADO

Para que a resposta em um NAP seja padronizada também é feita uma normalização no Grau de Contradição, e assim seus valores resultantes encontrados ficarão no intervalo real fechado entre 0 e 1. Tomando-se como referência a equação $G_{ct} = (\mu + \lambda) - 1$, é realizada a normalização no Grau de Contradição por:

$$\mu_{ctr} = \frac{G_{ct} + 1}{2} \quad (2.7)$$

ou

$$\mu_{ctr} = \frac{(\mu + \lambda)}{2} \quad (2.8)$$

Conforme Da Silva Filho, Abe e Lambert-Torres (2008), nota-se a correlação entre os valores do Grau de Contradição G_{ct} e do Grau de Contradição normalizado (μ_{ctr}) onde se pode representar por meio da Figura 14.

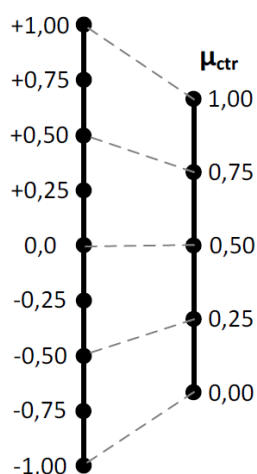


Figura 14 - Conversão de Grau de Contradição G_{ct} em Grau de Contradição normalizado μ_{ctr} .

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Uma vez que o Grau de Contradição Normalizado ficar acima de 0,5 tem significado de que há uma contradição entre os Graus de Evidência das entradas a

respeito da Proposição analisada. Logo, os valores de Graus de Contradição Normalizados acima de 0,5 e tendendo a 1,0 indicam que estão no sentido de estabelecer um estado lógico Inconsistente à Proposição analisada.

Quando o valor do Grau de Contradição Normalizado for igual a 1,0 existe uma contradição total à proposição, portanto o estado lógico é o totalmente Inconsistente. Por outro lado, quando o valor do Grau de Contradição Normalizado estiver abaixo de 0,5 significa que também existe uma contradição à proposição analisada. Portanto, os valores de Graus de Contradição Normalizados abaixo de 0,5 e tendendo a zero indicam que as evidências são contraditórias no sentido de estabelecer um estado lógico de Indeterminação à Proposição analisada.

Quando o valor do Grau de Contradição Normalizado for igual a zero, existe total contradição, portanto o estado lógico é totalmente Indeterminado.

2.2.11 NÓ DE ANÁLISE PARACONSISTENTE DA LPA2V COM SAÍDA DE GRAU DE EVIDÊNCIA RESULTANTE REAL

Segundo Da Silva Filho, Abe e Lambert-Torres (2008), o sistema ou algoritmo denominado de Nó de Análise Paraconsistente pode ser feito utilizando-se as equações obtidas no estudo dos NAPs. O sistema Paraconsistente de Tratamento de Incertezas pode ser utilizado em diversos campos do conhecimento em que informações incompletas e contraditórias receberão um tratamento adequado por meio das equações da LPA2v. O algoritmo de Análise paraconsistente para determinação do Grau de Certeza real e do Intervalo de Certeza é exposto a seguir:

Entre com os valores de Entrada.

μ */ Grau de Evidência favorável $0 \leq \mu \leq 1$

λ */ Grau de Evidência desfavorável $0 \leq \lambda \leq 1$

Calcule o Grau de Contradição Normalizado.

$$\mu_{ctr} = \frac{\mu + \lambda}{2}$$

Calcule o Intervalo de Evidência Resultante

$$\varphi_E = 1 - |2 \cdot \mu_{ctr} - 1|$$

Calcule o Grau de Certeza.

$$G_C = \mu - \lambda$$

Calcule o Grau de Contradição

$$G_{ct} = (\mu + \lambda) - 1$$

Calcule a distância D

$$D = \sqrt{(1 - |G_c|)^2 + G_{ct}^2}$$

Calcule o Grau de Certeza Real

Se $G_c > 0$, $GCR = (1 - D)$

Se $G_c < 0$, $GCR = (D - 1)$

Determine o sinal da Saída

Se $\varphi_E \leq 0,25$ ou $D > 1$, então faça:

$S1 = 0, 5$ e $S2 = \varphi_E(\pm) =$: Indefinição e vá para o fim. Senão vá para o próximo item

Calcule o Grau de Evidência Resultante real

$$\mu_{ER} = \frac{GCR + 1}{2}$$

Determine a sinalização do Intervalo de Evidência resultante

Se $G_{ct} < 0$ Sinalize negativo $\varphi(\pm) = \varphi(-)$

Se $G_{ct} > 0$ Sinalize positivo $\varphi(\pm) = \varphi(+)$

Se $G_{ct} = 0$ Sinalize zero $\varphi(\pm) = \varphi(0)$

Apresente os resultados na saída.

Faça $S1=\mu_{ER}$ e $S2= \varphi_E(\pm)$

Fim.

2.2.12 ALGORITMO PARACONSISTENTE EXTRATOR DE EFEITOS DA CONTRADIÇÃO

O algoritmo Paraconsistente Extrator de efeitos da Contradição faz uso dos conceitos de tratamento de incerteza em uma extensão da Lógica Paraconsistente Anotada com anotação de dois valores (LPA2v).

O Algoritmo Paraconsistente Extrator de efeitos da Contradição é capacitado para retirar gradualmente os resultados da contradição em sinais de informação promovidos de banco de dados de conhecimento não definidos. O Algoritmo Paraconsistente Extrator ($ParaExtr_{ctr}$) utiliza um grupo de sinais de informações demonstrados por Graus de Evidência com relação a uma certa proposição P e assim faz a verificação paraconsistente em seus valores, onde, gradualmente, vai retirando os resultados do efeito da contradição até o momento em que houver como saída apenas um Grau de Evidência com resultados reais.

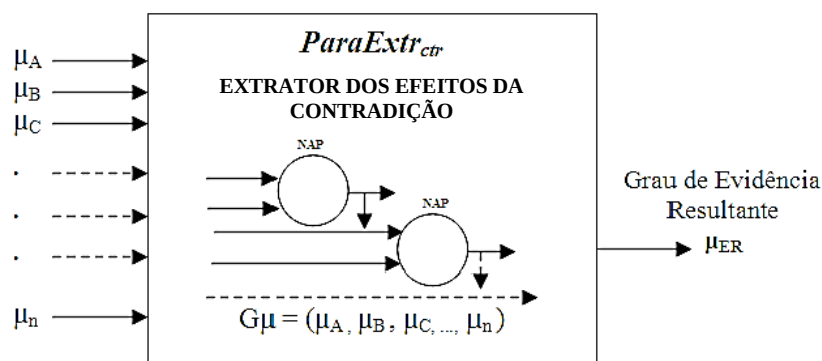


Figura 15 - Símbolo do Algoritmo Paraconsistente Extrator de efeitos da Contradição.

Fonte: (DA SILVA FILHO, 2009).

A descrição do algoritmo $ParaExtr_{ctr}$ é mostrada a seguir.

1. Apresente os n valores de Graus de Evidência que compõe o grupo em estudo

$$G\mu = (\mu A, \mu B, \mu C, \dots, \mu n) \text{ */Graus de Evidência } 0 \leq \mu \leq 1 \text{ */}$$

2. Selecione o maior valor entre os Graus de Evidência do grupo em estudo.

$$\mu_{\max A} = \max (\mu A, \mu B, \mu C, \dots, \mu n)$$

3. Considere o maior valor entre os Graus de Evidência do grupo em estudo em Grau de Evidência favorável.

$$\mu_{\max A} = \mu$$

4. Selecione o menor valor entre os Graus de Evidência do grupo em estudo.

$$\mu_{\min A} = \min (\mu A, \mu B, \mu C, \dots, \mu n)$$

5. Transforme menor valor em Grau de Evidência desfavorável.

$$1 - \mu_{\min A} = \lambda$$

6. Faça a análise Paraconsistente entre os valores selecionados:

$$\mu_{R1} = \mu \diamond \lambda \text{ */ Utilização de um NAP */}$$

7. Acrescente o valor obtido μ_{R1} no grupo em estudo, excluindo deste os dois valores $\mu_{\max}$ e $\mu_{\min}$ selecionados anteriormente.

$$G\mu = (\mu A, \mu B, \mu C, \dots, \mu n, \mu_{R1}) - (\mu_{\max A}, \mu_{\min A})$$

8. Retorne ao item 2 até que o Grupo em estudo tenha um único elemento resultante das análises

$$G\mu = (\mu_{ER}).$$

Com relação à parte de análise que o Algoritmo ParaExtrctr aplica, os sinais de informação podem ser extraídos de banco de dados não definidos. Desta maneira, as informações extraídas podem ser configuradas por números que resultam em análise de quantidade evidenciado por tabelas, formas de porcentagens e até mesmo por meio de programas computacionais (DA SILVA FILHO, 2009).

Com relação à aplicação do Algoritmo ParaExtrctr, o procedimento de extração de informações de várias procedências começa pela aquisição dos Graus de Evidencia favoráveis e desfavoráveis através de equações de normalização (DA SILVA FILHO, 2009). Os graus estruturarão grupos que serão verificados por blocos de NAPs que constituem os Algoritmos Extratores de Contradição. Com isso, a rede de algoritmos extrai informações em fontes juntamente com os efeitos das contradições até a verificação finalizar e ser obtido somente um valor de Grau de

Evidência. Será então o representante entre os mais variados graus executados como evidência da proposição em análise.

2.1.13 REDES DE ANÁLISE PARACONSISTENTE – RAP

Uma Rede de Análise paraconsistente RAP para tratamento de incertezas são diversos sistemas, ou Nós de Análises Paraconsistentes (NAP), convenientemente interligados para analisar evidências provenientes de fontes incertas. Mesmo com informações conflitantes, essa Rede de Análise da Lógica Paraconsistente Anotada de anotação de dois valores (LPA2v) é capaz de fornecer resultados suficientes para originar uma ação.(DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Uma RAP compõe-se de dois ou mais NAPs interconectados onde em cada nó é efetuado a análise de uma única preposição. No último NAP (Nó da Rede) há uma proposição objeto denominada Po, e, para se chegar até ela, se faz necessária a análise das proposições em cada nó. Desse modo para que se obtenham valores suficientes para tomada de decisão sobre a proposição objeto o resultado da análise paraconsistente produzido em cada NAP é aliado aos resultados dos outros NAPs. Essas junções de resultados levam ao estabelecimento de determinado Grau de Certeza à Proposição objeto, que demonstra-se como objetivo da análise resultante de Rede de Análise Paraconsistente.

Observa-se em Da Silva Filho, Abe e Lambert-Torres (2008) que as combinações dos NAPs em uma RAP devem considerar três circunstâncias:

- ✓ *As proposições analisadas em cada nó podem ser logicamente combinadas através de Graus de Certeza reais resultantes originando diferentes interligações;*
- ✓ *Os valores dos Graus de Certeza reais resultantes e os Intervalos de Certeza Reais advindos dos NAPs de diferentes proposições poderão fazer uso de conectivos “E” e disjunção “OU” conforme desenho topológico da RAP;*
- ✓ *Os valores dos Graus de Certeza reais resultantes poderão ser normalizados em valores entre 0 e 1 no intervalo real e assim considerados como Graus de Evidência usados na entrada de outras proposições que estão sendo analisados por diferentes NAPs.*

Assim, em uma configuração básica, a análise preliminar no NAP apresenta um valor de intervalo de Certeza sinalizado $\varphi(\pm)$ e um Grau de Certeza real G_{CR} referente a uma única proposição. Em vista disso, uma RAP de decisão paraconsistente deve ser projetada de tal forma que os vários valores de Graus de Evidência a respeito de determinada proposição analisados pelos nós de análise paraconsistente produzirão um único valor de Evidência (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

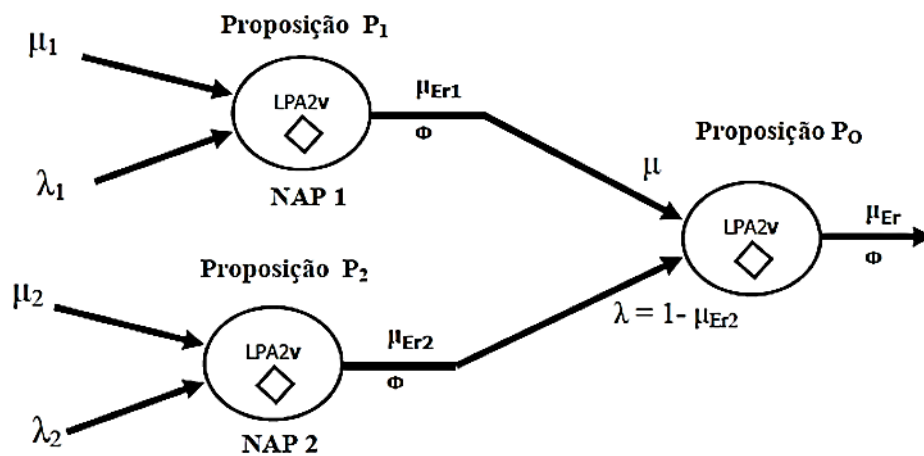


Figura 16 - Rede de Análise Paraconsistente em Configuração Simples.

Fonte: (DA SILVA FILHO, ABE e LAMBERT-TORRES, 2008).

Considerando o exposto, obtemos que, com a normalização para o Grau de Evidência Resultante real, os valores dos sinais (aplicados e obtidos na saída) ficam com os seus valores dentro do intervalo real fechado entre 0 e 1 permitindo assim que numa RAP as saídas sejam utilizadas como Graus de Evidência para outras proposições subsequentes. Esse conceito remete a possibilidade de diferentes topologias serem modeladas para RAP de decisão, cada qual de acordo com a finalidade a que foi projetada.

2.2 INTERCONEXÃO DE REDES DE COMPUTADORES

Em sua grande maioria, as empresas utilizam enlaces dedicados oferecidos pelas operadoras de telecomunicações para obter acesso à *Internet* ou para a comunicação entre matriz e filiais e para endereçar os *hosts*, utilizam identificadores fornecidos pela própria operadora (COMER, 2006). Atualmente utiliza-se o protocolo IP (em sua versão 4), definido pela RFC 791, predominantemente como referência de cada equipamento conectado à rede. Uma das “regras” do protocolo IP é que cada computador tenha um identificador único, conhecido como endereço IP (COMER, 2015). Como não pode haver repetição, a distribuição desses números deve ser feita de forma organizada. Atualmente existe uma hierarquia de entidades que controlam essa atribuição de endereços. A IANA (*Internet Assigned Numbers Authority*) coordena a atividade globalmente, no exercício de suas atribuições repassa para órgãos, distribuídos geograficamente pelo mundo, a responsabilidade de distribuir os endereços IP e alocação de números de identificação de Sistemas Autônomos. Tais órgãos são chamados de Registro Regional da *Internet* (em inglês: RIR's - *Regional Internet Registry*), são eles:

- LACNIC (*Latin American and Caribbean Internet Addresses Registry*);
- RIPE NCC (*Réseaux IP Européens Network Coordination Centre*);
- APNIC (*Asia-Pacific Network Information Centre*);
- ARIN (*American Registry for Internet Numbers*);
- AfriNIC (*African Network Information Centre*). (IANA, 2015)

A Figura 17 abaixo mostra qual a abrangência de cada organização:



Figura 17 - Mapa da área de atuação das entidades RIRs.

Fonte: IANA (2015)

2.2.1 A Rede do protocolo de *Internet* – REDE IP

A rede do protocolo de *Internet* – Rede IP é uma coleção de nós que utilizam o protocolo da *Internet* para comunicação. Todos os nós em uma rede IP são configurados com o pacote TCP/IP (*Transmission Control Protocol/Internet Protocol*). Cada nó em uma rede IP recebe um endereço IP lógico exclusivo que é usado para diferenciá-lo entre outros nós.

A comunicação de rede IP ocorre quando um *host* (equipamento conectado a rede) envia um pacote de dados para outro *host* usando seu endereço IP (BAKER, 1995). Da mesma forma, o *host* receptor identifica o *host* de envio pelo seu endereço IP.

2.2.2 Sistemas Autônomos

O conceito mais reconhecido de um Sistema Autônomo (AS – *Autonomous System*) é de que ele representa um conjunto de roteadores sob uma gerência técnica unificada, fazendo uso de protocolos de roteamento interno - IGP (*Interior Gateway Protocol*) e métricas comuns para encaminhar datagramas dentro do mesmo AS, e usando um protocolo de roteamento externo - EGP (*Exterior Gateway Protocol*) para rotear datagramas para AS's vizinhos (TANNENBAUM, 2011). Podemos inclusive afirmar que um AS é um grupo conectado, de um ou mais prefixos IP, executados pela mesma gerência técnica cuja política de

roteamento é comum aos membros desse grupo (HAWKINSON e BATES, 1996). O uso da terminologia "prefixo" pode ser empregado para blocos IP cuja possibilidade de agregação com CIDR (*classless Interdomain Routing*), por exemplo: 10.100.0.0/24 - 10.100.1.0/24 - 10.100.2.0/24 - 10.100.3.0/24 é viável, como no exemplo podem ser simplesmente referidos como: 10.100.0.0/22. Cada AS possui vinculado a si um prefixo designado pelo RIR que o gerencia. A política de roteamento é definida como o modo pelo qual as decisões para o encaminhamento de datagramas para outro(s) AS(s) serão tomadas.

Os ASN (*Autonomous System Number*), números de identificação dos Sistemas Autônomos, foram definidos na RFC 1930 (HAWKINSON e BATES, 1996) e se utilizam para sua identificação números inteiros entre 0 e 65535. Da mesma forma, os números de sistemas autônomos de 32 bits foram definidos pela RFC 4893 (VOHRA e CHEN, 2007) e são utilizados para sua identificação números inteiros de 0 a 4294967295. A IANA ainda designou o intervalo de ASN's entre 64512 até 65534 para uso privado.

2.2.3 Caracterização e classificação dos protocolos de roteamento

As redes de telecomunicações são as responsáveis pelo envio de informações entre os elementos comunicadores. Suas condições de operação como padrão de tráfego, topologia, nível de carga e capacidade de vazão, sofrem diversas alterações ao longo do tempo, muitas não previstas, elevando a complexidade e dinamismo do ambiente (MARREIRO e GARCIA, 2016).

Diante desse contexto, estão as rotas de comunicação (BERTSEKAS e GALLAGER, 1992). Estas rotas são obtidas com uso de equipamentos de interligação (exemplo: roteadores) que, através de protocolos de roteamento, dinamicamente gerenciam informações recebidas de outros equipamentos de interligação e de suas próprias *interfaces* (FORTZ e THORUP, 2000). Estes protocolos fazem uso de algoritmos de roteamento, que representam uma parte do *software* da camada de rede responsável pela decisão sobre qual *interface* de saída a ser usada na transmissão do pacote de informação que acabou de passar pela

interface de entrada (TANEMBAUM e WETHERALL, 2011).

Os algoritmos de roteamento podem ser classificados como: algoritmos não-adaptativos, aqueles em que a definição das rotas não são baseadas em medidas, topologias ou estimativas de tráfego, determinando previamente todo o caminho e permanecendo essa escolha durante toda a operação da rede e, algoritmos adaptativos, cujas decisões de roteamento refletem as mudanças no ambiente de rede (TANEMBAUM e WETHERALL, 2011). Ao fazerem uso de algoritmos adaptativos esses protocolos passam a serem reconhecidos como protocolos de roteamento dinâmico e sua classificação pode ser definida como a seguir: (WALLACE, 2014).

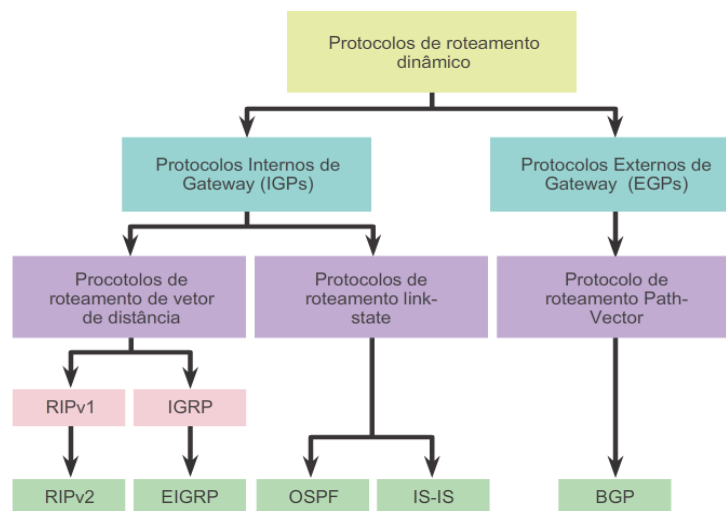


Figura 18 - Classificação dos Protocolos de Roteamento dinâmico.

Fonte: (NETACAD, 2016).

O roteamento em redes IP faz uso de um conjunto de protocolos que auxilia na determinação do caminho mais adequado que os pacotes de dados devem seguir de origem para destino. Os dados são encaminhados de origem para destino através de uma série de equipamentos de interconexão (exemplo: roteadores) e em várias redes.

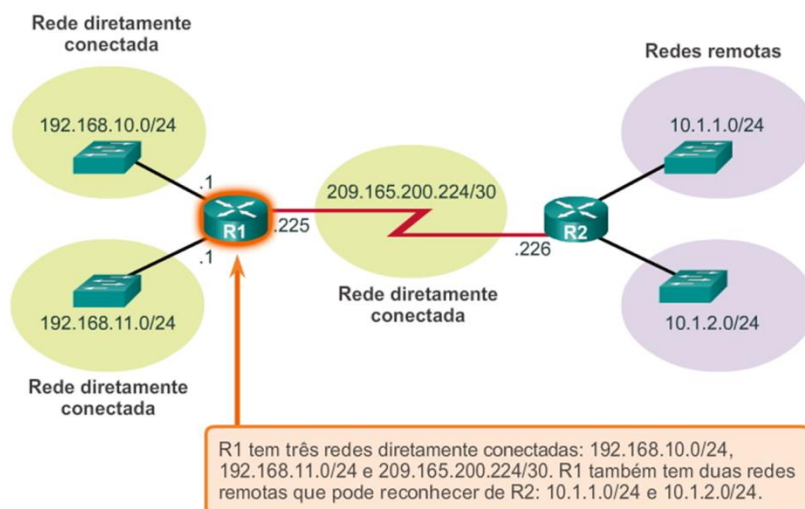


Figura 19 - Decisão de encaminhamento do datagrama no equipamento de interconexão.

Fonte: (NETACAD, 2016).

Os protocolos de roteamento permitem que os roteadores criem uma tabela de roteamento que associe os destinos finais aos próximos endereços de salto. Quando um pacote IP deve ser roteado, um roteador usa sua tabela de roteamento para determinar o próximo salto para o destino do pacote (com base no endereço IP de destino no cabeçalho do pacote IP) e encaminha o pacote adequadamente. O próximo roteador repete esse processo usando sua própria tabela de roteamento e o processo continua até o pacote chegar ao seu destino. Em cada etapa, o endereço IP presente no cabeçalho do pacote é suficiente para determinar o próximo salto.

Uma tabela de roteamento é um conjunto de informações usado para determinar a direção na qual os pacotes de dados devem trafegar. Todos os dispositivos habilitados para IP, incluindo roteadores e comutadores de camada 3, usam tabelas de roteamento (FORTZ, THORUP e REXFORD, 2002).

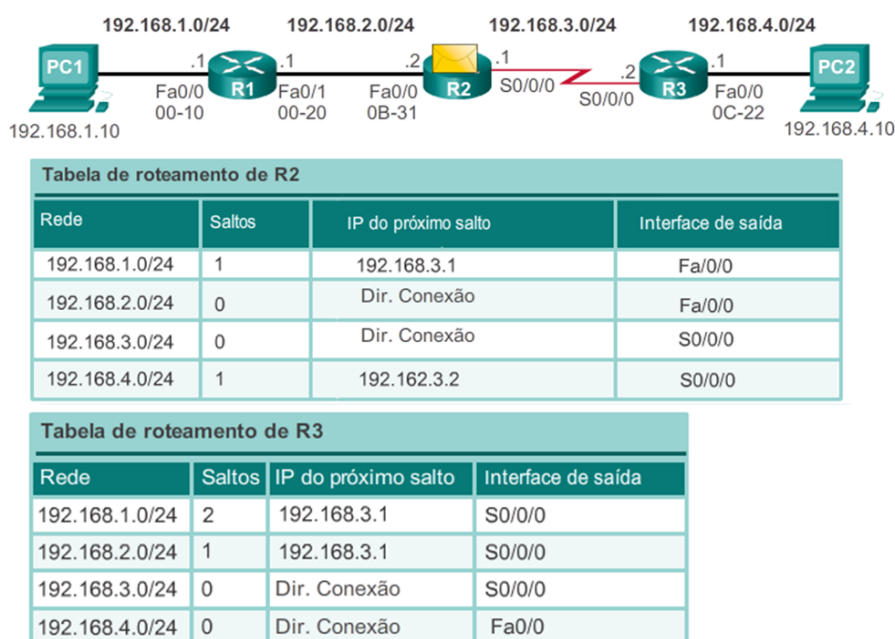


Figura 20 - Exemplo de tabelas de roteamento em equipamentos de interconexão.

Fonte: (NETACAD, 2016).

Como se observa na figura 20, a tabela de roteamento contém as informações necessárias para encaminhar um pacote ao longo do melhor caminho em direção ao seu destino. Cada pacote contém informações sobre sua origem e destino. Quando um pacote é recebido, um dispositivo de rede examina o pacote e combina com a entrada da tabela de roteamento fornecendo a melhor combinação para seu destino. A tabela fornece ao dispositivo as instruções para enviar o pacote para o próximo salto em sua rota na rede.

2.2.4 ROTEAMENTO INTERNO

Conhecido como IGP – *Internal Gateway Protocol* é constituído de um grupo de protocolos usados para comunicação entre roteadores em um mesmo sistema autônomo (FOROUZAN e MOSHARRAF, 2013). Incluem protocolos como RIP, EIGRP, OSPF e IS-IS

2.2.5 ROTEAMENTO EXTERNO

Conhecido como EGP – *External Gateway Protocol* é constituído de um grupo de protocolos usados para a interconexão entre roteadores que se encontram em diferentes sistemas autônomos. Protocolos estes utilizados pela *Internet* com o intuito de que mantenham informações consistentes para fomentar o funcionamento do roteamento global.

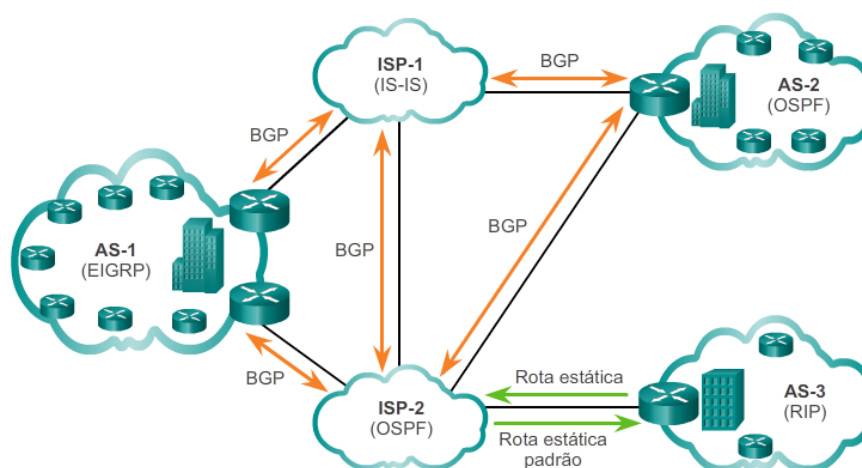


Figura 21 - Protocolos de roteamento IGP em relação à EGP.

Fonte: (NETACAD, 2016).

2.2.6 PROTOCOLO BGP – *BORDER GATEWAY PROTOCOL*

O BGP é um protocolo de roteamento dinâmico utilizado para comunicação entre sistemas autônomos (ASs). Baseados nas trocas de mensagens de configuração desse protocolo, os sistemas autônomos conseguem obter informações e determinar o melhor caminho para as redes que formam a *Internet* (HALABI e MCPHERSON, 2000). Tal característica é muito importante sabendo que a todo o momento as redes podem sofrer alterações, quedas de suas conexões ou até mesmo receber anúncios de rotas inválidas, aplicar políticas, manter a

conectividade por outros caminhos, adaptando-se rapidamente e mantendo a consistência de seus anúncios de forma eficiente torna-se um grande diferencial de funcionamento do protocolo.

A divulgação das informações de roteamento BGP é efetuada entre roteadores que estabelecem uma relação chamada de “vizinhança” (*peers*), ocorrendo sempre aos pares (também conhecida como *peering*). Estabelecido esse *peering*, são trocadas as informações contidas nas tabelas de roteamento BGP de cada um destes. Para estabelecer uma relação de vizinhança é necessário que dois roteadores tenham uma conexão direta entre eles, ou que algum protocolo de roteamento interno - IGP estabeleça essa conectividade.

2.2.7 PROTOCOLO SNMP – SIMPLE NETWORK MANAGEMENT PROTOCOL

O SNMP é um conjunto de especificações desenvolvidas pelo IETF (*Internet Engineering Task Force*), com o objetivo de gerir redes IP, utilizando um protocolo simples. A versão original do SNMP derivou do protocolo SGMP (*Simple Gateway Monitoring Protocol*), em 1998, possibilitando a gestão de servidores, impressoras, comutadores, roteadores, etc, desde que estes aceitem a requisição/alteração de informação através de SNMP.

O modelo de gerenciamento de redes utilizando SNMP é composto por quatro pilares como fundamentos (STALLINGS, 1999), (SCHMIDT e MAURO, 2005).

Estação de Gestão: Posto de monitorização e controle, onde o modelo de funcionamento é criado. Faz a ligação entre o gestor da rede e o sistema a gerir. O gestor da rede dispõe de um *software* que lhe permite lidar com as tarefas necessárias para a gestão da rede. Por vezes os gestores são denominados NMS (*Network Management Stations*), responsáveis por fazer *polling* e receber *traps* dos agentes da rede. A ação de *polling* consiste no envio de pedidos aos agentes para solicitar determinadas informações, enquanto que os *traps* são enviados pelos agentes para notificar a estação de gestão de eventos importantes;

Agente: *Software* presente nos dispositivos que serão gerenciados. Pode ser um programa separado ou poderá estar incorporado no sistema operacional. Nos momentos mais atuais, a maioria dos equipamentos IP já vem com um agente SNMP incluso. Os agentes providenciam informação de gerenciamento para a estação de gestão. São responsáveis por responder aos pedidos enviados e de enviar autonomamente informação importante para a estação de gestão. Eventualmente poderão receber da estação de gerenciamento pedidos para a alteração dos seus valores;

Protocolo de Gestão: O protocolo de gerenciamento é utilizado na comunicação entre a estação de gerenciamento e os agentes, especificando os seguintes tipos de operação: - *get* - permite à estação de gerenciamento consultar um determinado parâmetro de um agente; - *set* - permite à estação de gerenciamento modificar um determinado parâmetro de um agente; - *trap* - permite que cada agente notifique a ocorrência de eventos extraordinários à estação de gestão.

Informação de Gestão: O SNMP por si só não define a informação que um sistema a ser gerido oferece. Esta é definida pelas MIBs (*Management Information Base*). As MIBs podem conter um conjunto de objetos, ou seja, um conjunto de variáveis que caracterizam um determinado equipamento, tais como o tempo de operação, contacto, nome, localização, entre outros. A função das MIBs é guardar as informações dos agentes de uma forma acessível à estação de gestão. Os objetos são normalizados para determinadas categorias de equipamentos;

2.2.8 SNMPv1

A primeira versão da arquitetura SNMP é simples, centralizada e rígida (CASE et al., 1990). São especificados cinco PDUs (TANENBAUM e WETHERALL, 2011):

GetRequest: Pedido enviado por parte do gestor para o agente com o objetivo de aceder ao valor de uma das variáveis. O tipo de PDU na trama fica preenchido com o valor 0;

GetNextRequest: Pedido do gestor para o agente, de forma a descobrir as

variáveis disponíveis para gestão e quais os seus valores. O tipo de PDU na trama fica preenchido com o valor 1;

GetResponse: Resposta do agente às operações *GetRequest*, onde retorna o valor da variável em questão, e *GetNextRequest* contendo a resposta com a variável seguinte da estrutura de dados, ou para confirmar a operação *SetRequest*. O tipo de PDU na trama fica preenchido com o valor 2;

SetRequest: Pedido do gestor para que o agente altere o valor de uma determinada variável. O tipo de PDU na trama fica preenchido com o valor 3;

Trap: Notificação proveniente do agente e enviada para o gestor, indicando um evento significativo. Esta mensagem é enviada automaticamente para o gestor. O tipo de PDU na trama fica preenchido com o valor 4.

2.2.9 SNMPv2

Com o aumento do número de utilizadores, foi sentida a necessidade de acrescentar mais funcionalidades, particularmente no que diz respeito à questão da segurança. O SNMPv1 apresentava limitações na gestão de grandes redes, devido ao polling, capaz de criar problemas de desempenho. A versão anterior também não era adequada para a transferência de grandes quantidades de informação e as mensagens *trap* não eram confirmadas, pelo que não havia garantia de que mensagens críticas fossem entregues. Nesta nova versão do SNMP, o desempenho melhorou e houve alteração dos formatos das PDUs já existentes. Para, além disso, segundo Presuhn (2002), foi implementado o suporte em múltiplos protocolos e introduzidas três novas PDUs descritas na RFC 3416:

GetBulkRequest: Versão otimizada do *GetNextRequest* - permite pedir várias instruções desta operação melhorando a eficiência da operação de percorrer e descobrir as diferentes variáveis num agente. O tipo de PDU na trama fica preenchido com o valor 5;

InformRequest: Utilizada na comunicação entre estações de gestão. O tipo de PDU na trama fica preenchido com o valor 6;

SNMPv2-Trap: Substitui o *Trap* do SNMPv1. Difere essencialmente no formato da PDU. O tipo de PDU na trama fica preenchido com o valor 7;

A operação *Trap* da primeira versão do protocolo foi substituída pela operação SNMPv2-Trap, mas as restantes operações do SNMPv1 continuam a ser suportadas. Nesta segunda versão do protocolo foi feita uma tentativa de implementação de novos mecanismos de segurança no SNMP, no entanto não foram estabelecidas medidas consensuais e robustas, tornando este protocolo mais complexo e inadequado para algumas operações de configuração.

2.2.10 MIB – MANAGEMENT INFORMATION BASE

Uma MIB é a coleção estruturada de objetos, ou seja, de dados a serem geridos, como o tempo de operação, o contato, o nome e o número de *interfaces* de um dispositivo. A MIB no protocolo SNMP surge como uma base de dados organizada em árvore, que contém informações sobre o estado dos recursos geridos pelo sistema (LOPES, 2002). Para que as MIBs sejam utilizadas de uma maneira eficaz pelos sistemas de gestão, os objetos que caracterizam um recurso específico devem ser os mesmos para cada sistema e deve ser definida uma estrutura comum de representação e gestão da informação. A SMI (*Structure of Management Information*) descreve o formato da definição do objeto gerido: providencia uma maneira de definir os objetos especificando, desta forma, o modo como são definidas e construídas as MIBs. As MIBs podem ser públicas ou privadas. As MIBs privadas contêm informações específicas dos equipamentos, tais como configurações e colisões, de uma determinada organização. Os objetos geridos contêm três atributos: o nome, o tipo e sintaxe e a codificação (STALLINGS, 1999), (MAURO e SCHMIDT, 2005).

Nome dos Objetos: Identifica univocamente o objeto, sendo também denominado como OID (*Object Identifier*). É representado por uma sequência de números inteiros ou nomes separados por pontos. A cada nome coincide um número único. Cada OID identifica uma variável que pode ser lida ou alterada através do

SNMP.

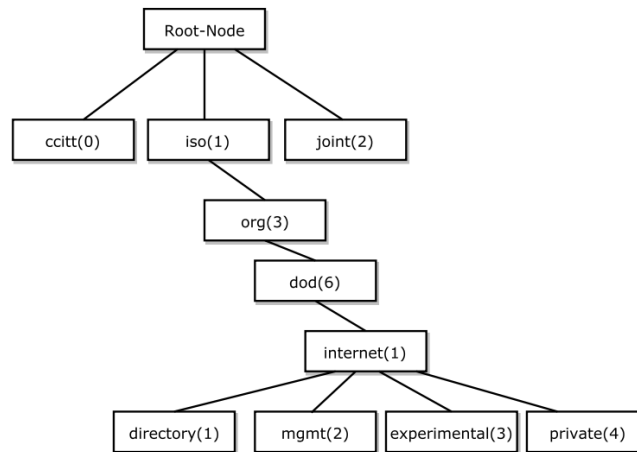


Figura 22 - Ramificação SMIPv1.

Fonte: (SCHMIDT e MAURO, 2005).

A partir da raiz da árvore dos objetos, representada na Figura acima, pode-se observar que são definidos três ramos: o ccitt(0), referente aos objetos geridos pelo CCITT (*Comité Consultatif International Téléphonique et Télégraphique*), agora ITU (*International Telecommunication Union*), o iso(1), referente aos objetos geridos pela ISO (*International Organization for Standardization*) e o joint(2), referente aos objetos geridos em conjunto pelas duas entidades. O ramo iso(1) é o único que contém uma subtree a iso(1).org(3).dod(6).internet(1). Assim sendo, o ramo internet(1) terá um OID único: 1.3.6.1, que pode também ser representado por iso.org.dod.internet. Abaixo do nó internet(1) são definidos quatro ramos, tal como se pode verificar na Figura acima (STALLINGS, 1999):

- directory(1): reservado para utilização com o diretório OSI (X.500);
- mgmt(2): também denominado como management, é utilizado para definir um conjunto de standards de gerenciamento dos objetos da *Internet*;
- experimental(3): usado para identificar objetos utilizados em experiências e em investigações;
- private(4): utilizado para identificar objetos definidos unilateralmente, ou seja, é utilizando este ramo que é feita a definição dos objetos próprios de cada

organização, sendo que estas ficam responsáveis pela sua gestão.

Ainda sobre a figura acima podemos considerar que nessa árvore de objetos, o nó no topo da árvore é chamado de raiz, qualquer coisa que tiver filhos é chamada de sub-árvore e o que não tiver nada é chamado de folha.

Tipo e Sintaxe (MAURO e SCHMIDT, 2005): O tipo do objeto é definido utilizando o ASN.1 (*Abstract Syntax Notation One*). Esta linguagem é utilizada para especificar como é que a informação transmitida é representada entre a estação de gerenciamento e o agente. Ou seja, serve apenas para definir o tipo de informação que o objeto gerido pode suportar. Os tipos de dados suportados pelo SMIv1 são:

Quadro 1 - Tipo de dados SMIv1.

TIPO DE DADO	DEFINIÇÃO
Integer	Usado para representar números inteiros e diferentes de zero
Octet String	Armazena uma sequência de octetos. Dele se originam três tipos: OctetBitString, PhysAddress e DisplayString.
Counter	Usado para representar um contador cujo valor é unicamente incrementado e ao chegar em seu valor máximo retorna ao zero.
Object Identifier	Representa objetos gerenciados objeto dentro da árvore da MIB.
Null	Atualmente não é usado no SNMP.
Sequence	Define uma lista ordenada de tipos de dados ASNs diferentes.
Sequence of	É uma lista gerenciada de objetos do tipo "SEQUENCE".
IpAddress	Representa um endereço lógico IPv4 composto de 32 bits, essa estrutura não contempla o endereço IPv6
NetworkAddress	O mesmo que "IpAddress", mas pode representar tipos diferentes de endereços de redes.
Gauge	Pode aumentar ou diminuir aleatoriamente, mas nunca pode ultrapassar seu valor máximo.
TimeTicks	É um tipo de dados usado para medições de tempos em centésimos de segundos.
Opaque	Permite que outra codificação ASN.1 ocupe um Octet String.

Fonte: Adaptado pelo autor (SCHMIDT e MAURO, 2005).

Assim, com o aparecimento da segunda versão do protocolo SNMP, foi criada também uma segunda versão da SMI, mantendo e expandindo a estrutura original: a SMIv2. Nesta segunda versão é possível ter um maior controle sobre a maneira

como se acede ao objeto. Tal como se pode verificar na árvore dos objetos representada na Figura abaixo, foi acrescentado um ramo para esta segunda versão da SMI, contendo o ramo snmpV2 com OID 1.3.6.1.6.

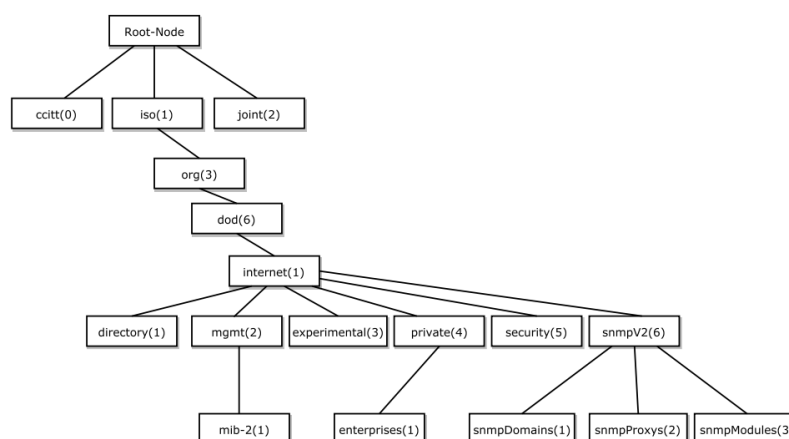


Figura 23 - Ramificação SMIv2.

Fonte: (SCHMIDT e MAURO, 2005).

Codificação: Cada instância de um objeto gerido é codificada utilizando o BER (*Basic Encoding Rules*).

2.3 TELECOMUNICAÇÕES: MÉTRICAS DE DESEMPENHO E QUALIDADE

Um ambiente de telecomunicações corporativo sustenta um conjunto de serviços para os quais existem demandas aleatórias e diversificadas, nesse contexto os serviços individualmente podem requerer um nível de qualidade e utilizar um conjunto de recursos por um período indeterminado de tempo (FORTZ, THORUP e REXFORD, 2002). A utilização desses recursos de maneira descontrolada pode degradar os parâmetros de QoS (*Quality of Service*) e, conseqüentemente, levar o ambiente a um desempenho aquém do satisfatório, seja do ponto de vista da aplicação (recursos disponibilizados) quanto do usuário (tempo de resposta). Esse comportamento nos remete a necessidade de caracterizarmos a funcionalidade através de métricas permitindo-nos o uso efetivo

de uma gerência de desempenho eficaz. Estatísticas de desempenho auxiliam na administração, planejamento e manutenção de grandes redes. Estas informações podem ser utilizadas para identificar eventos de gargalo antes que causem problemas para o usuário final.

Ações corretivas podem ser programadas e efetivadas, tais como, alterar a divulgação de rotas em tabelas de roteamento para balancear ou redistribuir a carga de tráfego durante intervalos de pico, ou ainda, a longo prazo, indicar a necessidade de expansão de enlaces de comunicação para uma determinada rede de interconexão.

2.3.1 LARGURA DE BANDA DE VAZÃO

A Largura de banda indica a capacidade máxima de transmissão nominal de uma conexão, enquanto que a taxa de uso dos canais de comunicação envolvidos (conhecida como vazão ou *throughput*) trata-se da quantidade de dados transferidos de um ponto a outro da rede em um determinado intervalo de tempo (FOROUZAN, 2008). Em ambientes cuja arquitetura de comunicação usada é Ethernet, a banda passante máxima absoluta será igual à taxa de dados, porém em situações realistas, esses números não podem ser alcançados, devido aos campos adicionais para que os quadros possam ser transportados e pelo espaçamento entre quadros, necessário para o funcionamento da rede. Os pacotes maiores têm uma vazão efetiva maior do que a dos pacotes menores, isso ocorre por conta da inclusão dos bytes de preâmbulo e do espaço entre pacotes, que não contam como dados. A vazão máxima que pode ser obtida para os diversos tamanhos de quadro é apresentada na tabela 1 (BURGESS, 2004):

Tabela 1 - Vazão máxima para diferentes tipos de pacotes.

Sistemas de 10 Mbits/s			
Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	7,62 Mbits/s	2,38 Mbits/s	14,88

128 bytes	8,65 Mb/s	1,35 Mb/s	8,45
256 bytes	9,28 Mb/s	0,72 Mb/s	4,53
512 bytes	9,62 Mb/s	0,38 Mb/s	2,35
1024 bytes	9,81 Mb/s	0,19 Mb/s	1,2
1280 bytes	9,85 Mb/s	0,15 Mb/s	0,96
1518 bytes	9,87 Mb/s	0,13 Mb/s	0,81
1522 bytes	9,87 Mb/s	0,13 Mb/s	0,81

Fonte: (BURGEISS, 2004).

Tabela 2 - Vazão máxima para diferentes tipos de pacotes.

Sistemas de 100 Mb/s			
Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	76,19 Mb/s	23,81 Mb/s	148,81
128 bytes	86,49 Mb/s	13,51 Mb/s	84,46
256 bytes	92,75 Mb/s	7,25 Mb/s	45,29
512 bytes	96,24 Mb/s	3,76 Mb/s	23,5
1024 bytes	98,08 Mb/s	1,92 Mb/s	11,97
1280 bytes	98,46 Mb/s	1,54 Mb/s	9,62
1518 bytes	98,70 Mb/s	1,30 Mb/s	8,13
1522 bytes	98,70 Mb/s	1,30 Mb/s	8,11

Fonte: (BURGEISS, 2004).

Tabela 3 - Vazão máxima para diferentes tipos de pacotes.

Sistemas de 1000 Mb/s			
Tamanho do Quadro	Vazão de Dados	Preâmbulo e IGP	Quadros por Segundo
64 bytes	761,90 Mb/s	238,10 Mb/s	1488,1

128 bytes	864,86 Mb/s	135,14 Mb/s	844,59
256 bytes	927,54 Mb/s	72,46 Mb/s	452,9
512 bytes	962,41 Mb/s	37,59 Mb/s	234,96
1024 bytes	980,84 Mb/s	19,16 Mb/s	119,73
1280 bytes	984,62 Mb/s	15,38 Mb/s	96,15
1518 bytes	987,00 Mb/s	13,00 Mb/s	81,27
1522 bytes	987,03 Mb/s	12,97 Mb/s	81,06

Fonte: (BURGESS, 2004).

Cálculo da taxa de bits pode ser expresso por (em Mb/s):

$$\text{taxa_bits} = (\text{frame_len} / (\text{preamb} + \text{frame_len} + \text{igp})) * 100$$

Para um dado tamanho de frame e uma dada taxa de bits, pode-se obter o IGP a partir de:

$$\text{igp} = ((\text{frame_len} * 100) / \text{taxa_bits}) - \text{preamb} - \text{frame_len}$$

A largura de banda expressa a maior capacidade que pode ser obtida através da transferência. A vazão representa a taxa na qual a informação trafega nivelado pelo menor valor de transferência.

2.3.2 Perda de Pacotes

A perda de pacotes avalia quantidade de pacotes que foram enviados pelo transmissor e que nunca foram recebidos em seu destino. É normalmente chamada de taxa de perda de pacotes (*Packet Loss Ratio*), sendo expressa como uma porcentagem do número total de pacotes transmitidos. Os pacotes podem ser perdidos ou descartados por várias razões, incluindo erros, vazão insuficiente e atraso excessivo (BURGESS, 2004).

A perda de pacotes é outro item crítico que implica de forma direta na

qualidade de serviço. Pacotes perdidos em aplicações que utilizam o protocolo UDP (*User Datagram Protocol*) e RTP (*Real Time Protocol*) não podem ser retransmitidos e mesmo que pudessem não seria nada interessante já que duas mensagens enviadas em sequência poderiam chegar em ordem inversa, o que não é tolerável em aplicações de tempo real.

2.3.3 Latência

O tempo de resposta (latência ou atraso da rede): estima o tempo total que um datagrama demora a sair desde sua origem até chegar ao seu destino. Em geral, a latência da rede é medida como o atraso de ida e volta de um datagrama na rede e é calculado considerando a soma dos atrasos de propagação no meio físico de transmissão e o processamento nos elementos de interconexão da rede, ela também é conhecida como RTT (*Round Trip Time*) (MCBRIDE, 2010).

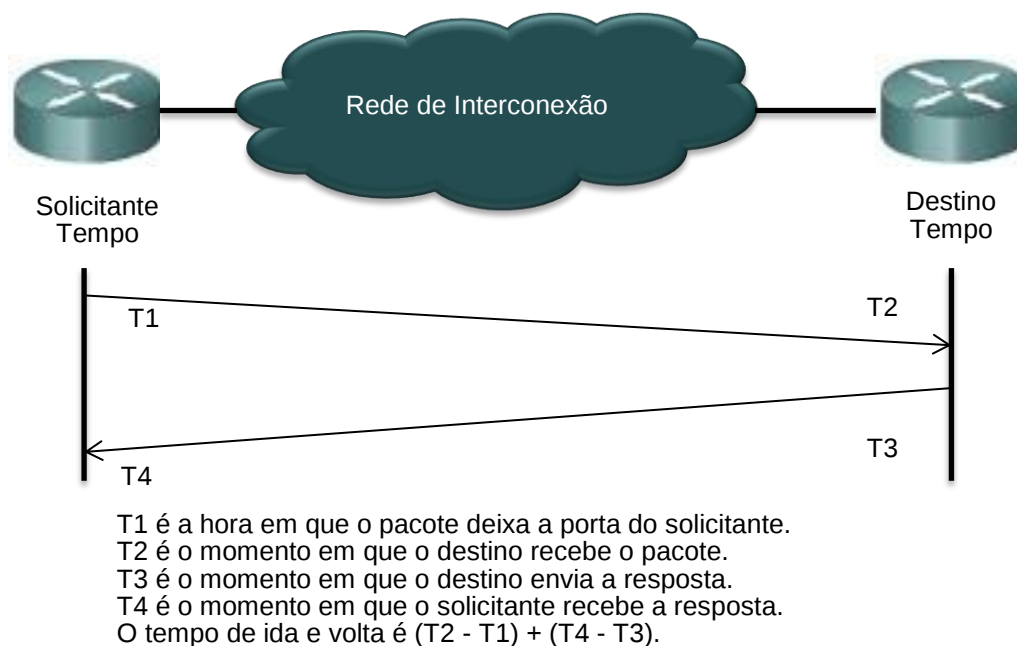


Figura 24: Round Trip Time.

Segundo Comer (2015), parte do atraso em uma rede se deve ao fato de que um sinal exige uma pequena quantidade de tempo para trafegar através de um meio físico. Esses atrasos são conhecidos como atrasos de propagação (*propagation delays*) e são, em muitos casos, proporcionais à distância atendida.

Dispositivos eletrônicos em uma rede de computadores (por exemplo: *pontes*, *comutadores de pacotes*) proporcionam outra origem de atraso conhecida como atraso de comutação (*switching delays*). Tal equipamento espera até que todos os bits de um pacote tenham chegado e então leva uma pequena quantidade de tempo para escolher o próximo *hop* antes de enviar um pacote. A evolução eletrônica desses equipamentos tem tornado os atrasos de comutação menos significativos.

Como a maioria das LANs usa meios compartilhados, os computadores devem esperar até que o meio esteja disponível. Para esse tipo de arquitetura os atrasos, que não são normalmente grandes, são conhecidos como atrasos de acesso (*access delays*).

Já em redes metropolitanas (MAN) e/ou redes de grande cobertura geográfica (WAN) com tecnologia de comutação de pacotes a cada *switch* de pacote, há uma fila de pacotes sendo recebidos como parte do processo de armazenamento e encaminhamento. Caso a fila já contenha pacotes, o novo pacote entrará na fila e aguardará enquanto a CPU encaminha pacotes que entraram nessa ordenação em instantes anteriores. Esses atrasos são conhecidos como atrasos de filas (*queueing delays*).

2.3.4 VARIAÇÃO DE ATRASO (JITTER)

A variação de tempo entre a chegada de cada datagrama do endereço IP de origem para o destino denomina-se *Jitter*. A figura 25 caracteriza o efeito do *jitter* entre o envio de datagramas na origem e o seu processamento no destino. Esse efeito causa não unicamente uma entrega com periodicidade variável (Variação de Pacotes por Atraso), como também a entrega de datagramas fora de ordem.

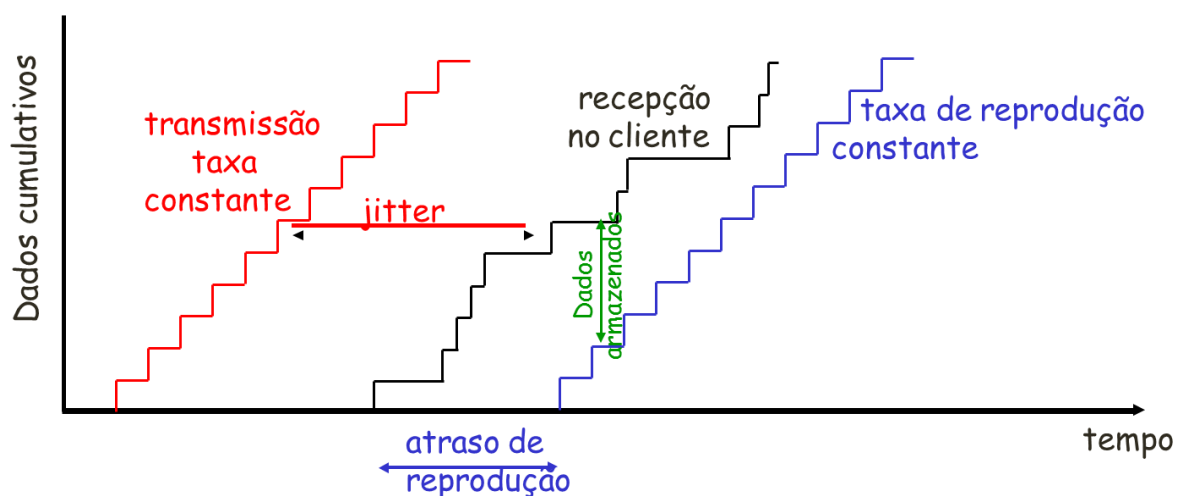


Figura 25 - Variação no atraso (*Jitter*) e compensação no receptor.

Fonte: (KUROSE e ROSS, 2010).

2.3.5 CISCO IP SLA® - IP SERVICE LEVEL AGREEMENT

Um Acordo de Nível de Serviço (ANS) é um acordo formal negociado entre duas partes especificando as características de um serviço. É um contrato que existe entre clientes e seu provedor de serviços, ou entre provedores de serviços. Registra a compreensão dos serviços, prioridades, responsabilidades, garantia etc. com os principais objetivos de acordo com o nível de serviço. Por exemplo, pode especificar os níveis de disponibilidade, facilidade de manutenção, desempenho, operação ou outros atributos do serviço, como faturamento e até incentivos de desempenho e / ou penalidades quando determinado limite de nível de serviço é atingido.

A ferramenta IP SLA é um agente embutido no *software* IOS® (*Internetwork Operating System*) nos equipamentos do fabricante Cisco projetado para medir e monitorar métricas de desempenho de rede como *jitter*, latência (atraso) e perda de pacotes. O IP SLA pode ser usado em todo o ciclo de vida de um SLA como uma ferramenta para quantificar o desempenho da rede em diferentes estágios bem como para uma abordagem proativa e para atender aos requisitos de SLA.

2.3.6 COMPONENTES DO IP SLA

Uma arquitetura básica de IP SLA tem dois componentes principais, conforme figura 26

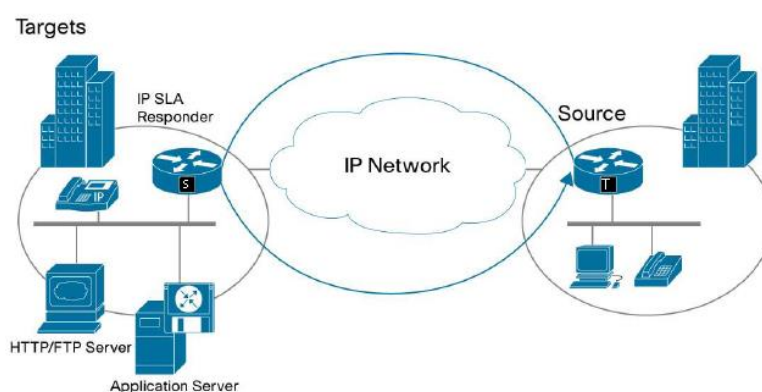


Figura 26 - Componentes do IP SLA.

Fonte: (CISCO WHITEPAPER, 2007).

Source / Fonte (S)

Esta fonte é onde as operações IP SLA são definidas. Com base nos parâmetros de configuração, a fonte gera pacotes específicos para as operações SLA IP definidas e analisa os resultados e os registra de modo que possa ser acessado através de CLI (*Command Line Interface – Interface de linha de comando*) ou SNMP. Um roteador de origem pode ser qualquer roteador Cisco que possa suportar a operação IP SLA que está sendo configurada.

Target / Alvo (T)

O alvo SLA IP depende do tipo de operação IP SLA que foi definida. Para operações FTP / HTTP, o destino seria um servidor FTP / HTTP. Para *Real Time Protocol* (RTP) e *jitter* UDP (voz sobre IP [VoIP]), o alvo deve ser um dispositivo Cisco com o recurso de resposta habilitado, uma vez que tanto a fonte quanto o alvo participam da medição de desempenho. O IP SLA responder tem um benefício adicional de precisão porque *timestamps* são inseridos na carga útil do pacote e,

portanto, mede o tempo de CPU gasto. O IP SLA responder pode ser habilitado com o comando: <ip sla responder>.

Esse é um componente presente apenas nos equipamentos Cisco que permite ao sistema antecipar e responder aos pedidos. Deve ser configurado nos equipamentos de destino de uma operação IP SLA, mas não é obrigatório para todos os tipos de operações. O protocolo de controle de IP SLAs é usado para que o responder seja notificado de que porta deverá escutar e responder. Ele numa porta específica escuta as mensagens de controlo enviadas por uma operação e quando as recebe irá ativar a porta especificada (seja *Transmission Control Protocol* (TCP) ou *User Datagram Protocol* (UDP)) durante um período fixo de tempo. Depois aceitará pedidos e, na sequência, respondê-los, sendo que desativa a porta quando envia a resposta ou o período de tempo especificado expira. Para equipamentos que não sejam Cisco não é possível a sua configuração pelo que o IP SLA apenas envia pacotes de serviços nativos desses aparelhos.

A Figura 27 ilustra o seu funcionamento, onde a partir da origem é enviado um pacote para o equipamento de destino, que após o receber e tendo em conta o tipo de operação a que está associado responde com a informação necessária para na origem ser calculada o valor da métrica.

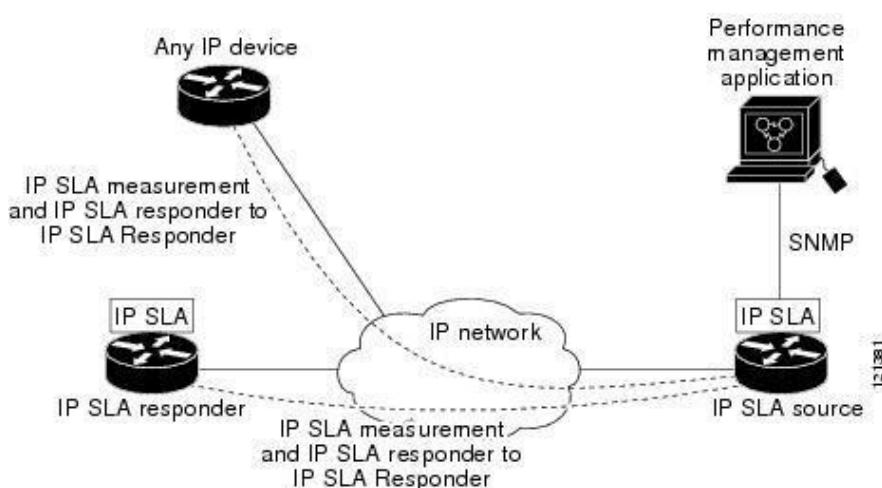


Figura 27 - Funcionamento Cisco IP SLA.

Fonte: (CISCO WHITEPAPER, 2007).

2.3.7 OPERAÇÕES SUPORTADAS PELO IP SLA

- As várias operações IP SLA também podem ser classificadas da seguinte forma:
- Operações baseadas em ICMP para *echo*, *echo* de caminho e *jitter* de caminho;
- As operações baseadas em UDP, como *echo*, *jitter*, DNS (*Domain Name Service*) e DHCP (*Dynamic Host Configuration*);
- As operações baseadas em TCP, como TCP *connect*, FTP (*File Transfer Protocol*) e HTTP (*HyperText Transfer Protocol*);
- As operações de camada 2, como Frame Relay, ATM (*Asynchronous Transfer Mode*) e MPLS (*Multiprotocol Label Switching*);
- Operações VoIP relacionadas, tais como *jitter* VoIP, monitoramento de atraso de registro de *gatekeeper* VoIP e monitoramento de configuração de chamada VoIP (atraso de postagem).

Quadro 2 - Requerimentos e métricas para monitorar operações IP SLA.

	Tráfego de dados	Acessibilidade	Gerenciamento de Nível de Serviço	VoIP	Transmissão de vídeo
Requerimentos	• Minimizar atraso, perda de pacotes • Verificar qualidade do serviço (QoS)	• Teste de conectividade • Teste de aplicação	• Medir atraso, perda de pacote, <i>jitter</i> • Mão única	• Minimizar atraso, perda de pacote, <i>jitter</i>	• Minimizar atraso, perda de pacote
Métricas ANS IP	• <i>Jitter</i> • Perda de pacote • Latência • por Qos	• Testes de conectividade para IP • Testes de conectividade para serviços de rede • Conectividade de rede	• <i>Jitter</i> • Perda de pacote • Latência • Mão única • Precisão aprimorada • NTP	• <i>Jitter</i> • Perda de pacote • Latência • MOS, ICPIF • Pontuação de qualidade de voz	• <i>Jitter</i> • Perda de pacote • Latência

Operação ANS IP	• <i>Jitter</i>	• Echo • TCP • FTP, HTTP • DNS, DHCP • DLSW +, MPLS, ATM, Frame Relay	• UDP <i>jitter</i>	• VoIP UDP <i>jitter</i> • VoIP RTP • VoIP configuração de chamada • VoIP	• UDP <i>jitter</i>
------------------------	---	---	---	--	---

Fonte: Adaptado pelo Autor (CISCO WHITEPAPER, 2007).

Tabela 4 - Limite de desempenho recomendado.

Tipo de Tráfego	Perda máxima de pacotes	Atraso máximo em fluxo de sentido único	<i>Jitter</i> Máximo
VoIP	1%	120 ms	30 ms
Videoconferência	1%	150 ms	50 ms
Fluxo contínuo de Video	2%	5 s	N/A

Fonte: (CISCO WHITEPAPER, 2007).

3. MATERIAIS E MÉTODOS

Um dos grandes desafios para o uso de sistemas de gerenciamento baseados em políticas para distribuição de tráfego em redes de telecomunicações é, em tempo real, coletar informações e correlacioná-las de forma que, mesmo previamente tendo sido estabelecido uma rota, seja capaz de alterá-la para prover uma maior qualidade de serviço para determinadas aplicações de produção (RESENDE et al., 2005).

Na avaliação funcional do sistema proposto observou-se a necessidade de:

- ✓ *Aproveitamento da tecnologia Cisco IOS IP SLA;*
- ✓ *Possibilidade de configuração remota automática de operações IP SLA;*
- ✓ *Captura e visualização dos dados de operações;*
- ✓ *Monitoração simultânea de múltiplas operações em múltiplos equipamentos;*
- ✓ *Capacidade de coletar as informações de rotas divulgadas pelo protocolo BGP através do uso de protocolo de gerenciamento SNMP versão 1 ou versão 2;*

3.1 Desenvolvimento do Sistema Especialista paraconsistente “SharpNet ParaControl”

O sistema especialista paraconsistente proposto nesse trabalho doravante chamado de **SharpNet ParaControl** e representado em blocos na figura 28, considera o uso dos fundamentos da Lógica Paraconsistente Anotada Evidencial Et e é composto por:

- a) Um componente chamado Monitor, usado para a coleta das informações dos equipamentos de interconexão de rede;
- b) Um módulo Registrador onde são armazenadas métricas, tipos de interligação e demais informações dos enlaces de comunicação para servirem de entrada para o próximo componente como fontes de

informação;

- c) Bloco de análise paraconsistente que chamaremos de controlador paraconsistente com a função de analisar as informações de entrada e fornecer como saída, a informação que definirá se deve ou não mudar a rota do tráfego para outra rota com melhor qualidade dentre os disponíveis no cache de rotas;
- d) O módulo Avaliador de mudanças que, a partir da informação recebida do Bloco controlador paraconsistente, escolhe se existente, outra rota disponível dentro das rotas avaliadas e em caso de não evidência de degradação envia a informação para o módulo de gerência;
- e) O módulo de Gerência, cuja função é enviar a informação para alteração da rota aos equipamentos de interconexão.

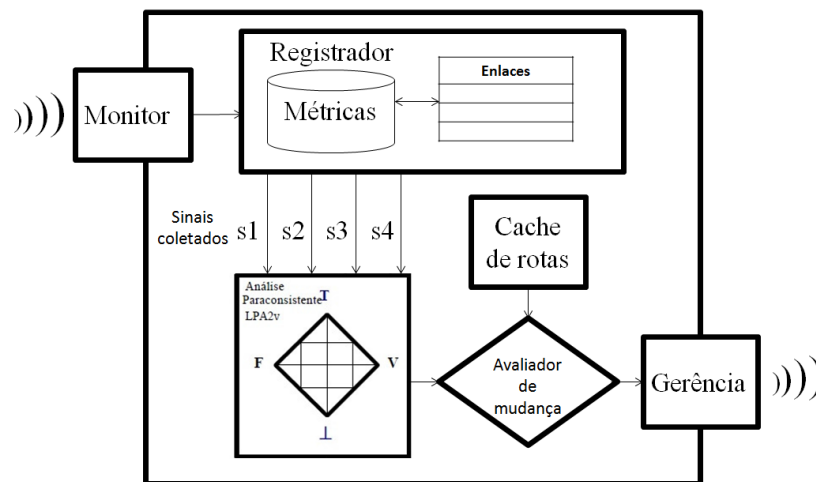


Figura 28 - Diagrama em blocos do Sistema especialista de gerenciamento usando Lógica Paraconsistente Evidencial E_{τ} .

3.1.1 Fundamento Básico do Controlador Paraconsistente

As análises de sinais e evidências são feitas por algoritmos originados dos fundamentos da Lógica Paraconsistente Anotada Evidencial E_{τ} que buscam valores de tempo de latência da rota de comunicação (RTT), perda de pacotes (PEP),

variação no atraso de transmissão (*jitter-SD*), variação no atraso de recepção (*jitter-DS*) e consumo de processamento (CPU) em um banco de dados originado da coleta em tempo real dos sinais originados nos equipamentos de interconexão e modelagem de sinais do módulo Monitor. O Controlador Paraconsistente faz uso de uma RNAP interligada ao algoritmo extrator dos efeitos da contradição e é representado na figura 29.

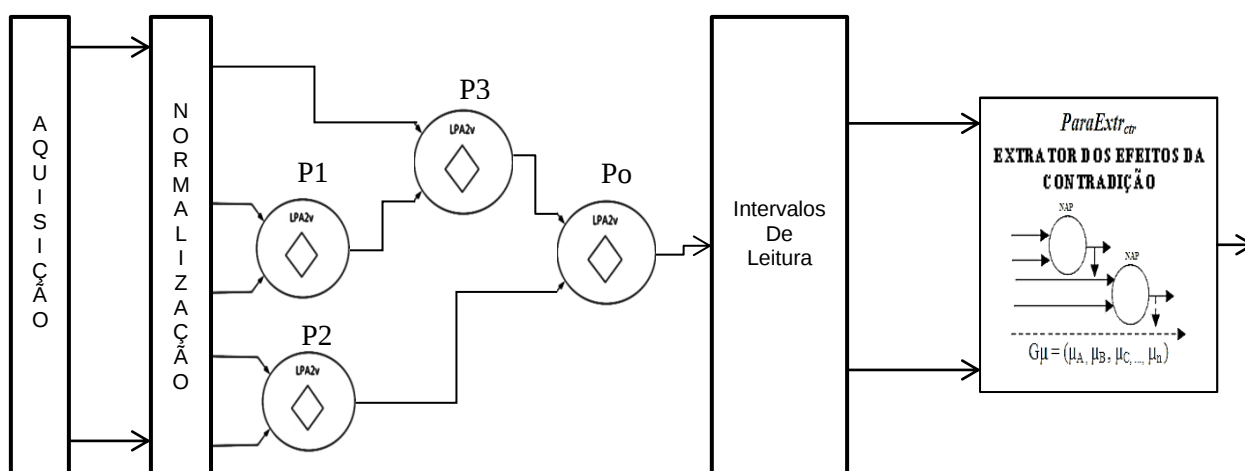


Figura 29 - Controlador Paraconsistente.

Com os dados recebidos na entrada do controlador três etapas são executadas:

1) Normalização

Nessa primeira etapa os sinais em suas unidades de métricas originais entram em um processo de modelagem, que se inicia com a seleção de um Intervalo de Interesse ou Universo de Discurso. A seguir, são normalizados e seus valores inseridos dentro de um intervalo fechado $[0,1]$ pertencente ao conjunto dos números reais, os quais representam Graus de evidência μ_E para a LPA2v (DA SILVA FILHO, 1999).

2) Inserção das evidências na RNAP

Aplicação das evidências favoráveis às proposições na RNAP para obtenção dos valores de evidência real que serão analisados na próxima etapa após concluírem um grupo de 10 leituras, essa quantidade foi definida pelo autor para melhor veracidade da análise, eliminando possíveis divergências ou inconsistências

causadas por leituras efetuadas em instantes de instabilidade momentânea da rota ou de eventos pontuais de rajadas de tráfego concorrente nos enlaces.

3) *Extração dos efeitos da Contradição*

Nessa etapa os sinais representados por Graus de Evidência são analisados por Algoritmos da Lógica Paraconsistente compostos por uma rede de Análises Paraconsistente combinada com um Extrator de Efeitos da Contradição, estes por sua vez, recebem um grupo de sinais e, independentemente de outras informações externas tem, como função, fazer uma análise paraconsistente em seus valores subtraindo os efeitos causados pela contradição e apresentando na saída um único Grau de Evidência resultante real (DA SILVA FILHO, 1999).

O grau de Evidência da proposição: “**Existe degradação no enlace**” para cada arco de comunicação que compõe a rota entre os pontos comunicadores pelos quais os pacotes de informação devem passar é extraído e avaliado. Após a análise, a rota composta por esses enlaces que possuem um valor de Grau de Evidência Favorável acima de um determinado limiar e considerados degradados, não deve ser usada para o tipo de tráfego proposto na análise.

3.1.2 **Interface do Sistema e suas funcionalidades**

A *interface* foi desenvolvida em linguagem de programação Java através do *software* Netbeans IDE 8.2, pela sua extensa biblioteca de funções assim como pela capacidade de programação orientada a objetos. O NetBeans é um ambiente de desenvolvimento utilizado por programadores que permite escrever, compilar, depurar e instalar programas, bem como, pode suportar um número extenso de outras linguagens de programação. Existe também um grande número de módulos para estender suas funcionalidades (GONÇALVES, 2008).

A escolha da linguagem de programação Java é a facilidade de possuir bibliotecas de classe que são conhecidas como APIs (*Application Programming Interfaces*). Portanto, o primeiro aspecto é a linguagem Java em si onde se pode programar as próprias classes ou fazer uso de classes já existentes nas bibliotecas

(DEITEL e DEITEL, 2010).

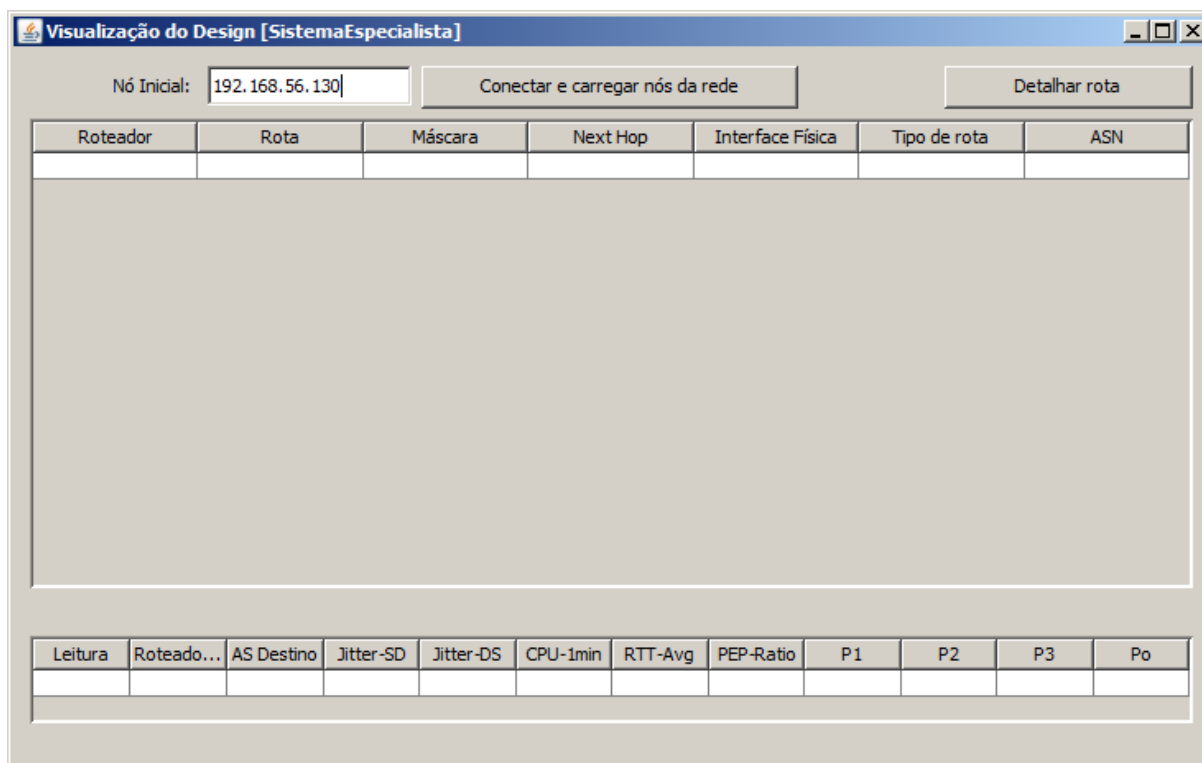


Figura 30 - Interface do Sistema Especialista SharpNet ParaControl.

Na tela inicial do sistema (Figura 30), deverá ser informado um endereço de rede do equipamento de onde se iniciará a pesquisa da estrutura da rede (nó inicial). Este endereço (*IP – Internet Protocol*) deve ser utilizado com objetivo de se obter informações da estrutura de conexão entre os equipamentos.

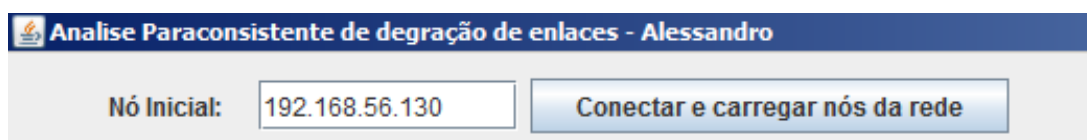


Figura 31 - Fonte de pesquisa da estrutura de conexões: nó inicial de rede.

Ao clicar no botão “Conectar e carregar nós da rede” serão exibidas as informações do módulo Registrador:

Análise Paraconsistente de degração de enlaces - Alessandro

Nó Inicial: 192.168.56.130 Conectar e carregar nós da rede Detalhar rota

Roteador	Rota	Mascara	Next Hop	Interface Física	Tipo de rota
192.168.56.130	172.30.30.0	255.255.255.252	0.0.0.0	LOCAL	3
192.168.56.130	172.30.30.4	255.255.255.252	0.0.0.0	LOCAL	3
192.168.56.130	172.30.30.8	255.255.255.252	172.30.30.2	3	4
192.168.56.130	172.30.30.9	255.255.255.255	172.30.30.2		4
192.168.56.130	172.30.30.10	255.255.255.255	172.30.30.2		4
192.168.56.130	172.30.30.12	255.255.255.252	172.30.30.6	4	4
192.168.56.130	172.30.30.13	255.255.255.255	172.30.30.6		4
192.168.56.130	172.30.30.14	255.255.255.255	172.30.30.6		4
192.168.56.130	172.30.30.16	255.255.255.252	172.30.30.2	3	4
192.168.56.130	172.30.30.20	255.255.255.252	172.30.30.6	4	4
192.168.56.130	172.30.30.24	255.255.255.252	172.30.30.2	3	4
192.168.56.130	172.30.30.25	255.255.255.255	172.30.30.2		4
192.168.56.130	172.30.30.26	255.255.255.255	172.30.30.2		4
192.168.56.130	172.30.30.28	255.255.255.252	172.30.30.6	4	4
192.168.56.130	172.30.30.29	255.255.255.255	172.30.30.6		4
192.168.56.130	172.30.30.30	255.255.255.255	172.30.30.6		4

Figura 32 - Módulo Registrador - Painel de rotas e interfaces dos equipamentos.

Na figura 32 observa-se que o sistema buscou em tempo real todas as informações de *interfaces* e interconexões dos equipamentos de rede a partir do nó inicial informado, na sequência o Painel gráfico (figura 33) exibirá as conexões existentes entre os equipamentos.

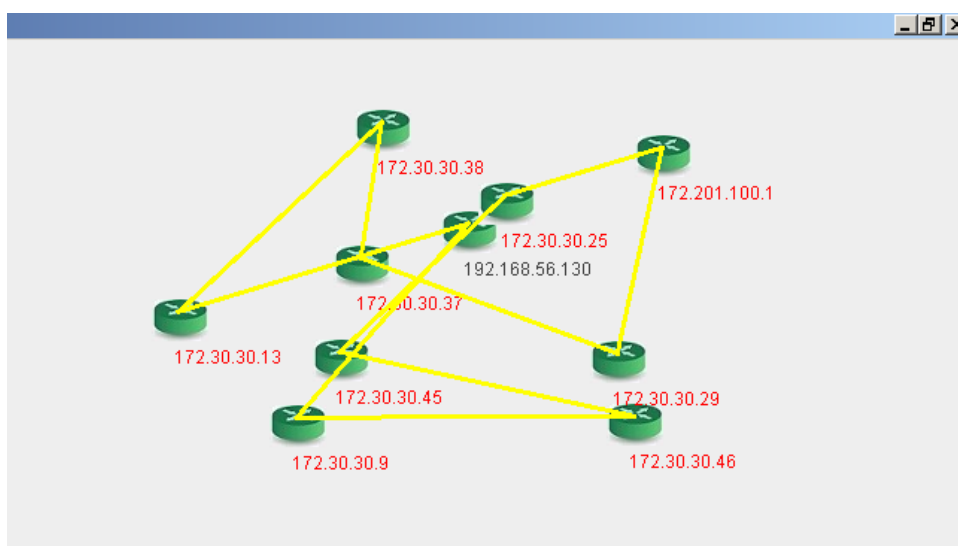


Figura 33 - Módulo Registrador - Painel gráfico com as conexões existentes entre os equipamentos.

No próximo passo é selecionada no painel de rotas a linha que contém a

rota a ser avaliada pelo sistema especialista conforme figura 34.

Análise Paraconsistente de degradação de enlaces - Alessandro

Nó Inicial: 192.168.56.130 Conectar e carregar nós da rede Detalhar rota

Roteador	Rota	Mascara	Next Hop	Interface Física	Tipo de rota	ASN
192.168.56.130	172.30.30.32	255.255.255.252	172.30.30.2	3	4	65100
192.168.56.130	172.30.30.36	255.255.255.252	172.30.30.6	4	4	65100
192.168.56.130	172.30.30.44	255.255.255.252	172.30.30.2	3	4	65100
192.168.56.130	172.30.30.48	255.255.255.252	172.30.30.6	4	4	65100
192.168.56.130	172.100.100.0	255.255.252.0	0.0.0.0	LOCAL	3	65100
192.168.56.130	172.101.100.0	255.255.252.0	0.0.0.0	LOCAL	3	65100
192.168.56.130	172.200.100.0	255.255.252.0	172.30.30.6	3	4	65100
192.168.56.130	172.201.100.0	255.255.252.0	172.30.30.6	3	4	65100
192.168.56.130	192.168.56.0	255.255.255.0	0.0.0.0	LOCAL	3	65100
172.30.30.2	172.30.30.0	255.255.255.252	0.0.0.0	LOCAL	3	65101
172.30.30.2	172.30.30.4	255.255.255.252	172.30.30.1	1	4	65101
172.30.30.2	172.30.30.8	255.255.255.252	0.0.0.0	LOCAL	3	65101
172.30.30.2	172.30.30.10	255.255.255.255	0.0.0.0	LOCAL	3	65101
172.30.30.2	172.30.30.12	255.255.255.252	172.30.30.1	1	4	65101
172.30.30.2	172.30.30.13	255.255.255.255	172.30.30.1		4	65101
172.30.30.2	172.30.30.14	255.255.255.255	172.30.30.1		4	65101

Figura 34 - Seleção da rota para a rede destino a ser analisada pelo sistema especialista.

Ao selecionar a linha desejada e clicar no botão “Detalhar rota” o módulo monitor é ativado para que se inicie a coleta de informações, também nesse instante o Painel gráfico altera a cor para verde dos enlaces que compõem a rota selecionada como observado na figura 35:

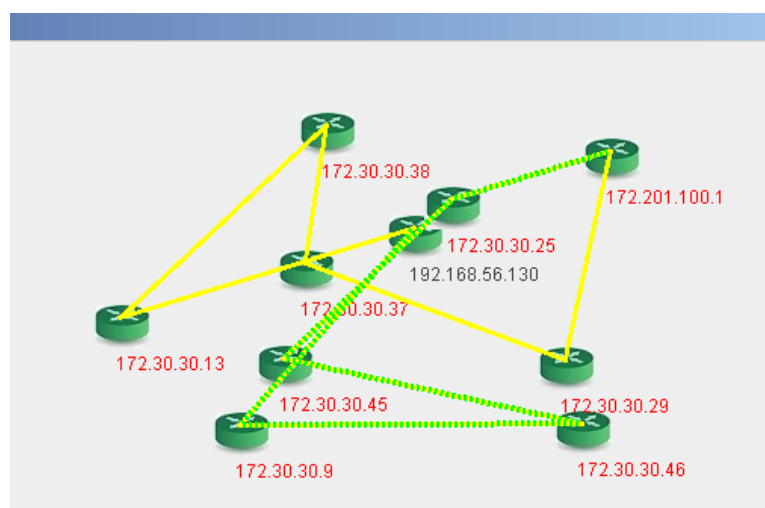


Figura 35 - Indicação da rota selecionada no Painel gráfico.

Uma vez ativado o módulo monitor a coleta se inicia naquele instante e, a

cada intervalo de 1 minuto, as informações são capturadas nos equipamentos e inseridas na base de dados (tabela na parte superior da figura 36) e usadas para a análise da RNAP. Como se observa na parte inferior da figura, após dez leituras, é executado o algoritmo extrator de contradição e obtido o grau de evidência resultante real de toda a estrutura paraconsistente.

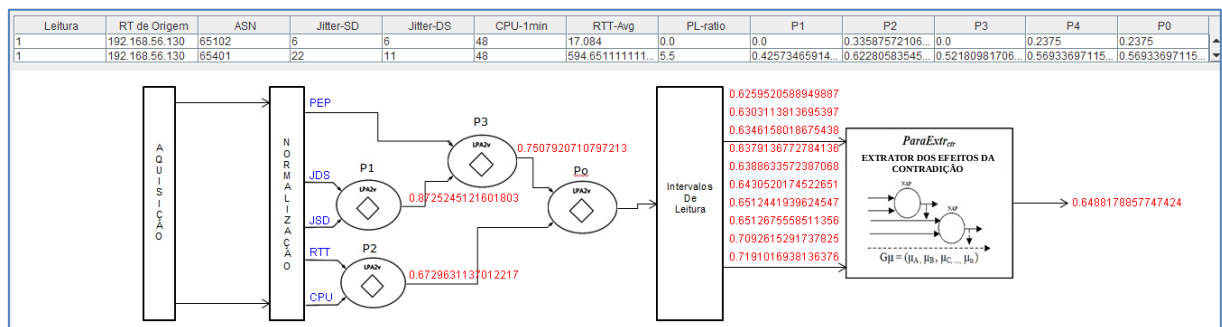


Figura 36 - Módulo Monitor efetuando coleta em tempo real e ativando a análise paraconsistente.

Como último passo da *interface* gráfica, uma função grava as informações coletadas/geradas em formato de planilha para posterior consulta e validação dos ensaios.

	A	B	C	D	E	F
1	SharpNet ParaControl - 1ª leitura					
2						
3	Valores capturados					
4						
5	AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
6	65101	11	7	19	57.13855421686747	0.04
7	65301	26	16	19	1024.9019607843138	7.45
8	65300	28	19	19	1064.0725806451612	7.52
9	65302	30	21	19	1124.0	7.48
10	65201	33	23	19	1293.1544715447155	7.54
11	65200	35	21	19	1339.717213114754	7.56
12	Valores modelados					
13						
14	AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
15	65101	0.05	0.0	0.1125	0.0	0.0
16	65301	0.8	0.3	0.1125	1.0	0.9214285714285715
17	65300	0.9	0.45	0.1125	1.0	0.9314285714285714
18	65302	1.0	0.55	0.1125	1.0	0.9257142857142858
19	65201	1.0	0.65	0.1125	1.0	0.9342857142857143
20	65200	1.0	0.55	0.1125	1.0	0.937142857142857
21	Valores obtidos nas proposições					
22						
23	AS-Destino	P1	P2	P3	P0	
24	65101	0.03535533905932742	0.0795495128834866	0.025000000000000022	0.058962382075353814	
25	Resultado1-21062017123109 / Resultado2-21062017123209 / Resultado3-21062017123309 / Resultado4-21062017123409					

Figura 37 - Função de exportação dos dados em formato de planilha e sua exibição.

3.2 VALORES PARA DEFINIÇÃO DE MÉTRICAS

Em termos de *desempenho*, um tempo de atraso elevado na transmissão do datagrama, bem como a própria variação desse atraso ou a existência de perda de pacotes na rede pode tornar inviável a utilização de aplicações sensíveis a estas métricas. Aplicações como o *voice over IP* (VoIP) e videoconferência que se aproveitam do tráfego em tempo real, podem ser direta e negativamente afetadas com a existência de perda de pacotes e/ou de um atraso elevado. Dessa necessidade de desempenho adequado as empresas buscam garantir o valor mínimo possível para suas métricas em um contrato de SLA. Para esse trabalho foram definidas as métricas e seus respectivos valores de referência como fontes de informação do sistema desenvolvido (SOARES VAZ, 2011).

Variação no atraso: variação no atraso de transmissão de um pacote ou datagrama entre a origem e o destino ou vice-versa.

Fiabilidade: representada por uma porcentagem de pacotes que uma vez enviados para a rede IP endereçada não chegam ao seu destino enquanto transportados pelo *Backbone* IP do provedor ou demais elementos de interconexão. Este efeito denomina-se por taxa perda de pacotes (*Packet Loss Ratio*).

Latência Tempo de Trânsito ou o período de tempo que um pacote IP demora a transitar na rede IP do provedor até chegar ao equipamento de interconexão de acesso na rede IP do provedor no ponto de saída para o seu destino. A contabilização deste atraso é expressa em milissegundos e é medido e definido unicamente para os pacotes que atingem o seu destino com fiabilidade. Para esse trabalho considerou-se o tempo de chegada e retorno dos pacotes.

Consumo de CPU: Representado pela porcentagem de uso da unidade de processamento central (CPU – *Central Processing Unit*), esse consumo impacta diretamente no tempo de transferência de uma *interface* física para outra dentro do equipamento de interconexão.

Tabela 5 - Valores para definições de métricas

Métrica	Valores de referência	
	Minima	máxima
Variação no atraso:		
<i>Jitter DS(Destination/Source)</i>	10 ms	50 ms
<i>Jitter SD(Source/Destination)</i>		
Fiabilidade– <i>Packet Loss</i>	< 1%	8%
Latência total - RTT	160 ms	680 ms
Consumo de CPU	30%	90%

3.3 Coleta de dados e Rede Piloto

Para o desenvolvimento da pesquisa foi considerada a arquitetura de uma rede de comunicação de dados típica de distribuição entre localidades distintas (Figura 38) para servir como fonte de dados primária. Para a função de coleta de dados que alimenta o módulo Monitor do sistema proposto, utilizaram-se acessos de leitura com o protocolo SNMP, tanto para informações de perda de pacotes, como para *jitter*, consumo de CPU e latência. Cada coleta foi executada em intervalos de 1 minuto. Essa frequência de coleta foi definida levando-se em consideração que o consumo de CPU (uma das fontes de informação) tem sua leitura via protocolo SNMP limitada a um mínimo de 1 minuto. A partir desta informação a operação IP SLA utilizada nos equipamentos da rede piloto para verificação das métricas entre dois sistemas autônomos distintos é a *UDP-Jitter* (CISCO WHITEPAPER, 2007), a vantagem dessa operação, conforme figura 27, é de que cada equipamento da rede gerará informações que poderão ser usadas como evidências para o sistema especialista desenvolvido. Em todos os equipamentos de interconexão da rede piloto será configurada essa operação tratando como destino cada um dos demais equipamentos, permitindo que as métricas sejam geradas entre todos os nós de interconexão. Essa operação será configurada e ativada com os seguintes comandos em cada equipamento (quadro 3):

Quadro 3 - Comandos de configuração e ativação da operação IP SLA

```
ip sla monitor <operation-number>
type jitter dest-ipaddr <ip-address> dest-port 16548 codec g711alaw codec-interval 20 codec-numpackets
1000 codec-size 25 control enable advantage-factor 0
ip sla monitor schedule <operation-number> start-time now life forever
ip sla monitor responder
```

onde:

<operation-number> será representado pelo número do sistema autônomo destino;

<ip-address> será representado pelo endereço IP do sistema autônomo destino.

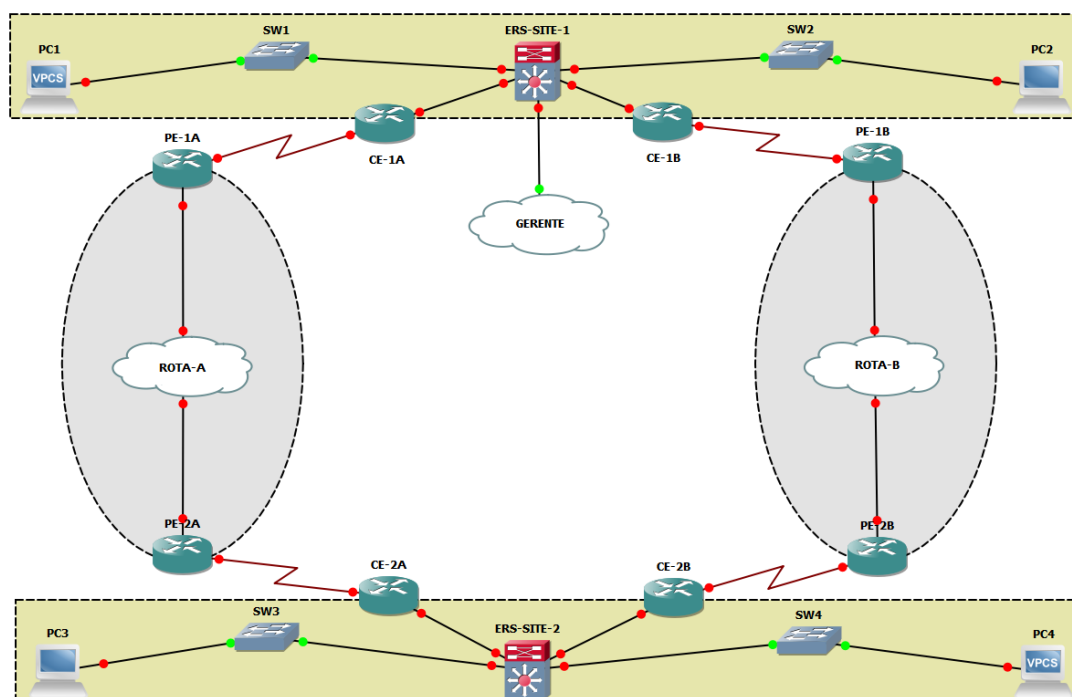


Figura 38 - Ambiente avaliado com roteamento de rede por rotas distintas.

Foi projetada uma rede piloto com equipamentos do fabricante Cisco para o estudo das diversas tecnologias de interconexão e controle de tráfego em um sistema de transmissão de dados e voz sobre o protocolo IP (*Internet Protocol*) (WALLACE, 2014). Para aplicação da configuração proposta na figura 38 utilizou-se equipamentos da família 3945, 1911, 2911, 2921, 3750X e 7200.

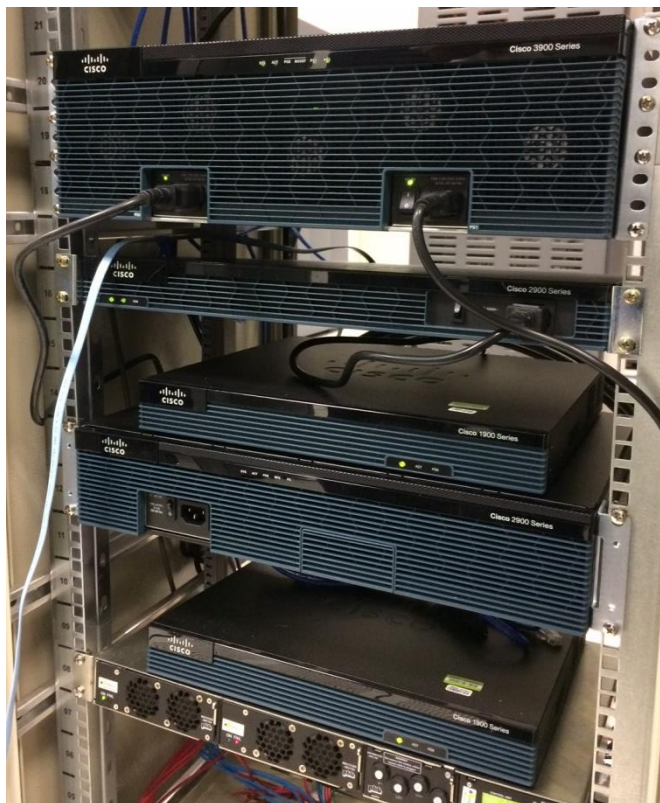


Figura 39 - Roteadores instalados na rede piloto.



Figura 40 - Comutadores de rede instalados na rede piloto.

A rede seguiu um plano de endereçamento IP (*Internet Protocol*) conforme informações abaixo:

Tabela 6 - Endereçamento da localidade 01 da rede piloto.

LOCALIDADE-01					
EQUIPAMENTOS INTERFACES	PC1	PC2	ERS-SITE-1	CE-1A	CE-1B
ETHERNET-0	172.100.100.254/22	172.101.100.254/22			
FASTETHERNET-1/0			172.100.100.1/22	172.30.30.2/30	172.30.30.6/30
FASTETHERNET-2/0			172.101.100.1/22		
FASTETHERNET-3/0			172.30.30.1/30		
FASTETHERNET-4/0			172.30.30.5/30		
SERIAL-0/1				172.30.30.9/30	172.30.30.13/30
ASN			65100	65101	65102

Tabela 7 - Endereçamento da localidade 01 da rede piloto.

LOCALIDADE-02					
EQUIPAMENTOS INTERFACES	PC3	PC4	ERS-SITE-2	CE-2A	CE-2B
ETHERNET-0	172.200.100.254/22	172.201.100.254/22			
FASTETHERNET-1/0			172.200.100.1/22	172.30.30.18/30	172.30.30.22/30
FASTETHERNET-2/0			172.201.100.1/22		
FASTETHERNET-3/0			172.30.30.17/30		
FASTETHERNET-4/0			172.30.30.21/30		
SERIAL-0/0				172.30.30.25/30	172.30.30.29/30
ASN			65200	65201	65202

Tabela 8 - Endereçamento da rota A da rede piloto.

ROTA-A			
EQUIPAMENTOS INTERFACES	PE-1A	PE-2A	BACKBONE-A
GERÊNCIA/LOOPBACK			
FASTETHERNET-0/0	172.30.30.46/30	172.30.30.34/30	
FASTETHERNET-1/0			172.30.30.45/30
FASTETHERNET-2/0			172.30.30.33/30
SERIAL-0/0	172.30.30.10/30	172.30.30.26/30	
ASN	65301	65302	65300

Tabela 9 - Endereçamento da rota B da rede piloto.

ROTA-B			
EQUIPAMENTOS INTERFACES	PE-1B	PE-2B	BACKBONE-B
GERÊNCIA/LOOPBACK			
FASTETHERNET-0/0	172.30.30.38/30	172.30.30.50/30	
FASTETHERNET-1/0			172.30.30.37/30
FASTETHERNET-2/0			172.30.30.49/30
SERIAL-0/0	172.30.30.14/30	172.30.30.30/30	
ASN	65401	65402	65400

A partir desse ponto, toda a configuração envolvida foi padronizada em um conjunto de comandos encontrados no Apêndice A, onde também está detalhada sua sequência por equipamento utilizado no experimento dentro da rede piloto.

3.5 MODELAGEM E NORMALIZAÇÃO DOS DADOS COLETADOS

Para o processo de normalização define-se um universo de discurso com valores das grandezas e obtêm-se os Graus de Evidência a partir de uma equação da reta. O Valor limite máximo do Universo de Discurso para o valor da Grandeza será: a_2 . O valor limite mínimo do Universo de Discurso para o valor da Grandeza será: a_1 . A forma gráfica de uma grandeza que varia aumentando proporcionalmente e sendo relacionada com o Grau de Evidência Normalizado μ , será representada conforme a gráfico 1.

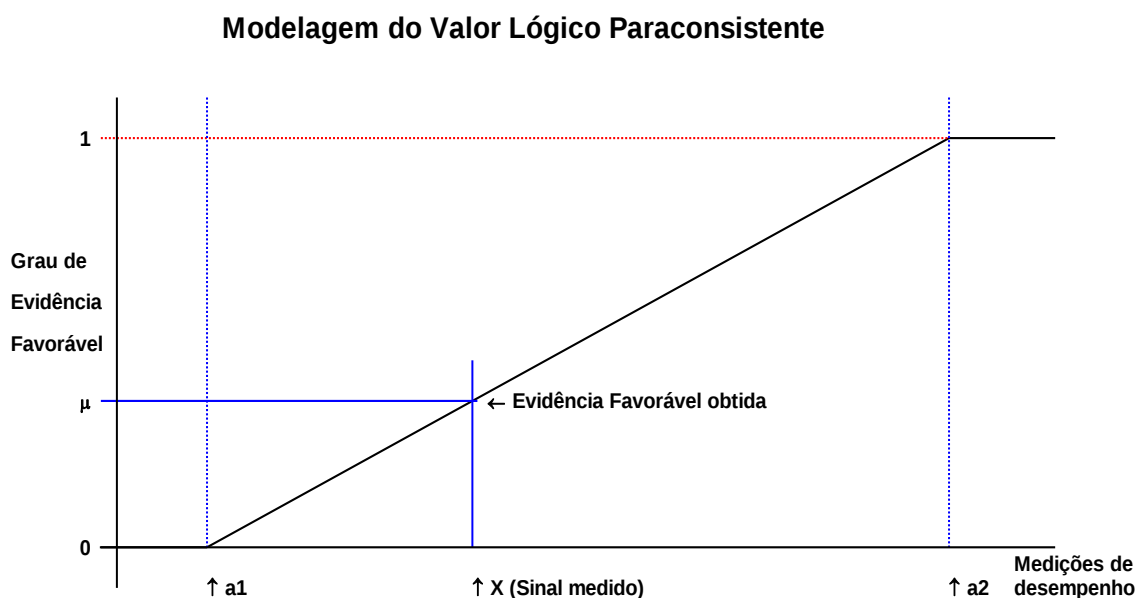


Gráfico 1: Valoração do Grau de Evidência com variação linear e diretamente proporcional a grandeza medida.

Dessa forma o Grau de Evidência para uma variação linear ascendente será encontrado através das equações de normalização a seguir:

$$\mu(x) = \begin{cases} \frac{x-a1}{a2-a1}, & \text{se } x \in [a1, a2] \\ 1, & \text{se } x > a2 \\ 0, & \text{se } x < a1 \end{cases}$$

Onde: x é o valor medido da grandeza.

a1 = Menor valor do universo de discurso a ser analisado

a2 = Maior valor do universo de discurso a ser analisado

μ = Grau de evidência favorável obtido (medição da grandeza normalizada)

Para a determinação do grau de evidência da intensidade da fonte de informação em cada rota de comunicação foram considerados os eventos de menor e maior valor referenciados na tabela 5 e aplicados ao alvo da análise. Após a conclusão desta etapa, empiricamente foi adotado a normalização de valores das medidas de leituras dos equipamentos através de modelagem com variação linear e diretamente proporcional à grandeza medida, resultando em um valor normalizado entre 0 e 1, demonstrando assim, o grau de evidência do sinal obtido da fonte de informação.

Considerando o referendado acima, cada medição caracterizou a obtenção do Grau de Evidência Favorável de cada grandeza conforme proposições parciais e proposição objeto como se segue:

Para o NAP P1 que responde à proposição “Existe variação de atraso na transmissão”, duas fontes de informação são utilizadas como graus de evidência favorável:

μ_1 = Evidência Favorável *Jitter Source/Destination* modelada no gráfico 2;

μ_2 = Evidência Desfavorável *Jitter Destination/Source* modelada no gráfico 3;

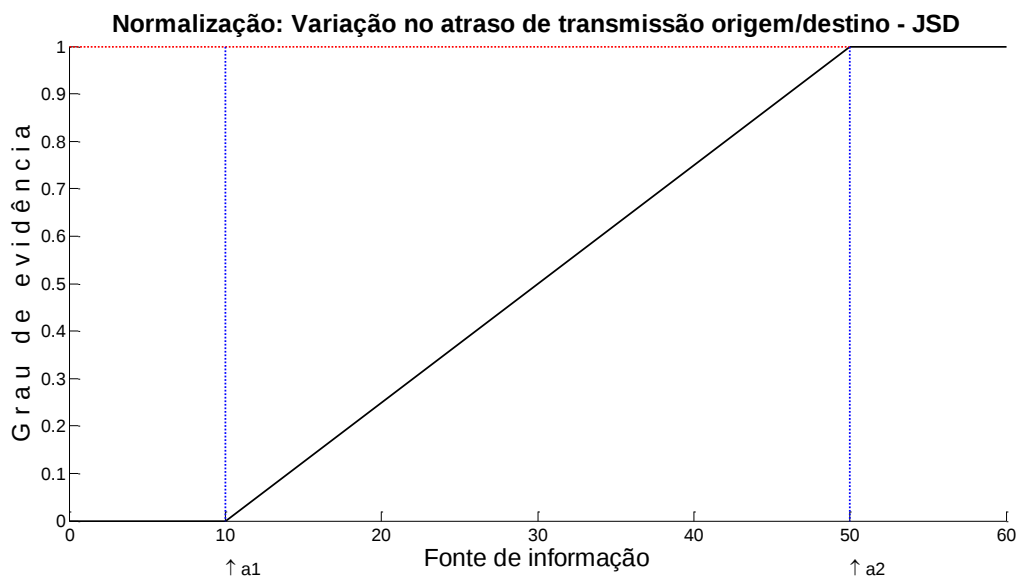


Gráfico 2 - Grandeza da fonte de informação – Variação no atraso de transmissão origem/destino (JSD) - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.

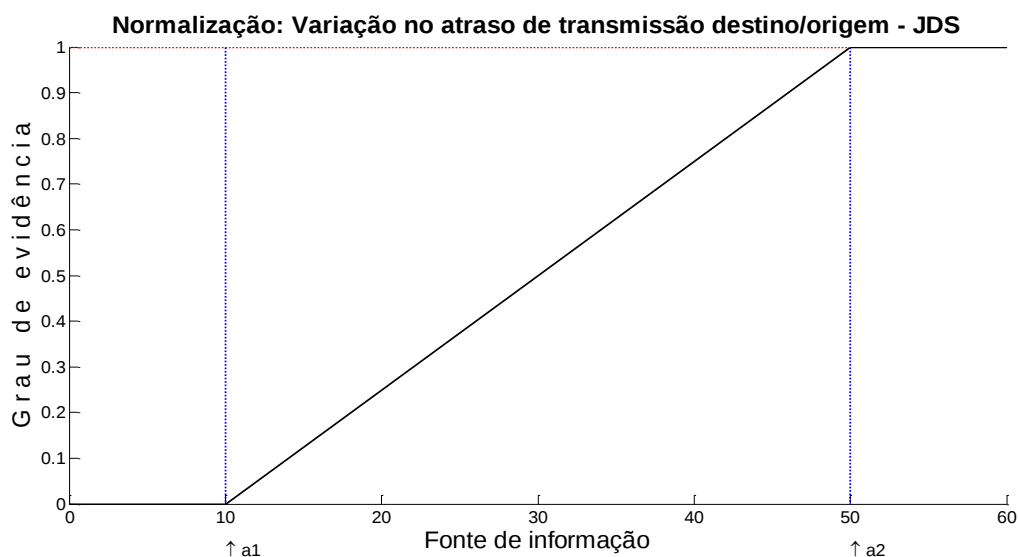


Gráfico 3 - Grandeza da fonte de informação – Variação no atraso de transmissão destino/origem (JDS) - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.

Para o NAP P2 que responde à proposição “Existe fator de degradação controlável”, duas fontes de informação são utilizadas como graus de evidência

favorável:

μ_1 = Evidência Favorável *Round Trip Time* modelada no gráfico 4;

μ_2 = Evidência Desfavorável *Busy CPU*(consumo de processamento) modelada no gráfico 5;

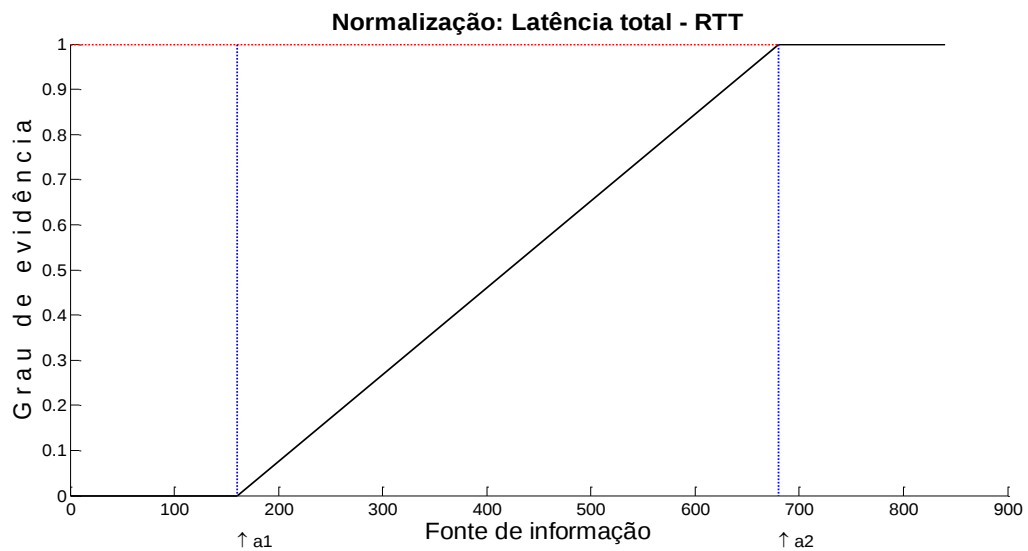


Gráfico 4 - Grandeza da fonte de informação – Latência Total/RTT - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.

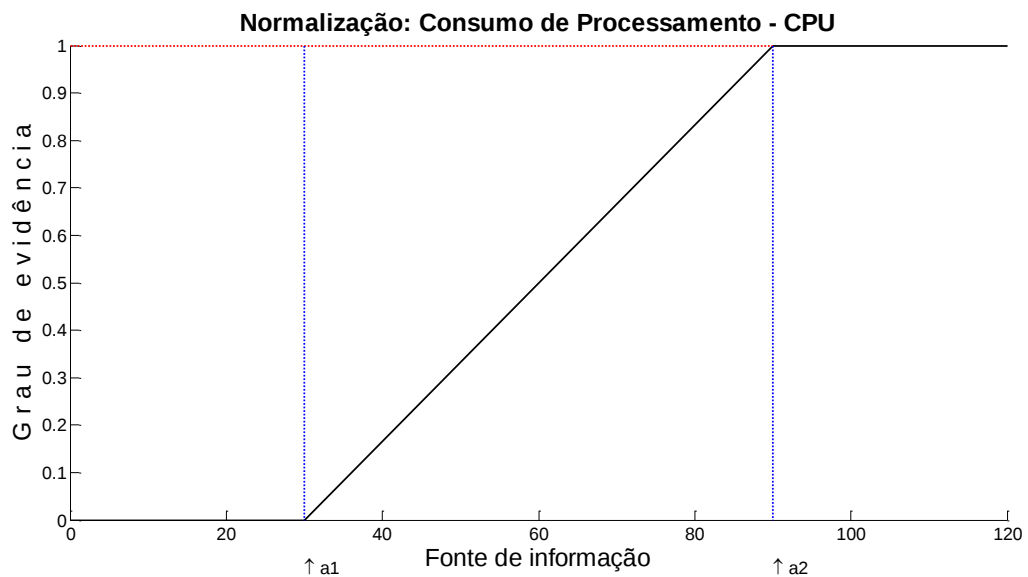


Gráfico 5 - Grandeza da fonte de informação – Consumo de Processamento/CPU - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.

Para o NAP P3 que responde à proposição “Existe fator de degradação não-controlável”, duas fontes de informação são utilizadas como graus de evidência favorável:

μ_1 = Evidência Favorável μ_{ErP1} , evidência Resultante Real obtida no NAP P1;

μ_2 = Evidência Desfavorável *PEP-Packet Loss Ratio* (Taxa de Perda de Pacotes) modelada no gráfico 6;

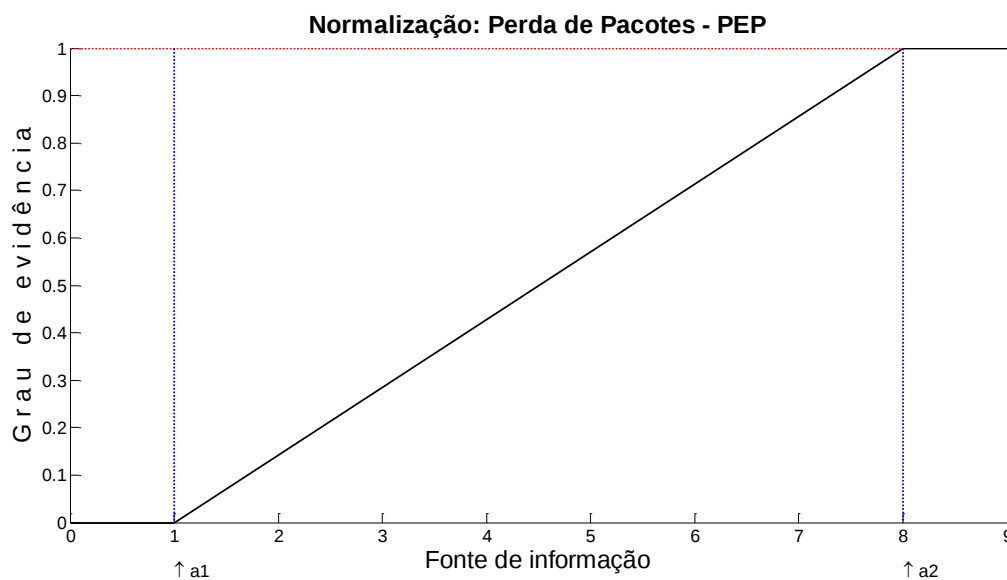


Gráfico 6 - Grandeza da fonte de informação – Perda de Pacotes - variando de modo diretamente proporcional relacionada com o Grau de Evidência Normalizado.

Para o NAP Po que responde à proposição objeto “Existe degradação do enlace”, duas fontes de informação são utilizadas como graus de evidência favorável:

μ_1 = Evidência Favorável μ_{ErP3} evidência Resultante Real obtida no NAP P3;

μ_2 = Evidência Desfavorável μ_{ErP2} evidência Resultante Real obtida no NAP P2;

A saída desse NAP pode ser analisada com base na tabela 10 a seguir:

Tabela 10 - Característica da análise do grau de evidência resultante real obtido na saída do algoritmo.

(Φ_E) - Intervalo de Evidência Resultante	(μ_{ER}) - Grau de Evidência Resultante Real	Análise da saída
1.00	0.000	Falso F
0.75	0.125	Limite para o Estado F
0.50	0.250	Dados válidos para classificação
0.25	0.375	Dados válidos para classificação
0.00	0.500	Indefinido
0.25	0.625	Dados válidos para classificação
0.50	0.750	Dados válidos para classificação
0.75	0.875	Limite para o Estado V
1.00	1.000	Verdadeiro V

3.6 Aplicação do algoritmo extrator de efeitos da contradição

De posse dos graus de evidência real da proposição objeto após 10 leituras subsequentes de informação, foi aplicado o Algoritmo Extrator de Efeitos da Contradição para obtenção do grau de evidência da intensidade do nível de degradação da rota selecionada. O processo de extração reduz os efeitos das inconsistências e apresenta como resposta uma valoração de saída mais próxima da realidade.

Quando o Grau de Evidência resultante for igual a 1 denota que as evidências analisadas e representadas pelas proposições parciais estão confirmando a proposição objeto. À medida que o valor do Grau de Evidência resultante se distancia de 1 e aproxima-se de 0,5, por consequência, do estado Indefinido,

significa que as informações estão trazendo evidências que enfraquecem a afirmativa à proposição. Nestas condições a análise indica que alguns parâmetros estão violados apesar da rota de comunicação estar funcional e com tráfego. Um procedimento não automatizado de averiguação de forma pontual nos NAPs sobre os valores dos graus de evidência das proposições parciais e seus intervalos de evidência, permite uma validação da possível origem de violação dos parâmetros e das contradições que estão provocando essa diminuição do Grau de Evidência resultante da proposição objeto.

Em contrapartida quando o Grau de Evidência resultante avança o valor de indefinição 0,5 e se aproxima de zero significa que as informações que levam as evidências para a análise sobre as proposições parciais estão indicando uma maior contestação à proposição objeto. Portanto, as evidências de fatores de degradação, relacionados à atual configuração do Sistema Especialista e às restrições, sugerem que está se aproximando de uma situação de bom estado da rota de comunicação.

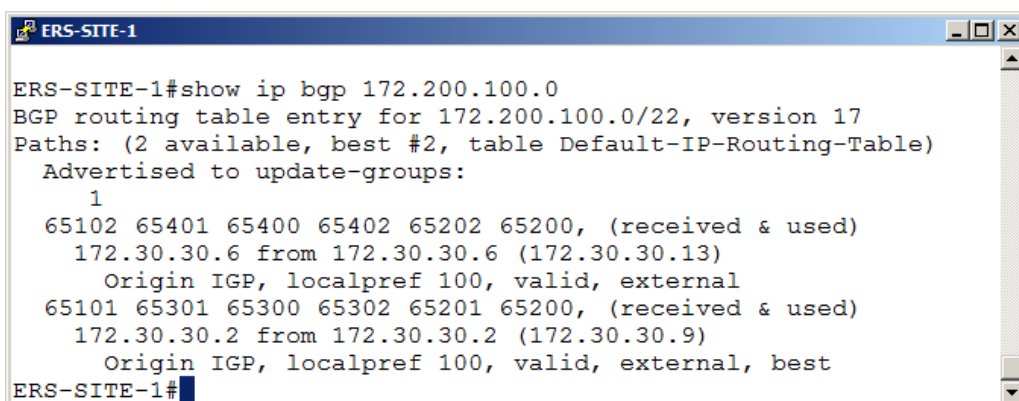
4. RESULTADOS E DISCUSSÃO

4.1 Ensaio do Sistema Especialista na Rede Piloto sem degradação (ensaio 01)

Neste ensaio considerou-se na rede piloto:

- ✓ *Todos os nós de interconexão ativos e funcionais;*
- ✓ *Rede de origem: SITE-1 (172.100.100.0);*
- ✓ *Rede de destino: SITE-2 (172.200.100.0);*
- ✓ *Quantidade de leituras prévias para execução da última etapa do controlador Paraconsistente: 10;*
- ✓ *Intervalo de tempo entre leituras: 1 minuto.*
- ✓ *Limite inferior de modelagem do sinal CPU em 10%*
- ✓ *Limite superior de modelagem do sinal Jitter em 30ms*

Observa-se na figura 41 que a rota de comunicação traçada pelo algoritmo de roteamento do protocolo BGP indica que o caminho pela rota A (65101 – 65301-65300 – 65302 – 65201 - 65200) foi definido como melhor (*best*) conforme características do próprio algoritmo.



```
ERS-SITE-1#show ip bgp 172.200.100.0
BGP routing table entry for 172.200.100.0/22, version 17
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  65102 65401 65400 65402 65202 65200, (received & used)
    172.30.30.6 from 172.30.30.6 (172.30.30.13)
    Origin IGP, localpref 100, valid, external
  65101 65301 65300 65302 65201 65200, (received & used)
    172.30.30.2 from 172.30.30.2 (172.30.30.9)
    Origin IGP, localpref 100, valid, external, best
ERS-SITE-1#
```

Figura 41 - Confirmação da rota entre a rede de origem e destino (ensaio 01).

Ao executar o Sistema Especialista Paraconsistente, seleciona-se na aplicação para que seja analisada a mesma rota sugerida pelo protocolo. Os dados da tabela 11 demonstram as informações coletadas:

Tabela 11 – 1ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65101	11	7	19	57.13855421686747	0.04
65301	26	16	19	1024.9019607843138	7.45
65300	28	19	19	1064.0725806451612	7.52
65302	30	21	19	1124.0	7.48
65201	33	23	19	1293.1544715447155	7.54
65200	35	21	19	1339.717213114754	7.56
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65101	0.05	0.0	0.1125	0.0	0.0
65301	0.8	0.3	0.1125	1.0	0.9214285714285715
65300	0.9	0.45	0.1125	1.0	0.9314285714285714
65302	1.0	0.55	0.1125	1.0	0.9257142857142858
65201	1.0	0.65	0.1125	1.0	0.9342857142857143
65200	1.0	0.55	0.1125	1.0	0.937142857142857
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65101	0.03535533905932742	0.0795495128834866	0.025000000000000022	0.058962382075353814	
65301	0.5	0.5	0.6421079287077212	0.5652088232876168	
65300	0.6047152924789525	0.5	0.7163170424432175	0.5935052150345818	
65302	0.6818019484660536	0.5	0.7689498243379387	0.6105233102780929	
65201	0.7525126265847083	0.5	0.8189359680293476	0.6239786018898197	
65200	0.6818019484660536	0.5	0.7706519888813473	0.6110266653071952	

Os dados da tabela 11 demonstram a rota percorrida entre os Sistemas Autônomos – ASs e valores de evidências obtidos em cada enlace percorrido.

Para a rede destino localizada no AS 65200, essa primeira leitura demonstra um grau de evidência resultante real de 0,61102667.

*As leituras subsequentes exibem apenas informações da rede de destino final do pacote e as proposições que determinam seu estado.

Tabela 12 – 2ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	29	21	19	1434.844827586207	7.68
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.95	0.55	0.1125	1.0	0.9542857142857143
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.6798437881283577	0.5	0.7713192225848801	0.6112231372887633	

Tabela 13 – 3ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	24	21	19	1415.2264957264956	7.66
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.7	0.55	0.1125	1.0	0.9514285714285714
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.6175735364805411	0.5	0.7274113138137706	0.5973186173680645	

Tabela 14 – 4ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	32	22	19	1374.1506276150628	7.61
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.6	0.1125	1.0	0.9442857142857143
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.717157287525381	0.5	0.7961568229831409	0.6181937396949033	

Tabela 15 – 5ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	37	26	19	1425.3564814814815	7.84
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.8	0.1125	1.0	0.9771428571428571
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.8585786437626906	0.5	0.8987022977072239	0.6392637913309811	

Tabela 16 – 6ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	32	25	19	1358.0697674418604	7.85
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.75	0.1125	1.0	0.9785714285714285
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.8232233047033631	0.5	0.8740849816871129	0.63540804189016	

Tabela 17 – 7ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	28	24	19	1388.2465753424658	7.81
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.9	0.7	0.1125	1.0	0.9728571428571428
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.776393202250021	0.5	0.8407254968711602	0.6289418055432956	

Tabela 18 – 8ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	38	22	19	1418.837837837838	7.78
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.6	0.1125	1.0	0.9685714285714286
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.717157287525381	0.5	0.7987690939467289	0.6188872361419652	

Tabela 19 – 9ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	33	28	20	1585.7149758454107	7.93
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.9	0.125	1.0	0.99
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.9292893218813452	0.5	0.9495024753081895	0.6446480617753718	

Tabela 20 – 10ª Leitura da rota selecionada no ensaio 01.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	32	26	19	1366.6711711711712	7.78
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.8	0.1125	1.0	0.9685714285714286
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.8585786437626906	0.5	0.8975603711885854	0.6391025924511091	

Tabela 21 – Algoritmo ParaExtrator aplicado às evidências da rota selecionada no ensaio 01.

ParaExtrator											
Evid.	1º Ciclo	1º Ciclo Ordenado	2º Ciclo Ordenado	3º Ciclo Ordenado	4º Ciclo Ordenado	5º Ciclo Ordenado	6º Ciclo Ordenado	7º Ciclo Ordenado	8º Ciclo Ordenado	9º Ciclo Ordenado	μEr
μ1	0,6110267	0,5973186	0,6110267	0,6112231	0,6181937	0,6188872	0,6202453	0,6234596	0,6238809	0,624181	0,6242804
μ2	0,6112231	0,6110267	0,6112231	0,6181937	0,6188872	0,6202453	0,6238809	0,6238809	0,624181	0,6243798	
μ3	0,5973186	0,6112231	0,6181937	0,6188872	0,6202453	0,6248794	0,6248794	0,6248794	0,6248794		
μ4	0,6181937	0,6181937	0,6188872	0,6202453	0,6248794	0,6249038	0,6249038	0,6249038			
μ5	0,6392638	0,6188872	0,6202453	0,6248794	0,6249038	0,6267016	0,6267016				
μ6	0,635408	0,6289418	0,6289418	0,6289418	0,6289418	0,6289418					
μ7	0,6289418	0,635408	0,635408	0,635408	0,635408						
μ8	0,6188872	0,6391026	0,6391026	0,6391026							
μ9	0,6446481	0,6392638	0,6392638								
μ10	0,6391026	0,6446481									
μMax		0,6446481	0,6392638	0,6391026	0,635408	0,6289418	0,6267016	0,6249038	0,6248794	0,6243798	
μMin		0,5973186	0,6110267	0,6112231	0,6181937	0,6188872	0,6202453	0,6234596	0,6238809	0,624181	
μEr		0,6202453	0,6248794	0,6249038	0,6267016	0,6238809	0,6234596	0,624181	0,6243798	0,6242804	

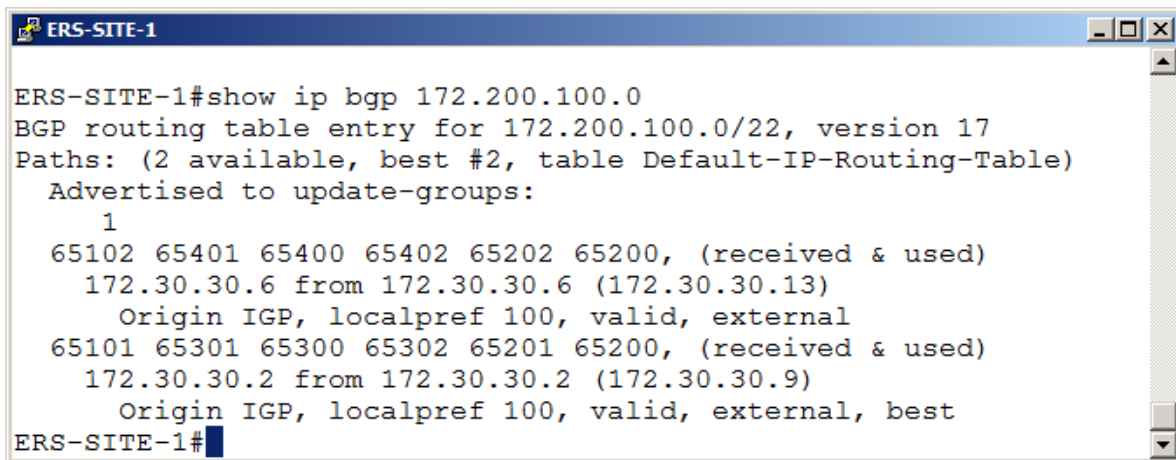
Neste ensaio nota-se a presença de algumas evidências de degradação dos enlaces que compõem a rota, porém o grau de evidência final, se comparado à parametrização da tabela 10, revela a não confirmação da proposição objeto após a extração do efeito da contradição entre as 10 leituras realizadas pelo módulo de monitoramento.

4.2 Ensaio do Sistema Especialista na Rede Piloto com degradação (ensaio 02)

Neste ensaio considerou-se na rede piloto:

- ✓ *Todos os nós de interconexão ativos e funcionais;*
- ✓ *Rede de origem: SITE-1 (172.100.100.0);*
- ✓ *Rede de destino: SITE-2 (172.200.100.0);*
- ✓ *Quantidade de leituras prévias para execução da última etapa do controlador Paraconsistente: 10;*
- ✓ *Intervalo de tempo entre leituras: 1 minuto;*
- ✓ *Maior volume de tráfego na rota de comunicação selecionada;*
- ✓ *Maior uso de CPU nos equipamentos;*
- ✓ *Limite inferior de modelagem do sinal CPU em 10%;*
- ✓ *Limite superior de modelagem do sinal Jitter em 30ms.*

Observa-se na figura 42 que a rota de comunicação traçada pelo algoritmo de roteamento do protocolo BGP indica que o caminho pela rota A (65101 – 65301-65300 – 65302 – 65201 - 65200) foi definido como melhor (*best*) conforme características do próprio algoritmo.



```
ERS-SITE-1#show ip bgp 172.200.100.0
BGP routing table entry for 172.200.100.0/22, version 17
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  65102 65401 65400 65402 65202 65200, (received & used)
    172.30.30.6 from 172.30.30.6 (172.30.30.13)
      Origin IGP, localpref 100, valid, external
  65101 65301 65300 65302 65201 65200, (received & used)
    172.30.30.2 from 172.30.30.2 (172.30.30.9)
      Origin IGP, localpref 100, valid, external, best
ERS-SITE-1#
```

Figura 42 - Confirmação da rota entre a rede de origem e destino (ensaio 02).

Ao executar o Sistema Especialista Paraconsistente, seleciona-se na aplicação para que seja analisada a mesma rota sugerida pelo protocolo. Os dados da tabela 22 demonstram as informações coletadas:

Tabela 22 – 1ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65101	7	6	48	20.0	0.0
65301	20	12	48	532.6666666666666	4.78
65300	19	14	48	544.2906309751434	4.77
65302	21	15	48	568.2380952380952	4.75
65201	20	19	48	721.0846456692914	4.92
65200	23	22	48	736.3300395256917	4.94
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65101	0.0	0.0	0.475	0.0	0.0
65301	0.5	0.1	0.475	0.7763888888888888	0.54
65300	0.45	0.2	0.475	0.8006054811982153	0.5385714285714285
65302	0.55	0.25	0.475	0.8504960317460316	0.5357142857142857
65201	0.5	0.45	0.475	1.0	0.5599999999999999
65200	0.65	0.6	0.475	1.0	0.562857142857143
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65101	0.0	0.3358757210636101	0.0	0.2375	
65301	0.3605551275463989	0.5964984950385279	0.4591296113299599	0.5228447622386121	
65300	0.34820970692960296	0.6028959996876162	0.45349155652198714	0.5223164929281847	
65302	0.4272001872658766	0.6140100801033247	0.48450479663176055	0.5446300828131571	
65201	0.4756574397610112	0.6287689398770626	0.5159880577516822	0.568676420631222	
65200	0.6241675905406773	0.6287689398770626	0.5923580752970689	0.6101382047600008	

Os dados da tabela 22 demonstram a rota percorrida entre os Sistemas Autônomos – ASs e valores de evidências obtidos em cada enlace percorrido.

Para a rede destino localizada no AS 65200, essa primeira leitura demonstra um grau de evidência resultante real de 0,6101382.

*As leituras subseqüentes exibem apenas informações da rede de destino final do pacote e as proposições que determinam seu estado.

Tabela 23 – 2ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	26	26	49	862.3278350515463	5.15
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.8	0.8	0.4875	1.0	0.5928571428571429
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.8	0.6376077746418944	0.6792467411526042	0.6577933533219844	

Tabela 24 – 3ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	42	49	48	1730.2099737532808	6.19
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.475	1.0	0.7414285714285714
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6287689398770626	0.8171623894360498	0.7073892587098565	

Tabela 25 – 4ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	31	28	48	1129.8036529680364	5.62
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	0.9	0.475	1.0	0.66
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.9292893218813452	0.6287689398770626	0.7544394168438265	0.6852679711246408	

Tabela 26 – 5ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	46	41	54	1333.9398734177216	6.84
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.55	1.0	0.8342857142857143
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6818019484660536	0.8828223048319436	0.7602286378183396	

Tabela 27 – 6ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	61	62	52	2575.669117647059	7.28
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.525	1.0	0.8971428571428571
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6641242789363899	0.9272690167922408	0.7569955803710894	

Tabela 28 – 7ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	56	42	54	1823.4501718213057	7.09
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.55	1.0	0.87
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6818019484660536	0.9080761184457489	0.7657992314273926	

Tabela 29 – 8ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	53	46	55	1578.7210144927535	7.09
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.5625	1.0	0.87
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6906407832308854	0.9080761184457489	0.7717971023409211	

Tabela 30 – 9ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	55	51	52	1867.1901408450703	7.16
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.525	1.0	0.88
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6641242789363899	0.9151471862576143	0.7550382682948212	

Tabela 31 – 10ª Leitura da rota selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	50	38	52	1638.173202614379	6.91
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	1.0	1.0	0.525	1.0	0.8442857142857143
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	1.0	0.6641242789363899	0.8898933726438091	0.7500640388141844	

Tabela 32 – Algoritmo ParaExtrator aplicado às evidências da rota selecionada no ensaio 02.

ParaExtrator											
Evid.	1º Ciclo	1º Ciclo Ordenado	2º Ciclo Ordenado	3º Ciclo Ordenado	4º Ciclo Ordenado	5º Ciclo Ordenado	6º Ciclo Ordenado	7º Ciclo Ordenado	8º Ciclo Ordenado	9º Ciclo Ordenado	μEr
μ1	0,6101382	0,6101382	0,6577934	0,6805718	0,685268	0,7067805	0,7073893	0,7175777	0,7188351	0,7233249	0,7234803
μ2	0,6577934	0,6577934	0,6805718	0,685268	0,7067805	0,7073893	0,7175777	0,7188351	0,7236358	0,7236358	
μ3	0,7073893	0,685268	0,685268	0,7067805	0,7073893	0,7175777	0,7188351	0,7278888	0,7278888		
μ4	0,685268	0,7073893	0,7073893	0,7073893	0,7175777	0,7188351	0,7298297	0,7298297			
μ5	0,7602286	0,750064	0,750064	0,750064	0,750064	0,750064	0,750064				
μ6	0,7569956	0,7550383	0,7550383	0,7550383	0,7550383	0,7550383					
μ7	0,7657992	0,7569956	0,7569956	0,7569956	0,7569956						
μ8	0,7717971	0,7602286	0,7602286	0,7602286							
μ9	0,7550383	0,7657992	0,7657992								
μ10	0,750064	0,7717971									
μMax		0,7717971	0,7657992	0,7602286	0,7569956	0,7550383	0,750064	0,7298297	0,7278888	0,7236358	
μMin		0,6101382	0,6577934	0,6805718	0,685268	0,7067805	0,7073893	0,7175777	0,7188351	0,7233249	
μEr		0,6805718	0,7067805	0,7175777	0,7188351	0,7298297	0,7278888	0,7236358	0,7233249	0,7234803	

Neste ensaio nota-se a presença de evidências de degradação dos enlaces que compõem a rota cujo grau de evidência final, se comparado à parametrização da tabela 10, revela a confirmação da proposição objeto após a extração do efeito da contradição entre as 10 leituras realizadas pelo módulo de monitoramento.

Com esse resultado, o sistema especialista verifica se há outra rota disponível para acesso a rede destino, neste ensaio a alternativa de tráfego pela rota B existe e está disponível (figura 42), o sistema então realiza a mesma análise paraconsistente dessa nova rota. Os dados da tabela 33 demonstram as informações coletadas:

Tabela 33 – 1ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65102	3	3	14	16.811	0.0
65401	12	5	14	735.824295010846	5.39
65400	12	6	14	745.2255965292842	5.39
65402	13	7	14	768.3709327548806	5.39
65202	13	10	14	823.9405520169852	5.29
65200	13	11	14	829.2415254237288	5.28
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65102	0.0	0.0	0.05	0.0	0.0
65401	0.1	0.0	0.05	1.0	0.6271428571428571
65400	0.1	0.0	0.05	1.0	0.6271428571428571
65402	0.15	0.0	0.05	1.0	0.6271428571428571
65202	0.15	0.0	0.05	1.0	0.6128571428571429
65200	0.15	0.05	0.05	1.0	0.6114285714285714
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65102	0.0	0.03535533905932742	0.0	0.025000000000000022	
65401	0.07071067811865478	0.5	0.44626682784255095	0.4738956011784943	
65400	0.07071067811865478	0.5	0.44626682784255095	0.4738956011784943	
65402	0.10606601717798214	0.5	0.44975446816307785	0.4755413134695307	
65202	0.10606601717798214	0.5	0.43979761115257343	0.47086194302338247	
65200	0.11180339887498947	0.5	0.43951387802843256	0.4707294599765304	

Os dados da tabela 33 demonstram a rota alternativa selecionada e percorrida entre os Sistemas Autônomos – ASs e valores de evidências obtidos em cada enlace percorrido.

Para a rede destino localizada no AS 65200, essa primeira leitura demonstra um grau de evidência resultante real de 0,470729.

*As leituras subsequentes exibem apenas informações da rede de destino final do pacote e as proposições que determinam seu estado.

Tabela 34 – 2ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	14	13	15	985.5879629629629	5.68
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.2	0.15	0.0625	1.0	0.6685714285714285
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.17677669529663698	0.5	0.4889978298019536	0.4945295125424874	

Tabela 35 – 3ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	12	9	15	830.4201312910285	5.43
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.1	0.0	0.0625	1.0	0.6328571428571428
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.07071067811865478	0.5	0.45028222442447474	0.4757909633613553	

Tabela 36 – 4ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	13	11	15	851.7682119205298	5.47
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.15	0.05	0.0625	1.0	0.6385714285714286
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.11180339887498947	0.5	0.4584067350005643	0.4796544249216709	

Tabela 37 – 5ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	13	11	14	840.5733041575493	5.43
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.15	0.05	0.05	1.0	0.6328571428571428
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.11180339887498947	0.5	0.4544272016865331	0.47775730325796856	

Tabela 38 – 6ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	13	11	13	930.9848156182212	5.39
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.15	0.05	0.0375	1.0	0.6271428571428571
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.11180339887498947	0.5	0.4504487558342825	0.47586977295929034	

Tabela 39 – 7ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	13	11	15	888.0432900432901	5.38
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.15	0.05	0.0625	1.0	0.6257142857142857
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.11180339887498947	0.5	0.44945431767140626	0.4753994024362407	

Tabela 40 – 8ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	15	11	14	1002.9510022271714	5.51
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.25	0.05	0.05	1.0	0.6442857142857142
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.18027756377319948	0.5	0.4730772038645769	0.4867247891860073	

Tabela 41 – 9ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	9	9	14	780.3144876325089	4.34
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.0	0.0	0.05	1.0	0.47714285714285715
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.0	0.5	0.33739094988043833	0.4265165020613062	

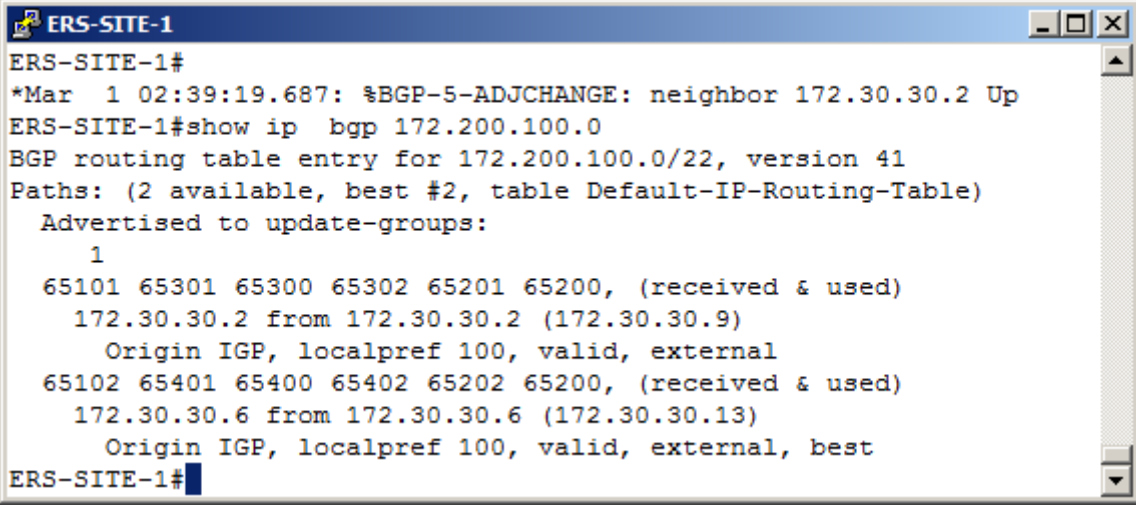
Tabela 42 – 10ª Leitura da rota alternativa selecionada no ensaio 02.

Valores capturados					
AS-Destino	JITTER-SD	JITTER-DS	CPU-Busy1min	RTT-Avg	PEP-Ratio
65200	11	9	14	690.9199178644764	5.13
Valores modelados					
AS-Destino	Evidência-JSD	Evidência-JDS	Evidência-CPU	Evidência-RTT-Avg	Evidência-PEP-Ratio
65200	0.05	0.0	0.05	1.0	0.59
Valores obtidos nas proposições					
AS-Destino	P1	P2	P3	Po	
65200	0.03535533905932742	0.5	0.41794138344988047	0.46080093315877735	

Tabela 43 – Algoritmo ParaExtrator aplicado às evidências da rota alternativa selecionada no ensaio 02.

ParaExtrator											
Evid.	1º Ciclo	1º Ciclo Ordenado	2º Ciclo Ordenado	3º Ciclo Ordenado	4º Ciclo Ordenado	5º Ciclo Ordenado	6º Ciclo Ordenado	7º Ciclo Ordenado	8º Ciclo Ordenado	9º Ciclo Ordenado	μEr
μ1	0,4707295	0,4265165	0,4608009	0,4617769	0,4707295	0,4708005	0,4733419	0,4739401	0,4742564	0,4744634	0,4745157
μ2	0,4945295	0,4608009	0,4617769	0,4707295	0,4708005	0,4739401	0,4739401	0,4742564	0,474568	0,474568	
μ3	0,475791	0,4707295	0,4707295	0,4739401	0,4739401	0,4742564	0,4742564	0,474568	0,4746703		
μ4	0,4796544	0,4753994	0,4753994	0,4753994	0,4753994	0,4753994	0,4753994	0,4753994			
μ5	0,4777573	0,475791	0,475791	0,475791	0,475791	0,475791	0,475791				
μ6	0,4758698	0,4758698	0,4758698	0,4758698	0,4758698	0,4758698					
μ7	0,4753994	0,4777573	0,4777573	0,4777573	0,4777573						
μ8	0,4867248	0,4796544	0,4796544	0,4796544							
μ9	0,4265165	0,4867248	0,4867248								
μ10	0,4608009	0,4945295									
μMax		0,4945295	0,4867248	0,4796544	0,4777573	0,4758698	0,475791	0,4753994	0,4746703	0,474568	
μMin		0,4265165	0,4608009	0,4617769	0,4707295	0,4708005	0,4733419	0,4739401	0,4742564	0,4744634	
μEr		0,4617769	0,4739401	0,4708005	0,4742564	0,4733419	0,474568	0,4746703	0,4744634	0,4745157	

Neste ensaio o sistema especialista verificou a outra rota disponível para acesso a rede destino (alternativa de tráfego pela rota B) e, após a análise paraconsistente, foi constatado um grau de evidência que refuta a proposição objeto de degradação do enlace permitindo que o sistema envie as informações para o módulo de gerência que, por sua vez, envia o comando de reconfiguração da rota invertendo a escolha padrão do protocolo de roteamento para uso da rota alternativa conforme resultado visualizado na figura 43.



```

ERS-SITE-1#
*Mar  1 02:39:19.687: %BGP-5-ADJCHANGE: neighbor 172.30.30.2 Up
ERS-SITE-1#show ip  bgp 172.200.100.0
BGP routing table entry for 172.200.100.0/22, version 41
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  65101 65301 65300 65302 65201 65200, (received & used)
    172.30.30.2 from 172.30.30.2 (172.30.30.9)
      Origin IGP, localpref 100, valid, external
  65102 65401 65400 65402 65202 65200, (received & used)
    172.30.30.6 from 172.30.30.6 (172.30.30.13)
      Origin IGP, localpref 100, valid, external, best
ERS-SITE-1#

```

Figura 43 - Confirmação da nova rota entre a rede de origem e destino (ensaio 02).

4.3 Discussão

Em uma análise preliminar pode-se sugerir que o controlador só atuaria em situações de degradação, porém observa-se que o sistema pode ser configurado para atuar de maneira decisória permitindo a distribuição de tráfego entre rotas redundantes bastando estabelecermos outros níveis de parametrização na tabela de comparação na saída do algoritmo.

Em uma análise mais detalhada dos resultados apresentados nas tabelas 32 e 43, considera-se que o uso do algoritmo ParaExtrator contribuiu para melhor veracidade da análise, eliminando possíveis divergências causadas por leituras efetuadas em instantes de instabilidade momentânea da rota. Observa-se também que a RNAP estruturada proporcionou corretamente a importância à fonte de informação PEP – Perda de Pacotes (*Packet Loss Ratio*).

Baseado em uma visão próxima ao “estado da arte” foi desenvolvido um cenário na rede piloto onde todos os equipamentos estão funcionais e podem ser acessados e monitorados por uma mesma gerência via protocolo SNMP mesmo estando em sistemas autônomos distintos. Nesse cenário pode-se também notar que o tempo de convergência do protocolo BGP segue a troca de mensagens do tipo *keep-alive* que, por padrão é enviada para o *peer* (vizinho) a cada 60 segundos para que o vizinho saiba que há conectividade IP. Caso essa mensagem atrase

(como em cenários de falha), o equipamento de interconexão iniciará a contagem de *hold-time* (tempo de tolerância) equivalente a 180 segundos e, se nesse período não for recebida uma nova mensagem do tipo *keep-alive* a sessão entre os *peers* é finalizada. Como as rotas são compostas por três ou mais *peers* confirma-se que o tempo definido para análise paraconsistente (10 coletas de 1 minuto) está abaixo do tempo de convergência estimado para esse cenário.

Em um cenário que contemple o uso de enlaces de comunicação fornecidos por uma operadora de telecomunicações há a possibilidade de uso do protocolo BGP em conjunto com a “nuvem” MPLS (*Multiprotocol Label Switching*) para divulgação das rotas através de *Labels* MPLS. Nessa configuração, por questões de gerência e segurança, a operadora não permite acesso aos equipamentos dessa nuvem MPLS via protocolo SNMP, portanto os alvos do IP SLA deverão ser direcionados para equipamentos do cliente instalados em cada uma das localidades e que originem as rotas a serem divulgadas via protocolo BGP.

Em cenários *multihomed* – onde os enlaces de comunicação são fornecidos por mais de uma operadora – considera-se as observações do cenário anterior bem como a necessidade de criação de filtros de rotas configurados nos equipamentos do cliente para que não sejam divulgadas rotas entre as operadoras evitando *loops* de roteamento.

5. CONCLUSÃO

O uso de algoritmos adaptativos proporciona características fundamentais para a transmissão entre elementos comunicadores, como resiliência dos enlaces de comunicação em casos de interrupções no ambiente de rede bem como a não necessidade de intervenção direta do administrador da rede para reestabelecimento da comunicação como em ocorrências de falha usando algoritmos não adaptativos.

Entre os inúmeros desafios propostos na área de sistemas Inteligentes o que trata de otimizar caminho utilizando Sistemas de busca/determinação com Algoritmos adaptativos e lógicas não clássicas destaca-se entre os mais interessantes. O estudo para traçar os melhores caminhos e a melhor distribuição de “cargas” para cada um deles pode ser aplicado ao ambiente de telecomunicações, em logísticas de transporte bem como em sistemas de dutos, modelando a melhor maneira de se chegar à determinada cidade contida em um mapa, como aos robôs, especificando pontos de chegada para máquinas que se movimentam em ambientes diversos e sem rotas previamente estabelecidas. Os resultados e testes obtidos neste trabalho evidenciam a importância da utilização da Lógica Paraconsistente em projetos de sistemas especialistas e controladores de processo, manipulando de forma flexível e eficaz, dados que contenham incertezas e inconsistências. Conseguiu-se, assim, a implementação de um sistema especialista inteligente sem intervenções externas e com possibilidade de gerenciamento de ambientes de redes não estruturados aplicando a Lógica Paraconsistente Anotada Evidencial E_{τ} .

5.1 Trabalhos futuros

Em redes de comunicação de dados o aproveitamento da disponibilidade dos enlaces de comunicação entre as redes de origem e destino considerando políticas de tráfego e degradações dos meios de comunicação representa um grande desafio técnico e econômico, encontrar novas formas de distribuir de maneira

eficiente o tráfego de aplicações entre localidades interligadas por enlaces redundantes de telecomunicações aplicando algoritmos estruturados em Lógica Paraconsistente Anotada controlando toda a decisão de roteamento, se projeta como um grande campo para estudos e trabalhos futuros.

A pesquisa bem como a proposta do sistema especialista paraconsistente aqui apresentados na forma de uma estrutura funcional com quatro nós de análises paraconsistente em conjunto com o extrator de contradição, apresentam importante projeção para o desenvolvimento de novas configurações em projetos de pesquisa que possam abranger outras áreas de tomada de decisão.

Os resultados obtidos com esta configuração apontam que o uso da lógica Evidencial E_{τ} no núcleo decisório de um sistema especialista combinada a protocolos de roteamento que fazem uso de algoritmos adaptativos, pode apresentar características diferenciadas e de rápida resposta. Espera-se que novos trabalhos sejam desenvolvidos a partir dessa contribuição, fazendo uso de possíveis acréscimos de fontes de informação como volume de tráfego, capacidade do enlace, entre outros, permitindo uma nova e flexível configuração desse sistema.

Ainda como trabalhos futuros, avalia-se propor as seguintes realizações:

A investigação do uso da lógica evidencial E_{τ} na identificação de degradações de *interfaces* de entrada e saída de pacotes em equipamentos de interconexão.

Acrescentar ao sistema desenvolvido as características que permitam que este possa realizar a exibição gráfica dos valores de saída e de entrada do controlador paraconsistente.

Aumentar a RNAP para tratar situações de desativação de NAP.

Criar um procedimento automatizado de averiguação de forma pontual nos NAPs sobre os valores dos graus de evidência das proposições parciais e seus intervalos de evidência de forma que permita uma validação da possível origem de violação dos parâmetros e das contradições que estão provocando a diminuição ou aumento do Grau de Evidência resultante da proposição objeto.

REFERÊNCIAS

ABE, J. M. **Remarks on Paraconsistent Annotated Evidential Logic Et**. Unisanta Science and Technology, 2014.

ABE, J. M.; TORRES, C. R.; LAMBERT-TORRES, G.; NAKAMATSU, K.; KONDO, M. **Intelligent Paraconsistent Logic Controller and Autonomous Mobile Robot Emmy II**. In: 10th International Conference on Knowledge-Based, Intelligent Information & Engineering Systems, KES2006, 2006.

BAKER, F. **“Requirements for IP version 4 routers”** IETF RFC 1812, June 1995.

BAPTISTA, R., DA SILVA FILHO, J. I. MORILLA, J. C. **Proposal of Automatic Control three-way Valve through algorithms of Paraconsistent Annotated logic**, Science and Technology, ISSN: 2317-1316, Vol 2, No 2, p.p.69-73, 2013.

BERTSEKAS, D.; GALLAGER, R. **Data networks**. Prentice-Hall, 1992.

BURGESS, N. **RFC 2544 Testing of Ethernet Services in Telecom Networks**. Agilent Technologies, 2004.

CASE, J.; FEDOR, M.; SCHOFFSTALL, M.; DAVIN, J. **“A simple network management protocol (snmp)”**, RFC 1157, 1990.

CHEN, S.; NAHRSTEDT, K. **An overview of quality of service routing for next-generation high-speed networks: problems and solutions**. *IEEE Networks*, 12:64 – 79, November/December 1998.

CISCO WHITEPAPER. **CISCO IOS IP SERVICE LEVEL AGREEMENTS – USER GUIDE 2005**. Disponível em https://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.pdf. Acessado em 15 de maio de 2017.

CISCO WHITEPAPER. **IP Service Level Agreement (IP SLA) 2007**. Disponível em https://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806bfb52.pdf. Acessado em 15 de maio de 2017.

COMER, D. E. **The Internet Book: Everything You Need to Know About Computer Networking and How the Internet Works**, 4ª Edição, 2006.

COMER, D. E. **Interligação de redes com TCI/IP**. Rio de Janeiro: Elsevier, 6ª Edição, 2015.

CUNHA, D. M.; LIMA, M. F.; CABRITA, P. H. C. M.; GURGEL, D. L.; GADELHA, M. A., **Lógica Paraconsistente**. Disponível em <http://aquilesburlamaqui.wdfiles.com/local--files/logica-aplicada-a->

computacao/texto_paraconsistente.pdf. Acessado em 15 de maio de 2017.

DA COSTA, N. C. A.; ABE, J. M.; DA SILVA FILHO, J. I.; MUROLO, A. C. **Lógica Paraconsistente Aplicada**, 2ª. Ed., Editora Atlas, 1999, 214 p

DA COSTA, N. C. A.; KRAUSE, D. **NOTAS DE LÓGICA Parte I: Lógicas Proposicionais Clássica e Paraconsistente**. Florianópolis, 2004.

DA SILVA FILHO, J.I. **“Implementação de circuitos Lógicos fundamentados em uma classe de Lógicas Paraconsistentes Anotada”** Dissertação de Mestrado EPUSP, São Paulo, 1997.

DA SILVA FILHO, J.I. **Métodos de Aplicações da Lógica Paraconsistente Anotada de anotação com dois valores LPA2v com construção de Algoritmo e Implementação de Circuitos Eletrônicos**. Tese de doutorado EPUSP, São Paulo, 1999.

DA SILVA FILHO, J. I. **Métodos de Aplicações da Lógica Paraconsistente Anotada de anotações com dois valores - LPA2v**. Revista Seleção Documental, Março 2006.

DA SILVA FILHO, J. I.; ABE, J. M.; LAMBERT-TORRES, G., **Inteligência Artificial com as Redes de Análises Paraconsistentes: Teoria e Aplicações**. Rio de Janeiro, Editora LTC, 1ª. Ed., pp.4-5, pp.40-84, pp.101-185. 2008.

DA SILVA FILHO, J. I. ; LAMBERT-TORRES, G. ; FERRARA, L. F. P. ; MARIO, M. C. ; Santos, M. R.; Onuki,A. S. ; CAMARGO, J. M. ; ROCCO, A. . **Paraconsistent Algorithm Extractor of Contradiction Effects - Paraextrctr**. Journal of Software Engineering and Applications, v. 4, p. 579-584, 2011.

DA SILVA FILHO, J. I. **Algoritmo Paraconsistente Extrator de efeitos da Contradição - ParaExtrctr**, Artigo Técnico, Revista Seleção Documental, N.15 Ano 4 ISSN 1809-0648, - Ed. Paralogike - Santos – SP-Brasil, 2009 pp 21-24

DEITEL P, DEITEL H. **Java Como Programar**, 8ª,; tradução Edson Furmankiewicz; revisão técnica Fábio Luís Picelli Lucchini. São Paulo. Editora: Pearson Prentice Hall. 2010 p. 1114.

FIGUEIREDO CHAGAS, E. M. P. **Apresentando alguns aspectos históricos do desenvolvimento da lógica clássica, ciências das idéias e dos processos da mente**. Millenium (Viseu), v. 29, p. 109-122, 2004

FOROUZAN, B. A. **Comunicação de Dados e Redes de Computadores**. 4ª Edição. Porto Alegre. Amgh Editora. 2008.

FOROUZAN, B. A.; MOSHARRAF, F. **Redes de Computadores: Uma Abordagem Top-down**. 1ª Edição. Porto Alegre. Amgh Editora. 2013.

FORTZ, B.; THORUP, M. **Increasing internet capacity using local search**. Technical Report IS-MG 2000/21, Université Libre de Bruxelles, 2000.

FORTZ, B.; THORUP, M.; REXFORD, J. **Traffic engineering with traditional ip routing protocols**. *IEEE Communications Magazine*, 40:118–124, October 2002.

GONÇALVES, E. **Desenvolvendo Aplicações WEB com NetBeans IDE 6**. São Paulo: Ciência Moderna, 2008

HALABI, S.; MCPHERSON, D., **Internet Routing Architectures**, Second Edition. Indianapolis – USA : Cisco Press, 2000.

HAWKINSON, J.; BATES, T. **Guidelines for creation, selection, and registration of an Autonomous System (AS)**. Março 1996.

IANA, Internet Assigned Numbers Authority. **ICANN: The IANA Functions**. Disponível em <http://www.iana.org/about/informational-booklet.pdf>. Acessado em 15 de maio de 2017.

KUIPERS, F. A.; KORKMAZ, T.; KRUNZ, M.; MIEGHEM, P. Van. **An overview of constraint-based path selection algorithms for Qos routing**. *IEEE Communications Magazine*, 40:50 – 55, Dezembro 2002.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet: uma abordagem top-down**. 5a edição. São Paulo: Addison Wesley, 2010.

LOPES, R. P. S. de C. **Gestão Distribuída em SNMP**. PhD thesis, Universidade de Aveiro, 2002.

MARREIRO, A. de L.; GARCIA, D. V. **Análise computacional do emprego de algoritmos adaptativos para aumento de resiliência em enlaces de comunicação entre sistemas de monitoramento e equipamentos industriais**, Artigo técnico, ENPG, Santos, 2016.

MASIP-BRUIN, X.; SÁNCHEZ-LÓPEZ, S.; SOLÉ-PARETA, J.; DOMINGO-PASCUAL, J. **Qos routing algorithms under inaccurate routing information for bandwidth constrained applications**. In ICC 2003 - IEEE International Conference on Communications, volume 3, pages 1743 – 1748, Anchorage, Alaska, May 2003. IEEE.

MAURO, D. R.; SCHMIDT, K. J. **Essential SNMP, Second Edition**. O'Reilly Media, Inc., 2005.

MCBRIDE, A. **The Basics of Cisco IP SLA – Volume 2**. SolarWinds, 2010.

NETACAD, Cisco Networking Academy, Routing and Switching Essential – **Capítulo 7: Roteamento Dinâmico**, Cisco Instructor Material, 2016

PRESUHN, R., **“Version 2 of the protocol operations for the simple network management protocol (snmp),”** IETF RFC 3416, 2002.

RESENDE, R.A.; NASSIF, N.A.; DE SIQUEIRA, M.A.; DA SILVA, A.E., LIMA-MARQUES, M **“Quality of Service control in IP Networks using Fuzzy Logic for Policy Condition Evaluation”** The 14th IEEE International Conference on Fuzzy Systems. 2005, p.p. 448-453.

SOARES VAZ, P. J. L. **Monitorização de SLA IP.** Dissertação de Mestrado integrado em Engenharia Elétrica e de computadores, UNIFEI – Universidade do Porto, Portugal, 2011, 92 p.

SOUZA, V. S.; ABE, J. M.; DA SILVA, J. D. S. **Redes Neurais Paraconsistentes Aplicadas no Estudo de Fraudes à Conta de Clientes acessadas via Internet.** 2005.

STALLINGS, W. **SNMP, SNMPv2, SNMPv3, and RMON 1 and 2.** Addison Wesley Longman, Inc., 1999.

TANNENBAUM, A; WETHERALL, D. **Redes de computadores.** Editora Campus. 5ª Edição, 2011.

TORRES, C. R. **Sistema Inteligente Paraconsistente para Controle de Robôs Móveis Autônomos.** Dissertação de Mestrado em Engenharia Elétrica, UNIFEI – Universidade Federal de Itajubá, Itajubá, 2004, 85 p

TORRES, C. R.; ABE, J. M.; LAMBERT-TORRES, G. **Sistema inteligente paraconsistente para controle de robôs móveis autônomos.** Revista de Ciências Exatas, Taubaté, SP, v.11, n.1, pp.21–27, 2005.

TORRES, C.R., **Sistema Inteligente Baseado na Lógica Paraconsistente Anotada Evidencial E_{τ} para Controle e Navegação de Robôs Móveis Autônomos em um Ambiente Não-estruturado,** UNIFEI, Tese de Doutorado, Itajubá, Brasil, 2009.

TORRES, R. C.; ABE, J. M.; LAMBERT-TORRES, G.; DA SILVA FILHO, J. I. **Autonomous Mobile Robot Emmy III,** Artigo técnico, Jornal Intechopen, Brasil, 2011, pp 1-3.

VOHRA, Q.; CHEN, E. **BGP Support for Four-octet AS Number Space,** IETF RFC 4893, Maio 2007.

WALLACE, K. **CCNP routing and switching ROUTE 300-101: Official cert guide.** Indianapolis: Cisco press (2014).

APÊNDICE A – COMANDOS DE CONFIGURAÇÃO DOS EQUIPAMENTOS DE REDE

Quadro 4 – Configuração dos equipamentos: ERS SITE 1 e 2

ERS - SITE 1	ERS-SITE-2
Enable	enable
conf t	Configure terminal
hostname ERS-SITE-1	hostname ERS-SITE-2
int fast 1/0	<i>Interface</i> fastethernet 1/0
ip add 172.100.100.1 255.255.252.0	ip address 172.200.100.1 255.255.252.0
no shutdown	no shutdown
Exit	exit
int fast 2/0	<i>interface</i> fastethernet 2/0
ip add 172.101.100.1 255.255.252.0	ip address 172.201.100.1 255.255.252.0
no shutdown	no shutdown
Exit	exit
int fast 3/0	<i>interface</i> fastethernet 3/0
ip add 172.30.30.1 255.255.255.252	ip address 172.30.30.17 255.255.255.252
no shutdown	no shutdown
Exit	exit
int fast 4/0	<i>interface</i> fastethernet 4/0
ip add 172.30.30.5 255.255.255.252	ip address 172.30.30.21 255.255.255.252
no shutdown	no shutdown
Exit	exit
router bgp 65100	router bgp 65200
no synchronization	no synchronization
bgp log-neighbor-changes	bgp log-neighbor-changes
network 172.100.100.0 mask 255.255.252.0	network 172.200.100.0 mask 255.255.252.0
network 172.100.100.0 mask 255.255.252.0	network 172.200.100.0 mask 255.255.252.0
redistribute connected	redistribute connected
neighbor 172.30.30.2 remote-as 65101	neighbor 172.30.30.18 remote-as 65201
neighbor 172.30.30.2 description *** CE-1A***	neighbor 172.30.30.18 description *** CE-2A***
neighbor 172.30.30.2 send-community both	neighbor 172.30.30.18 send-community both

neighbor 172.30.30.2 soft-reconfiguration inbound	neighbor 172.30.30.18 soft-reconfiguration inbound
ERS - SITE 1	ERS - SITE 2
neighbor 172.30.30.6 remote-as 65102	neighbor 172.30.30.22 remote-as 65202
neighbor 172.30.30.6 description *** CE-1B***	neighbor 172.30.30.22 description *** CE-2B***
neighbor 172.30.30.6 send-community both	neighbor 172.30.30.22 send-community both
neighbor 172.30.30.6 soft-reconfiguration inbound	neighbor 172.30.30.22 soft-reconfiguration inbound
no auto-summary	no auto-summary
Exit	exit
snmp-server community paralogike-inet rw	snmp-server community paralogike-inet rw
Exit	exit
Write memory	Write memory

Quadro 5 – Configuração dos equipamentos: PC-1 / 2 / 3 / 4

PC1	PC3
IP 172.100.100.254/22 172.100.100.1	IP 172.200.100.254/22 172.200.100.1
save	save
PC2	PC4
IP 172.101.100.254/22 172.101.100.1	IP 172.201.100.254/22 172.201.100.1
save	save

Quadro 6 - Configuração dos equipamentos: CE-1A e CE - 1B

CE-1A	CE-1B
enable	enable
Configure terminal	Configure terminal
hostname CE-1A	hostname CE-1B
<i>Interface</i> fastethernet 1/0	<i>Interface</i> fastethernet 1/0
ip address 172.30.30.2 255.255.255.252	ip address 172.30.30.6 255.255.255.252
no shutdown	no shutdown
exit	exit
<i>interface</i> serial 0/0	<i>interface</i> serial 0/0
ip address 172.30.30.9 255.255.255.252	ip address 172.30.30.13 255.255.255.252
encapsulation ppp	encapsulation ppp
clock rate 64000	clock rate 64000
no shutdown	no shutdown
exit	exit
snmp-server community paralogike-inet rw	snmp-server community paralogike-inet rw
exit	exit
Write memory	Write memory

Quadro 7 - Configuração dos equipamentos: PE-1A e PE-1B

PE-1A	PE-1B
enable	enable
Configure terminal	Configure terminal
hostname PE-1A	hostname PE-1B
<i>Interface</i> fastethernet 1/0	<i>Interface</i> fastethernet 1/0
ip address 172.30.30.41 255.255.255.252	ip address 172.30.30.33 255.255.255.252
no shutdown	no shutdown
exit	exit
<i>interface</i> serial 0/0	<i>interface</i> serial 0/0
ip address 172.30.30.10 255.255.255.252	ip address 172.30.30.14 255.255.255.252
encapsulation ppp	encapsulation ppp
no shutdown	no shutdown
exit	exit
snmp-server community paralogike-inet rw	snmp-server community paralogike-inet rw
exit	exit
Write memory	Write memory

Quadro 8 - Configuração dos equipamentos: CEA-2A e CE-2B

CE-2A	CE-2B
enable	enable
Configure terminal	Configure terminal
hostname CE-2A	hostname CE-2B
<i>Interface</i> fastethernet 1/0	<i>Interface</i> fastethernet 1/0
ip address 172.30.30.18 255.255.255.252	ip address 172.30.30.22 255.255.255.252
no shutdown	no shutdown
exit	exit
<i>interface</i> serial 0/0	<i>interface</i> serial 0/0
ip address 172.30.30.25 255.255.255.252	ip address 172.30.30.29 255.255.255.252
encapsulation ppp	encapsulation ppp
CLOCK RATE 64000	clock rate 64000
no shutdown	no shutdown
exit	exit

snmp-server community paralogike-inet rw	snmp-server community paralogike-inet rw
exit	exit
Write memory	Write memory

Quadro 9 - Configuração dos equipamentos: PE-2A e PE-2B

PE-2A	PE-2B
enable	enable
Configure terminal	Configure terminal
hostname PE-2A	hostname PE-2B
<i>Interface</i> fastethernet 1/0	<i>Interface</i> fastethernet 1/0
ip address 172.30.30.45 255.255.255.252	ip address 172.30.30.37 255.255.255.252
no shutdown	no shutdown
exit	exit
<i>interface</i> serial 0/0	<i>interface</i> serial 0/0
ip address 172.30.30.26 255.255.255.252	ip address 172.30.30.30 255.255.255.252
encapsulation ppp	encapsulation ppp
no shutdown	no shutdown
exit	exit
snmp-server community paralogike-inet rw	snmp-server community paralogike-inet rw
exit	exit
Write memory	Write memory

APÊNDICE B – Algoritmo de extração das rotas dos equipamentos de interconexão

```

public String[][] carregaRotas (String sEnderecoIP, String [][] Interfaces) {
    String[] baseIDs = {"1.3.6.1.2.1.4.24.4.1.1",
                       "1.3.6.1.2.1.4.24.4.1.2",
                       "1.3.6.1.2.1.4.24.4.1.4",
                       "1.3.6.1.2.1.4.24.4.1.5",
                       "1.3.6.1.2.1.4.24.4.1.6"};
    String[] coordenadas = new String[]{"", "", "", "", "", ""};
    String[][] retorno= new String[100][7];

    //retorno[0][3]=sEnderecoIP;
    InetAddress hostAddress = null;
    try {
        hostAddress = InetAddress.getByName(sEnderecoIP);
    } catch (UnknownHostException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE, null,
ex);
    }

    String community = "paralogike-inet";
    int version = 0; // SNMPv1

    SNMPv1CommunicationInterface comInterface = null;
    try {
        comInterface = new SNMPv1CommunicationInterface(version, hostAddress,
community);
    } catch (SocketException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE, null,
ex);
    }

    SNMPVarBindList tableVars = null;
    try {
        tableVars = comInterface.retrieveMIBTable(baseIDs);
    } catch (IOException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE, null,
ex);
    }
    } catch (SNMPBadValueException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE, null,
ex);
    }
    } catch (SNMPGetException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE, null,
ex);
    }
    }

    Integer controle = baseIDs.length;
    Integer controla_laco = 1;
    Integer controla_linha = 0;
    for (int i = 0; i < tableVars.size(); i++)

```

```

{
    SNMPSequence pair = (SNMPSequence)(tableVars.getSNMPObjectAt(i));

    SNMPObjectIdentifier snmpOID = SNMPObjectIdentifier(pair.getSNMPObjectAt(0);

    SNMPObject snmpValue = pair.getSNMPObjectAt(1);

    coordenadas[controla_laco-1]=snmpValue.toString();

    if (controla_laco < controle)
    {
        controla_laco=controla_laco+1;
    }
    else
    {
        if (!"0.0.0.0".equals(coordenadas[2]))
        {
            coordenadas[3]=retornainterfasesaida(sEnderecoIP,
coordenadas[1],coordenadas[2], Interfaces);
        }
        else
        {
            coordenadas[3]= "LOCAL";
        }
        retorno[controla_linha][0]=sEnderecoIP;
        retorno[controla_linha][1]=coordenadas[0];
        retorno[controla_linha][2]=coordenadas[1];
        retorno[controla_linha][3]=coordenadas[2];
        retorno[controla_linha][4]=coordenadas[3];
        retorno[controla_linha][5]=coordenadas[4];
        controla_linha=controla_linha+1;
        controla_laco=1;

        String Mensagem = "Endereco IP: "      +sEnderecoIP  +
            " ipCidrRouteDest: "  +coordenadas[0]+
            " ipCidrRouteMask: "  +coordenadas[1]+
            " ipCidrRouteNextHop: " +coordenadas[2]+
            " ipCidrRouteIfIndex: " +coordenadas[3]+
            " ipCidrRouteType: "  +coordenadas[4];

    }
}
return retorno;
}

```



```

        "1.3.6.1.4.1.9.9.42.1.5.2.1.47",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.48",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.26",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.27",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.1",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.2",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.28",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.30",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.29",
        "1.3.6.1.4.1.9.9.42.1.5.2.1.46"};

    try {
        tableVars = comInterface.retrieveMIBTable(baseIDs);
    } catch (IOException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE,
null, ex);
    } catch (SNMPBadValueException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE,
null, ex);
    } catch (SNMPGetException ex) {
        Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE,
null, ex);
    }
}

Integer controle = baseIDs.length;
Integer controla_laco = 1;
Integer controla_linha = a;

for (int i = 0; i < tableVars.size(); i++)
{
    SNMPSequence pair = (SNMPSequence)(tableVars.getSNMPObjectAt(i));

    SNMPObjectIdentifier snmpOID =
(SNMPObjectIdentifier)pair.getSNMPObjectAt(0);
    String OIDpesquisado = snmpOID.toString();

    if ((OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.5."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.4."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.47."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.48."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.26."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.27."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.1."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.2."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.28."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.30."+sASPATH[a]))||
        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.29."+sASPATH[a]))||

```

```

        (OIDpesquisado.equals("1.3.6.1.4.1.9.9.42.1.5.2.1.46."+sASPATH[a]))){

SNMPObject snmpValue = pair.getSNMPObjectAt(1);

coordenadas[controla_laco-1]=snmpValue.toString();

if (controla_laco < controle)
{
    controla_laco=controla_laco+1;
}
else
{

    retorno[controla_linha][0]=sASPATH[a];
    retorno[controla_linha][1]=coordenadas[0];
    retorno[controla_linha][2]=coordenadas[1];
    retorno[controla_linha][3]=coordenadas[2];
    retorno[controla_linha][4]=coordenadas[3];
    retorno[controla_linha][5]=coordenadas[4];
    retorno[controla_linha][6]=coordenadas[5];
    retorno[controla_linha][7]=coordenadas[6];
    retorno[controla_linha][8]=coordenadas[7];
    retorno[controla_linha][9]=coordenadas[8];
    retorno[controla_linha][10]=coordenadas[9];
    retorno[controla_linha][11]=coordenadas[10];
    retorno[controla_linha][12]=coordenadas[11];

String itemID = "1.3.6.1.4.1.9.9.109.1.1.1.7.1";

SNMPVarBindList newVars = null;
try {
    newVars = comInterface.getMIBEntry(itemID);
} catch ( IOException | SNMPBadValueException | SNMPGetException ex) {
    Logger.getLogger(SistemaEspecialista.class.getName()).log(Level.SEVERE,
null, ex);
} catch (Exception e)
{
    System.out.println("Ocorreu uma exceção dentro da funcao
listavaloresIPSLA: " + e + sEnderecoOrigem + "\n");
}

SNMPSequence par = (SNMPSequence)(newVars.getSNMPObjectAt(0));
SNMPObjectIdentifier OID = (SNMPObjectIdentifier)par.getSNMPObjectAt(0);
SNMPObject snmpValor = par.getSNMPObjectAt(1);

//Consumo de CPU no ultimo minuto

```

```

coordenadas[12]= snmpValor.toString();
retorno[controla_linha][13]=coordenadas[12];

//Average Round-Trip Time (ms)
double AvgRTT =
Double.parseDouble(coordenadas[7])/Double.parseDouble(coordenadas[6]);

//Packet Loss Ratio (%)
double PacketLossRatio = ((Double.parseDouble(coordenadas[5]) +
    Double.parseDouble(coordenadas[4]) +
    Double.parseDouble(coordenadas[10]))* 10 ) /
    (Double.parseDouble(coordenadas[4])+
    Double.parseDouble(coordenadas[5])+
    Double.parseDouble(coordenadas[10])+
    Double.parseDouble(coordenadas[9]) +
    Double.parseDouble(coordenadas[8])+
    Double.parseDouble(coordenadas[6]));

retorno[controla_linha][14]=Double.toString(AvgRTT);
retorno[controla_linha][15]=Double.toString(PacketLossRatio);

EvidenciaRTTAvg  = ModelaSinal(AvgRTT,160, 640, 1);
EvidenciaPacketLossRatio = ModelaSinal(PacketLossRatio,1, 8, 1);
EvidenciaJitterSD =
ModelaSinal(Double.parseDouble(coordenadas[2]),10, 30, 1);
EvidenciaJitterDS  =
ModelaSinal(Double.parseDouble(coordenadas[3]),10, 30, 1);
EvidenciaCPUBusy1min  =
ModelaSinal(Double.parseDouble(coordenadas[12]),10, 90, 1);

//Jitter SD e JitterDS

P1 = NAP.evidencia_resultante_real(EvidenciaJitterSD,
    EvidenciaJitterDS);

retorno[controla_linha][16] = Double.toString(P1[0]);

// RTT-AVG e CPU Busy1min

P2 = NAP.evidencia_resultante_real(EvidenciaRTTAvg,
    EvidenciaCPUBusy1min);

retorno[controla_linha][17] = Double.toString(P2[0]);

//PEP-Ratio e Jitter

```

```

P3 = NAP.evidencia_resultante_real(EvidenciaPacketLossRatio,
                                   P1[0]);

retorno[controla_linha][18] = Double.toString(P3[0]);

Po = NAP.evidencia_resultante_real(P3[0],
                                   P2[0]);
retorno[controla_linha][19] = Double.toString(Po[0]);

retorno[controla_linha][20] = Double.toString(Po[0]);

retorno[controla_linha][21] = Double.toString(EvidenciaJitterSD);
retorno[controla_linha][22] = Double.toString(EvidenciaJitterDS);
retorno[controla_linha][23] = Double.toString(EvidenciaCPUBusy1min);
retorno[controla_linha][24] = Double.toString(EvidenciaRTTAvg);
retorno[controla_linha][25] =
Double.toString(EvidenciaPacketLossRatio);
//
controla_linha=controla_linha+1;
controla_laco=1;

    }
  }
}

a++;
}
return retorno;

}

```

APÊNDICE D – Algoritmo extrator de efeitos da contradição

```

public double ParaExtrator(double[] vr_matriz_evidencias){
    NAP nap = new NAP();
    double[] vr_resultado = null;
    double[] vr_vetor_auxiliar=new double[10];
    int vr_limite_linha = 2; // quantidade de linhas
    int vr_limite_coluna = 10;
    double [] vr_matriz_evidencias_exibicao=new double[11];
    double vr_grau_evidencia_minimo;
    double vr_grau_evidencia_maximo;
    double [] vr_resultado_nap;
    double retorno= 0.0;
    int i = 1;

    int a=0;
    //
    for (a=0;a<10;a++){
        vr_matriz_evidencias_exibicao[a] =vr_matriz_evidencias[a];
    }

    vr_matriz_evidencias_exibicao[a]=0.0;

    for( int vr_contador_linha = 1; vr_contador_linha< vr_limite_linha;
        vr_contador_linha++){

        vr_vetor_auxiliar = vr_matriz_evidencias

        int vr_tamanho = vr_vetor_auxiliar.length;

        Integer vr_exclutor_celula = vr_tamanho-1;

        for(i=0;i<(vr_tamanho-1);i++){

            Arrays.sort(vr_vetor_auxiliar);

            vr_grau_evidencia_maximo = vr_vetor_auxiliar[vr_exclutor_celula];

            vr_planilha[10][i+1]=vr_grau_evidencia_maximo;

            vr_grau_evidencia_minimo=vr_vetor_auxiliar[0];

            vr_planilha[11][i+1]=vr_grau_evidencia_minimo;

            //Efetua a analise paraconsistente atraves de uma funcao NAP

```

```
        vr_resultado_nap = nap.evidencia_resultante_real(vr_grau_evidencia_maximo,
vr_grau_evidencia_minimo);

        vr_planilha[12][i+1]=vr_resultado_nap[0];

        vr_vetor_auxiliar=Arrays.copyOfRange(vr_vetor_auxiliar,0,vr_exclutor_celula);

        vr_vetor_auxiliar[0]=vr_resultado_nap[0];
        if (vr_exclutor_celula==1){
            vr_matriz_evidencias_exibicao[(vr_limite_coluna)]=vr_vetor_auxiliar[0];
        }

        vr_exclutor_celula=vr_exclutor_celula-1;
    }
    retorno= vr_vetor_auxiliar[0];
    return retorno;
}
```

APÊNDICE E – Algoritmo Nó de Análise Paraconsistente – NAP

```

public static double[] evidencia_resultante_real(double u1,double u2) {
    double [] vr_resultado_nap = new double [3];
    double s1 = 0;
    double vr_complemento;
    double gc;
    double gct;
    double vr_gcr=0;
    double gcrtn;
    double vr_grau_certeza_estimado = 0;
    double fi;
    double d;
    double s2 = 0;
    String msg;
    double vr_intervalo_certeza = 0;
    double vr_grau_evidencia_desfavoravel;
    double vr_grau_evidencia_favoravel;

    if ((u1<0) || (u1>1)){
        //disp(" ");
        //disp("Grau de evidência fora da faixa solicitada.");
    }
    else
    {
        //disp(" ");
        if ((u2<0) || (u2>1)){
            //disp(" ");
            //disp("Grau de evidência fora da faixa solicitada.");
        }
        else
        {

            vr_complemento=1-u2;

            gc=u1-vr_complemento;

            gct=(u1+vr_complemento)-1;

            gcrtn=(u1+vr_complemento)/2;

            vr_intervalo_certeza=1-abs(gct);
            double vr_grau_certeza_max_verdadeiro=vr_intervalo_certeza;
            double vr_grau_certeza_max_falso=-vr_intervalo_certeza;

            if (gc>0){

```

```

    vr_grau_certeza_estimado=(gc+(1-vr_intervalo_certeza));
}
else if (gc<0)
{
    vr_grau_certeza_estimado=(gc+(vr_intervalo_certeza-1));
}

vr_grau_evidencia_desfavoravel=vr_complemento-gct;

vr_grau_evidencia_favoravel=vr_complemento+vr_grau_certeza_estimado;

fi=1-abs(2*gcrtn -1);

d=Math.sqrt(Math.pow((1-abs(gc)),2)+Math.pow(gct,2));

if ((fi<=0.25) || (d>1))
{
    s1=0.5;
    s2=fi;
    msg="indefinição ln";
}
else
{
    if (gc>0)
    {
        vr_gcr=1-d;
    }
    else if (gc<0){

        vr_gcr=d-1;
    }
}
if (gct<0){
    s2=-abs(vr_intervalo_certeza);
}
else if (gct>0){
    s2=abs(vr_intervalo_certeza);
}
else{
    s2=0;
}
s1=(vr_gcr+1)/2;

}
}

vr_resultado_nap[0]=s1;

```

```
vr_resultado_nap[1]=vr_gcr;  
vr_resultado_nap[2]=s2;  
return vr_resultado_nap;  
}
```

APÊNDICE F – Algoritmo de normalização da fonte de informação

```
public double ModeloSinal(double Sinal, int LimiteInferior, int LimiteSuperior, int
SentidoNormalizacao){
    double retorno;

    if (SentidoNormalizacao==1)
    {
        if (Sinal>LimiteSuperior)
        {
            retorno=1;
        }
        else if (Sinal<LimiteInferior)
        {
            retorno=0;
        }
        else
        {
            retorno = (Sinal-LimiteInferior)/(LimiteSuperior-LimiteInferior);
        }
    }
    else
    {
        if (Sinal>LimiteSuperior)
        {
            retorno=0;
        }
        else if (Sinal<LimiteInferior)
        {
            retorno=1;
        }
        else
        {
            retorno = (Sinal-LimiteSuperior)/(LimiteInferior-LimiteSuperior);
        }
    }

    return retorno;
}
```

APÊNDICE G – Algoritmo de exportação dos dados em formato de planilha

```

public static void GeraPlanilha(String[][] args, String NomeAba, int Contador)
throws Exception {
    String[][]args2 = new String[10][6];

    String file= "d:/ResultadoNAP.xlsx";
    Workbook wb;
    Sheet sheet;
    try{
        wb = WorkbookFactory.create(new FileInputStream(file));
    }
    catch (IOException | EncryptedDocumentException | InvalidFormatException e)
    {
        System.out.println("Arquivo nao encontrado "+ "\n");
        wb = new XSSFWorkbook();
    }

    Map<String, CellStyle> styles = createStyles(wb);

    sheet = wb.createSheet("Resultado"+Contador+"-"+NomeAba);
    PrintSetup printSetup = sheet.getPrintSetup();
    printSetup.setLandscape(true);
    sheet.setFitToPage(true);
    sheet.setDisplayGridlines(false);
    sheet.setHorizontallyCenter(true);

    Row titleRow = sheet.createRow(0);
    Cell titleCell = titleRow.createCell(5);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(4);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(3);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(2);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(1);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(0);
    titleCell.setCellStyle(styles.get("title"));
    titleCell.setCellValue("SharpNet ParaControl - "+ Contador + "'o leitura");

    sheet.addMergedRegion(CellRangeAddress.valueOf("$A$1:$F$1"));

```

```
int contador = 0;
```

```
for (int i=0; i<args.length;i++)
    if (args[i][0]!=null)
    {
        args2[i][0]=args[i][0];
        args2[i][1]=args[i][3];
        args2[i][2]=args[i][4];
        args2[i][3]=args[i][13];
        args2[i][4]=args[i][14];
        args2[i][5]=args[i][15];
        contador++;
    }
```

```
int rownum=2;
Row headerRow;
Cell headerCell;
```

```
titleRow = sheet.createRow(rownum);
titleCell = titleRow.createCell(5);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(4);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(3);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(2);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(1);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(0);
titleCell.setCellStyle(styles.get("title"));
titleCell.setCellValue("Valores capturados");
```

```
String sRange= ("A$(rownum+1):F$(rownum+1)");
sheet.addMergedRegion(CellRangeAddress.valueOf(sRange));
```

```
rownum = rownum +3;
int controlalinha=rownum;
```

```
headerRow = sheet.createRow(rownum-1);
for (int i = 0; i < sinais.length; i++) {
    headerCell = headerRow.createCell(i);
    headerCell.setCellValue(sinais[i]);
    headerCell.setCellStyle(styles.get("header"));
}
```

```

for (int i = 0; i < contador; i++) {
    Row row = sheet.createRow(rownum++);
    for (int j = 0; j < sinais.length; j++) {
        Cell cell = row.createCell(j);
        cell.setCellStyle(styles.get("cell"));
    }
}

for (int i = 0; i < contador; i++) {
    Row row = sheet.getRow(controlalinha + i);
    for (int j = 0; j < sinais.length; j++) {
        if(args2[i][j] == null) continue;

        if(args2[i][j] instanceof String) {
            row.getCell(j).setCellValue((String)args2[i][j]);
        }
    }
}

rownum = rownum + 3;
controlalinha=rownum;

    titleRow = sheet.createRow(rownum-3);
    //titleRow.setHeightInPoints(45);
    titleCell = titleRow.createCell(5);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(4);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(3);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(2);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(1);
    titleCell.setCellStyle(styles.get("title"));
    titleCell = titleRow.createCell(0);
    titleCell.setCellStyle(styles.get("title"));
    titleCell.setCellValue("Valores modelados");

    sheet.addMergedRegion(CellRangeAddress.valueOf("$A$"+(rownum-
2)+":$F$"+(rownum-2)));

    headerRow = sheet.createRow(rownum-1);
    for (int i = 0; i < evidencias.length; i++) {
        headerCell = headerRow.createCell(i);
        headerCell.setCellValue(evidencias[i]);
        headerCell.setCellStyle(styles.get("header"));
    }

```

```

for (int i = 0; i < contador; i++) {
    Row row = sheet.createRow(rownum++);
    for (int j = 0; j < evidencias.length; j++) {
        Cell cell = row.createCell(j);
        cell.setCellStyle(styles.get("cell"));
    }
}
//insere os dados
int tamanhobloco = 20+evidencias.length;
for (int i = 0; i < contador; i++) {
    Row row = sheet.getRow(controlalinha + i);
    for (int j = 20; j < tamanhobloco; j++) {
        if(args[i][j] == null) continue;
        if (j==20)
        {
            row.getCell(j-20).setCellValue((String)args2[i][0]);
        }
        else
        {
            if(args[i][j] instanceof String) {
                row.getCell(j-20).setCellValue((String)args[i][j]);
            }
        }
    }
}

rownum = rownum +3;
controlalinha=rownum;

titleRow = sheet.createRow(rownum-3);
titleCell = titleRow.createCell(4);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(3);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(2);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(1);
titleCell.setCellStyle(styles.get("title"));
titleCell = titleRow.createCell(0);
titleCell.setCellStyle(styles.get("title"));
titleCell.setCellValue("Valores obtidos nas proposições");

sheet.addMergedRegion(CellRangeAddress.valueOf("$A$"+(rownum-2)+":$E$"+(rownum-2)));

```

```

headerRow = sheet.createRow(rownum-1);
for (int i = 0; i < proposicoes.length; i++) {
    headerCell = headerRow.createCell(i);
    headerCell.setCellValue(proposicoes[i]);
    headerCell.setCellStyle(styles.get("header"));
}

for (int i = 0; i < contador; i++) {
    Row row = sheet.createRow(rownum++);
    for (int j = 0; j < proposicoes.length; j++) {
        Cell cell = row.createCell(j);
        cell.setCellStyle(styles.get("cell"));
    }
}

tamanhobloco = 15 + proposicoes.length;
for (int i = 0; i < contador; i++) {
    Row row = sheet.getRow(controlalinha + i);
    for (int j = 15; j < tamanhobloco; j++) {
        if(args[i][j] == null) continue;
        if (j==15)
        {
            row.getCell(j-15).setCellValue((String)args2[i][0]);
        }
        else
        {
            if(args[i][j] instanceof String) {
                row.getCell(j-15).setCellValue((String)args[i][j]);
            }
        }
    }
}

sheet.setColumnWidth(0, 23*256);
for (int i = 1; i < 16; i++) {
    sheet.setColumnWidth(i, 23*256);
}
for (int i = 14; i < 26; i++) {
    sheet.setColumnWidth(i, 23*256);
}
FileOutputStream out = new FileOutputStream(file);
wb.write(out);
out.close();
}

```